Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Πληροφορικης

ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ

Μια Θεωρητική Εισαγωγή

Διπλωματικη Εργασια

του

ΚΑΡΑΜΕΡΗ ΜΑΡΚΟΥ

Επιβλέπων: Λαμπροπούλου Σοφία
Καθηγήτρια Ε.Μ.Π.

Αθήνα, Δεκέμβριος 2018

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Πληροφορικής

ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ

Μια Θεωρητική Εισαγωγή

Διπλωματικη Εργασια

του

ΚΑΡΑΜΕΡΗ ΜΑΡΚΟΥ

Επιβλέπων: Λαμπροπούλου Σοφία
Καθηγήτρια Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 28η Σεπτεμβρίου 2018.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Λαμπροπούλου Σοφία	Παγουρτζής Αριστείδης	Κοντογεώργης Αριστείδης
Καθηγήτρια Ε.Μ.Π.	Αν.Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Κ.Π.Α

Αθήνα, Δεκέμβριος 2018

(Υπογραφή)

.....

Καραμερης Μαρκος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Πληροφορικής

Περίληψη

Σκοπός της εργασίας αυτής είναι η παρουσίαση των βασικών θεωρημάτων των ελλειπτικών καμπυλών από θεωρητική άποψη. Αρχικά ορίζουμε τα θεμελιώδη εργαλεία που θα χρησιμοποιήσουμε από την αλγεβρική γεωμετρία (Κεφάλαια 1-2) και στη συνέχεια με βάση αυτά προχωράμε στη μελέτη των ελλειπτικών καμπυλών ως γεωμετρικά αντικείμενα(Κεφάλαιο 3). Στην συνέχεια μελετάμε τις ισογένιες δηλαδή τους μορφισμούς μεταξύ ελλειπτικών καμπυλών (Κεφάλαιο 4). Αυτό το κάνουμε με δύο τρόπους δίνουμε δηλαδή επιπλέον μια συγκεκριμένη μορφή που χαρακτηρίζει της ισογένιες και διατυπώνουμε με βάση αυτή τα αντίστοιχα θεωρήματα και την μορφή που λαμβάνουν αν χρειαστεί να τα ελέγξει κάποιος υπολογιστικά. Στρέφουμε στη συνέχεια τη προσοχή μας σε ελλειπτικές καμπύλες πάνω από πεπερασμένα σώματα όπως το $\mathbb{F}_q$ (Κεφάλαιο 5). Στο τέλος του κεφαλαίου αποδεικνύουμε τις εικασίες του Weil για ελλειπτικές καμπύλες. Στο επόμενο κεφάλαιο (Κεφάλαιο 6) εξετάζουμε ελλειπτικές καμπύλες στο $\mathbb{C}$ και βλέπουμε την αντιστοιχία τους με το μιγαδικό τόρο δηλαδή τα δικτυωτά στους μιγαδικούς. Τέλος κάνουμε λόγο για ελλειπτικές καμπύλες στο $\mathbb{Q}$ (Κεφάλαιο 7) και την δομή της ομάδας μιας καμπύλης περιορισμένη στο $\mathbb{Q}$.

Λέξεις κλειδιά: Ελλειπτικές Καμπύλες, Προβολικές Πολλαπλότητες, Αλγεβρική Γεωμετρία, Riemann Roch, Πρότυπο Tate, ισογένιες, Δικτυωτά

Σημείωση: Το σύμβολο (**) δηλώνει πρωτότυπη απόδειξη/πόρισμα στην εργασία. Θα ήθελα να διευκρινίσω ότι ενδεχομένως κάποιες/α εκ΄ των αποδείξεων/πορισμάτων αυτών να υπάρχουν στην εκτενέστατη βιβλιογραφία για το αντικείμενο και με τον όρο ¨πρωτότυπη' εννοώ ότι δεν διάβασα κάπου τη συγκεκριμένη απόδειξη/αποτέλεσμα. Το κεφάλαιο 8 αποτελεί εξ΄ ολοκλήρου ¨πρωτότυπη' δουλειά ως προς τις αποδείξεις με εξαιρέσεις που αναγράφονται.

Abstract

The scope of this thesis is to present the reader with an overview of Elliptic Curves from a purely theoretical perspective. In this manner we chose to present the basic Algebraic Geometry (Chapter 1-2) and then proceed to study Elliptic Curves as geometric objects (Chapter 3). We then shift to the study of isogenies, that is morphism between Elliptic Curves (Chapter 4). We provide a theoretical and a more concrete/computational aproach to isogenies, highlighting the exact form an isogeny can attain as a rational morphism. We then turn to Elliptic curves over finite fields and specifically over $\mathbb{F}_q$ (Chapter 5). We present the Weil conjectures at the end of the chapter. In Chapter 6 we examine Elliptic curves over $\mathbb{C}$ and note their relation to complex tori, or lattices over the complex plane. In the final chapter (Chapter 7) we talk about Elliptic Curves over $\mathbb{Q}$ and their form as a finitelly generated group over $\mathbb{Q}$.

keywords: Elliptic Curves, Algebraic Geometry, Projective Varieties, Riemann-Roch, Tate module, Isogenies, Lattices

Note: The symbol $\{**\}$ is used to indicate the author's own proof/result, meaning it is not written in a textbook or published paper to the best of the author's knowledge.

Ευχαριστίες: Πριν την παρουσίαση της εργασίας θα ήθελα να ευχαριστήσω όλους τους καθηγητές που με βοήθησαν όλα αυτά τα χρόνια και με ενέπνευσαν με τη στάση και το έργο τους και ειδικά τον κύριο **Ι.Σακελλαρίδη** που με τη συνεχή καθοδήγησή του έπαιξε καθοριστικό ρόλο στην ολοκλήρωση αυτής της εργασίας.

Περιεχόμενα

1 Αλγεβρικές Πολλαπλότητες

1.1 Αφινικές Πολλαπλότητες

Έστω ένας **Αφινικός χώρος** επί του K, $A^n = A^n(\bar{K}) = \{P = (x_1, \ldots, x_n) : x_i \in \bar{K}\}$ όπου $\bar{K}$ η αλγεβρική κλειστότητα του K. Το $A^n(K)$ είναι τότε τα ρητά σημεία του A^n.

Έστω τα πολυώνυμα επί του $\bar{K}$, $\bar{K}[X] = \bar{K}[X_1, \ldots, X_n]$, σε κάθε ιδεώδες του I αντιστοιχίζουμε το $V_I = \{P \in A^n : f(P) = 0, \forall f \in I\}$ (δηλαδή το σύνολο των σημείων που ικανοποιούν ένα σύστημα πολυωνυμικών εξισώσεων).

Τα σύνολα της μορφής V_I ονομάζονται **αλγεβρικά**. Αν ένα σύνολο είναι αλγεβρικό τότε ορίζουμε το ιδεώδες του ως $I(V) = \{f \in \bar{K}[X] : f(P) = 0, \forall P \in V\}$. Αν το ιδεώδες ενός αλγεβρικού συνόλου μπορεί να παραχθεί από πολυώνυμα στο $K[X]$ τότε λέμε ότι ορίζεται στο K και γράφουμε V/K. Γενικά: $I(V/K) = I(V) \cap K[X]$.

Ορισμός 1.1.1. *Αν το ιδεώδες ενός αλγεβρικού συνόλου V είναι πρώτο στο $\bar{K}(X)$ (ή ισοδύναμα το V είναι ανάγωγο) τότε το V ονομάζεται Αφινική Πολλαπλότητα.*

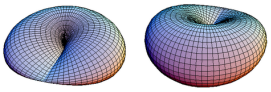
Αν το $I(V)$ μιας πολλαπλότητας δίνεται από μία πολυωνυμική εξίσωση $f(X_1, \ldots, X_n) = 0$ τότε λέμε ότι έχει **ιδιάζον σημείο** ανν $\frac{\partial(f)}{\partial X_1} = \cdots = \frac{\partial(f)}{\partial X_n} = 0$.

Ορισμός 1.1.2. *Μια πολλαπλότητα χωρίς ιδιάζοντα σημεία λέγεται **ομαλή** ή **μη-ιδιάζουσα** (Ο ίδιος ορισμός ισχύει και για προβολικές πολλαπλότητες για αυτό δε γράφουμε Αφινική πολλαπλότητα).*

1.2 Προβολικές Πολλαπλότητες

Αν και είμαστε συνηθισμένοι στους Αφινικούς χώρους, η μελέτη χώρων που παράγονται από μηδενικά πολυωνύμων διευκολύνεται αρκετά αν προσθέσουμε εμπειρικά ένα ¨σημείο στο άπειρο' και κάνουμε χρήση του θεωρήματος του Bézout λαμβάνοντας έτσι το μέγιστο αριθμό μηδενικών που μπορούμε.

Ορισμός 1.2.1. *Ορίζουμε ως **Προβολικό επίπεδο** πάνω στο K με σύμβολο P^n το σύνολο όλων των πλειάδων $(x_0, \ldots, x_n) \in A^{n+1}$ με τουλάχιστον ένα $x_i \neq 0$ modulo την κλάση ισοδυναμίας $[x_0, \ldots, x_n]$ όπου: $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ ανν υπάρχει $\lambda \in \bar{K}^* : x_i = \lambda y_i, \forall i$. Δύο πλειάδες δηλαδή είναι ισοδύναμες στον P^n ανν ανήκουν στην ίδια ευθεία του A^{n+1}.*



Σχήμα 1: Το πραγματικό Προβολικό Επίπεδο P^2

Ορισμός 1.2.2. *Ένα πολυώνυμο $f \in \bar{K}[X]$ βαθμού d ονομάζεται **ομογενές** ανν $f(lx_0, \ldots, lx_n) = l^d f(x_0, \ldots, x_n)$ $\forall l \in \bar{K}$.*

Τα πολυώνυμα ορίζονται δηλαδή κατά τέτοιο τρόπο ώστε το $f(P)$ να εξαρτάται μόνο από τη κλάση ισοδυναμίας του P. Αντίστοιχα με τα αλγεβρικά σύνολα ορίζουμε τα **προβολικά αλγεβρικά σύνολα** για ομογενή ιδεώδη I: $V_I = \{P \in P^n : f(P) = 0, \forall$ ομογενές $f \in I\}$. Αντίστοιχα το ιδεώδες του V, $I(V)$ είναι το ιδεώδες που παράγεται από τα $\{f \in \bar{K}[X] : f$ ομογενές και $f(P) = 0, \forall P \in V\}$. Για κάθε συνάρτηση $f \in \bar{K}[X]$ μπορούμε να ορίσουμε $f^*(X_1, \ldots, X_n) = {X_i}^d f(\frac{X_1}{X_i}, \ldots, \frac{X_n}{X_i})$ όπου $d = deg(f)$ ο μικρότερος ακέραιος για τον οποίο το f^* είναι πολυώνυμο. Αυτή η διαδικασία $A^n \to P^n$ ονομάζεται ομογενοποίηση ως προς X_i. Αντίστοιχα με τις Αφινικές πολλαπλότητες:

Ορισμός 1.2.3. *Αν το ιδεώδες ενός προβολικού συνόλου V είναι πρώτο στο $\bar{K}(X)$ τότε ονομάζεται Προβολική Πολλαπλότητα.*

Παράδειγμα 1.2.1. *Έστω η προβολική πολλαπλότητα (1) $Y^2 = X^3 - X^2 + 5$ τότε η ομογενής μορφή της είναι: $ZY^2 = X^3 - ZX^2 + 5Z$. Για $Z = 0$ έχουμε προφανώς $X^3 = 0$ και άρα $X = 0$, δηλαδή η (1) έχει ένα σημείο στο άπειρο $(0, Y, 0) \sim (0, 1, 0)$*

Μια πολύ χρήσιμη έννοια για αλγεβρικές πολλαπλότητες είναι οι συναρτήσεις που μπορούν να οριστούν σε αυτές. Ορίζουμε για αρχή το **πεδίο συναρτήσεων** του P^n ως το υπόσωμα του $\bar{K}[X]$ που αποτελείται από τις ρητές συναρτήσεις της μορφής $F(X) = \frac{f(X)}{g(X)}$ όπου f, g ομογενή πολυώνυμα ίδιου βαθμού. Το να είναι ίδιου βαθμού τα πολυώνυμα εξυπρετεί στο να μπορούμε να τα απομογενοποιήσουμε και να καταλήγουμε σε συνάρτηση με μια μεταβλητή λιγότερη στο A^n. Προφανώς η $F(X)$ είναι καλά ορισμένη μόνο όπου $g(P) \neq 0$.

Ορισμός 1.2.4. *Ως πεδίο συναρτήσεων μιας προβολικής πολλαπλότητας V ορίζουμε το υπόσωμα ρητών συναρτήσεων της μορφής $F(X) = \frac{f(X)}{g(X)}$ και συμβολίζουμε $K[V] = K[X]/I(V/K) = K[X]/(I(V) \cap K[X])$ όπου:*

1. *f, g ομογενή πολυώνυμα ίδιου βαθμού*
2. *$g \notin I(V)$*
3. *$f_1/g_1 = f_2/g_2 \iff f_1g_2 - f_2g_1 \in I(V)$*

Ορισμός 1.2.5. *Ορίζουμε ένα ιδεώδες του $\bar{K}(V)$, $M_P = \{f \in \bar{K}(V) : f(P) = 0\}$ το οποίο είναι μέγιστο αφού έχουμε ισομορφισμό: $\bar{K}(V)/M_P \to \bar{K}, f \to f(P)$. Ένας γεννήτορας του M_P ονομάζεται πρώτο στοιχείο. Ορίζουμε τέλος $ord_P(f) = sup\{d \in Z : f \in {M_P}^d\}$, δηλαδή την τάξη μηδενισμού της συνάρτησης f στο P. Από τον ορισμό $ord_P(t) = 1$ αν η συνάρτηση t είναι πρώτο στοιχείο.*

Ο παραπάνω ορισμός ισχύει με τις αντίστοιχες παραλλαγές και για Αφινικές πολλαπλότητες.

1.3 Χάρτες μεταξύ πολλαπλοτήτων

Ορισμός 1.3.1. *Έστω πολλαπλότητες V_1, V_2, ένας ρητός χάρτης μεταξύ τους είναι ένας χάρτης $f : V_1 \to V_2$, με $f = [f_0, \ldots, f_n]$ όπου $f_i \in \bar{K}[V_1]$ τέτοιες ώστε σε κάθε σημείο που είναι καλώς ορισμένες να έχουμε $f(P) = [f_0(P), \ldots, f_n(P)] \in V_2$.*

Επειδή ένας χάρτης ενδέχεται να μην ορίζεται καλώς σε κάθε σημείο P του V_1 μπορούμε να πολλαπλασιάσουμε με μια συνάρτηση g ώστε να υπολογίσουμε την $f(P)$.

Ορισμός 1.3.2. *Ένας χάρτης που είναι παντού ορισμένος ονομάζεται **μορφισμός**. Ένας χάρτης $V_1 \to V_2$ λέγεται ορισμένος στο $P \in V_1$ αν υπάρχει $g \in \bar{K}[V_1]$:*

1. *κάθε gf_i είναι καλώς ορισμένη συνάρτηση στο P*
2. *υπάρχει i για το οποίο $gf_i(P) \neq 0$*

Παράδειγμα 1.3.1. *Έστω η πολλαπλότητα $V : X^2 + Y^2 = Z^2$, τότε αν θεωρήσουμε την ευθεία που διέρχεται από το $O(0, 0)$ σε αφινικές συντεταγμένες και τέμνει την V στο $(x, y) : x^2 + y^2 = 1$ λαμβάνουμε έναν χάρτη $A^1 \to V'$, $[(S^2 - T^2)/(S^2 + T^2), 2ST/(S^2 + T^2)]$ και άρα έναν χάρτη $P^1 \to V$, $[S^2 - T^2, 2ST, S^2 + T^2]$. Ο αντίστροφος χάρτης $V \to P^1$ είναι ο $[X+Z, Y]$ και είναι ορισμένος παντού εκτός ίσως από το $(1, 0, -1)$. Είναι όμως μορφισμός διότι: $[X+Z, Y] \sim [(X+Z)(X-Z), Y(X-Z)] \sim [-Y^2, Y(X-Z)] \sim [-Y, X-Z] = [0, 2] \neq (0, 0)$.*

Ορισμός 1.3.3. *Έστω δύο πολλαπλότητες V_1, V_2. Λέμε ότι είναι ισομορφικές και γράφουμε $V_1 \simeq V_2$ ανν υπάρχουν μορφισμοί $\phi : V_1 \to V_2$ και $\psi : V_2 \to V_1$: $\phi \circ \psi = id_{V_2}$ και $\psi \circ \phi = id_{V_1}$.*

2 Καμπύλες

Ορισμός 2.0.1. *Καμπύλη ονομάζεται μια προβολική πολλαπλότητα διάστασης* 1.

2.1 Μορφισμοί μεταξύ καμπυλών

Πρόταση 2.1.1. *Έστω ϕ μορφισμός μεταξύ των καμπυλών C_1, C_2, τότε ϕ είναι σταθερή συνάρτηση ή επί.*

Πρόταση 2.1.2. *Έστω ϕ μορφισμός μεταξύ των καμπυλών C_1, C_2 τότε ο ϕ ορίζει έναν 1-1 χάρτη $\phi^* : K(C_2) \to K(C_1)$ στα πεδία συναρτήσεων των C_1, C_2 αντίστοιχα με $\phi^* \circ f = f \circ \phi$.*

Αποδεικνύεται επίσης ότι το $K(C_1)$ είναι πεπερασμένη επέκταση του $\phi^*(K(C_2))$ και πιο συγκεκριμένα:

Ορισμός 2.1.1. *Αν ϕ μορφισμός μεταξύ των C_1, C_2 και ϕ σταθερός τότε $deg(\phi) = 0$ αλλιώς $deg(\phi) = [K(C_1) : \phi^*(K(C_2))]$. Αντίστοιχα με τη διαχωρισιμότητα ή μη της παραπάνω επέκτασης σωμάτων ορίζεται και η διαχωρισιμότητα του ϕ. Από αυτό το σημείο και έπειτα θα αναφερόμαστε στο βαθμό ενός μορφισμού με $deg_s(\phi)$ για το διαχωρίσιμο και $deg_i(\phi)$ για το μη-διαχωρίσιμο μέρος του. Φυσικά ισχύει $deg(\phi) = deg_s(\phi)deg_i(\phi)$.*

Πρόταση 2.1.3. *Ένας μορφισμός μεταξύ δύο ομαλών καμπυλών είναι ισομορφισμός ανν έχει $deg(\phi) = 1$.*

Απόδειξη. ($\implies$) *Προφανές.*
($\impliedby$) *Επειδή $deg(\phi) = 1$ έχουμε $K(C_1) \simeq \phi^*(K(C_2))$ και άρα ο χάρτης: $\phi^{*-1} : K(C_1) \to K(C_2))$ είναι ρητός χάρτης και επομένως επειδή C_1, C_2 ομαλές είναι μορφισμός από την C_2 στην C_1. Επίσης $(\phi \circ \psi)^* = id_{K(C_2)}, (\psi \circ \phi)^* = id_{K(C_1)} \implies \phi \circ \psi = id_{C_2}, \psi \circ \phi = id_{C_1}$.*

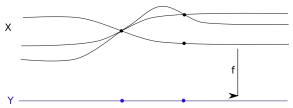
Ορίζουμε τον δακτύλιο $\bar{K}(E)_P$ σε μια καμπύλη E ως το δακτύλιο των ρητών συναρτήσεων στην E που ορίζονται στο P. Αυτός ο δακτύλιος έχει ένα μοναδικό μέγιστο ιδεώδες m_P που είναι όλες οι ρητές συναρτήσεις που έχουν σημείο φυγής/μηδενισμού το P (vanishing point). Το m_P παράγεται από ένα ακριβώς στοιχείο που ονομάζεται **πρώτο στοιχείο**(uniformizer). Μπορούμε να ορίσουμε την πολλαπλότητα τομής $ord_P(f) = max\{d \in \mathbb{Z} : f \in {m_P}^d\}$. Αν $ord_P(f) = d$ τότε $f = ut^d$ όπου u μοναδιαίο στοιχείο. Μοναδιαία στοιχεία στο $\bar{K}(E)_P$ είναι φυσικά όλα τα στοιχεία που δεν μηδενίζονται στο P και άρα διαισθητικά πράγματι παίρνουμε τη ¨μέγιστη τάξη μηδενισμού' όπως θέλαμε.

Ορισμός 2.1.2. *Έστω μορφισμός μεταξύ ομαλών καμπυλών $\phi : C_1 \to C_2$. Ορίζουμε ως δείκτη διακλάδωσης της ϕ στο P: $e_\phi(P) = ord_P(\phi^*(t_{\phi(P)}))$ όπου $t_{\phi(P)}$ πρώτο στοιχείο του $\bar{K}(C_2)_\phi(P)$.*

Διαισθητικά ο χάρτης ϕ είναι τοπικά e_ϕ προς 1 σε μια γειτονιά του P εκτός του σημείου P. Ο μη εξοικειωμένος αναγνώστης μπορεί να σκέφτεται το $ord_P(f)$ όπου $f \in K[V]$ ως την τάξη του πρώτου όρου στο ανάπτυγμα Laurent της f με κέντρο το P ή ως την πολλαπλότητα της τομής της $f = 0$ και της V στο σημείο P.

Παράδειγμα 2.1.1. *Έστω $\phi(X, Y) = [X^3(X - Y)^2, Y^5]$ τότε $\phi^{-1}([1, 0]) = [1, 0]$ και άρα η ϕ δίνει έναν χάρτη $A^1 \to A^1$ με Y σταθερό. Αν θέλουμε να υπολογίσουμε το δείκτη διακλάδωσης για τα δύο σημεία στην $\phi^{-1}([0, 1]) = \{[0, 1], [1, 1]\}$ θα έχουμε για $Y = 1$ το χάρτη $\phi(X) = X^3(X-1)^2$ με πρώτα στοιχεία στο 0 το x και στο 1 το $x-1$ οπότε $e_\phi([0, 1]) = 3$ και $e_\phi([1, 1]) = 2$ ή αλλιώς οι τάξεις μηδενισμού στα 0,1.*

Πρόταση 2.1.4. *Γενικά για έναν μορφισμό ϕ έχουμε ότι $e_\phi(P) = 1$ σε κάθε σημείο P είναι ισοδύναμο με $\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = |\phi^{-1}(Q)| = deg(\phi)$.*



Σχήμα 2: Χάρτης f με σημειωμένα με τελείες τα σημεία διακλάδωσης με αντίστοιχους δείκτες διακλάδωσης 3 και 2.

2.2 Διαιρέτες

Ορισμός 2.2.1. *Η* ***ομάδα διαιρετών*** *μιας καμπύλης C συμβολίζεται $Div(C)$ και είναι η ελεύθερη αβελιανή ομάδα που παράγεται από σημεία της καμπύλης. Ένας διαιρέτης είναι δηλαδή ένα άθροισμα της μορφής $D = \sum_{P\in C} n_P(P)$ όπου $n_P \in Z$ και $n_P = 0$ για όλα εκτός από πεπερασμένο αριθμό σημείων. Ο βαθμός του διαιρέτη ορίζεται ως $deg(D) = \sum_{P\in C} n_P$.*

Η υποομάδα των διαιρετών με βαθμό 0 συμβολίζεται $Div^0(C)$. Έστω μια ομαλή καμπύλη C με $f \in K^*(C)$, τότε ορίζουμε $div(f) = \sum_{P\in C} ord_p(f)(P)$ Ένας διαρέτης λέγεται **πρωταρχικός** αν $D = div(f), f \in K^*(C)$. Για δύο διαιρέτες D_1, D_2 ορίζουμε $D_1 \sim D_2$ ανν ο $D_1 - D_2$ είναι πρωταρχικός διαιρέτης. Το πηλίκο του $Div(C)$ με την υποομάδα των προταρχικών διαιρετων του είναι το Picard group του C ή $Pic(C)$.

Μπορούμε να ορίσουμε για έναν χάρτη $\phi : C_1 \to C_2$, με $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ και $\phi_* : \bar{K}(C_1) \to \bar{K}(C_2)$ μεταξύ καμπυλών τον αντίστοιχο χάρτη $\phi_* : Div(C_2) \to Div(C_1)$, $P \to \phi(P)$ και $\phi^* : Div(C_1) \to Div(C_2)$, $(Q) \to \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P)$.

Πρόταση 2.2.1. *Έστω η ομαλή καμπύλη C και $f \in \bar{K}^*$ τότε:*

1. *$div(f) = 0$ ανν $f = c \in K^*(C)$*
2. *$deg(div(f)) = 0$*

Απόδειξη.
1. *Η f δεν έχει πόλους ούτε μηδενικά και άρα είναι η σταθερή συνάρτηση στο $K^*(C)$*
2. *Αφού η f έχει ίδιο αριθμό πόλων και μηδενικών και από τον ορισμό $div(f) = f^*((0) - (\infty))$ άρα έχουμε $deg(div(f)) = degf - degf = 0$*

Γενικά σε μια συνάρτηση f θα συμβολίζουμε $div_\infty(f) = \sum_{P\in C} n_p(P), n_p < 0$ και $div_0(f) = \sum_{P\in C} n_p(P), n_p > 0$

2.3 Διαφορικές Μορφές

Στην υποενότητα αυτή θα αφερθούμε στις διαφορικές μορφές που ορίζονται επί μιας καμπύλης. Οι διαφορικές μορφές παίζουν τον τυπικό ρόλο που έχουν στην ανάλυση ως γραμμικοποιητές ενώ μπορούν να μας δώσουν πληροφορίες για το πότε ένας αλγεβρική χάρτης είναι διαχωρίσιμος.

Ορισμός 2.3.1. *Έστω καμπύλη C, τότε ο χώρος των διαφορικών μορφών πάνω στη C είναι ο $\bar{K}(C)$-διανυσματικός χώρος που συμβολίζουμε Ω_C και αποτελείται από σύμβολα της μορφής dx τέτοια ώστε:*

1. *$d(x + y) = dx + dy$, $x, y \in \bar{K}(C)$*
2. *$dxy = ydx + xdy$, $x, y \in \bar{K}(C)$*
3. *$da = 0, \forall a \in \bar{K}$*

Παρατήρηση. *Έστω $\phi : C_1 \to C_2$ χάρτης μεταξύ καμπύλων. Η ϕ^* τότε ορίζει έναν χάρτη $\phi^* : \Omega_{C_2} \to \Omega_{C_1}, \phi^*(\sum f_i dx_i) \to \sum \phi^*(f_i) d(\phi^*(x_i))$.*

Είναι γνωστό αποτέλεσμα ότι σε καμπύλες το Ω_C έχει διάσταση 1, το οποίο διατυπώνουμε χωρίς απόδειξη. Επίσης αν έχουμε μια συνάρτηση $x \in \bar{K}(C)$ τότε το dx αποτελεί βάση του Ω_C ανν $\bar{K}(C) \backslash \bar{K}(x)$ είναι πεπερασμένη διαχωρίσιμη επέκταση σωμάτων. Διατυπώνουμε έτσι την ακόλουθη πολύ σημαντική πρόταση:

Πρόταση 2.3.1. *Έστω $\phi : C_1 \to C_2$ χάρτης μεταξύ καμπύλων. Τότε η ϕ είναι διαχωρίσιμη ανν $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ είναι $1-1$ δηλαδή ισοδύναμα διάφορος του 0.*

Απόδειξη. *Έστω $y \in \bar{K}(C_2) : \Omega_{C_2} = \bar{K}(C_2)dy$ και $\bar{K}(C_2)/\bar{K}(y)$ διαχωρίσιμη επέκταση σωμάτων, τότε η ϕ είναι $1-1 \iff d(\phi^* y) \neq 0 \iff d(\phi^* y)$ είναι βάση του $\Omega_{C_1} \iff \bar{K}(C_1)/\bar{K}(\phi^* y) \iff \bar{K}(C_1)/\phi^* \bar{K}(C_1)$.*

Χωρίς απόδειξη διατυπώνουμε και την ακόλουθη χρήσιμη πρόταση:

Πρόταση 2.3.2. *Έστω η καμπύλη C με $P \in C$ και t ένα πρώτο στοιχείο στο P τότε:*

1. *$\forall \omega \in \Omega_C, \exists! g \in \bar{K}(C) : \omega = g dt$.*
2. *αν η f είναι καλώς ορισμένη στο P τότε και η df/dt είναι καλώς ορισμένη στο P.*
3. *η ποσότητα $ord_P(\omega/dt)$ δεν έξαρταται από το t και άρα γράφουμε απλά $ord_P(\omega)$.*
4. *έστω $x, f \in \bar{K}(C)$ με $x(P) = 0$ τότε αν $char(K) = 0$ ή $char(K) \not| ord_P(x)$: $ord_P(fdx) = ord_P(f) + ord_P(x) - 1$, αλλιώς $ord_P(fdx) \geq ord_P(f) + ord_P(x)$.*
5. *$ord_P(\omega) = 0$, για όλα εκτός από πεπερασμένο αριθμό P.*

Ορισμός 2.3.2. *Ο διαιρέτης μιας διαφορικής μορφής ορίζεται ως $div(\omega) = \sum_{P \in C} ord_P(\omega)(P)$ και η διαφορική μορφή λέγεται ολόμορφη αν $ord_P(\omega) \geq 0, \forall P \in C$).*

Ορισμός 2.3.3. *Κατά αντιστοιχία με την κλάση προταρχικών διαιρετών ορίζουμε την κλάση **κανονικών** διαιρετών. Κανονικοί λέγονται οι διαιρέτες που ισούνται με κάποιο $div(\omega), \omega \in \Omega_C$.*

2.4 Το Θεώρημα Riemann-Roch

Ορίζουμε αρχικά μια σχέση διάταξης σε διαιρέτες:

Ορισμός 2.4.1. *Ένας διαιρέτης λέμε ότι είναι **θετικός** και γράφουμε $D \geq 0$ αν $n_P \geq 0, \forall P \in C$. Ορίζουμε ακόμη $D1 \geq D_2$ ανν $D_1 - D_2 \geq 0$.*

Ο συγκεκριμένος ορισμός μας επιτρέπει να περιγράφουμε μέσω ανισοτήτων μεταξύ διαιρετών τους πόλους και μηδενικά συναρτήσεων πάνω από καμπύλες.

Ορισμός 2.4.2. *Ορίζουμε $\mathcal{L}(D) = \{f \in \bar{K}(C)^* : div(f) \geq -D\} \cup \{0\}$. Το $\mathcal{L}(D)$ είναι διανσματικός χώρος επί του $\bar{K}$ με διάσταση $\ell(D)$.*

Απόδειξη. *Μπορούμε εύκολα να δείξουμε ότι: $n_P(f+g) \geq min(n_P(f), n_P(g))$ και άρα αν $f, g \in \mathcal{L}(D)$ τότε $f + g \in \mathcal{L}(D)$. Ακόμη $div(af) = div(f)$. Από αυτές τις δύο ιδιότητες τα 8 αξιώματα που πληρούν οι διανυσματικοί χώροι έπονται εύκολα.*

Πρόταση 2.4.1. *Αν $deg(D) < 0$ τότε $\mathcal{L}(D) = \{0\}$ και προφανώς $\ell(D) = 0$.*

Απόδειξη. *Έστω $f \in \mathcal{L}(D)$ ή ισοδύναμα $div(f) + D \geq 0$, τότε $deg(div(f)) + deg(D) \geq 0$ και $deg(div(f)) = 0$, επομένως $deg(D) \geq 0$.*

Σε αυτά τα πλαίσια γίνεται εμφανής η σχέση ισοδυναμίας που ορίσαμε μεταξύ διαιρετών στη Πρόταση 2.2 μέσω της ακόλουθης παρατήρησης.

Παρατήρηση. *Αν $D_1 \sim D_2$ με $D_1 - D_2 = div(g)$ τότε ο χάρτης $f \to fg$ είναι ισομορφισμός $\mathcal{L}(D_1) \to \mathcal{L}(D_2)$. Άρα $D_1 \sim D_2 \Rightarrow \mathcal{L}(D_1) \cong \mathcal{L}(D_2)$.*

Παρατήρηση. *Αν K_C κανονικός διαιρέτης και $f \in \mathcal{L}(K_C)$ τότε $div(f\omega) \geq 0$ άρα f ολόμορφη και αντίστροφα αν $f\omega$ ολόμορφη τότε $f \in \mathcal{L}(K_C)$. Αφού κάθε διαφορική μορφή στο Ω_C είναι της μορφής $f\omega$ (θυμίζουμε ότι ο Ω_C έχει διάσταση 1), έχουμε τον ισομορφισμό $\mathcal{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ ολόμορφη}\}$*

Με αυτά τα εργαλεία θα περάσουμε σε ένα θεμελιώδες θεώρημα της αλγεβρικής γεωμετρίας το οποίο χρησιμοποιούμε χωρίς απόδειξη.

Θεώρημα 2.4.1. ***Riemann-Roch*** *Έστω ομαλή καμπύλη C και K_C κανονικός διαιρέτης(δηλαδή $K_C = div(\omega)$) σε αυτήν, τότε υπάρχει ένας φυσικός αριθμός g τέτοιος ώστε για κάθε διαιρέτη $D \in Div(C)$:*

$$\ell(D) - \ell(K_C - D) = deg(D) - g + 1 \tag{1}$$

Πρόταση 2.4.2. *1. $\ell(K_C) = g$*

2. $deg(K_C) = 2g - 2$

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

Απόδειξη. *1. για $D = 0$ έχουμε $\ell(0) = 1, deg(D) = 0$ και το ζητούμενο έπεται.*

2. για $D = K_C$ ομοίως

3. από το 2., $deg(D) > 2g-2 = deg(K_C)$, άρα $deg(K_C - D) < 0$ και άρα από την Πρόταση 2.4.1: $\ell(K_C - D) = 0$ και το ζητούμενο έπεται από το Θεώρημα 2.4.1.

Για να κατανοήσουμε καλύτερα την ισχύ αυτού του θεωρήματος ας δούμε την ακόλουθη εφαρμογή.

Παράδειγμα 2.4.1. *Έστω C καμπύλη στο K με ένα ρητό σημείο και γένος $g = 0$. Τότε $C \cong P^1$ στο K.*

Απόδειξη. *Αφού P ρητό τότε $deg(P) = [K(P) : K] = [K : K] = 1$, επομένως έχουμε $deg(P) = 1 > 2g - 2$ και άρα από θεώρημα 2.4.1,3 έχουμε $\ell(P) = deg(P) - 0 + 1 = 2$ άρα $\exists f \in \mathcal{L}(P)$ με ακριβώς ένα πόλο στο P. Άρα $div_\infty(f) = P$ που είναι βαθμού 1 και άρα από την Πρόταση 2.1.3 η f είναι ισομορφισμός μεταξύ της C και του P^1.*

3 Γεωμετρία Ελλειπτικών Καμπυλών

3.1 Η εξίσωση μιας Ελλειπτικής Καμπύλης

Ορισμός 3.1.1. ***Ελλειπτικές Καμπύλες*** *ονομάζονται οι καμπύλες γένους 1 μαζί με ένα συγκεκριμένο σημείο βάσης.*

Οι ελλειπτικές καμπύλες ορίζονται στο P^2 και έχουν ακριβώς ένα σημείο βάσης στο άπειρο O. Όπως θα αποδείξουμε παρακάτω, κάθε ελλειπτική καμπύλη στο K χαρακτηρίζεται από μια εξίσωση **Weierstrass** της μορφής:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2}$$

με $a_1, \ldots, a_6 \in K$ ή ισοδύναμα σε μη ομογενή μορφή:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3}$$

Από την Εξίσωση 2 βλέπουμε ότι για $Z = 0$ έχουμε $X = 0$ και άρα ακριβώς ένα σημείο στο άπειρο $(0, a, 0) \sim O(0, 1, 0)$. Αν το $\bar{K}$ δεν έχει χαρακτηριστική 2 τότε μπορούμε να συμπληρώσουμε το τετράγωνο θέτοντας: $y \longmapsto \frac{1}{2}(y - a_1x - a_3)$ οπότε έχουμε:

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{4}$$

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

Υποθέτοντας ότι το $\bar{K}$ δεν έχει χαρακτηριστική ούτε 3 με την αντικατάσταση: $(x, y) \longmapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ φτάνουμε σε μια καμπύλη της μορφής:

$$y^2 = x^3 + Ax + B \tag{5}$$

στην οποία αντιστοιχίζουμε τις ποσότητες: $\Delta = -14(4A^3+27B^2)$ και $j = -1728\frac{4A^3}{\Delta}$, δηλαδή τη **διακρίνουσα** και την **j-αναλλοίωτη** ή απλά αναλλοίωτη της καμπύλης.

Εκτός από τις ποσότητες j και Δ θα ορίσουμε και το αναλλοίωτο διαφορικό μιας καμπύλης με εξίσωση Weierstrass δηλαδή το διαφορικό που θα παραμένει αναλλοίωτο υπό κάποιον χάρτη μεταφοράς.

Ορισμός 3.1.2. *Το αναλλοίωτο διαφορικό μιας καμπύλης που ορίζεται μέσω της Εξίσωσης 2 είναι η ποσότητα* $\omega = \frac{dx}{2y+a_1y+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y}$.

Πρόταση 3.1.1. *Για το διαφορικό* ω *όπως ορίστηκε παραπάνω ισχύει* $div(\omega) = 0$.

Απόδειξη. *Η βασική ιδέα της απόδειξης είναι ότι αν* $P = (x_o, y_o)$ *τότε* $\omega = \frac{d(x-x_o)}{F_y(x,y)} = \frac{d(y-y_o)}{F_x(x,y)}$ *και άρα δε μπορεί το* P *να είναι πόλος του* ω. *Από την Πρόταση (2.3.2.4) έχουμε επομένως* $div(\omega) = deg_P(x - x_o) - ord_P(F_y) - 1 = 2 - 1 - 1 = 0$. *Το σημείο* O *εξετάζεται ξεχωριστά.*

Παρατήρηση. *Η διακρίνουσα και η ποσότητα* j *είναι αναλλοίωτες υπό μεταφορά, δηλαδή υπό την αντικατάσταση* $(x, y) \longmapsto (x + a, y + b)$.

Πρόταση 3.1.2. *Έστω η ελλειπτική καμπύλη* E *με διακρίνουσα* Δ, *τότε η* E *είναι μη-ιδιάζουσα αν* $\Delta \neq 0$.

Απόδειξη. *Παρατηρούμε καταρχήν ότι το* $O(0, 1, 0)$ *δε μπορεί να είναι ιδιάζον σημείο αφού* $\frac{\partial F}{\partial Z} = 1$. *Άρα* $z \neq 0$ *και άρα μπορούμε να εξετάσουμε την αφινική μορφή της* C. *Η* C *είναι ιδιάζουσα από την Εξίσωση 3 αν* $\exists x_o \in K$: $2y_o = 12{x_o}^2 + 2b_2x_o + 2b_4 = 0$ *και άρα το* x_o *είναι διπλή ρίζα του* $4x^3 + b_2x^2 + 2b_4x + b_6$ *το οποίο συμβαίνει αν η διακρίνουσα του* $16\Delta = 0$.

Αφού είδαμε τη μορφή μιας ελλειπτικής καμπύλης στο P^2 θα αποδείξουμε τώρα την ισοδυναμία με τον αυστηρό ορισμό δηλαδή:

Θεώρημα 3.1.1. *Για κάθε ελλειπτική καμπύλη E/K υπάρχουν δύο συναρτήσεις συντεταγμένων $x, y \in K(E)$ έτσι ώστε ο χάρτης $\phi : E \to P^2, \phi = [x, y, 1]$ να είναι ισομορφισμός σε μια εξίσωση Weierstrass και μάλιστα $\phi(O) = [0, 1, 0]$.*

Απόδειξη. *Έστω ο διανυσματικός χώρος $\mathcal{L}(n(O))$. Για $n > 0$ έχουμε $deg(n(O)) = n > 2g - 2 = 2 - 2 = 0$ άρα από την Πρόταση 2.4.2.3 έχουμε $\ell(n(O)) = deg(n(O)) - g + 1 = deg(n(O)) = n$. Άρα $\ell(2(O)) = 2$ και $\ell(3(O)) = 3$ επομένως υπάρχουν x, y: $1, x$ είναι βάση του $\mathcal{L}(2(O))$ και $1, x, y$ είναι βάση του $\mathcal{L}(3(O))$ με πόλους τάξεως ακριβώς 2 και 3 στο O αντίστοιχα. Για το $\mathcal{L}(6(O))$ όμως έχουμε $\ell(6(O)) = 6$ και $\{1, x, y, xy, x^2, y^2, x^3\} \in \mathcal{L}(6(O))$, δηλαδή επτά στοιχεία και άρα έχουν γραμμική εξάρτηση: $A_1 + A_2x + A_3y + A_4xy + A_5x^2 + A_6y^2 + A_7x^3$. Με αντικατάσταση $(x, y) \longmapsto (-A_6A_7x, A_6{A_7}^2y)$ προκύπτει το ζητούμενο. Για να δείξουμε ότι ο ϕ είναι ισομορφισμός αρκεί να παρατηρήσουμε ότι $[K(E) : K(x, y)]$ διαιρεί το $[K(E) : K(x)] = 2$ και $[K(E) : K(x, y)]$ διαιρεί το $[K(E) : K(y)] = 3$, άρα $[K(E) : K(x, y)] = 1$ και άρα $deg(f) = 1$.*

Αποδεικνύεται και η αντίστροφη πρόταση μέσω Riemann-Roch: αφου $div(\omega) = 0$ έχουμε $deg(\omega) = 2g - 2 \implies 2g - 2 = 0 \implies g = 1$.

Θεώρημα 3.1.2. *Οι μόνοι ισομορφισμοί μεταξύ δύο καμπυλών Weiestrass είναι της μορφής: $(x, y) \longmapsto (u^2x' + r, u^3y' + su^2x' + t)$.*

Απόδειξη. *Έστω οι συναρτήσεις συντεταγμένων (x, y) και (x', y') στην ελλειπτική καμπύλη E. Τότε οι x, x' έχουν πόλο τάξεως 2 στο O και οι y, y' πόλο τάξεως 3. Άρα έχουμε βάσεις για το διανυσματικό χώρο $\mathcal{L}(2(O))$ τις $\{1, x\}, \{1, x'\}$ και για το $\mathcal{L}(3(O))$ τις $\{1, x, y\}, \{1, x', y'\}$, άρα $x = u_1x' + r$ και $y = u_2y' + sx' + t$ για κάποια $u_1, u_2, r, s, t \in K^*$. Αφού οι εξισώσεις μας έχουν συντελεστές 1 στα X^3, Y^2 έχουμε ${u_1}^3 = {u_2}^2$ και άρα για $u = \frac{u_1}{u_2}$ έχουμε το ζητούμενο.*

Είναι σχετικά εύκολο να διαπιστώσουμε ότι η αναλλοίωτη j αποτελεί παράμετρο άρρηκτα δεμμένη με την καμπύλη C,για την ακρίβεια:

Πρόταση 3.1.3. *Δύο ελλειπτικές καμπύλες με $\Delta \neq 0$ είναι ισομορφικές στο $\bar{K}$ ανν έχουν την ίδια αναλλοίωτη j.*

Απόδειξη. *Έστω $j = j'$ τότε $\frac{4A^3}{4A^3+27B^2} = \frac{4A'^3}{4A'^3+27B'^2} \implies A^3B'^2 = A'^3B^2$. Θα δείξουμε ότι υπάρχει ισομορφισμός μεταξύ τους της μορφής $(x, y) \longmapsto (u^2x', u^3, y')$. Αν $A \neq 0$ τότε $u = (B/B')^{\frac{1}{6}}$*

1. *Αν $A = 0$ τότε $u = (B/B')^{\frac{1}{6}}$*
2. *Αν $B = 0$ τότε $u = (A/A')^{\frac{1}{4}}$*
3. *Αν $A, B \neq 0$ τότε $u = (A/A')^{\frac{1}{4}} = (B/B')^{\frac{1}{6}}$*

Το αντίστροφο βασίζεται στην Πρόταση 3.1.2 αφού αν η καμπύλη έχει τη μορφή της εξίσωσης 5 τότε μόνο αυτοί οι ισομορφισμοί υπάρχουν που διατηρούν το j.

3.2 Η Δομή Ομάδας σε Ελλειπτικές Καμπύλες

Η ομάδα μιας ελλειπτικής καμπύλης μέσω της εξίσωσης Weierstrass

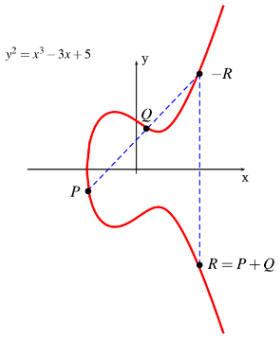
Πριν αναφερθούμε στην δομή ομάδας που συναντάμε σε μια ελειπτική καμπύλη ας θυμηθούμε τον λόγο για τον οποίο τις ορίσαμε στο P^2:

Πρόταση 3.2.1. *Κάθε ευθεία στο P^2 τέμνει μια ελλειπτική καμπύλη σε ακριβώς τρία (μη διακριτά) σημεία.*

Απόδειξη. *Άμεση εφαρμογή του θεωρήματος του Bézout.*

Είμαστε έτοιμοι τώρα να ορίσουμε μια πράξη μεταξύ δύο σημείων μιας ελλειπτικής καμπύλης:

Ορισμός 3.2.1. *Έστω P, Q δύο σημεία μιας ελλειπτικής καμπύλης, τότε η ευθεία που διέρχεται από τα P, Q τέμνει την καμπύλη σε ένα τρίτο σημείο $-R$ από την Πρόταση 3.2.1. Ομοίως και η ευθεία μεταξύ των $-R, O$ τέμνει την καμπύλη σε ένα ακόμα σημείο R. Ορίζουμε τελικά $P + Q = R$.*



Σχήμα 3: Η πρόσθεση σε ελλειπτικές καμπύλες στο P^2

Από την ακόλουθη πρόταση είναι εμφανές ότι τα σημεία μιας ελλειπτικής καμπύλης με την παραπάνω πράξη πρόσθεσης αποτελούν ομάδα και μάλιστα αβελιανή.

Πρόταση 3.2.2. *1. Αν P, Q, R ανήκουν στην ίδια ευθεία τότε $(P + Q) + R = 0$*

2. *$P + O = P$ για κάθε σημείο της καμπύλης P*
3. *$P + Q = Q + P$, $\forall Q, P$*
4. *για κάθε σημείο της καμπύλης P υπάρχει ένα σημείο $-P$: $P + (-P) = O$*
5. *ισχύει η επιμεριστική ιδιότητα $(P + Q) + R = P + (Q + R)$*
6. *αν η E είναι ορισμένη πάνω στο K τότε $E(K) \leq E$*

Απόδειξη. *Όλες οι ιδιότητες $1 - 4$ είναι προφανείς και έπονται άμεσα από τον Ορισμό 3.2.1, η επιμεριστική ιδιότητα μπορεί να προκύψει μετά από πράξεις ή από το Θεώρημα 3.2.1, ενώ η 6 είναι προφανής αφού η ευθεία μεταξύ δύο σημείων στο K έχει συντελεστές στο K και άρα οι συντεταγμένες του τρίτου σημείου θα είναι πάντα κάποια ρητή συνάρτηση των συντεταγμένων των άλλων δύο και άρα θα είναι και αυτό στο K.*

Από αυτό το σημείο και έπειτα θα γράφουμε $[m]P$ όταν θέλουμε να πούμε $\overbrace{P + P + \cdots + P}^{m\text{-φορές}}$ αν $m > 0$ ή $\overbrace{-P - P - \cdots - P}^{m\text{-φορές}}$ άν $m < 0$. Παρακάτω θα δώσουμε συγκεκριμένους τύπους για την πρόσθεση σημείων σε μια ελλειπτική καμπύλη. Αρχικά θέτουμε $P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3)$ και στη συνέχεια διακρίνουμε περιπτώσεις:

1. Αν $x_1 \neq x_2$ τότε $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ και $\upsilon = \frac{y_1 x_2 - x_2 y_1}{x_2 - x_1}$.

2. Αν $x_1 = x_2$ τότε $\lambda = \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}$ και $v = \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}$.

Τα παραπάνω προκύπτουν από την ευθεία μεταξύ των P, Q ή την εφαπτομένη στο $P = Q$ αντίστοιχα με εξίσωση $y = \lambda x + v$. Τελικά για το R έχουμε:

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

Μια αλγερική προσέγγιση της ομάδας μιας ελλειπτικής καμπύλης

Ξεκινάμε αυτό το κεφάλαιο με μια παρατήρηση για την κλάση ισοδυναμίας δύο διαιρετών σε μια καμπύλη γένους 1.

Παρατήρηση. *Έστω δύο σημεία P, Q σε μια καμπύλη C γένους 1 τότε $(P) \sim (Q)$ ανν $P = Q$.*

Απόδειξη. *Αν $(P) \sim (Q)$ τότε $(P) - (Q) = div(f)$ και άρα $f \in \mathcal{L}((Q))$ όμως $\ell((Q)) = 1$ οπότε περιέχει μόνο σταθερές συναρτήσεις και άρα $(P) - (Q) = div(a) = 0, a \in \bar{K}$ και άρα $P = Q$.*

Θα ορίσουμε τώρα ένα μια ομάδα με βάση το $Pic^0(E)$ και θα δείξουμε την ισοδυναμία της με την δομή που ορίσαμε στο προηγούμενο κεφάλαιο.

Πρόταση 3.2.3. *Έστω ελλειπτική καμπύλη E τότε:*

1. *$\forall D \in Div^0(E)$ υπάρχει μοναδικό $P \in E$: $D \sim (P)-(O)$ και άρα μπορούμε να ορίσουμε την απεικόνιση $\sigma : Div^0(E) \to E$ που στέλνει το D στο αντίστοιχο P. Προφανώς $\sigma((P) - (O)) = P$ και άρα η σ είναι επί.*

2. *$\sigma(D_1) = \sigma(D_2)$ ανν $D_1 \sim D_2$ και άρα ο σ είναι 1-1 στο $Pic^0(E)$.*

3. *Η αντίστροφη απεικόνιση της σ είναι η $\kappa : E \to Pic^0(E)$ με $P \longmapsto$ (κλάση διαιρετών του $(P)-(O)$)*

Απόδειξη.

1. *Από Πρόταση 2.4.2.3 $deg(D+(O)) = 1 > 2g-2 = 0$ άρα $\ell(D+(O)) = 1$ και επομένως $\exists f \in \bar{K}(E)$: $div(f) \geq -D-(O)$ και $deg(div(f)) = 0$. Συνεπώς $div(f) = -D-(O)+(P)$ για κάποιο $P \in E$ και άρα $D \sim (P)-(O)$. Η μοναδικότητα του P έπεται άμεσα από την παραπάνω παρατήρηση.*

2. *$\sigma(D_1) = \sigma(D_2) \iff P_1 = P_2 \iff (P_1) \sim (P_2) \iff (P_1)-(O) \sim (P_2)-(O) \iff D_1 \sim D_2$.*

3. *Προφανές.*

Θεώρημα 3.2.1. *Η αλγεβρική προσέγγιση και η γεωμετρική προσέγγιση της ομάδας μιας ελλειπτικής καμπύλης E ταυτίζονται. Δηλαδή έχουμε ισομορφισμό ομάδων $\kappa : E \to Pic^0(E)$.*

Απόδειξη. *Αρκεί να δείξουμε ότι το κ είναι ομομορφισμός και τα υπόλοιπα έπονται από το 1-1 και επί της Πρότασης 3.2.3. Αρκεί δηλαδή να δείξουμε ότι $\kappa(P + Q) = \kappa(P) + \kappa(Q)$. Έστω f η ευθεία μεταξύ των P, Q, R και f' η ευθεία μεταξύ των R, O τότε $div(f/Z) = (P) + (Q) + (R) - 3(O)$ και $div(f'/Z) = (R) + (P + Q) - 2(O)$ και άρα $0 \sim div(f/f') = ((P + Q) - (O)) - ((P) - (O)) - ((Q) - (O)) \implies (P + Q) - (O) \sim ((P) - (O)) + ((Q) - (O)) \implies \kappa(P + Q) = \kappa(P) + \kappa(Q)$.*

Παρατήρηση. *Από την ισοδυναμία των δύο ορισμών η επιμεριστική ιδιότητα της Πρότασης 3.2.2 έπεται άμεσα!*

Μπορούμε επίσης να χαρακτηρίσουμε εύκολα τους προταρχικούς διαιρέτες σε ελλειπτικές καμπύλες με την παρακάτω πρόταση:

Πρόταση 3.2.4. *Έστω ελλειπτική καμπύλη E και $D = \sum n_p(P) \in Div(E)$. Ο D είναι πρωταρχικός διαιρέτης ανν: $\sum_{P\in E} n_p = 0$ και $\sum_{P\in E}[n_p](P) = O$.*

Απόδειξη. *Για να είναι ένας διαιρέτης πρωταρχικός θα πρέπει προφανώς $deg(D) = 0$. Επίσης έχουμε $D \sim 0 \iff \sigma(D) = O \iff \sigma(\sum n_p(P) - \sum n_p(O)) = 0 \iff \sum_{P\in E} n_p\sigma((P) - (O)) = 0 \iff \sum_{P\in E} n_pP$.*

4 Ισογένιες

Αφού ορίσαμε τα αντικείμενα που θα μελετήσουμε, δηλαδή τις ελλειπτικές καμπύλες, μένει τώρα να ορίσουμε τους μορφισμούς/σχέσεις μεταξύ τους ως έννοια της θεωρίας κατηγοριών. Αυτή τη συσχέτιση θα μας επιτρέψει η έννοια της ισογένιας μεταξύ δύο ελλειπτικών καμπυλών.

Ορισμός 4.0.1. ***Ισογένια*** *ονομάζεται ένας μορφισμός μεταξύ δύο ελλειπτικών καμπυλών $\phi : E_1 \to E_2$ τέτοια ώστε $\phi(O) = O$. Ο βαθμός της ισογένιας είναι ο βαθμός του αντίστοιχου μορφισμού και όλες οι ιδιότητες που αφορούν σε διαχωρισιμότητα έπονται από τη διαχωρισιμότητα της επέκτασης $[\bar{K}(E_1) : \phi(\bar{K}(E_2))]$.*

Από τον ορισμό έπεται άμεσα η ακόλουθη παρατήρηση:

Παρατήρηση. *Αν ϕ ισογένια μεταξύ δύο ελλειπτικών καμπυλών τότε η ϕ είναι είτε η τετριμμένη ισογένια (στέλνει όλα τα σημεία στο O) είτε επί.*

Απόδειξη. *Άμεσα από την Πρόταση 2.1.1.*

Από σύβαση θα θεωρούμε $deg([0]) = 0$ όπου $[0]$ η τετριμμένη ισογένια. Έτσι έχουμε $deg(f \circ g) = deg(f)deg(g)$. Ο λόγος που ορίζουμε τις ισογένιες είναι εμφανής από το ακόλουθο θεώρημα:

Θεώρημα 4.0.1. *Μια ισογένια $\phi : E_1 \to E_2$ είναι ομομορφισμός ομάδων μεταξύ των E_1 και E_2. Δηλαδή για κάθε $P, Q \in E_1$ ισχύει $\boldsymbol{\phi(P+Q) = \phi(P) + \phi(Q)}$.*

Απόδειξη. *Για την τετριμμένη ισογένια η απόδειξη είναι προφανής. Αλλιώς η ϕ έχει έναν αντίστοιχο ομομορφισμό $\phi_* : Pic(E_1) \to Pic(E_2)$ που ορίζεται ως $\phi_*(\text{κλάση του} \sum n_i(P_i)) \mapsto$ κλάση του $\phi(\sum n_i(P_i))$. Αφού $Pic(E_i) \approx E_i$ και ϕ_* ομομορφισμός τότε και ο ϕ ομομορφισμός. Η απόδειξη συνοψίζεται στο ακόλουθο αντιμεταθετικό διάγραμμα.*

$$\begin{array}{ccc} E_1 & \xrightarrow[\kappa_1]{\cong} & \mathrm{Pic}^0(E_1) \\ \phi \downarrow & & \downarrow \phi_* \\ E_2 & \xrightarrow[\kappa_2]{\cong} & \mathrm{Pic}^0(E_2). \end{array}$$

Ορισμός 4.0.2. *Το σύνολο όλων των ισογενιών $\phi : E_1 \to E_2$ το συμβολίζουμε ως $\boldsymbol{Hom(E_1, E_2)}$ και αποτελεί ομάδα (με πράξη την $(\phi + \psi)(P) = \phi(P) + \psi(P)$) λόγω του ότι η ομάδα μιας ελλειπτικής καμπύλης είναι αβελιανή. Συμβολίζουμε επίσης $Hom(E, E) = End(E)$ και είναι δακτύλιος με δεύτερη πράξη τη σύνθεση $\phi \circ \psi = \phi\psi$.*

Παρατήρηση. *Γενικά το $End(E)$ ενδέχεται να μην είναι αντιμεταθετικός δακτύλιος όμως για κάθε ισογένια ϕ έχουμε $[m]\phi = \phi[m]$ αφού $[m] \circ \phi(P) = m\phi(P) = \phi(mP) = \phi \circ [m]$.*

Παρατήρηση. *Αν ορίσουμε έναν χάρτη μετάθεσης $\tau : E \to E, \tau_Q(P) = P + Q$ τότε ένας οποιοσδήποτε μορφισμός $F : E_1 \to E_2$ μπορεί να μετατραπεί στην αντίστοιχη ισογένια: $\phi = \tau_{-F(O)} \circ F$. Επίσης έχουμε $F = \tau_{F(0)} \circ \phi$ δηλαδή κάθε μορφισμός είναι σύνθεση μιας ισογένιας και μιας μετάθεσης.*

Το ακόλουθο θεώρημα δείχνει την ουσιαστική μορφή μιας ισογένιας που χρησιμοποιούμε στην πράξη:

Θεώρημα 4.0.2. *Κάθε ισογένια είναι της μορφής $\phi(x, y) = (\frac{p(x)}{q(x)}, \frac{r(x)}{t(x)}y)$ όπου p, q, r, s πολυώνυμα.*

Απόδειξη. *Επειδη κάθε ισογένια είναι μορφισμός έχει τη μορφή:* $\phi = (h(x,y), g(x,y))$ *όπου* f, g *ρητές συναρτήσεις στο* P^2. *Επειδή* $y^2 = f(x)$ *από την εξίσωση Weierstrass έχουμε ότι* $y^2 k = f^2 k(x)$ *και άρα* $h(x,y) = \frac{f_1(x)+f_2(x)y}{f_3(x)+f_4(x)y} = \frac{(f_1(x)+f_2(x)y)(f_3(x)-f_4(x)y)}{{f_3}^2(x)-{f_4}^2(x)y^2} = h_1(x) + h_2(x)y$ *και ομοίως* $g(x,y) = g_1(x) + g_2(x)y$ *όπου* h_i, g_i *ρητές συναρτήσεις. Αλλά η* ϕ *είναι ομομορφισμός ομάδων και άρα* $\phi(x,-y) = -\phi(x,y) \implies h_1(x) - h_2(x)y = h_1(x) + h_2(x)y \implies h_2(x) = 0$ *και* $g_1(x) - g_2(x)y = -g_1(x) - g_2(x)y \implies g_1(x) = 0$. *Το ζητούμενο έπεται άμεσα.*

Η παραπάνω μορφή μιας ισογένιας θα μας επιτρέψει να αναλύσουμε τις ιδιότητές της πιο πρακτικά και να υπολογίσουμε πιο εύκολα στην πράξη το βαθμό και την διαχωρισιμότητά της. Πριν από αυτά ωστόσο ας θυμηθούμε ότι μια ισογένια είναι στην ουσία ένας ομομορφισμός μεταξύ των ομάδων δύο ελλειπτικών καμπυλών και ένα από τα πιο θεμελιώδη χαρακτηριστικά που πρέπει να εξετάσουμε είναι ο πυρήνας του $ker(\phi)$. Ο πυρήνας είναι ακριβώς τα στοιχεία που πηγαίνουν στο O δηλαδή σε αφινικές συντεταγμένες οι πόλοι της $\phi(x,y)$.

4.1 Ο πυρήνας μιας ισογένιας

Πρόταση 4.1.1. *Έστω ισογένια* $\phi : E_1 \to E_2$ *της μορφής:* $\phi(x,y) = (\frac{p(x)}{q(x)}, \frac{r(x)}{t(x)}y)$ *τότε* $q^3 | t^2$ *και* $t^2 | q^3 f_1(x)$ *όπου* $f_1(x) = y^2$ *η εξίσωση της* E_1.

Απόδειξη. *Με αντικατάσταση της* $\phi(x,y)$ *στην εξίσωση της καμπύλης* E_1 *προκύπτει* $q^3 r^2 f_1 = t^2 w$ *και* $gcd(q,w) = gcd(r,t) = 1$ *από το οποίο το ζητούμενο έπεται άμεσα.*

Σαν άμεση συνέπεια της παραπάνω πρότασης προκύπτει ότι τα q, t έχουν τις ίδιες ρίζες.

Θεώρημα 4.1.1. *Έστω ισογένια* $\phi : E_1 \to E_2$ *της μορφής:* $\phi(x,y) = (\frac{p(x)}{q(x)}, \frac{r(x)}{t(x)}y)$, *τα στοιχεία του πυρήνα της ισογένιας είναι ακριβώς οι ρίζες της* $q(x) = 0$.

Απόδειξη. *Για να ανήκει κάποιο* x *στο πυρήνα πρέπει μετά από ομογενοποίηση:* $\phi(x,y) = (p(x)t(x), p(x)q(x)y, t(x)q(x)) = (0,1,0)$ *και άρα αφού* $q^3 | t^3$ *κάθε ρίζα* x_0 *του* $t(x)$ *έχει μεγαλύτερη πολλαπλότητα από ότι στο* $q(x)$, *διαιρώντας με τη μέγιστη δυνατή δύναμη του* $x - x_0 z$ *που μπορούμε έχουμε απαλοιφή της ρίζας του* $q(x)$ *από τον μεσαίο όρο* $\phi_y \neq 0$ *ενώ οι* $\phi_x, \phi_z = 0$. *Άρα αν* $y_0 \neq 0$ *τότε η απόδειξη τελείωσε. Αν* $y_0 = 0$ *τότε* $(p(x)t(x), p(x)q(x)y, t(x)q(x)) = (yp(x)t(x), p(x)q(x)y^2, t(x)q(x)y)$ *και* x_0 *απλή ρίζα αφού η καμπύλη είναι μη ιδιάζουσα. Αντικαθιστούμε τώρα το* y^2 *και διαιρούμε με τη μέγιστη δύναμη του* $x - x_0 z$ *οπότε λαμβάνουμε πάλι* $\phi_y \neq 0$ *και* $\phi_x, \phi_z = 0$.

Πρόταση 4.1.2. *Ο πυρήνας μιας ισογένιας είναι πεπερασμένος.*

Απόδειξη. *Προφανές αφού* $|ker(\phi)| \leq deg(q)$.

Πριν περάσουμε στην μελέτη του πυρήνα θα εξετάσουμε πρώτα τι συμβαίνει γενικά με τις προεικόνες κάποιου στοιχείου σε έναν μορφισμό με την ακόλουθη πρόταση την οποία διατυπώνουμε χωρίς απόδειξη:

Πρόταση 4.1.3. *Έστω* $\phi : E_1 \to E_2$ *μορφισμός καμπυλών τότε:*

1. *Για κάθε* Q *στην* E_2 *έχουμε:* $\sum_{\phi \in \phi^{-1}(Q)} e_\phi(P) = deg(\phi)$.
2. $|\phi^{-1}(Q)| = deg_s(\phi)$ *για όλα εκτός από πεπερασμένα* $Q \in E_2$.

Από την παραπάνω πρόταση και το ότι ϕ ομομορφισμός έχουμε ότι:

Θεώρημα 4.1.2. *Αν $\phi : E_1 \to E_2$ ισογένια τότε $|\phi^{-1}(Q)| = deg_s(\phi)$,$\forall Q \in E_2$. Άρα $|ker(\phi)| = |\phi^{-1}(O)| = deg_s(\phi)$*

Απόδειξη. *Για κάθε $Q, Q' \in E_2$ επειδή ϕ ομομορφισμός ομάδων $\phi^{-1}(Q) = \phi^{-1}(Q')$ και άρα από το Πόρισμα 4.1.3 (2), έχουμε $|\phi^{-1}(Q)| = deg_s(\phi)$, $\forall Q \in E_2$.*

Το επόμενο θεώρημα που θα διατυπώσουμε είναι εξαιρετικά σημαντικό και μας βοηθάει να διακρίνουμε άμεσα και υπολογιστικά πότε μια ισογένια είναι διαχωρίσισμη:

Θεώρημα 4.1.3. *(**) Έστω ισογένια $\phi : E_1 \to E_2$ της μορφής: $\phi(x, y) = (\frac{p(x)}{q(x)}, \frac{r(x)}{t(x)}y) = (\phi_x, \phi_y)$ τότε ϕ διαχωρίσιμη αν $(\phi_x)' = (\frac{p(x)}{q(x)})' \neq 0$.*

Απόδειξη. *Από τη Πρόταση 2.3.1 έχουμε ότι ϕ διαχωρίσιμη ανν $\phi^*\omega \neq 0 \iff \frac{(d(\phi_x)/dx)dx}{2\phi_y + A\phi_x + B} \neq 0 \iff (\phi_x)' \neq 0$.*

Λήμμα 4.1.1. *Αν u, v πολυώνυμα σε σώμα K με χαρακτηριστική p και $gcd(u, v) = 1$ τότε: $(\frac{u}{v})' = 0 \iff u' = v' = 0 \iff u = f(x^p), v = g(x^p)$*

Απόδειξη. *$(\frac{u}{v})' = 0 \iff uv' = u'v$ και $gcd(u, v) = 1 \implies u|u', v|v' \implies u' = v' = 0$ αφού $deg(u') < deg(u), deg(v') < deg(v)$. Αν $u(x) = \sum_n a_n x^n$ τότε $u'(x) = \sum na_n x^{n-1} = 0 \mod p$ και άρα $a_n = 0$ για κάθε n που δεν είναι πολλαπλάσιο του p. Άρα $u(x) = \sum_p ma_p m x^p m$ και ομοίως το v. Το αντίστροφο είναι προφανές αφού: $u(x) = px^p - 1f'(x^p) = 0 \mod p$ και ομοίως το v.*

Παρατήρηση. *Σε σώμα χαρακτηριστικής 0 όλες οι ισογένιες είναι διαχωρίσισμες αλλιώς από το παραπάνω Λήμμα θα είχαμε ότι η ισογένια είναι σταθερή και άρα η τετριμμένη ισογένια.*

Πρόταση 4.1.4. *Αν $\phi(x, y) = (\frac{u(x)}{v(x)}, \frac{r(x)}{t(x)}y)$ μη διαχωρίσιμη ισογένια σε σώμα K με χαρακτηριστική p τότε: $\phi(x, y) = (r_1(x^p), r_2(x^p)y^p)$ όπου r_1, r_2 ρητές συναρτήσεις στο $K(x)$.*

Απόδειξη. *Όπως στην απόδειξη της Πρότασης 4.1.1 έχουμε $(r^2 f/t^2)' = (w/v^3)'$ και άρα από το Λήμμα 4.1.1 $r^2(x)f(x) = g(x^p)$ και $t^2(x) = g(x^p)$. Αφού η f δεν έχει πολλαπλή ρίζα στο $\bar{K}$ ως μη ιδιάζουσα καμπύλη τότε: $r^2(x)f(x) = (h(x^p)f^p(x))^2 = h^2(x^p)y^p$ και το ζητούμενο έπεται άμεσα.*

Περνάμε έτσι στο εξής θεώρημα:

Θεώρημα 4.1.4. *(**) Αν ϕ ισογένια μεταξύ ελλειπτικών καμπυλών σε ένα σώμα K με χαρακτηριστική $p > 0$ τότε $\phi = \phi_{sep} \circ \pi^n$ όπου π ο μορφισμός Frobenius $(x, y, z) \longmapsto (x^p, y^p, z^p)$. Προφανώς τότε $deg(\phi) = p^n deg(\phi_{sep})$.*

Απόδειξη. *Από την παραπάνω πρόταση είναι προφανές ότι κάθε μη διαχωρίσιμη ισογένια μπορεί να γραφτεί ως $\phi(x, y) = (r_1(x^p), r_2(x^p)y^p) = \phi_1 \circ \pi$. Επαναλαμβάνοντας τη διαδικασία παρατηρούμε ότι $deg(\pi) = p$ και άρα $deg(\phi_i) < deg(\phi_{i-1})$ άρα κάποτε τερματίζει η διαδικασία και έπεται το ζητούμενο.*

Τώρα μπορούμε να ορίσουμε το βαθμό μιας ισογένιας με πιο βολικό αλλά ισοδύναμο τρόπο.

Ορισμός 4.1.1. *Αν $\phi(x, y) = (\frac{u(x)}{v(x)}, \frac{r(x)}{t(x)}y)$ ισογένια τότε $deg(\phi) = max\{deg(u), deg(v)\}$.*

Θεώρημα 4.1.5. *(**) Οι δύο ορισμοί για το βαθμό μιας ισογένιας είναι ισοδύναμοι.*

Απόδειξη. *Θα δείξουμε ότι* $deg(\phi_{sep}) = |ker(\phi)| = max\{deg(u), deg(v)\}$. *Παρατηρούμε καταρχήν ότι* $ker(\pi) = O$ *αφού* $(x^p, y^p, z^p) = (0,1,0) \implies (x,y,z) = (0,1,0)$ *και άρα* $|ker(\phi)| = |ker(\phi_{sep})|$ *Έστω* $F(a,b) = ((x_0,y_0) \in E_1(\bar{K}) : \phi(x_0,y_0) = (a,b))$. *Αφού* ϕ *ομομορφισμός τότε* $|F(a,b)| = |ker(\phi)|$ *οπότε είναι πεπερασμένο και επειδή το* y_0 *είναι συνάρτηση του* x_0 *έχουμε ότι* $F(a,b) = F(a)$. *Ένα σημείο* $(x_0,y_0) \in F(a) \iff \frac{u(x_0)}{v(x_0)} = a \iff u(x_0) - av(x_0) = 0$ *αν* $g(x) = u(x) - av(x)$ *τότε διαλέγουμε ένα σύνολο* $F(a)$: $deg(g) = max\{deg(u), deg(v)\}$ *δηλαδή να μην απαλοίφονται οι μεγαλύτεροι όροι των δύο πολυωνύμων. Άρα* $|F(a,b)| = |x_0 : (x_0,y_0) \in E_1(\bar{K}), g(x_0) = 0|$. *Αρκεί να δείξουμε ότι οι ρίζες του* g *είναι διακριτές. Πράγματι αν* $g(x_0) = g'(x_0) = 0$ *τότε* $au(x_0) = v(x_0)$ *και* $v'(x_0) = au'(x_0)$ *και άρα* $u(x_0)v'(x_0) = u'(x_0)v(x_0)$ *δηλαδή* $\frac{d(u(x)/v(x))}{dx}|_{x_0} = 0$. *Άλλα η* $(\frac{p(x)}{q(x)})' = 0$ *έχει πεπερασμένες λύσεις και άρα υπάρχουν πεπερασμένα* a *για τα οποία το* $g(x) = 0$ *έχει διπλή ρίζα ενώ το* $F(a)$ *είναι άπειρο επομένως υπάρχει κάποιο* $a : (a,b) \in E_1(\bar{K})$ *και η* $g(x) = 0$ *έχει μόνο απλές ρίζες. Άρα τελικά:* $|F(a,b)| = |ker(\phi)| = max\{deg(u), deg(v)\}$.

Παράδειγμα 4.1.1. *Έστω οι καμπύλες* $E_1 : y^2 = x^3 + Ax^2 + Bx$ *και* $E_2 : y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$. *Τότε η* $\phi(x,y) = (\frac{y^2}{x^2}, \frac{B-x^2}{x^2}y)$ *είναι ισογένια και έχει βαθμό* $max\{deg(x^2 + Ax + B), deg(x)\} = 2$. *Επίσης* $ker(\phi) = \{O, (0,0)\}$ *όπως φαίνεται από τις ρίζες της* $x^2 = 0$ *πάνω στην* E_1.

Παράδειγμα 4.1.2. *Αν εξετάσουμε τον τύπο διπλασιασμού ενός σημείου σε μια ελλειπτική καμπύλη* E *προκύπτει ότι* $x' = \lambda^2 + \lambda a_1 - a_2 - 2x_1$ *και* λ *ρητή συνάρτηση βαθμού* 2. *Άρα η ισογένια* $[2]P$ *έχει βαθμό* 4. *Θα δούμε ότι γενικά* $deg([m]) = m^2$.

Από όσα είπαμε για τις μη διαχωρίσιμες ισογένιες περιμένουμε σίγουρα ο μορφισμός Frobenius να είναι μη διαχωρίσιμος και πράγματι αυτό ισχύει:

Πρόταση 4.1.5. *Ο μορφισμός Frobenius της* $E(\mathbb{F}_q)$ *είναι μη διαχωρίσιμος και βαθμού* q.

Απόδειξη. *Επειδή* $\pi_q(x,y) = (x^q, y^q)$ *έπεται άμεσα από τον ορισμό ότι* $deg(\pi_q) = q$ *και* $(x^q)' = qx^{q-1} = 0 \mod q$.

Περνάμε τώρα στην εξέταση του πως επηρεάζεται μια ισογένια από τον πυρήνα της με την ακόλουθη πρόταση:

Πρόταση 4.1.6. *Για μια καμπύλη* E *υπάρχει ακριβώς μία καμπύλη* E' *(ή μια ισομορφική της) και μια διαχωρίσιμη ισογένια με πυρήνα μία δεδομένη υποομάδα* G *της* E *(αυτή που περιγράφεται στην παρατήρηση παραπάνω).*

Πριν αποδείξουμε την πρόταση παρατηρούμε ότι αν υποθέσουμε την ύπαρξη δύο ισογενιών ϕ, ψ με ίδιο πυρήνα τότε: αν $\phi : E_1 \to E_2$ και $\psi : E_1 \to E_3$ με $ker(\phi) = ker(\psi)$ τότε από πρώτο θεώρημα ισομορφισμού και το ότι οι ισογένιες είναι επί: $E_2 = \phi(E_1) \simeq E_1/ker(\phi) = E_1/ker(\psi) \simeq \psi(E_1) = E_3$. Άρα $E_2 \simeq E_3$ οπότε $\phi, \psi : E_1 \to E_2$. Θα χρειαστούμε το ακόλουθο λήμμα στην απόδειξή μας:

Λήμμα 4.1.2. *Υπάρχει ισομορφισμός* $\psi : ker(\phi) \to Aut(\bar{K}(E_1)/\phi^*\bar{K}(E_2))$.

Απόδειξη. *Παρατηρούμε ότι* $\forall T \in ker(\phi)$ *ισχύει ότι* $\phi(P+T) = \phi(P)$ *ή ισοδύναμα* $\phi \circ \tau_T = \phi$. *Ας θεωρήσουμε τον χάρτη* $\psi : T \to \tau_T$. *Ο* $\psi : T \to \tau_T$ *είναι ομομορφισμός επειδή προφανώς* $\psi(P+T) = \tau_{P+T} = \tau_P \circ \tau_T = \psi(P)\psi(T)$. *Έχουμε ακόμη ότι* $\forall f \in \bar{K}(E_1)$, $\tau_T^*(\phi^*(f)) = (\phi \circ \tau_T)^* f = \phi^* f$. *Επομένως* $|Aut(\bar{K}(E_1)/\phi^*\bar{K}(E_2))| \leq deg(\phi)$ *από θεωρία Galois. Όμως ο* ψ *είναι 1-1 (αν* $\psi(T) = \tau_T = \tau_O$ *τότε το* τ_T^* *διατηρεί όλο το* $\bar{K}(E_1)$ *και άρα και την συνάρτηση* x *επομένως* $\tau_T^*(x) = \tau_O^*(x) \implies T = O$*)και άρα* $|Aut(\bar{K}(E_1)/\phi^*\bar{K}(E_2))| = deg(\phi)$ *οπότε προκύπτει ισομορφισμός.*

Περνάμε τώρα στην απόδειξη της **Πρότασης 4.1.6**:

Απόδειξη. *Έστω $\bar{K}(E)^G$ το υπόσωμα που διατηρείται σταθερό από την G τότε $\bar{K}(E)$ είναι Galois επέκταση του (αν ϕ διαχωρίσιμη) με ομάδα Galois ισομορφική στη G. Ακόμη το $\bar{K}(E)^G$ έχει βαθμό υπέρβασης 1 επί του $\bar{K}$ και άρα από γνωστό θεώρημα της αλγεβρικής γεωμετρίας έχουμε ότι υπάρχει ομαλή καμπύλη $C/\bar{K}$ και ακριβώς ένας μορφισμός $\phi : E \to C$ με $\phi^*\bar{K}(C) = \bar{K}(E)^G$. Τελικά έχουμε δηλαδή για κάθε συνάρτηση $f \in \bar{K}(C)$: $f(\phi(P+T)) = (\tau_T{}^* \circ \phi^*)f(P) = f(\phi(P))$ και άρα $\phi(P+T) = \phi(P)$. Παρατηρούμε ακόμη ότι $\phi^{-1}(Q) \supseteq P+T, T \in G$ και $|G| = deg(\phi) \geq \phi^{-1}(Q)$ άρα η ϕ έχει δείκτη διακλάδωσης 1 σε κάθε σημείο Q. Από τη φόρμουλα Riemann-Hurwitz τελικά: $2genus(E) - 2 = deg(\phi)(2genus(C) - 2)$ και άρα και η C είναι ελλειπτική καμπύλη.*

Παρατήρηση. *(Velu) Δεδομένης μιας ελλειπτικής καμπύλης E και μιας υποομάδας της G μπορούμε να υπολογίσουμε μια ισογένια $\phi : ker(\phi) = G$ με τον ακόλουθο τύπο: $\phi(P) = (x(P) + \sum_{Q \in G \neq O} x(P+Q) - x(Q), y(P) + \sum_{Q \in G \neq O} y(P+Q) - y(Q))$ αν $P \neq O, \phi(O) = O$ αλλιώς. Παρατηρούμε ότι για κάθε P $\phi(P+Q) = \phi(P) \iff Q \in G$ οπότε ο πυρήνας της απεικόνησης είναι το G. Παρακάτω θα δούμε ότι οι ελλειπτικές καμπύλες είναι αβελιανές πολλαπλότητες γένους 1, δηλαδή ένας μιγαδικός τόρος. Αβελιανή πολλαπλότητα σημαίνει ότι είναι προβολική αλγεβρική πολλαπλότητα με δομή ομάδας. Με αυτή τη παρατήρηση έχουμε ότι η δομή ομάδας στην E επιβάλλει δομή ομάδας στην εικόνα της ϕ με ρητές απεικονίσεις και άρα η εικόνα της ϕ είναι ελλειπτική καμπύλη. Ακόμα πιο γενικά μπορούμε να πούμε ότι σε μία αλγεβρική πολλαπλότητα E ο ομομορφισμός $E \to E/G$ είναι μορφισμός για κάθε πεπερασμένη ομάδα αυτομορφισμών G. Μία αυστηρή απόδειξη μπορεί να δωθεί με χρήση της φόρμουλας Riemann-Hurwitz αφού αποδείξουμε φυσικά ότι η ϕ έχει παντού δείκτη διακλάδωσης 1(είναι στην αγγλική ορολογία unramified) που ισχύει διότι όλα τα $Q \in E$ έχουν προεικόνα μεγέθους $\phi^{-1}(Q) = |G|$. Από την πρόταση 4.1.6 και το ότι η ισογένια αυτή είναι διαχωρίσιμη έπεται η μοναδικότητα αυτής. Για περισσότερα για τον τύπο του (Velu) βλ.[7]*

Για διευκόλυνση των πράξεων θα θεωρούμε $x_P = x(P), P \neq O$ και $\phi(O) = O$. Φυσικά στον τελικό τύπο θα έχουμε ξεχωριστά την περίπτωση $P = O$ όπως και παραπάνω αλλά τελικά το αποτέλεσμα δεν αλλάζει.

Πρόταση 4.1.7. *(**) Έστω διαχωρίσιμες $\phi : E_1 \to E_2$ και $\psi : E_1 \to E_3$ με $G' = ker(\phi) \subset ker(\psi) = G$ τότε υπάρχει ισογένια $\lambda : \lambda \circ \phi = \psi$.*

Απόδειξη. *Από την παραπάνω παρατήρηση έχουμε ότι $\phi(P) = (\sum_{Q \in G'}(x_{P+Q} - x_Q), \sum_{Q \in G'}(y_{P+Q} - y_Q))$. Τότε έστω $\lambda(P) = (\sum_{g \in G/G'}(x_{P+\phi(g)} - \phi_x(g)), \sum_{g \in G/G'}(y_{P+\phi(g)} - \phi_y(g)))$. Παρατηρούμε ότι: $x_{\phi(P)+\phi(g)} = x_{\phi(P+g)}$ και ομοίως για το y οπότε έχουμε: $\lambda \circ \phi(P) = (\sum_{g \in G/G'}(\phi_x(P+g) - \phi_x(g)), \sum_{g \in G/G'}(\phi_y(P+g) - \phi_y(g))) = (\sum_{g \in G/G'}(\sum_{Q \in G'}(x_{P+g+Q} - x_{g+Q})), \sum_{g \in G/G'}(\sum_{Q \in G'}(y_{P+g+Q} - y_{g+Q})) = (\sum_{Q \in G}(x_{P+Q} - x_Q), \sum_{Q \in G}(y_{P+Q} - y_Q))$(για ομομορφισμό h με κανονική υποομάδα G', $\sum_{g \in G} h(g) = \sum_{g \in G/G'} \sum_{Q \in G} h(q+Q)$). Άρα τελικά έχουμε ισογένια με πυρήνα το G και από την Πρόταση 4.1.6 για μοναδικότητα $\lambda \circ \phi(P) = \psi(P)$. Το ότι η λ είναι ισογένια $E_2 \to E_3$ είναι προφανές αφού $\lambda(O) = \lambda(\phi(O)) = \psi(O) = O$ και $\lambda(E_2) = \lambda(\phi(E_1)) = \psi(E_1) = E_3$ καθώς ϕ, ψ είναι επί ως μη τετριμμένοι μορφισμοί καμπυλών.*

4.2 Επίδραση του αναλλοίωτου διαφορικού σε ισογένιες

Σε αυτή την ενότητα θα μελετήσουμε το αναλλοίωτο διαφορικό και πως αυτό αλληλεπιδρά με τις ισογένιες. Καταρχήν θα αποδείξουμε ότι το αναλλοίωτο διαφορικό είναι αναλλοίωτο υπό μεταφορά.

Πρόταση 4.2.1. *Έστω E ελλειπτική καμπύλη και ω το ολόμορφο διαφορικό της, τότε* ${\tau_Q}^*\omega = \omega$.

Απόδειξη. *Επειδή Ω_C έχει διάσταση 1 υπάρχει συνάρτηση $a(Q) \in \bar{K}(E)^* : {\tau_Q}^*\omega = a(Q)\omega$. Τότε $div(a(Q)) + div(\omega) = div({\tau_Q}^*\omega) \implies div(a(Q)) = {\tau_Q}^* div(\omega) = 0$ διότι $div(\omega) = 0$ ως ολόμορφη. Άρα $a(Q) \in \bar{K}^*$. Τέλος $a(Q) = a(O) = 1$.*

Ο ρόλος του διαφορικού είναι γενικά η γραμμικοποίηση σύνθετων τύπων κάτι που σίγουρα θα θέλαμε για την άθροιση σημείων σε μια ελλειπτική καμπύλη. Να μπορούμε δηλαδή να εφαρμόζουμε το αναλλοίωτο διαφορικό σε προσθετικές σχέσεις μιας ελλειπτικής καμπύλης. Πράγματι αν $P = Q + R$ τότε $\omega(P) = \omega(Q) + \omega(R)$. Η πιο απλή απόδειξη είναι απλά με πράξεις και για αυτό την παραλείπουμε.

Πρωτού περάσουμε στη συνέχεια ας δούμε μια σημαντική ιδιότητα της ϕ^* που θα μας χρησιμεύσει παρακάτω και ειδικά όταν εξετάσουμε τη δυϊκή ισογένια:

Πρόταση 4.2.2. *Έστω ισογένιες $\phi, \psi : E_1 \to E_2$ τότε $(\phi + \psi)^* = \phi^* + \psi^*$.*

Απόδειξη. *Έστω ο πρωταρχικός διαιρέτης: $div(f) = ((\phi + \psi)(P_1)) - (\phi(P_1)) - (\psi(P_1)) + (O), P_1 \in K(E_1)$. Τότε θα έχουμε $div(f) = ((\phi+\psi)^*(P_2)) - (\phi^*(P_2)) - (\psi^*(P_2)) + (O), P_2 \in K(E_1)$ από άμεση εξέταση του κάθε πόλου και μηδενικού της f. Όμως τώρα $(\phi+\psi)^* = \phi^*+\psi^*$ από την Πρόταση 3.2.4.*

Θεώρημα 4.2.1. *Έστω $\phi, \psi : E_1 \to E_2$ ισογένιες τότε $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$.*

Απόδειξη. *Άμεση εφαρμογή του αναλλοίωτου διαφορικού στη σχέση $(\phi+\psi)^*(P) = \phi^*(P) + \psi^*(P)$.*

Πρόταση 4.2.3. *Αν ω το αναλλοίωτο διαφορκό σε μια ελλειπτική καμπύλη E τότε $[m]^*\omega = m\omega$.*

Απόδειξη. *Άμεση εφαρμογή του παραπάνω θεωρήματος με επαγωγή.*

4.3 Η Δυϊκή ισογένια

Σε αυτή την ενότητα θα ασχοληθούμε ουσιαστικά με τον χάρτη $\phi^* : Pic(E_2) \to Pic(E_1)$ που σχετίζεται με την αντίστοιχη ισογένια $\phi : E_1 \to E_2$. Διατυπώνουμε το παρακάτω θεώρημα χωρίς απόδειξη (βλ. άσκηση 3.7 Silverman):

Θεώρημα 4.3.1. *Έστω ελλειπτική καμπύλη E τότε: $m(x, y) = (\phi_m(x)/{\psi_m}^2(x), \omega_m(x, y)/{\psi_m}^3(x, y))$. Επίσης $\phi_m(x) = x(\psi_m)^2(x) - \psi_{m-1}(x)\psi_{m+1}(x)$ και $\psi_{2m+1} = \psi_{m+2}{\psi_m}^3 - \psi_{m-1}\psi_m + 1^3, m \geq 2$ και $\psi_1(x) = 1$. Από επαγωγή προκύπτει ότι: $\phi_m(x) = x^{m^2} + \dots$ και ${\psi_m}^2(x) = m^2 x^{m^2-1} + \dots$.*

Πρόταση 4.3.1. *(**) Έστω E/K με χαρακτηριστική p τότε η ισογένια $[m]$ είναι διαχωρίσιμη ανν $p \nmid m$.*

Απόδειξη. *Έχουμε $gcd(\phi_n, \psi_n) = 1$ αφού αν $\phi_n(x_0) = \psi_n(x_0) = 0$ τότε $nP = 0$ και από το Θεώρημα 4.3.1 $\psi_{m-1}(x_0)\psi_{m+1}(x_0) = 0$ και άρα $(n-1)P = O$ ή $(n+1)P = O$ οπότε από $nP = O$ έχουμε $P = O$ που είναι άτοπο. Αντίστροφα αν $p \nmid m$ τότε ο μεγιστοβάθμιος όρος της ϕ_m δεν μηδενίζεται και άρα $(\frac{\phi_n(x)}{{\psi_n}^2(x)})' \neq 0$ οπότε η ισογένια είναι διαχωρίσισμη. Αντίστροφα αν $p|m$ τότε $m^2 x^{m^2-1} = 0 \mod p$ και άρα $deg(\phi) \neq |ker(\phi)|$ οπότε η ισογένια δεν είναι διαχωρίσιμη.*

Παρατήρηση. *Από την παραπάνω πρόταση και τον Ορισμό 4.1.1 έχουμε ότι $deg([m]) = m^2$.*

Παρατήρηση. *Για τον μορφισμό Frobenius $\pi : E \to E^{(q)}$ ισχύει ότι $\pi(P+Q) = \pi(P) + \pi(Q)$ για κάθε P, Q σημεία της καμπύλης αφού η πράξη της πρόσθεσης σημείων είναι ρητή συνάρτηση στο F_q και άρα δε μεταβάλεται αν πάρουμε τον εκθέτη q. Ισχύει συνεπώς ότι $\pi \circ [m] = [m] \circ \pi$.*

Περνάμε έτσι στο βασικό μας θεώρημα:

Θεώρημα 4.3.2. *Έστω ισογένια $\phi : E_1 \to E_2$ με βαθμό m, τότε υπάρχει μοναδική ισογένια $\hat{\phi} : E_2 \to E_1$ τέτοια ώστε: $\hat{\phi} \circ \phi = [m]$. Αυτή η ισογένια $\hat{\phi} : E_2 \to E_1$ ονομάζεται η δυϊκή ισογένια της $\phi : E_1 \to E_2$.*

Απόδειξη. *Διακρίνουμε δύο περιπτώσεις:*

1. *ϕ διαχωρίσισμη: τότε $|ker(\phi)| = m$ και άρα κάθε στοιχείο του πηρύνα έχει τάξη που διαιρεί το m οπότε $\forall P \in ker(\phi), [m]P = O \implies P \in ker([m])$. Άρα από την Πρόταση 4.1.7 υπάρχει $\hat{\phi} : E_2 \to E_1$ τέτοια ώστε $\hat{\phi} \circ \phi = [m]$. (Προφανώς αν $[m]$ μη διαχωρίσιμη τότε $[m] = 0$ στο K και άρα προφανώς ισχύει)*

2. *ϕ μη διαχωρίσισμη: τότε $\phi = \phi_{sep} \circ \pi^n$ από Θεώρημα 4.1.4. Επομένως αν ορίσουμε $\hat{\phi} = \hat{\pi}^n \circ \hat{\phi_{sep}}$ τότε $\hat{\phi} \circ \phi = \hat{\pi}^n \circ deg_{sep}(\phi) \circ \pi^n = \hat{\pi}^n \circ \pi^n \circ deg_{sep}(\phi) = [deg_i(\phi)] \circ [deg_{sep}(\phi)] = [deg_i(\phi) deg_{sep}(\phi)] = [deg(\phi)]$ από την παραπάνω παρατήρηση και το ότι $[deg_i(\phi)], [deg_{sep}(\phi)] \in End(E)$. Αρκεί να βρούμε επομένως το δυϊκό ενός μορφισμού Frobenius. Επειδή π^n είναι σύνθεση του π με τον εαυτό του n φορές αρκεί να βρούμε το δυϊκό του π. Αφού όμως σε σώμα χαρακτηριστικής p η ισογένια $[p]$ είναι μη διαχωρίσιμη τότε: $[p] = [p]_{sep} \circ \pi^k$ και άρα ο ζητούμενος χάρτης είναι ο $\psi = [p]_{sep} \pi^{k-1}$.*

Αν ϕ' είναι μια δεύτερη τέτοια ισογένια τότε $(\hat{\phi} - \phi')(\phi) = [0]$ και επομένως $\hat{\phi} = \phi'$. Η μοναδικότητα έπεται άμεσα συνεπώς.

Ορίζουμε τον χάρτη $sum : Div^0(E) \to E, sum(\sum_{P \in E} n_p(P)) \to \sum_{P \in E} [n_P]P$.Τότε:

Θεώρημα 4.3.3. *Η ισογένια $\hat{\phi}$ είναι στην ουσία η $E_2 \xrightarrow{\kappa_2} Div^0(E_2) \xrightarrow{\phi^*} Div^0(E_1) \xrightarrow{sum} E_1$.*

Απόδειξη. *Αν $Q \in E_2$ τότε $sum(\phi^*((Q)-(O))) = \sum_{P \in \phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T \in \phi^{-1}(Q)} [e_\phi(T)]T$ και $e_\phi(P) = 1$ για όλα τα σημεία της E_2 οπότε: $sum(\phi^*((Q)-(O))) = [deg_i(\phi)](\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}(O)} T) = [deg_i(\phi)](\sum_{T \in \phi^{-1}(O)} (P+T) - \sum_{T \in \phi^{-1}(O)} T) = [deg_i(\phi)] \circ [|\phi^{-1}(O)|]P = [deg_i(\phi)] \circ [deg_{sep}(\phi)]P = [deg(\phi)]P$.*

Ας αναλύσουμε τώρα μερικές ιδιότητες της δυϊκής ισογένιας με το ακόλουθο θεώρημα:

Θεώρημα 4.3.4. *Έστω ισογένια $\phi : E_1 \to E_2$ με βαθμό m και $\hat{\phi}$ η δυϊκή της. Τότε:*

1. *$\hat{\phi} \circ \phi = [m]$ στην E_1 και $\phi \circ \hat{\phi} = [m]$ στην E_2.*
2. *αν $\lambda : E_2 \to E_3$ μια άλλη ισογένια τότε $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$*
3. *αν $\psi : E_1 \to E_2$ τότε $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$*
4. *για κάθε m, $[\hat{m}] = [\hat{m}]$*
5. *$deg(\hat{\phi}) = deg(\phi)$*
6. *$\hat{\hat{\phi}} = \phi$*

Απόδειξη. 1. $(\phi \circ \hat{\phi}) \circ \phi = \phi \circ (\hat{\phi} \circ \phi) = \phi \circ [m] = [m] \circ \phi \implies (\phi \circ \hat{\phi} - [m]) \circ \phi = 0 \implies \phi \circ \hat{\phi} = [m]$

2. *Επειδή ξέρουμε ότι η δυϊκή μιας ισογένιας είναι μοναδική αρκεί να δείξουμε ότι* $\hat{\phi} \circ \hat{\lambda} \circ \lambda \circ \phi = [mn]$ *που είναι προφανές.*

3. *Από το Θεώρημα 4.3.3 έχουμε ότι* $\widehat{\phi + \psi} = sum((\phi + \psi)^*) = sum(\phi^* + \psi^*) = sum(\phi^*) + sum(\psi^*) = \hat{\phi} + \hat{\psi}$.

4. *Άμεσα από το προηγούμενο ερώτημα* $\widehat{[m+1]} = [\hat{m}] + [\hat{1}]$ *και από επαγωγή προκύπτει το ζητούμενο.*

5. $m^2 = deg([m]) = deg(\hat{\phi})deg(\phi) = deg(\hat{\phi})m \implies deg(\hat{\phi}) = deg(\phi) = m$

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

4.4 Η Υποομάδα m-Στρέψης

Ορισμός 4.4.1. *Έστω ελλειπτική καμπύλη* E *τότε ως Υποομάδα* m*-Στρέψης της ορίζουμε την υποομάδα της* E*:* $E[m] = \{P \in E : [m]P = O\}$.

Είναι προφανές ότι $E[m] = ker([m])$ και άρα ξέρουμε ότι $|E[m]| = m^2$.

Πρόταση 4.4.1. *Έστω ελλειπτική καμπύλη* E *και* $m \in \mathbb{Z}^*$ *τότε:*

1. $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *αν* $char(K) \nmid m$ *ή* $char(K) = 0$.

2. $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ *ή* $\{O\}$ *αν* $char(K) = p$.

Απόδειξη. 1. *Για κάθε* $d|m$ *έχουμε* $|E[d]| = d^2$. *Επειδή η* $E[m]$ *είναι πεπερασμένη αβελιανή ομάδα μπορούμε να την γράψουμε σαν γινόμενο κυκλικών ομάδων της μορφής* $\mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$ *και κάθε* ${p_i}^{e_i}|m$ *επομένως υπάρχει δύο φορές στο γινόμενο και το ζητούμενο έπεται άμεσα.*

2. *Έχουμε* $|E[p^e]| = (deg_s(\hat{\phi}\phi))^e = (deg_s(\hat{\phi}))^e$ *και άρα αν* $\hat{\phi}$ *μη διαχωρίσιμη τότε* $|E[p^e]| = 1$ *αλλιώς* $deg(\hat{\phi}) = deg(\phi) = p$ *οπότε* $|E[p^e]| = p^e$ *και άρα* $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ *από θεώρημα Sylow.*

4.5 Το πρότυπο του Tate

Η κατασκευές αυτού του κεφαλαίου γίνονται με σκοπό τη μελέτη της υποομάδας στρέψης $E[m]$. Η ομάδα αυτή είναι είδαμε στη γενική περίπτωση ισομορφική με την $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ αλλά έχουμε πολλά περισσότερα πράγματα που μπορούμε να συμπεράνουμε για αυτήν πέραν από τις ιδιότητές της σαν αφηρημένη ομάδα. Ας εξετάσουμε για παράδειγμα την ομάδα Galois $G_{\bar{K}/K}$. Κάθε $\sigma \in G_{\bar{K}/K}$ δρα επί της $E[m]$ αφού $P \in E[m] \implies [m](P^\sigma) = ([m]P)^\sigma = O$. Έτσι παίρνουμε τελικά μια αναπαράσταση $G_{\bar{K}/K} \to Aut(E[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z})$. Ο δεύτερος ισομορφισμός προκύπτει αν διαλέξουμε μια βάση για το $E[m]$. Αυτή η αναπαράσταση όμως δεν είναι ικανοποιητική αφού είναι πάνω από ένα δακτύλιο χαρακτηριστικής m ενώ θα θέλαμε έναν δακτύλιο χαρακτηριστικής 0. Για αυτό το λόγο θα κατασκευάσουμε μια δομή παρόμοια με τους $p-$αδικούς ακεραίους.

Ορισμός 4.5.1. *Έστω ελλειπτική καμπύλη* E *και* p *πρώτος. Ορίζουμε το* ($p-$*αδικό) Tate πρότυπο ως την ομάδα* $T_p(E) = \varprojlim_n E[p^n]$. *Όπου το αντίστροφο όριο λαμβάνεται ως προς την απεικόνιση:* $E[p^{n+1}] \xrightarrow{[p]} E[p^n]$.

Το πρότυπο του Tate είναι επομένως $\mathbb{Z}_p$-πρότυπο και επειδή ο πολλαπλασιασμός επί p είναι επί σαν χάρτης έχει ακριβώς και την τοπολογία ενός προτύπου στο Z_p.

Πρόταση 4.5.1. *Το πρότυπο του Tate έχει την παρακάτω δομή ως $\mathbb{Z}_p$-πρότυπο:*

1. $T_p \cong \mathbb{Z}_p \times \mathbb{Z}_p$ *αν* $p \neq char(K)$
2. $T_p \cong \mathbb{Z}_p$ *ή* 0 *αλλιώς.*

Απόδειξη. *Άμεσα από την πρόταση 4.4.1.*

Επειδή η δράση της $G_{\bar{K}/K}$ σε κάθε $E[p^n]$ αντιμετατίθεται με τον χάρτη πολλαπλάσιασμού $[p]$ (που χρησιμοποιούμε για το αντίστροφο όριο) θα έχουμε δράση της $G_{\bar{K}/K}$ και στο $T_p(E)$. Γενικά σαν σύμβαση θα έχουμε από αυτό το σημείο ότι $p \neq char(K)$.

Παρατήρηση. *Αν διαλέξουμε μια $\mathbb{Z}_p$ βάση για το $T_p(E)$ τότε όπως και για τα σημεία στρέψης της E θα λάβουμε μια αναπαράσταση $G_{\bar{K}/K} \longmapsto GL_2(\mathbb{Z}_p)$. Όμως το $\mathbb{Z}_p$ δεν είναι σώμα. Έχουμε ωστόσο μια αναπαράσταση $G_{\bar{K}/K} \longmapsto GL_2(\mathbb{Q}_p)$ διότι προφανώς $\mathbb{Z}_p \subset \mathbb{Q}_p$ που έχει χαρακτηριστική 0.*

Γεννάται ένα εύλογο ερώτημα τώρα: Σε τι μας χρησιμεύει αυτή η κατασκευή τελικά· Η απάντηση είναι ότι θα μας επιτρέψει να αναλύσουμε τελικά τη δομή της $Hom(E_1, E_2)$. Αρχικά αρκεί να παρατηρήσουμε ότι αν έχουμε μια ισογένια $\phi : E_1 \to E_2$ τότε η ϕ περιορισμένη στην $E_1[p^n]$ θα μας δώσει έναν χάρτη $\phi : E_1[p^n] \to E_2[p^n]$. Έτσι θα έχουμε τελικά έναν χάρτη $\phi_p : T_p(E_1) \to T_p(E_2)$ και άρα έναν ομομορφισμό $Hom(E_1, E_2) \mapsto Hom(T_p(E_1), T_p(E_2)), \phi \to \phi_p$. Στη περίπτωση του $End(E)$ έχουμε μάλιστα ομομορφισμό δακτυλίων $End(E) \to End(T_p(E))$. Πριν περάσουμε στα υπόλοιπα ας αποπειραθούμε να δούμε το $Hom(E_1, E_2)$ σαν $\mathbb{Z}$-πρότυπο:

Πρόταση 4.5.2. *Η $Hom(E_1, E_2)$ είναι $\mathbb{Z}$-πρότυπο ελεύθερο στρέψης. Ακόμη ο δακτύλιος $End(E)$ έχει χαρακτηριστική 0 και δεν έχει μηδενοδιαιρέτες.*

Απόδειξη. *Έστω $[m] \circ \phi = [0]$ τότε $deg([m])deg(\phi) = 0 \implies \phi = [0]$. Το ότι το $End(E)$ έχει χαρακτηριστική 0 έπεται άμεσα ενώ αν είχε μηδενοδιαιρέτες $\phi \circ \psi = [0]$ τότε $deg(\phi)\deg(\psi) = 0 \implies \phi = 0$ ή $\psi = 0$.*

Θα διατυπώσουμε στη συνέχεια ένα αρκετά ισχυρό θεώρημα χωρίς απόδειξη:

Θεώρημα 4.5.1. *Ο χάρτης που ορίσαμε πριν $Hom(E_1, E_2) \bigotimes \mathbb{Z}_p \mapsto Hom(T_p(E_1), T_p(E_2)), \phi \to \phi_p$ είναι 1-1.*

Με αυτό το θεώρημα μπορούμε εύκολα να αποδείξουμε την ακόλουθη πρόταση:

Πρόταση 4.5.3. *Το $Hom(E_1, E_2)$ είναι $\mathbb{Z}$-πρότυπο ελεύθερο στρέψης με διάσταση το πολύ 4.*

Απόδειξη. *Επειδή το $Hom(E_1, E_2)$ είναι ελεύθερο στρέψης έχουμε ότι $rank_{\mathbb{Z}} Hom(E_1, E_2) = rank_{\mathbb{Z}_p} Hom(E_1, E_2) \bigotimes \mathbb{Z}_p$. Από το Θεώρημα 4.5.1 όμως έχουμε ότι $rank_{\mathbb{Z}_p} Hom(E_1, E_2) \bigotimes \mathbb{Z}_p \leq rank_{\mathbb{Z}_p} Hom(T_p(E_1), T_p(E_2))$, ενώ διαλέγοντας μια $\mathbb{Z}_p$ βάση για τα $T_p(E_1), T_p(E_2)$ προκύπτει ότι $Hom(T_p(E_1), T_p(E_2)) = M_2(\mathbb{Z}_p)$ (όπου $M_2(\mathbb{Z}_p)$ είναι η προσθετική ομάδα 2×2 πινάκων με συντελεστές στο $\mathbb{Z}_p$). Άρα αφού η διάσταση $rank_{\mathbb{Z}_p} Hom(T_p(E_1), T_p(E_2)) = 4$ τότε $rank_{\mathbb{Z}} Hom(E_1, E_2) \leq 4$.*

4.6 Η αντιστοίχηση του Weil

Γνωρίζουμε ότι γενικά σε κάθε ελεύθερο πρότυπο υπάρχει μια διακρίνουσα: στο $E[m]$ που είναι $\mathbb{Z}$-πρότυπο βαθμού 2 αν διαλέξουμε μια βάση T_1, T_2 θα έχουμε $det : E[m] \to \mathbb{Z}/m\mathbb{Z}, det(aT_1 + bT_2, cT_1 + dT_2) = ad - bc$ όπου φυσικά η τιμή της δεν εξαρτάται από τη βάση που επιλέξαμε. Έχουμε βέβαια το μειονέκτημα ότι η δράση της $G_{\bar{K}/K}$ δεν είναι η ίδια, δηλαδή γενικά αν $\sigma \in G_{\bar{K}/K}$ τότε $det(P^\sigma, Q^\sigma) \neq det(P, Q)^\sigma$. Μία λύση είναι να κατασκευάσουμε ένα διγραμμικό μετασχηματισμό που να έχει τη μορφή $\zeta^{det(P,Q)}$. Δε χρειάζεται βέβαια να επεκταθούμε μέχρι εκεί για να καταλάβουμε τη σημασία ενός διγραμμικού μετασχηματισμού όπως η αντιστοίχηση του Weil αφού είναι κάτι που ούτως ή άλλως δίνει πολλές πληροφορίες για τη δομή του $E[m]$ ως $\mathbb{Z}$-πρότυπο και στη σημερινή κρυπτογραφία επιτρέπει ακόμα και την αντιμετώπιση του προβλήματος του Διακριτού Λογαρίθμου σε κάποιες ελλειπτικές καμπύλες. Η γενική ιδέα πάντως είναι να ορίσουμε ένα διγραμμικό $E[m] \to \mu_m$ που να μην είναι τετριμμένος φυσικά.

Η κατασκευή θα είναι ως ακολούθως: χρησιμοποιώντας την Πρόταση 3.2.4 μπορούμε να ορίσουμε την συνάρτηση $f \in \bar{K}(E) : div(f) = m(T) - m(O), T \in E[m]$. Αν $T = [m]T'$ (υπάρχει σίγουρα τέτοιο T' διότι η $[m]$ ως ισογένια είναι επί) τότε ορίζουμε την $g \in \bar{K}(E) : div(g) = [m]^*((T) - (O))$ (μπορούμε επειδή $div(g) = \sum_{R \in E[m]}(T' + R) - (R)$ και άρα $sum(div(g)) = [m^2]T' = O$). Τότε $div(g^m) = [m]^*(m(T) - m(O))$ και $div(f \circ [m]) = [m]^* div(f) = [m]^*(m(T) - m(O)) = div(g^m)$ και άρα ως προς κάποια σταθερά $f \circ [m] = g^m$. Έστω τώρα $S \in E[m]$ και $X \in E$ τότε $g(X + S)^m = f([m](X + S)) = f([m]X) = g(X)^m$ και άρα η συνάρτηση $g(X + S)/g(X)$ είναι μια m-οστή ρίζα της μονάδας. Έτσι παίρνουμε τη ζητούμενη αντιστοίχηση $e_m(S, T) = \frac{g(X+S)}{g(X)}, X : g(X + S), g(X) \neq 0$.

Μπορούμε εναλλακτικά να παρατηρήσουμε ότι αν $g'(X) = g(X + S), S \in E[m]$ τότε $div(g') = \sum_{R \in E[m]}(T' - S + R) - (R - S) = \sum_{R \in E[m]}(T' + R) - (R) = div(g)$ αφού έχουμε άθροισμα πάνω σε όλη την $E[m]$ πάλι. Συνεπώς $g(X+S) = cg(X), \forall S \in E[m]$ και επαγωγικά προκύπτει ότι $g(X + [i]S) = c^i g(X)$ και άρα για $i = m : g(X) = g(X + [m]S) = c^m g(X)$ που σημαίνει $c^m = 1$ και άρα $g(X + S)^m = g(X)^m$. **Σε όλη την υποενότητα οι συναρτήσεις f, g όπου αναφέρονται θα είναι αυτές στην παραπάνω κατασκευή**.

Θα αποδείξουμε τώρα τις παρακάτω ιδιότητες της αντιστοίχησης του Weil που μας ενδιαφέρουν:

Θεώρημα 4.6.1. *1. (**) Διγραμμικότητα: $e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$ και $e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2)$.*

2. (**) $e_m(T, T) = 1$ και $e_m(S, T) = e_m(T, S)^{-1}$.

3. Μη εκφυλισμένη: $e_m(S, T) = 1, \forall S \in E[m] \implies T = O$.

4. Αναλλοίωτη υπό την δράση της $G_{\bar{K}/K}$: $e_m(P, Q)^\sigma = e_m(P^\sigma, Q^\sigma)$.

5. Αν $S \in E[mm']$ και $T \in E[m]$ τότε: $e_{mm'}(S, T) = e_m([m']S, T)$.

6. $\exists S, T \in E[m] : e_m(S, T) = \zeta_m$ (ή ισοδύναμα η αντιστοίχηση είναι επί στο μ_m).

Απόδειξη. *1.*

- *Για τη πρώτη περίπτωση θα έχουμε: $e_m(S_1+S_2, T) = \frac{g(X+S_1+S_2)}{g(X)} = \frac{g(X+S_1+S_2)}{g(X+S_2)} = \frac{g(X+S_2)}{g(X)} = e_m(S_1, T)e_m(S_2, T)$.*
- *Για τη δεύτερη: έστω $div(a) = (T_1 + T_2) - (T_1) - (T_2) + (O)$, τότε αν $h_i = [m]^*((T_i) - (O))$ και $div(h_{1,2}) = [m]^*((T_1+T_2)-(O)) = [m]^* div(a)+[m]^*((T_1)-(O))+[m]^*((T_2)-(O)) = div(a\circ[m])+div(h_1)+div(h_2) \implies div(h_{1,2}/a\circ[m]) = div(h_1h_2) \implies h_{1,2}/a \circ [m] = h_1h_2$ και $a \circ [m](X + S) = a \circ ([m]X + [m]S) =$*

$a\circ([m]X+O) = a\circ[m](X), \forall S \in E[m]$. *Επομένως* $e_m(S, T_1+T_2) = \frac{\frac{h_{1,2}(X+S)}{a\circ[m](X+S)}}{\frac{h_{1,2}(X)}{a\circ[m](X)}} = \frac{h_{1,2}(X+S)}{h_{1,2}(X)} = \frac{h_1(X+S)}{h_1(X)}\frac{h_2(X+S)}{h_2(X)} = e_m(S,T_1)e_m(S,T_2)$

2. *Έστω* $h(X) = g(X)g(X+T')\dots g(X+[m-1]T')$ *τότε* $div(h) = \sum_{R\in E[m]}((T'+R)-(R)+(R)-(R-T')+(R-T')-(R-2T')+\dots+(R-[m-2]T')-(R-[m-1]T')) = \sum_{R\in E[m]}(T+R-[m-1]T') - \sum_{R\in E[m]}(R-[m-1]T') = \sum_{R\in E[m]}(R-[m-1]T') - \sum_{R\in E[m]}(R-[m-1]T') = 0$ *και άρα* $h(X) = c \in \bar{K}$ *συνεπώς* $h(X+T') = h(X) \implies g(X+T')\dots g(X+[m]T') = g(X)\dots g(X+[m-1]T') \implies g(X+T) = g(X)$. *Λόγω διγραμμικότητας θα έχουμε ακόμη* $e_m(S+T, S+T) = e_m(S,S)e_m(T,T)e_m(S,T)e_m(T,S)$ *και άρα το δεύτερο ζητούμενο έπεται.*

3. *Επειδή* $g(X+S) = g(X), \forall S \in E[m]$ *θα έχουμε από το Λήμμα 4.1.2 ότι* $g \in [m]^*\bar{K}(E) \implies g = h\circ[m]$. *Όμως* $[m]^*((T)+(O)) = div(g) = div(h\circ[m]) = [m]^*div(h)$ *και επομένως* $div(h) = (T)-(O)$. *Τότε από την Πρόταση 3.2.4 έχουμε* $T = O$.

4. *Αν* $\sigma \in G_{\bar{K}/K}$ *τότε* $e_m(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma+S^\sigma)}{g(X^\sigma)} = (\frac{g(X+S)}{g(X)})^\sigma = e_m(S,T)^\sigma$.

5. *Έχουμε* $e_m m'(S,T) = \frac{g\circ[m'](X+S)}{g\circ[m'](X)} = \frac{g(Y+[m']S)}{g(Y)} = e_m([m']S, T)$.

6. *Αν ήταν απλά υποομάδα του* μ_m *τότε* $\exists d|m : e_m(S,T)^d = 1 \implies e_m(S,[d]T) = 1, \forall S \in E[m] \implies [d]T = O, \forall T \in E[m]$ *άτοπο.*

Θα δούμε τώρα τη συσχέτιση της αντιστοίχησης του Weil με τη δυϊκή ισογένια:

Πρόταση 4.6.1. *Έστω ισογένια* $\phi : E_1 \to E_2$ *τότε:* $e_m(\phi(S), T) = e_m(S, \hat{\phi}(T))$.

Απόδειξη. *Από το Θεώρημα 4.3.3 βλέπουμε ότι υπάρχει* $h \in \bar{K}(E) : div(h) = \phi^*(T) - \phi^*(O) - \hat{\phi}(T) + (O)$. *Τότε αν* $g' = \frac{g\circ\phi}{h\circ[m]}$ *θα έχουμε* $e_m(S, \hat{\phi}T) = \frac{g'(X+S)}{g'(X)} = \frac{g(\phi(X)+\phi(S))}{g(\phi(X))}\frac{h([m]X)}{h([m]X+[m]S)} = e_m(\phi(S), T)$.

Το επόμενο βήμα είναι να συνδυάσουμε την αντιστοίχησή μας με το πρότυπο του Tate και να παράγουμε έτσι μια νέα αντιστοίχηση $T_p(E)\times T_p(E) \to T_p(\mu)$.

Πρόταση 4.6.2. *Υπάρχει διγραμμική αντιστοίχηση με τις ίδιες ιδιότητες με την αντιστοίχηση του Weil,* $e : T_p(E)\times T_p(E) \to T_p(\mu)$.

Απόδειξη. *Αρκεί να δείξουμε ότι η αντιστοίχηση του Weil σέβεται το αντίστροφο όριο* $E[p^{n+1}] \xrightarrow{[p]} E[p^n]$. *Ότι δηλαδή* $e_{p^{n+1}}(P,Q)^p = e_{p^n}([p]P, [p]Q)$. *Έχουμε ότι* $e_{p^{n+1}}(P,Q)^p = e_{p^n p}(P, [p]Q)$ *και από το Θεώρημα 4.6.1* 5. *για* $m = [p^n], m' = [p]$ *τελικά* $e_{p^{n+1}}(P,Q)^p = e_{p^n}([p]P, [p]Q)$.

Έστω $\phi_p : T_p \to T_p$ όπου $\phi \in End(E)$ και έστω ότι διαλέγουμε μια βάση για το T_p και υπολογίζουμε τα $det(\phi_p)$ και $tr(\phi_p)$. Παρατηρούμε καταρχήν ότι ο πίνακας είναι 2×2 και άρα $det(\phi_p) = 1 + det(\phi_p) - det(I - \phi_p)$. Το αξιοσημείωτο είναι ότι η διακρίνουσα $det(\phi_p)$ και άρα και το ίχνος $tr(\phi_p)$ δεν εξαρτώνται από το p!

Πρόταση 4.6.3. *Έστω* $\phi_p : T_p \to T_p$ *όπου* $\phi \in End(E)$ *τότε* $det(\phi_p) = deg(\phi)$.

Απόδειξη. *Έστω* $\{u, v\}$ *μια* Z_p *βάση του* T_p. *Τότε* $\phi_p(u) = au + bv$ *και* $\phi_p(v) = cu + dv$, *επομένως* $\phi = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. *Έχουμε τότε:* $e(u,v)^{deg(\phi)} = e([deg(\phi)]u, v) = e(\hat{\phi}\phi u, v) = e(\phi u, \phi v) = e(au+bv, cu+dv) = e(u,v)^{ad}e(v,u)^{bc} = e(u,v)^{ad-bc} = e(u,v)^{det(\phi)}$ *και επειδή τα* u, v *είναι στοιχεία της βάσης και η αντιστοίχηση του Weil είναι μη εκφυλισμένη προκύπτει ότι* $det(\phi_p) = deg(\phi)$.

5 Ελλειπτικές καμπύλες πάνω από Πεπερασμένα Σώματα

5.1 Το θεώρημα του Hasse

Θα αρχίσουμε αυτό το κεφάλαιο με την ακόλουθη πολύ σημαντική πρατήρηση:

Παρατήρηση. *Έστω $E(\mathbb{F}_q), q = p^n$ με p πρώτο, τότε αν π_q ο μορφισμός Frobenius έχουμε ότι $\forall P \in E(\bar{\mathbb{F}}_q), P \in E(\mathbb{F}_q) \iff \pi_q(P) = P$. Συνεπώς $E(\mathbb{F}_q) = ker(1 - \pi_q)$.*

Ο χάρτης που πρέπει να μελετήσουμε επομένως είναι ο $1 - \pi_q$.

Πρόταση 5.1.1. *Η ισογένια $1 - \pi_q$ είναι διαχωρίσιμη.*

Απόδειξη. *Έστω ω το αναλλοίωτο διαφορικό, τότε ξέρουμε ότι $1 - \pi_q$ διαχωρίσιμος ανν $(1 - \pi_q)^*\omega \neq 0$. Όμως $[1] \circ \omega - \pi_q \circ \omega = \omega$ επειδή π_q μη-διαχωρίσιμη. Και άρα $(1 - \pi_q)^*\omega = \omega \neq 0$.*

Από το παραπάνω θεώρημα συνεπώς έχουμε ότι: $|E(\mathbb{F}_q)| = |ker(1 - \pi_q)| = deg(1 - \pi_q)$.

Το βασικότερο πρόβλημα που έχουμε στο $\mathbb{F}_q$ είναι ότι δεν έχουμε κλειστότητα και άρα πολλά από τα θεωρήματα που διατυπώσαμε για ισογένιες και άλλες δομές σε ελλειπτικές καμπύλες δεν ισχύουν. Στη συνέχεια θα προσπαθήσουμε να προσεγγίσουμε το $E(\mathbb{F}_q)$ συναρτήση του q. Για να το κάνουμε αυτό θα χρειαστούμε το θεώρημα του Hasse που χρησιμοποιεί το deg ως χάρτη $deg : Hom(E_1, E_2) \to \mathbb{Z}$. Θα ασχοληθούμε επομένως όσο χρειάζεται με θετικά ορισμένες τετραγωνικές μορφές.

Ορισμός 5.1.1. *Έστω A μια αβελιανή ομάδα (με προσθετικό συμβολισμό). Ονομάζουμε τετραγωνική μορφή μια συνάρτηση $f : A \to \mathbb{R}$ τέτοια ώστε:*

- *$f(a) = f(-a), \forall a \in A$*
- *Η αντιστοίχηση $A \times A \to \mathbb{R}, (a, b) \mapsto d(a + b) - d(a) - d(b)$ είναι διγραμμική.*

Επιπλέον αν $d(a) \geq 0, \forall a \in A$ και $d(a) = 0 \iff a = 0$ τότε η τετραγωνική μορφή ονομάζεται θετικά ορισμένη.

Θα χρησιμοποιήσουμε το ακόλουθο πόρισμα/ανισότητα για θετικά ορισμένες τετραγωνικές μορφές:

Λήμμα 5.1.1. *Έστω $d :\to \mathbb{R}^+$ μια θετικά ορισμένη τετραγωνική μορφή, τότε: $|d(\phi - \psi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}$.*

Απόδειξη. *Επειδή η $L(\phi, \psi) = d(\phi - \psi) - d(\phi) - d(\psi)$ είναι διγραμμική εξ' ορισμού, έχουμε: $0 \leq d(m\phi - n\psi) = m^2 d(\phi) + mnL(\phi, \psi) + n^2(\psi)$. Για $m = -L(\phi, \psi), n = 2d(\psi)$ προκύπτει τελικά: $0 \leq d(\psi)(4d(\psi)d(\phi) - L(\phi, \psi)^2)$ και το ζητούμενο έπεται άμεσα.*

Θα δείξουμε τώρα ότι ο βαθμός μιας ισογένιας όπως τον έχουμε ορίσει είναι μια θετικά ορισμένη τετραγωνική μορφή.

Πρόταση 5.1.2. *Ο χάρτης $deg : Hom(E_1, E_2) \to \mathbb{Z}$ είναι μια θετικά ορισμένη τετραγωνική μορφή.*

Απόδειξη. *Οι ιδιότητες είναι όλες προφανείς εκτός από την διγραμμικότητα. Έχουμε έτσι $L(\phi, \psi) = deg(\phi + \psi) - deg(\phi) - deg(\psi) = (\hat{\phi} + \hat{\psi})(\phi + \psi) - \hat{\phi}\phi - \hat{\psi}\psi = \hat{\phi}\psi + \hat{\psi}\phi$. Άρα $L(\phi_1 + \phi_2, \psi) = \hat{\phi_1}\psi + \hat{\phi_2}\psi + \hat{\psi}\phi_1 + \hat{\psi}\phi_2 = L(\phi_1, \psi) + L(\phi_2, \psi)$ και ομοίως για το ψ.*

Μπορούμε έτσι να περάσουμε στην απόδειξη του θεωρήματος του Hasse(βλ. και [12]):

Θεώρημα 5.1.1. *(Hasse) Έστω ελλειπτική καμπύλη $E/\mathbb{F}_q$, τότε $||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{g}$.*

Απόδειξη. *Από το Λήμμα 5.1.1 για $\phi = 1, \psi = \pi_q$ έχουμε: $||E(\mathbb{F}_q)| - deg(\pi_q) - deg([1])| \leq 2\sqrt{deg(\pi_q)deg([1])}$ και επειδή $deg(\pi_q) = q, deg([1]) = 1$ το ζητούμενο έπεται.*

5.2 Ισογένιες στο $\mathbb{F}_q$

Όπως είπαμε και στην προηγούμενη υποενότητα το $\mathbb{F}_q$ δεν είναι αλγεβρικά κλειστό και επομένως δε μπορούμε να χρησιμοποιήσουμε αρκετά από τα γεωμετρικά θεωρήματα που είδαμε στα προηγούμενα κεφάλαια. Ένα από αυτά είναι ότι κάθε μορφισμός μεταξύ καμπυλών (και άρα κατα συνέπεια κάθε ισογένια μεταξύ ελλειπτικών καμπυλών) είναι επί. Στην ουσία στο $\mathbb{F}_q$ άλλωστε μιλάμε απλά για πεπερασμένα σημεία με δομή ομάδας και όχι για ένα κατεξοχίν γεωμετρικό αντικείμενο. Μπορούμε όμως να χαρακτηρίσουμε πολύ πιο εύκολα τις ισογενείς καμπύλες με ένα αποτέλεσμα του Tate:

Θεώρημα 5.2.1. *(Tate) Δύο ελλειπτικές καμπύλες στο $\mathbb{F}_q$ είναι ισογενείς ανν $E_1(\mathbb{F}_q) = E_2(\mathbb{F}_q)$.*

Απόδειξη. *($\longrightarrow$)Έστω $\pi_{1,2}$ οι μορφισμοί Frobenius στις $E_{1,2}$ αντίστοιχα. Τότε αν υπάρχει $\phi : E_1 \to E_2$ στο $\mathbb{F}_q$ θα έχουμε $\phi \circ \pi_1 = \pi_2 \circ \phi$ (αφού εξ΄ ορισμού μια ισογένια είναι ομομορφισμός σωμάτων και ο μορφισμός Frobenius αντιμετατίθεται γενικά με ομομορφισμούς μεταξύ δακτυλίων ίδιας χαρακτηριστικής) $\implies \phi \circ ([1]_1 - \pi_1) = ([1]_2 - \pi_2) \circ \phi$ και άρα από τους αντίστοιχους βαθμούς: $E_1(\mathbb{F}_q)deg(\phi) = E_2(\mathbb{F}_q)\deg(\phi)$ και το ζητούμενο έπεται.*

($\longleftarrow$) βλ. [4].

Βλέπουμε έτσι ότι τις ιδιότητες μιας ελλειπτικής καμπύλης στο $\mathbb{F}_q$ καθορίζει σε μεγάλο βαθμό ο αριθμός σημείων της. Αυτό που παρατηρούμε άμεσα είναι ότι μια ισογένια σε κάποια αλγεβρική πλήρωση $\bar{K}$ του $\mathbb{F}_q$ θα υπάρχει και στο $\mathbb{F}_q$ αφού αν $\phi : E_1 \to E_2$ τότε $\pi_q \circ \phi : E_1(\mathbb{F}_q) \to E_2(\mathbb{F}_q)$. Όμως στο $\mathbb{F}_q$ έχουμε ισογένιες που δεν υπάρχουν στο $\bar{K}$ ακόμα και ισογενείς καμπύλες που δεν είναι όμως ισογενείς στο $\bar{K}$!

5.3 Οι εικασίες του Weil

Οι εικασίες του Weil διατυπώθηκαν το 1949 και αφορούν τον αριθμό των σημείων πολλαπλοτήτων στο $\mathbb{F}_q$. Θεωρούμε ότι η προβολική πολλαπλότητα V που μας ενδιαφέρει δίνεται απο ομογενή πολυώνυμα με συντελεστές στο $\mathbb{F}_q$. Θα ορίσουμε στη συνέχεια μια συνάρτηση Z από τη V.

Ορισμός 5.3.1. *Η συνάρτηση Z της $V/\mathbb{F}_q$ είναι η $Z(V/\mathbb{F}_q; T) = exp(\sum_{n=1}^{\infty} |V(\mathbb{F}_{q^n})|\frac{T^n}{n})$.*

Παρατήρηση. *Αν γνωρίζουμε την $Z(V/\mathbb{F}_q; T)$ τότε μπορούμε να βρούμε την $|V(\mathbb{F}_{q^n})| = \frac{1}{(n-1)!}\frac{d^n}{dT^n} logZ(V/\mathbb{F}_q; T)|_{T=0}$.*

Παράδειγμα 5.3.1. *Έστω $V = P^n$ δηλαδή το προβολικό επίπεδο. Έχουμε ότι εκτός της n-άδας $(0, ..., 0)$ όλες οι υπόλοιπες $q^{n(N+1)} - 1$ εμφανίζονται πολλαπλασιασμένες με κάθε στοιχείο του $\mathbb{F}_q^n/\{0\}$ και άρα έχουμε $P^n(\mathbb{F}_q^n/\{0\}) = \frac{q^{n(N+1)}-1}{q^n-1} = \sum_{i=0}^{N} q^{ni}$. Επομένως $log(Z(P^n/\mathbb{F}_q; T)) = \sum_{n=1}^{\infty}\sum_{i=0}^{N} q^{ni}\frac{T^n}{n} = \sum_{i=0}^{N}\sum_{n=1}^{\infty}\frac{(Tq^i)^n}{n} = \sum_{i=0}^{N} -log(1 - q^iT) \implies Z(P^n/\mathbb{F}_q; T) = \frac{1}{(1-T)(1-qT)...(1-q^nT)}$. Παρατηρούμε ότι $Z(P^n/\mathbb{F}_q; T) \in \mathbb{Q}[T]$, αυτή η παρατήρηση είναι και η πρώτη από τις εικασίες του Weil.*

Θεώρημα 5.3.1. *(οι εικασίες του Weil) Έστω $V/\mathbb{F}_q$ μια ομαλή προβολική πολλαπλότητα διάστασης N, τότε:*

1. *$Z(V/\mathbb{F}_q;T) \in \mathbb{Q}[T]$*
2. *(Συναρτησιακή Εξίσωση) Υπάρχει $\epsilon \in \mathbb{Z}$ γνωστό και ως χαρακτηριστική του Euler της V: $Z(V/\mathbb{F}_q;1/q^N T) = \pm q^{N\epsilon/2} T^\epsilon Z(V/\mathbb{F}_q;T)$.*
3. *(Υπόθεση του Riemann) $Z(V/\mathbb{F}_q;T) = \frac{P_0(T)...P_{2N-1}(T)}{P_1(T)...P_{2N}(T)}$ με $P_i \in \mathbb{Z}$, $P_0 = 1-T, P_{2N} = 1-q^N T$ και $P_i(T)/\mathbb{C} = \prod_{j=1}^{b_i}(1-a_{ij}T), |a_{ij}| = \sqrt{q}$.*

Στη συνέχεια θα παραθέσουμε μια απόδειξη των εικασιών του Weil στην περίπτωση ελλειπτικών καμπυλών. Θα αρχίσουμε με ένα θεώρημα που χαρακτηρίζει το $E(\mathbb{F}_{q^n})$.

Θεώρημα 5.3.2. *Έστω $a = q+1-|E(\mathbb{F}_q)|$ τότε:*

1. *Έστω $a_1, a_2 \in \mathbb{C}$ οι ρίζες του $T^2 - aT + q$ τότε $\bar{a_1} = a_2$ και $|a_1| = |a_2| = \sqrt{q}$ (παρατηρούμε την ομοιώτητα με τους συντελεστές που προβλέπει η Υπόθεση του Riemann) και $E(\mathbb{F}_{q^n}) = q^n + 1 - {a_1}^n - {a_2}^n$.*
2. *Για το μορφισμό του Frobenius ισχύει ότι ${\pi_q}^2 - a\pi_q + q = 0$.*

Απόδειξη. *Έστω $\pi_q = \phi$. Πριν περάσουμε στην απόδειξη του κάθε ερωτήματος παρατηρούμε ότι το χαρακτηριστικό πολυώνυμο του ϕ_ℓ είναι το $det(T-\phi_\ell) = T^2 - tr(\phi_\ell)T + deg(\phi_\ell) = T^2 - aT + q$.*

1. *Επειδή για κάθε $m/n \in \mathbb{Q}$ έχουμε $det(m/n - \phi_\ell) = \frac{1}{n^2} det(m - n\phi_\ell) = deg(m-n\phi_\ell) \geq 0$ θα ισχύει ότι $T^2 - aT + q \geq 0, \forall T \in \mathbb{Q} \implies T^2 - aT + q \geq 0, \forall T \in \mathbb{R}$. Άρα το πολυώνυμο $T^2 - aT + q$ έχει δύο συζηγείς μιγαδικές ή μια διπλή ρίζα και επομένως $a_1 a_2 = q$ και $|a_1| = |a_2| \implies |a_1| = |a_2| = \sqrt{q}$. Επειδή όμως $|E(\mathbb{F}_{q^n})| = deg(1-\pi_{q^n}) = deg(1-\phi^n)$ θα έχουμε $|E(\mathbb{F}_{q^n})| = det(T - {\phi_\ell}^n)$. Όμως αν $\phi_\ell = SBS^{-1}$ τότε $T - {\phi_\ell}^n = STS^{-1} - SB^nS^{-1} = S(T-B^n)S^{-1}$ και άρα $det(T - {\phi_\ell}^n) = (T - {a_1}^n)(T - {a_2}^n)$ και για $T = 1$ έχουμε τελικά: $|E(\mathbb{F}_{q^n})| = 1 - {a_1}^n - {a_2}^n + a_1 {a_2}^n = 1 - {a_1}^n - {a_2}^n + q^n$.*
2. *Έχουμε $deg(\phi^2 - a\phi + q) = det({\phi_\ell}^2 - a\phi_\ell + q) = 0$ από Caley-Hamilton για το χαρακτηριστικό πολυώνυμο της ϕ_ℓ. Άρα τελικά $\phi^2 - a\phi + q = 0$.*

Θα αποδείξουμε τώρα τις εικασίες του Weil για ελλειπτικές καμπύλες:

Θεώρημα 5.3.3. *(Εικασίες του Weil για Ελλειπτικές Καμπύλες) Έστω ελλειπτική καμπύλη E τότε: $Z(E/\mathbb{F}_q;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$ με $1 - aT + qT^2 = (1-a_1T)(1-a_2T)$ με $\bar{a_1} = a_2$ και $|a_1| = |a_2| = \sqrt{q}$. Ακόμη από αυτό έπεται ότι $Z(E/\mathbb{F}_q;1/qT) = Z(E/\mathbb{F}_q;T)$ (έχουμε δηλαδή $\epsilon = 0$).*

Απόδειξη. *Έχουμε $logZ(E/\mathbb{F}_q;T) = \sum_{n=1}^{\infty} \frac{(1+q^n - {a_1}^n - {a_2}^n)T^n}{n} = -log(1-T) + log(1-a_1T) + log(1-a_2T) - log(1-qT) = log\frac{(1-a_1T)(1-a_2T)}{(1-T)(1-qT)}$ και το ζητούμενο έπεται αφού $(1-a_1T)(1-a_2T) = T^2(1/T - a_1)(1/T - a_2) = T^2((1/T)^2 - a(1/T) + q)$ (από το προηγούμενο θεώρημα) και άρα $(1-a_1T)(1-a_2T) = 1 - aT + qT^2$.*

6 Ελλειπτικές Καμπύλες στο $\mathbb{C}$

Σε αυτή την ενότητα θα εξετάσουμε τις ελλειπτικές καμπύλες ορισμένες στο σύνολο των μιγαδικών αριθμών και θα γίνει πλέον αντιληπτός πλήρως ο λόγος που έχουν γένος 1 καθώς και η γεωμετρική τους δομή σαν επιφάνεια Riemann. Η δομή μιας ελλειπτικής καμπύλης στο $\mathbb{C}$ είναι διαισθητικά εύκολο να γίνει αντιληπτή μέσω της μελέτης ολοκληρωμάτων που σχετίζονται με το μήκος μιας έλλειψης. Η μελέτη τέτοιου είδους ολοκληρωμάτων ήταν αυτή που έστρεψε το ενδιαφέρον στις ελλειπτικές καμπύλες και για αυτόν τον λόγο ονομάστηκαν και ¨Ελλειπτικές¨.

Ελλειπτικά Ολοκληρώματα

Ορισμός 6.0.1. *Ελλειπτικά ονομάζονται τα ολοκληρώματα της μορφής* $\int_c^x R(t, \sqrt{P(t)})dt$ *όπου* R *ρητή συνάρτηση και* $P(t)$ *πολυώνυμο βαθμού 3 ή 4.*

Οι ελλειπτικές καμπύλες προκύπτουν από ελλειπτικά ολοκληρώματα της μορφής: $I(x) = \int_\infty^x \frac{dt}{\sqrt{f(t)}}$ όπου $y^2 = f(x)$ η εξίσωση Weierstrass. Αν γράψουμε αυτό το ολοκλήρωμα σε μια πιο οικεία μορφή παρατηρούμε ότι αυτό δεν είναι άλλο από το $I(P) = \int_O^P \omega$ πάνω στο $P^1(\mathbb{C})$ με την απεικόνιση $E(\mathbb{C}) \to P^1(\mathbb{C}), (x, y) \to x$. Παρατηρούμε τώρα ότι ο χάρτης $E(\mathbb{C}) \to \mathbb{C} : P \longmapsto I(P)$ δεν είναι καλά ορισμένος αλλά εξαρτάται από την καμπύλη στην οποία ολοκληρώνουμε. Αν $f(x) = (x-a)(x-b)(x-c)$ τότε η απεικόνιση $(x, y) \to x$ είναι διπλό κάλυμμα του $P^1(\mathbb{C})$ εκτός από τα σημεία με $x = a, b, c$ και το O ή ∞ στα οποία έχουμε διακλάδωση. Το πρόβλημα μας το δημιουργεί η τετραγωνική ρίζα δηλαδή που είναι διπλό κάλυμμα και για αυτό το λόγο θα ¨κόψουμε' το επίπεδο έτσι ώστε να είναι καλά ορισμένη. Ενώνοντας όμως τις ρίζες και κόβοντας πάνω στα αντίστοιχα μονοπάτια πχ το a με το ∞ και το b με το c κατασκευάζουμε δύο χωρία στα οποία η τετραγωνική ρίζα είναι μονοσήμαντα ορισμένη και άρα μπορούμε να ολοκληρώσουμε κανονικά σε αυτά. Ενώνουμε τώρα τις τομές που κάναμε μεταξύ τους και αποκτάμε ένα γνωστό σχήμα: τον τόρο!

6.1 Ελλειπτικές Συναρτήσεις και Δικτυωτά στο $\mathbb{C}$

Αφού δώσαμε μια διαισθητική προσέγγιση για τη μορφή μιας ελλειπτικής καμπύλης στο $\mathbb{C}$ και τον λόγο που ορίζεται σε έναν τόρο θα δούμε τώρα με αυστηρό τρόπο αυτή την ισοδυναμία. Σε αυτό το κεφάλαιο θα μελετήσουμε μερομορφικές συναρτήσεις στο $\mathbb{C}/\Lambda$ όπου Λ δικτυωτό δηλαδή $\Lambda = \mathbb{Z}\omega_1 \times \mathbb{Z}\omega_2$ όπου $\omega_{1,2} \in \mathbb{C}$ είναι μια βάση του δικτυωτού. Ορίζουμε επίσης ένα θεμελιώδες παραλληλόγραμμο ως $D = \{a + x_1\omega_1 + x_2\omega_2, x_{1,2} < 1 \text{ και } a \in \mathbb{C}\}$. Συμβολίζουμε ακόμη $\bar{D} = D \cup \partial D$ και $A(\Lambda)$ το εμβαδό του θεμελειώδους παραλληλογράμμου Λ. Μπορούμε τώρα να ορίσουμε τις ελλειπτικές συναρτήσεις ως εξής:

Ορισμός 6.1.1. *Ελειπτική συνάρτηση στο* Λ *ονομάζουμε μια συνάρτηση στο* $\mathbb{C}$ *τέτοια ώστε για κάθε* $z \in \mathbb{C}$ *και* $\omega \in \Lambda$*:* $f(z + \omega) = f(z)$*. Το σύνολο όλων των ελλειπτικών συναρτήσεων πάνω από ένα δικτυωτό* Λ *το συμβολίζουμε* $\mathbb{C}(\Lambda)$ *και είναι σώμα υπό τις πράξεις πρόσθεσης και πολλαπλασιασμού.*

Πρόταση 6.1.1. *Έστω ολόμορφη ελλειπτική συνάρτηση* f *επί ενός δικτυωτού* Λ*, τότε* f *σταθερή. Επίσης αν* f *δεν έχει μηδενικά τότε πάλι είναι σταθερή.*

Απόδειξη. *Αφού* f *συνεχής στο* $\bar{D}$ *που είναι συμπαγές τότε η* $|f|$ *παρουσιάζει μέγιστο στο* $\bar{D}$*. Όμως* $\sup_{z\in\bar{D}} |f| = \sup_{z\in\mathbb{C}} |f|$ *και άρα η* $|f|$ *είναι φραγμένη στο* $\mathbb{C}$ *οπότε από θεώρημα Liouville είναι σταθερή. Ομοίως αν δεν έχει μηδενικά η* f *τότε η* $1/f$ *είναι ολόμορφη άρα σταθερή.*

Παρατήρηση. *Επειδή $f(z+\omega)=f(z)$ έχουμε $f'(z+\omega)=f'(z)$ και άρα αν f είναι ελλειπτική στο Λ τότε και f' ελλειπτική στο Λ.*

Πρόταση 6.1.2. *Μια μη σταθερή ελλειπτική συνάρτηση έχει τουλάχιστον δύο πόλους(προσμετρώντας την πολλαπλότητα).*

Απόδειξη. *Έχουμε ότι: $\int_{\partial D} f(z)dz = 2\pi i \sum_{w\in D} Res(w)$ και επειδή η f είναι περιοδική έχουμε ότι $\int_{\partial D_1} f(z)dz = -\int_{\partial D_2} f(z)dz$ όπου $\partial D_1, \partial D_2$ συμμετρικές πλευρές του θεμελιώδους παραλληλογράμμου D. Επομένως $\int_{\partial D} f(z)dz = 0$ και άρα $\sum_{w\in D} Res_f(w) = 0$, αν έχουμε ακριβώς έναν πόλο z_0 επομένως τότε πρέπει $Res(z_0)=0$ και άρα η συνάρτηση μας είναι ολόμορφη ελλειπτική και επομένως από την Πρόταση 6.1.1 σταθερή.*

Ορισμός 6.1.2. *Ορίζουμε και στο $\mathbb{C}/\Lambda$ τους* **διαιρέτες** *$Div(\mathbb{C}/\Lambda)$ ως αθροίσματα της μορφής $\sum_{w\in\mathbb{C}/\Lambda} n_w(w)$, όπου $n_w \neq 0$ για πεπερασμένα w. Κατά αντιστοιχία ορίζουμε σε ελλειπτικές συναρτήσεις τους διαιρέτες $div(f) = \sum_{w\in\mathbb{C}/\Lambda} ord_w(f)(w)$. Ο βαθμός ενός διαιρέτη είναι κανονικά ο άθροισμα των συντελεστών.*

Κατασκευή Ελλειπτικών Συναρτήσεων

Παρατηρούμε ότι αφού θέλουμε μια συνάρτηση με $f:\mathbb{C}\to\mathbb{C}/\Lambda$ θα Όπως είδαμε πριν στον τύπο του Velu είναι σύνηθες όταν θέλουμε να κατασκευάσουμε μια συνάρτηση/μορφισμό με συγκεκριμένο πυρήνα G να αθροίζουμε συναρτήσεις της μορφής: $g(P-Q)-g(Q)$ όπου $Q\in G$. Καταλήγουμε συνεπώς στη μορφή: $p(z;\Lambda)=\sum_{\omega\in\Lambda} g(z-\omega)-g(\omega)$ Επειδή η συνάρτησή μας πρέπει από την Πρόταση 6.1.2 να έχει τουλάχιστον δύο πόλους καταλήγουμε ότι η g έχει σίγουρα πόλο και άρα εξετάζουμε τις πιο απλές περιπτώσεις $g(z)=1/z^n$. Αν $n=1$ τότε έχουμε προβλήματα σύγκλισης αφού αθροίζουμε πάνω σε άπειρο δικτυωτό Λ, άρα βάζουμε $n=2$ και παίρνουμε την **συνάρτηση** $\wp$ **Weierstrass**: $\wp(z;\Lambda)=\frac{1}{z^2}+\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}$.

Ορισμός 6.1.3. *Για ένα δικτυωτό Λ ορίζουμε τη συνάρτηση Weierstrass ως:*

$$\wp(z;\Lambda)=\frac{1}{z^2}+\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2} \tag{6}$$

και την σειρά Eisenstein βάρους $2k$:

$$G_{2k}(\Lambda)=\sum_{\omega\in\Lambda,\omega\neq 0}\omega^{-2k} \tag{7}$$

Θεώρημα 6.1.1. *1. (**) Η σειρά Eisenstein συγκλίνει απόλυτα για κάθε $k>1$.*

2. Η σειρά που ορίζει την συνάρτηση Weierstrass συγκλίνει απόλυτα και ομοιόμορφα σε κάθε συμπαγές υποσύνολο του $\mathbb{C}/\Lambda$.

3. Η συνάρτηση $\wp(z;\Lambda)$ είναι άρτια και ελλειπτική.

Απόδειξη. *1. (**) $|G_{2k}(\omega)|\leq\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{|\omega|^{2k}}\leq\sum_{N\in\mathbb{N}}\frac{|A_N|}{N^{2k}}$ όπου $A_N=\{\omega\in\Lambda : N\leq|\omega|<N+1\}$. Όμως υπάρχει $x_k\in\mathbb{N}: lim_{k\to\infty}x_kA(\Lambda)-\pi(kN)^2=0$ αφού αυξάνοντας επαρκώς το k ή ισοδύναμα εκλεπταίνοντας διαρκώς το Λ κατασκευάζοντας το $\frac{1}{k}\Lambda$ μπορούμε να προσεγγίσουμε το εμβαδόν του κύκλου κατά οποιοδήποτε $\epsilon>0$ χρησιμοποιώντας x_k παραλληλόγραμμα. Από το παραπάνω όριο προκύπτει ότι: $x_kA(\Lambda)=\pi N^2k^2+\epsilon_n$ με $\epsilon_n\to 0$ και άρα $x_n\approx\Theta(n^2)$ για αρκετά μεγάλο n. Αν $B_N=\{\omega\in\Lambda:|\omega|<N\}$ τότε $x_N\leq B_N\leq ux_N$ (έστω $\delta=\sqrt{2}|\omega_1+\omega_2|$ και $\phi_1=(\widehat{2\omega_1,\omega_2})$, $\phi_2=(\widehat{\omega_1,2\omega_2})$ τότε*

$u' = max\{\delta/\cos(\phi_1), \delta/\cos(\phi_2)\}$ *και συνεπώς με* $u = u'^2$ *αντίγραφα του αρχικού παραλληλογράμμου καλύπτουμε πλήρως το εσωτερικό του κύκλου) και άρα* $B_N = \Theta(N^2)$. *Τέλος* $A_N = B_{N+1} - B_N \approx c(N+1)^2 + O(N) - cN^2 - O(N) = c(2N+1) + O(N) = O(N)$ *και άρα* $A_N < cN$ *για κάποιο* $c > 0$ *επομένως* $\sum_{N\in\mathbb{N}} \frac{|A_N|}{N^{2k}} < c\sum_{N\in\mathbb{N}} \frac{1}{N^{2k-1}}$ *και το ζητούμενο έπεται άμεσα.*

2. *Αν* $|\omega| > 2|z|$ *τότε* $\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{z(2\omega - w)}{\omega^2(z-\omega)^2} \leq \frac{|z|2|\omega|+|z|}{|\omega|^2(|\omega|-|z|)^2} \leq \frac{10|z|}{|\omega|^2}$.

3. *Παρατηρούμε ότι* $\wp(-z;\Lambda) = \frac{1}{z^2} + \sum_{-\omega\in\Lambda,\omega\neq 0} \frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} = \wp(z;\Lambda)$ *άρα είναι άρτια. Επειδή έχουμε ομοιόμορφη σύγκλιση:* $\wp'(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}$ *που είναι ελλειπτική συνάρτηση και άρα* $\wp'(z+\omega) = \wp'(z)$. *Επομένως* $\wp(z+\omega) = \wp(z) + c(\omega)$ *και για* $z = -\omega/2$ *έχουμε:* $\wp(\omega/2) = \wp(-\omega/2) + c(\omega) \implies c(\omega) = 0$.

Παρατήρηση. *Επειδή* $\wp$ *άρτια προφανώς* $\wp'$ *περιττή συνάρτηση.*

Θα αποδείξουμε στη συνέχεια ότι όλες οι ελλειπτικές συναρτήσεις είναι ρητή συνάρτηση των $\wp(z)$ και $\wp'(z)$. Για τον σκοπό αυτό θα χρειαστούμε το ακόλουθο λήμμα:

Λήμμα 6.1.1. *Αν* f *ελλειπτική συνάρτηση στο* Λ *τότε* $\sum_{w\in\mathbb{C}/\Lambda} ord_w f = 0$.

Απόδειξη. *Επειδή* $f(z) = f(z+m\omega_1+n\omega_2)$ *έχουμε* $f'(z) = f'(z+m\omega_1+n\omega_2)$ *και επομένως* $f'(z)/f(z) = f'(z+m\omega_1+n\omega_2)/f(z+m\omega_1+n\omega_2)$ *που σημαίνει ότι* f'/f *ελλειπτική με βάση το* Λ. *Όμως* $\sum_{w\in\mathbb{C}/\Lambda} ord_w f = \sum_{w\in D} Res_{f'/f}(w) = 0$.

Παρατήρηση. *Το ότι* $Res_{f'/f}(z_0) = ord_{z_0} f = m$ *προκύπτει άμεσα αν γράψουμε* $f(z) = g(z)(z-z_0)^m$ *οπότε* $f'/f = \frac{g'(z)(z-z_0)^m + mg(z)(z-z_0)^{m-1}}{g(z)(z-z_0)^m} = \frac{g'(z)}{g(z)} + \frac{m}{z-z_0}$ *και προφανώς* $Res_{g'/g}(z_0) = 0$.

Θεώρημα 6.1.2. *Έστω* $f \in \mathbb{C}(\Lambda)$ *τότε* $f(z) = \mathbb{C}(\wp(z), \wp'(z))$.

Απόδειξη. *Επειδή* $f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2}$ *δηλαδή άθροισμά μιας άρτιας και μιας περιττής ελλειπτικής συνάρτησης τότε αρκεί να δείξουμε το θεώρημα για άρτιες συναρτήσεις αφού για περιττές ισχύει* $\wp'(z)g(z) = \wp'(-z)g(-z)$ *και άρα* $\wp'(z)g(z)$ *άρτια. Έστω* f *άρτια ελλειπτική συνάρτηση. Ας θεωρήσουμε για κάθε θεμελιώδες παραλληλόγραμμο* D *την διαμέριση του στο άνω και κάτω μισό* H. *Λόγω αρτιότητας έχουμε ότι* $ord_w f = ord_{-w} f$ *και αν πάρουμε το ανάπτυγμα Taylor έχουμε ότι αν* $2w \in \Lambda$ *τότε* $f(z) = b_m(z-w)^m + ... = f(-z+2w)$ *και άρα* $m = ord_w f$ *άρτιος. Άρα για κάθε ρίζα στο* H *μπορούμε να αντιστοιχίζουμε ακριβώς μία στο* D/H *ακόμα και αν* $2w \in \Lambda$. *Άρα* $div(f) = \sum_{w\in H} n_w((w) + (-w))$. *Εξετάζοντας τώρα τις ρίζες της* $\wp(z) - \wp(w)$ *έχουμε είτε διπλή ρίζα το* $w = -w$ $mod\Lambda$ *αν* $2w \in \Lambda$ *είτε δύο ρίζες* $z = \pm w$. *Κατασκευάζουμε τώρα την* $g(z) = \prod_{w\in H/\{0\}} (\wp(z) - \wp(w))^{n_w}$ *και παρατηρούμε ότι* $div(g) = div(f) + k(0)$ *αφού* $div(\wp(z) - \wp(w)) = (w) + (-w) - 2(0)$. *Όμως από Λήμμα 6.1.1 έχουμε ότι* $k = ord_0 g = ord_0 f = \sum_{w\in H/\{0\}} n_w((w) + (-w))$. *Άρα* f/g *ολόμορφη ελλειπτική συνάρτηση και επομένως σταθερή, οπότε* $f = cg$.

6.2 Ελλειπτικές Καμπύλες ως Δικτυωτά

Η συσχέτιση των ελλειπτικών συναρτήσεων και των δικτυωτών με τις ελλειπτικές καμπύλες αρχίζει να γίνεται εμφανής με το ακόλουθο θεώρημα:

Θεώρημα 6.2.1. *Για την συνάρτηση Weierstrass ισχύει ότι:*

$$\wp'(z)^2 = 4\wp^3(z) - 60G_4\wp(z) - 140G_6 \tag{8}$$

Απόδειξη. *Έστω* $f(z) = \wp'(z)^2 - 4\wp^3(z) + 60G_4\wp(z) + 140G_6$. *Τότε* $f(0) = 0$ *και* f *ελλειπτική στο* Λ. *Επίσης από σύγκριση των δυναμοσειρών του κάθε όρου προκύπτει ότι η* f *είναι ολόμορφη και επομένως σταθερή. Το ζητούμενο έπεται άμεσα.*

Από το παραπάνω θεώρημα έχουμε σαν επακόλουθο ότι κάθε δικτυωτό Λ αντιστοιχεί σε μια ελλειπτική καμπύλη E_Λ. Μπορούμε έτσι να ορίσουμε για ένα δικτυωτό Λ την αναλλοίωτή του $j(\Lambda) = j(E_\Lambda)$ και $\Delta(\Lambda) = \Delta(E_\Lambda)$. Ισχύει και το αντίστροφο ότι δηλαδή σε κάθε ελλειπτική καμπύλη με αναλλοίωτη $j(E)$ αντιστοιχεί ένα δικτυωτό που ορίζει μια εξίσωση σαν την (8) με αναλλοίωτη $j(\Lambda) = j(E)$. Αυτό είναι το λεγόμενο Uniformization Theorem και θα το δούμε παρακάτω. Φυσικά για να δείξουμε ότι η καμπύλη είναι όντως ελλειπτική θα πρέπει και να ισχύει ότι $\Delta(\Lambda) \neq 0$.

Πρόταση 6.2.1. *Η* $\wp'(z)^2 = 4\wp^3(z) - 60G_4\wp(z) - 140G_6 = 0$ *έχει* 3 *διαφορετικές ρίζες και άρα* $\Delta(\Lambda) \neq 0$.

Απόδειξη. *Έστω* $\omega_3 = (\omega_1+\omega_2)/2$. *Επειδή* $\wp'$ *περιττή θα έχουμε* $\wp'(\omega_i/2) = -\wp'(-\omega_i/2) = -\wp'(\omega_i/2)$ *και η* $\wp'$ *είναι τάξης* 3 *οπότε* $\wp'(z) = 0 \implies z = \omega_i/2$, $i = 1, 2, 3$. *Επειδη η* $\wp(z) - \wp(\omega_i/2)$ *έχει τάξη 2, οι ρίζες της είναι ακριβώς τα* $\omega_i/2, -\omega_i/2$. *Άρα* $\wp(\omega_i) = \wp(\omega_j) \iff i = j$.

Πρόταση 6.2.2. *Ο χάρτης* $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}), z \longrightarrow (\wp(z), \wp'(z), 1)$ *είναι ισομορφισμός επιφανιών Riemann και ομομορφισμός ομάδων.*

Απόδειξη. *Ο χάρτης είναι επί αφού για κάθε* $x \in E(\mathbb{C})$ *η συνάρτηση* $\wp(z) - x$ *είναι ελλειπτική (μη σταθερή) και άρα έχει μηδενικό από την Πρόταση 6.1.1. Αν* $\wp(z_0) = x$ *τότε* $\wp'(z_0) = y$ *ή* $-\wp'(z_0) = \wp'(-z_0) = y$. *Το 1-1 είναι επίσης προφανές αφού η* $\wp(z) - \wp(a) = 0$ *είναι τάξεως* 2 *και επομένως έχει ρίζες ακριβώς τις* $a, -a$ *ή την* a *αν* $2a \in \Lambda$. *Ότι είναι ομομορφισμός προκύπτει επειδή για κάθε* $z_{1,2}$ *αν* $div(f) = (z_1+z_2)-(z_1)-(z_2)+(0)$ *με* $f \in \mathbb{C}/\Lambda$ *υπάρχει* F *ρητή τέτοια ώστε* $f(z) = F(\wp(z), \wp'(z))$. *Τότε* $div(F) = (\phi(z_1 + z_2)) - (\phi(z_1)) - (\phi(z_2)) + (\phi(0))$ *και επομένως* $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$.

Βλέποντας αυτή την αντιστοιχία με το $\mathbb{C}/\Lambda$ γεννάται το ερώτημα τι μορφή έχουν τα υπόλοιπα θεωρήματα που διατυπώσαμε και οι δομές που ανακαλύψαμε στο $\mathbb{C}$. Πολλά από αυτά μπορούν πράγματι να γίνουν διαισθητικά αντιληπτά πολύ πιο εύκολα στους μιγαδικούς. Αυτό συμβαίνει για παράδειγμα με τις ισογένιες μεταξύ δύο ελλειπτικών καμπυλών που έχουν εξαιρετικά απλή μορφή σε αυτά τα πλαίσια. Συγκεκριμένα έστω $a \in \mathbb{C} : a\Lambda_1 \subset \Lambda_2$, τότε ο χάρτης $\phi_a : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ με $\phi_a(z) = az$
$mod\Lambda_2$ είναι καλώς ορισμένος και ολόμορφος ομομορφισμός.

Λήμμα 6.2.1. *Αν* $f : \mathbb{C} \to A$ *συνεχής συνάρτηση με* A *διακριτό σύνολο, τότε* $f = c \in \mathbb{C}$.

Απόδειξη. *Επειδή* f *συνεχής τότε το* $A = f(\mathbb{C})$ *έχει σημείο συσσώρευσης που όμως είναι άτοπο από τον ορισμό του διακριτού συνόλου.*

Πρόταση 6.2.3. *Για κάθε* $a \in \mathbb{C} : a\Lambda_1 \subset \Lambda_2$ *υπάρχει ακριβώς ένας ολόμορφος χάρτης* ϕ_a *με* $\phi_a(0) = 0$. *Όλοι ακόμη οι ολόμορφοι χάρτες* $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ *με* $\phi(0) = 0$ *είναι της μορφής* $\phi(z) = az$ *με* $a\Lambda_1 \subset \Lambda_2$.

Απόδειξη. *Η αντιστοιχία είναι αμφιμονοσήμαντη επειδή* $\phi_a = \phi_b \implies (a - b)z = 0$
$mod\Lambda_2, \forall z \in \mathbb{C}$. *Όμως τότε έχουμε ολόμορφο χάρτη* $\mathbb{C} \to \Lambda_2$ *που είναι διακριτό σύνολο και άρα από το Λήμμα 6.2.1 ο χάρτης είναι ο σταθερός δηλαδή* $a = b$. *Ακόμη αν θεωρήσουμε τις συναρτήσεις προβολής* $p_i : \mathbb{C} \to \mathbb{C}/\Lambda_i, i = 1, 2$, *τότε βλέπουμε ότι το* $\mathbb{C}$ *είναι ένας χώρος κάλυψης (covering space) του* $\mathbb{C}/\Lambda$ *και άρα μπορούμε να ορίσουμε για κάθε ολόμορφο χάρτη*

$\phi_a : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ *την ύψωσή (lifting) του* $f : \mathbb{C} \to \mathbb{C}$. *Ο χάρτης* $f = {p_2}^{-1} \circ \phi \circ p_1$ *είναι ολόμορφος ως σύνθεση ολόμορφων συναρτήσεων (οι συναρτήσεις προβολής είναι τοπικά διολομορφικές) και προφανώς* $\forall \omega \in \Lambda_1$, $p_2 \circ f(z) - p_2 \circ f(z+\omega) = \phi \circ p_1(z) - \phi \circ p_1(z+\omega) = 0 \implies f(z+\omega) = f(z) \mod \Lambda_2$. *Έτσι έχουμε πάλι από το Λήμμα 6.2.1 ότι η* $f(z+\omega) - f(z)$ *είναι συνεχής συνάρτηση* $\mathbb{C} \to \Lambda_2$ *και άρα σταθερή. Επειδή ακόμη* $f'(z+\omega) = f'(z)$ *είναι ολόμορφη και ελλειπτική στο* Λ_1, $f'(z) = a \implies f(z) = az + b$ *και αφού* $f(0) = 0$ *έχουμε τελικά:* $f(z) = az$ *και* $f(\Lambda_1) \subset \Lambda_2 \implies a\Lambda_1 \subset \Lambda_2$.

Θεώρημα 6.2.2. *Έστω ελλειπτικές καμπύλες* E_1, E_2 *με αντίστοιχα δικτυωτά τα* Λ_1, Λ_2. *Υπάρχει 1-1 και επί αντιστοιχία μεταξύ των ισογενιών* $E_1 \to E_2$ *και των ολόμορφων χαρτών* $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ *με* $\phi(0) = 0$.

Απόδειξη. *Παρατηρούμε καταρχήν ότι κάθε ισογένια είναι ρητή συνάρτηση ως μορφισμός και κατ΄ επέκταση ο αντίστοιχος χάρτης μεταξύ των μιγαδικών τόρων θα είναι ολόμορφος και 1-1. Το αντίστροφο έπεται άμεσα από την ακόλουθη παρατήρηση:* $\phi_a : (\wp(z, \Lambda_1), \wp'(z, \Lambda_1), 1) \longrightarrow (\wp(az, \Lambda_2), \wp'(az, \Lambda_2), 1)$ *και* $(\wp(az, \Lambda_2), \wp'(az, \Lambda_2), 1) = (\wp(az + a\omega, \Lambda_2), \wp'(az + a\omega, \Lambda_2), 1)$, $\forall \omega \in \Lambda_1$. *Άρα* $\wp(az, \Lambda_2), \wp'(az, \Lambda_2) \in \mathbb{C}(\Lambda_1)$ *και επομένως μπορούν να γραφτούν ως ρητές συναρτήσεις των* $\wp(z, \Lambda_1), \wp'(z, \Lambda_1)$. *Αυτές οι ρητές συναρτήσεις μας δίνουν ακριβώς την ζητούμενη ισογένια.*

Παρακάτω βλέπουμε ότι στα δικτυωτά η $j-$αναλλοίωτη παίζει τον ίδιο ρόλο όπως στο $E(C)$, διακρίνει δηλαδή τα δικτυωτά που δίνουν ισομορφικές ελλειπτικές καμπύλες.

Πρόταση 6.2.4. *Ισχύει ότι* $j(\Lambda_1) = j(\Lambda_2)$ *ανν* $a\Lambda_1 = \Lambda_2$.

Απόδειξη. *Αν* $a\Lambda_1 = \Lambda_2$ *τότε από τους τύπους των* $G_4(\Lambda), G_6(\Lambda)$ *παρατηρούμε ότι* $G_4(a\Lambda) = a^{-4}G_4(\Lambda)$ *και* $G_6(a\Lambda) = a^{-6}G_6(\Lambda)$ *και άρα* $j(a\Lambda) = j(\Lambda)$ *οπότε* $j(a\Lambda_1) = j(\Lambda_2) = j(\Lambda_1)$. *Αντίστροφα αν* $j(\Lambda_1) = j(\Lambda_2)$ *τότε από τις αντίστοιχες ισομορφικές ελλειπτικές καμπύλες:* $y^2 = 4x^3 - 60G_4(\Lambda_1)x - 140G_6(\Lambda_1)$, $y^2 = 4x^3 - 60G_4(\Lambda_2)x - 140G_6(\Lambda_2)$ *έχουμε ότι* $a^{-4}G_4(\Lambda_1) = G_4(a\Lambda_1) = G_4(\Lambda_2)$ *και* $a^{-6}G_6(\Lambda_1) = G_6(a\Lambda_1) = G_6(\Lambda_2)$. *Με απλή παραγώγιση έχουμε ότι* $\wp"(z) = \wp(z)^2 - 30G_4$ *και θέτοντας* $a_n = G_{2n+2}$ *προκύπτει με σύγκριση τω συντελεστών του όρου* z^{2n} *ότι* $a_n = f(n)\sum_{i=1}^{n-1} a_i a_{n-i}$. *Άρα η* $\wp(z)$ *καθορίζεται μοναδικά από τα* G_3, G_4 *και επομένως* $\wp(z, a\Lambda_1) = \wp(z, \Lambda_2) \implies a\Lambda_1 = \Lambda_2$.

Παρατήρηση. *Δύο ελλειπτικές καμπύλες* E_1, E_2 *είναι ισομορφικές ανν υπάρχει* $a \in \mathbb{C}$: $a\Lambda_1 = \Lambda_2$.

Ας εξετάσουμε τώρα πάλι τον πυρήνα μιας ισογένιας, αυτή τη φορά στο $\mathbb{C}$. Ο πυρήνας μιας ισογένιας ϕ μεταξύ δύο ελλειπτικών καμπυλών με αντίστοιχα δικτυωτά τα Λ_1, Λ_2 είναι $ker(\phi) = \{z \in \mathbb{C}/\Lambda_1 : az \in \Lambda_2\}$.

Πρόταση 6.2.5. *Στο* $\mathbb{C}$ *ισχύει ότι* $E[m] = \{\frac{i}{m}\omega_1 + \frac{j}{m}\omega_2, i, j \in \{0, \ldots, n-1\}\}$.

Απόδειξη. *Παρατηρούμε ότι για κάθε σημείο* $z_0 \in \{\frac{i}{m}\omega_1 + \frac{j}{m}\omega_2, i, j \in \{0, \ldots, n-1\}\} = A$ *έχουμε* $mz_0 = i\omega_1 + j\omega_2 \in \Lambda$ *και άρα* $A \supseteq E[m]$. *Επειδή όμως* $E[m] = |A|$ *έχουμε ότι* $E[m] = A$.

Πιο γενικά αν έχουμε μια ισογένια $\phi_a = az$ μεταξύ των Λ_1, Λ_2 με $a\Lambda_1 \subset \Lambda_2$ τότε ξέρουμε ότι αν $\{\omega_1, \omega_2\}$ μια βάση του Λ_2 θα έχουμε μια βάση του $a\Lambda_1$, $\{n_1\omega_1, n_2\omega_2\}$ και άρα μια βάση του Λ_1, $\{\frac{n_1}{a}\omega_1, \frac{n_2}{a}\omega_2\}$. Επειδή η βάση του $ker(\phi_a)$ είναι $\{\omega_1/a, \omega_2/a\}$ έχουμε ότι $ker(\phi_a) = \{\frac{i}{a}\omega_1, \frac{j}{a}\omega_2\}$ με $i \in \{0, .., n_1 - 1\}$ και $j \in \{0, .., n_2 - 1\}$. Άρα τελικά έχουμε την ακόλουθη παρατήρηση:

Παρατήρηση. *Αν $\phi_a = az$ ισογένια μεταξύ των Λ_1, Λ_2, με $\{\omega_1, \omega_2\}$ μια βάση του Λ_2 και $\{n_1\omega_1, n_2\omega_2\}$ μια βάση του $a\Lambda_1$ τότε $|ker(\phi_a)| = deg(\phi_a) = n_1n_2$.*

Με την παραπάνω παρατήρηση γίνεται σαφές ότι για να κατασκευάσουμε τη δυϊκή ισογένια της ϕ_a πρέπει να βρούμε μια ισογένια $\hat{\phi_a} : \hat{\phi_a} \circ \phi_a = [n_1n_2]$. Αυτή είναι η $\hat{\phi_a}(z) = \frac{n_1n_2}{a}z$.

Πρόταση 6.2.6. *(**) Με συμβολισμό όπως πριν έχουμε ότι η δυϊκή ισογένια της ϕ_a είναι η $\hat{\phi_a}(z) = \frac{n_1n_2}{a}z$.*

Απόδειξη. *Επειδή η βάση του $a\Lambda_1$ είναι $\{n_1\omega_1, n_2\omega_2\}$ έχουμε ότι $n_1n_2\Lambda_2 \subset a\Lambda_1 \implies \frac{n_1n_2}{a}\Lambda_2 \subset \Lambda_1$ και άρα έχουμε μια αντίστροφη ισογένια $\hat{\phi_a} : \Lambda_2 \to \Lambda_1$. Προφανώς $\hat{\phi_a} \circ \phi_a(z) = n_1n_2z$.*

Uniformization Theorem

Το **Uniformization Theorem** είναι η αντίστροφη κατεύθυνση του Θεωρήματος 6.2.1 που διατυπώσαμε στην προηγούμενη υποενότητα. Μας δείχνει ουσιαστικά την αντίστροφη αντιστοιχία ότι δηλαδή κάθε ελλειπτική καμπύλη E αντιστοιχεί μέσω των χαρτών που ορίζει η συνάρτηση Weierstrass σε ένα δικτυωτό Λ_E. Για να το δείξουμε αυτό θα ασχοληθούμε με ιδιότητες της $j(\Lambda)$ ως συνάρτηση από το άνω μιγαδικό ημιεπίπεδο $\mathbb{H}$ στο $\mathbb{C}$. Θα δείξουμε συγκεκριμένα ότι έχουμε έναν $1-1$ και επί χάρτη από το $\mathbb{H} \subset F \to \mathbb{C}$.

Ορισμός 6.2.1. *Ορίζουμε $j(\tau) = j([1, \tau])$ όπου $[1, \tau] = \Lambda_\tau$ το δικτυωτό με βάση τα $\tau, 1$ και $\tau \in \mathbb{H}$.*

Παρατήρηση. *Από την πρόταση 6.2.4 έχουμε ότι $j(\tau) = j(\tau') \iff \lambda[1, \tau] = [1, tau'] \iff \tau' = a\lambda\tau + b\lambda, 1 = c\lambda\tau + d\lambda \implies \tau' = \gamma\tau, \gamma \in SL_2(\mathbb{Z})$. Το ότι $\gamma \in SL_2(\mathbb{Z})$ προκύπτει επειδή $\tau' = \gamma\gamma'\tau'$ και $\tau \in \mathbb{H}$.*

Ορισμός 6.2.2. *Ορίζουμε το χωρίο $F = \{\tau \in \mathbb{H} : \Re(\tau) \in [-1/2, 1/2) \ \ \& \ \ |\tau| \geq 1 : \Re(\tau) > 0 \implies |\tau| > 1\}$.*

Για να μην πλατιάζουμε θα διατυπώσουμε την επόμενη πρόταση χωρίς απόδειξη και θα την χρησιμοποιήσουμε για να σκιαγραφήσουμε μια απόδειξη για το τελικό μας θεώρημα:

Πρόταση 6.2.7. *Για κάθε $\tau \in \mathbb{H}, \exists!\tau' \in F : \tau' = \gamma\tau, \gamma \in \Gamma$. Δηλαδή το F είναι ένα θεμελειώδες πεδίο ορισμού της $\mathbb{H}/\Gamma$.*

Απόδειξη. *βλ. Λήμμα 16.10 [5]*

Θεώρημα 6.2.3. *Η συνάρτηση $j : F \to \mathbb{C}$ είναι $1-1$ και επί.*

Απόδειξη. *Το $1-1$ έπεται από τη μοναδικότητα στην παραπάνω πρόταση. Έχουμε ότι $G_4(\tau) = 60(2\sum_{m=1}^{\infty} m^{-4} + \sum_{m,n\in\mathbb{Z},n\neq 0} \frac{1}{(m+n\tau)^4})$. Άρα $\lim_{\Im(\tau)\to\infty} G_4(\tau) = 120\zeta(4) = 4\pi^4/3$ και ομοίως $\lim_{\Im(\tau)\to\infty} G_6(\tau) = 280\zeta(6) = 8\pi^6/27$. Τότε όμως $\lim_{\Im(\tau)\to\infty} \Delta(\tau) = 0$ και $j(\tau) = G_4(\tau)^3/\Delta(\tau)$, επομένως $\lim_{\Im(\tau)\to\infty} j(\tau) = \infty$. Επειδή η j είναι μη σταθερή ολόμορφη συνάρτηση, το Θεώρημα Ανοικτής Απεικονήσεως μας λέει ότι η $j(\mathbb{H})$ είναι ένα ανοικτό υποσύνολο του $\mathbb{C}$. Έστω τώρα $j(\tau_i)$ μια συγκλίνουσα ακολουθία ($\lim_{i\to\infty} j(\tau_i) = u$) στο $j(\mathbb{H})$. Επειδή η j είναι Γ-αναλλοίωτη μπορούμε να θέσουμε $j(\tau_i') = j(\tau_i)$, όπου $\tau_i' \in F$. Τότε επειδή $\lim_{\Im(\tau)\to\infty} j(\tau) = \infty$ αλλά η ακολουθία συγκλίνει αυτό σημαίνει ότι η ακολουθία $\Im(\tau_i)$ είναι φραγμένη από κάποιο B και άρα όλα τα τ_i ανήκουν στο παραλληλόγραμμο $A = \{\tau : \Re(\tau) \in [-1/2, 1/2], \Im(\tau) \in$*

$[1/2, B]\}$. *Το* A *είναι συμπαγές σύνολο και άρα υπάρχει συγκλίνουσα υπακολουθία στο* $A \subset \mathbb{H}$: *με* $\lim_{i\to\infty} \tau_{j_i} = \tau$. *Λόγω συνέχειας όμως* $j(\tau) = u$ *και άρα το* $j(\mathbb{H})$ *περιέχει όλα του τα σημεία συσσώρευσης και επομένως είναι κλείστο. Επειδή το* $j(\mathbb{H})$ *είναι ανοιχτό και κλειστό μη κενό υποσύνολο του* $\mathbb{C}$ *θα έχουμε τελικά ότι:* $j(\mathbb{H}) = \mathbb{C}$.

Το θεώρημα Uniformization έπεται τώρα άμεσα αφού για κάθε ελλειπτική καμπύλη E αρκεί να διαλέξουμε δικτυωτό $\Lambda : j(\Lambda) = j(E)$ που υπάρχει από το παραπάνω θεώρημα.

7 Ελλειπτικές Καμπύλες στο $\mathbb{Q}$

Ένα πρόβλημα που από την αρχαιότητα γοήτευε τους μαθηματικούς ήταν η επίλυση εξισώσεων πάνω στο $\mathbb{Z}$ και το $\mathbb{Q}$. Ήδη από την εποχή του Διόφαντου έχουμε παραδείγματα από τέτοια προβλήματα όπως το ακόλουθο: δεδομένου ενός $n \in \mathbb{Z} : n = a^3 - b^3, a, b \in \mathbb{Z}$ να βρεθούν $u, v \in \mathbb{Q} : n = u^3 + v^3$. Από τέτοιου είδους παραδείγματα ξεκίνησε άλλωστε η γνωστή μας κατασκευή που δίνει δομή ομάδας σε μια ελλειπτική καμπύλη. Στο συγκεκριμένο παραδειγμα απλά παίρνουμε την εφαπτομένη στη καμπύλη $x^3 - y^3 = n$ και αν είναι θετική παίρνουμε την κάθετο στην εφαπτομένη.

Με αυτή την εισαγωγή θα αρχίσουμε τη μελέτη της $E(\mathbb{Q})$ με την αναφορά στο πρώτο μεγάλο θεώρημα που θα συναντήσουμε, το θεώρημα **Mordell-Weil**. Σε όλο το κεφάλαιο θα θεωρούμε ότι οι καμπύλες μας έχουν συντελεστές στο $\mathbb{Z}$ (και στο $\mathbb{Q}$ να ορίζονται άλλωστε θα έχουμε μια ισομορφική καμπύλη με συντελεστές στο $\mathbb{Z}$).

Θεώρημα 7.0.1. *(Mordell-Weil) Έστω ελλειπτική καμπύλη $E/\mathbb{Q}$. Τότε η υποομάδα $E(\mathbb{Q})$ είναι πεπερασμένα παραγώμενη αβελιανή ομάδα.*

Παρατήρηση. *Από το θεμελιώδες θεώρημα πεπερασμένα παραγώμενων αβελιανών ομάδων έχουμε ότι $E(\mathbb{Q}) = M \oplus Z^n, M = Z_{q_1} \oplus \cdots \oplus Z_{q_n}$. Η M λέγεται υποόμαδα στρέψης και περιέχει ακριβώς τα στοιχεία πεπερασμένης τάξης του $E(\mathbb{Q})$ ενώ το r λέγεται τάξη της καμπύλης. Παρατηρούμε ότι η $E(\mathbb{Q})$ είναι πεπερασμένη ανν $r = 0$.*

Το Θεώρημα Mordell-Weil έχει δύο τμήματα ουσιαστικά:

- Το ασθενές Mordell-Weil.
- Την αρχή της κατάβασης (Descend Argument Principle).

Εμείς θα υποθέσουμε το ασθενές Mordell-Weil και θα δώσουμε επικεντρωθούμε στο Descend Argument Principle αφού αυτές ήταν και οι πρώτες τεχνικές που χρησιμοποιήθηκαν από το Fermat για την επίλυση διοφαντικών εξισώσεων με τη μορφή $y^2 = x^3 - 2$.

Θεώρημα 7.0.2. *(Descend Argument Principle) Έστω αβελιανή ομάδα $(G, +)$ με μια συνάρτηση 'ύψους' $h : G \to \mathbb{R}^+$:*

1. *$\forall x \in \mathbb{R}$ το σύνολο $\{g \in G : h(g) \leq x\}$ είναι πεπερασμένο.*
2. *$\forall g_0 \in G, \exists c > 0 : h(g + g_0) \leq 2h(g) + c, \forall g \in G$.*
3. *$\exists c' > 0 : h(2g) \geq 4h(g - c')$*
4. *$|G : 2G| < \infty$*

τότε η G είναι πεπερασμένα παραγόμενη.

Απόδειξη. *Έστω $q_1, \ldots, q_n$ ένα σύστημα αντισπροσώπων του $G : 2G$. Από την τέταρτη πρόταση $n < \infty$. Τώρα αν $p \in G$ αυτό σημαίνει ότι $p + 2G \in q_i + 2G$, για κάποιο q_i και άρα $p = q_i + 2G \implies p = q_i + 2p_1$. Επαναλαμβάνοντας την ίδια διαδικασία για το p_1 και ξανά μετά θα έχουμε τελικά: $p_0 - q_{i_1} = 2p_1, p_1 - q_{i_2} = 2p_2, \ldots, p_{m-1} - q_{i_m} = 2p_m$ και με διαδοχικές αντικαταστάσεις έχουμε: $p = q_{i_1} + 2q_{i_2} + \ldots + 2^{m-1}q_{i_m} + 2^m p_m$. Βάζοντας στη δεύτερη σχέση $g_0 = -q_i$ παίρνουμε όμως $h(p - q_i) \leq 2h(p) + k_i, \forall p \in G$. Αν το κάνουμε αυτό για όλα τα i και κρατήσουμε το $k' = max k_1, \ldots, k_n$ θα πάρουμε τελικά $h(p - q_i) \leq 2h(p) + k', \forall p \in G, \forall i \in [1, \ldots, n]$. Από την τρίτη σχέση όμως έχουμε $4h(p_j) \leq 2h(p_j) + c$ και $2p_j = p_{j-1} - q_{i_j}$, συνεπώς $4h(p_j) \leq h(p_{j-1} - q_{i_j}) + c \leq 2h(p_{j-1}) + c + k' \implies h(p_j) \leq \frac{1}{2}h(p_{j-1}) + \frac{k'+c}{4} =$*

$\frac{3}{4}h(p_{j-1}) - \frac{1}{4}(h(p_{j-1}) - k' + c)$. *Άρα αν* $(h(p_{j-1}) \geq k' + c$ *τότε* $h(p_j) \leq \frac{3}{4}h(p_{j-1})$ *και υπάρχει τέτοιο* j *αφού κάθε φορά πολλαπλασιάζουμε με* $\frac{3}{4}$ *και αφαιρούμε κάτι θετικό. Δείξαμε επομένως ότι κάθε στοιχείο γράφεται ως* $p = q_{i_1} + 2q_{i_2} + ... + 2^{m-1}q_{i_m} + 2^m p_m$ *με* $m \leq n$ *και* $h(p_m) \leq k' + c$ *τα οποία από τη πρώτη πρόταση είναι πεπερασμένα όμως. Κάθε στοιχείο του* G *γράφεται επομένως ως γραμμικός συνδυασμός στοιχείων από το σύνολο* $\{q_1, \ldots, q_n\} \cup \{g \in G : h(g) \leq x\}$ *που είναι πεπερασμένο.*

7.1 Η συνάρτηση ύψους

Για να χρησιμοποιήσουμε το παραπάνω θεώρημα είναι απαραίτητο να ορίσουμε μια συνάρτηση ύψους σε μια ελλειπτική καμπύλη. Αυτή η συνάρτηση θα πρέπει να πλήρει φυσικά τις ιδιότητες του Θεωρήματος 7.0.2. Αυτή η συνάρτηση αποτελεί ένα μέτρο ¨πολυπλοκότητας' για τα σημεία της καμπύλης. Θα ορίσουμε μια συνάρτηση πρώτα στο $\mathbb{Q}$ και στη συνέχεια θα την προσαρμώσουμε σε ελλειπτικές καμπύλες.

Ορισμός 7.1.1. *Έστω* $q \in \mathbb{Q}$ *με* $q = \frac{a}{b}, gcd(a, b) = 1$. *Ορίζουμε* $H(q) = max\{a, b\}$ *και* $h(q) = lnh(q)$. *Και οι δύο συναρτήσεις αυτές λέγονται ύψος του* q.

Ορισμός 7.1.2. *Έστω* $P(x, y) \in E, P \neq O$ *τότε ορίζουμε* $h(P) = h(x)$ *ενώ* $h(O) = 0$.

Θα αρχίσουμε τώρα αποδεικνύοντας την πρώτη και πιο εύκολη ιδιότητα που θα χρειαστούμε.

Πρόταση 7.1.1. *Το σύνολο* $A_r = \{P \in E : h(P) < r\}$ *είναι πεπερασμένο* $\forall r \in \mathbb{R}$.

Απόδειξη. *Αφού* $r > h(P) = h(x) = ln(H(x))$ *ορίζουμε το σύνολο* $B_r = \{x \in \mathbb{Q} : H(x) < e^r\}$ *και παρατηρούμε ότι για κάθε στοιχείο του* B_r *θα έχουμε το πολύ δύο τιμές του* y. *Συνεπώς* $A_r \leq 2B_r$ *το οποίο είναι πεπερασμένο επειδή* $H(x) < e^r \iff max\{a_x, b_x\} < e^r$ *που έχει το πολύ* $(2\lfloor e^r \rfloor)^2$ *στοιχεία.*

Το επόμενο αποτέλεσμα θα μας βοηθήσει στην απόδειξη των ιδιοτήτων της h για ελλειπτικές καμπύλες.

Πρόταση 7.1.2. *Έστω* $(x, y) \in E(\mathbb{Q})$ *τότε* $\exists m, n, e \in \mathbb{Z} : gcd(m, e) = gcd(n, e)$ *και* $(x, y) = (\frac{m}{e^2}, \frac{n}{e^3})$.

Απόδειξη. *βλ.Proposition 2.2.5 [2]*

Πρόταση 7.1.3. *Για κάθε* $P_0 \in E(\mathbb{Q})$ *υπάρχει* $c : h(P + P_0) \leq 2h(P) + c, \forall P \in E(\mathbb{Q})$.

Απόδειξη. *Έχουμε ότι* $X(P+P_0) = (\frac{y-y_0}{x-x_0})^2 - a - x - x_0 = \frac{Ay+Bx^2+Cx+D}{Ex^2+Fx+G}$ *και από την προηγούμενη πρόταση επομένως:* $X(P + P_0) = \frac{Aen+Bm^2+Cme^2+De^4}{Em^2+Fme^2+Ge^4}$ *και* $H(P) = max\{|m|, e^2\}$. *Όμως* $n^2 = m^3 + am^2e^2 + bme^4 + ce^6 \implies n^2 \leq H(P)^3(1 + |a| + |b| + |c|) \implies |n| \leq H(P)^{3/2}k, k > 1$. *Έτσι έχουμε τελικά* $H(P - P_0) \leq max\{H(P)^2(|A|k + |B| + |C| + |D|), H(P)^2(|E| + |F| + |G|)\} \leq k'H(P)^2$ *και άρα* $h(P - P_0) \leq 2h(P) + ln(k')$.

Θα χρειαστούμε επίσης το ακόλουθο λήμμα την απόδειξη του οποίου παραλείπουμε αφού απαιτεί απλά θεωρήματα διαιρετότητας και την προφανή ανισότητα $max\{a, b\} \geq \frac{a+b}{2}$.

Λήμμα 7.1.1. *Έστω δύο πολυώνυμα* $\phi, \psi \in \mathbb{Z}[X]$ *χωρίς κοινές μιγαδικές ρίζες, τότε αν* $d = max\{deg\phi, deg\psi\}$ *υπάρχει* $c_1, \in \mathbb{R}$*:* $dh(m/n) - c_1 \leq h(\frac{\phi(m/n)}{\psi(m/n)})$.

Απόδειξη. *βλ. σελ.25 Remark 2.2.3 [2]*

Πρόταση 7.1.4. *Υπάρχει* $c \in \mathbb{R} : h(2P) \geq 4h(P) - c, \forall P \in E(\mathbb{Q})$.

Απόδειξη. *Έστω η εξίσωση της καμπύλης* $y^2 = f(x)$, *τότε αν* $2P = O$ *αρκεί να θέσουμε* $c_i = 4h(P)$ *και αφού έχουμε* $deg([2]) = 4$ *άρα είναι πεπερασμένα να διαλέξουμε το μεγαλύτερο εξ΄ αυτών. Αν* $2P \neq O$ *τότε* $x(2P) = \phi(x)/\psi(x)$ *όπου από το Θεώρημα 4.1.5* $4 = deg([2]) = max\{deg(\phi), deg(\psi)\}$. *Το παραπάνω Λήμμα μας δίνει τώρα άμεσα το ζητούμενο.*

Η απόδειξη αυτή φυσικά χρειάζεται και ένα ακόμα αποτέλεσμα:

Θεώρημα 7.1.1. *(Weak Mordell-Weil)*
Έστω ελλειπτική καμπύλη $E/\mathbb{Q}$. *Τότε* $|E : 2E| < \infty$.

Απόδειξη. *βλ. σελ.4 [3]*

7.2 Η δομή της $E(\mathbb{Q})$

Επειδή η $E(\mathbb{Q})$ είναι πεπερασμένα παραγόμενη αβελιανή ομάδα όπως προείπαμε θα έχει την εξής δομή: $E(\mathbb{Q}) = M \oplus Z^n, M = Z_{q_1} \oplus \cdots \oplus Z_{q_n}$. Η M δομή της επομένως εξαρτάται αποκλειστικά από το r και τη M. Παρατηρούμε ότι η $E(\mathbb{Q})$ είναι πεπερασμένη ανν $r = 0$ και τότε έχουμε μόνο στοιχεία πεπερασμένης τάξης. Σε αντίθεση με το βαθμό r που είναι εξαιρετικα δύσκολο να υπολογιστεί, η δομή της M είναι αρκετά εύκολο να βρεθεί για μια δεδομένη ελλειπτική καμπύλη με το θεώρημα Nagell-Lutz ενώ το θεώρημα του Mazur περιγράφει πλήρως τις 15 πιθανές δομές της M.

Θεώρημα 7.2.1. *(Nagell-Lutz) Έστω ελλειπτική καμπύλη* $E/\mathbb{Q}$ *τότε αν* $(x, y) \in E(\mathbb{Q})_{Tor}$ *θα ισχύει ότι* $x, y \in \mathbb{Z}$ *και* $y^2|\Delta$.

Απόδειξη. *βλ. κεφάλαιο 8 [1]*

Παρατήρηση. *Μια ενδιαφέρουσα παρατήρηση είναι ότι αν έχουμε την εξίσωση μιας ελλειπτικής καμπύλης και βρούμε ένα ρητό σημείο που δεν έχει ακέραιες συντεταγμένες τότε η καμπύλη αυτή έχει βαθμό* $r \geq 1$ *αφού έχουμε ένα ρητό σημείο που δεν ανήκει στην υποομάδα στρέψης της καμπύλης. Και αντίστροφα όμως μια καμπύλη με βαθμό* $r = 0$ *θα έχει μόνο ακέραιες λύσεις στο* $\mathbb{Q}$.

Παράδειγμα 7.2.1. *Έστω η καμπύλη με εξίσωση* $y^2 = x^3 + 1$. *Τότε* $\Delta = -27$ *και επομένως* $y \in E(\mathbb{Q})_{Tor} \implies y^2|27 \implies y|3$ *και επομένως έχουμε σημεία στρέψης μόνο τα* $(x, y) = (0, 1), (1, \pm 1), (2, \pm 3)$. *Με τεχνικές όπως αυτές που χρησιμοποιούνται στην απόδειξη του ασθενούς Mordell-Weil μπορούμε να δείξουμε ότι η καμπύλη αυτή έχει βαθμό* $r = 0$ *και άρα αυτές είναι όλες οι ρητές λύσεις της.*

Μια ενδιαφέρουσα ιδιότητα που έχουν οι ισογένιες είναι ότι διατηρούν την υποομάδα που είναι ισομορφική με τη $\mathbb{Z}^r$. Αυτό συνεπάγεται ότι οι ομάδες στην ίδια κλάση ισογενών καμπυλών θα έχουν είτε όλες άπειρα ρητά σημεία είτε όλες πεπερασμένα ρητά σημεία.

Θεώρημα 7.2.2. *(**) Έστω ισογενείς καμπύλες* E_1, E_2 *με* $E_1(\mathbb{Q}) \simeq E_1(\mathbb{Q})_{Tor} \oplus \mathbb{Z}^{r_1}$ *και* $E_2(\mathbb{Q}) \simeq E_2(\mathbb{Q})_{Tor} \oplus \mathbb{Z}^{r_2}$, *τότε* $r_1 = r_2$.

Απόδειξη. *Έστω* $\phi : E_1 \to E_2$ *τότε* $\phi \supseteq E_1(\mathbb{Q})$. *Περιορίζοντας την* ϕ *στην ισομορφική στη* Z^{r_1} *ομάδα του* $E_1(\mathbb{Q})$ *έχουμε επομένως* $\phi' : \mathbb{Z}^{r_1} \to \mathbb{Z}^{r_2}$ *και επειδή* $ker(\phi') = O$ *(γιατί* $a\phi(x) = O \implies \phi(ax) = O \implies ax \in E_1(\mathbb{Q})_{Tor} \implies x \in E_1(\mathbb{Q})_{Tor}$*) ο ομομορφισμός αυτός είναι* $1 - 1$. *Επειδή όμως έχουμε και τη δυική ισογένια έχουμε και έναν δεύτερο ομομορφισμό* $\bar{\phi}' : \mathbb{Z}^{r_2} \to \mathbb{Z}^{r_1}$ *που είναι επίσης* $1 - 1$. *Έτσι έχουμε* $\mathbb{Z}^{r_1} \leq \mathbb{Z}^{r_2}$ *και* $\mathbb{Z}^{r_2} \leq \mathbb{Z}^{r_1}$ *και άρα* $\mathbb{Z}^{r_1} = \mathbb{Z}^{r_2} \implies r_1 = r_2$.

Ένα άμεσο επακόλουθο είναι ότι μπορούμε να φράξουμε των αριθμό ρητών σημείων σε καμπύλες ίδιας κλάσης ισογένιας. Να σημειώθει ότι ο υπολογισμός του r σε μια δεδομένη ελλειτική καμπύλη είναι ένα πολύ δύσκολο σε γενικές γραμμές πρόβλημα από μόνο του, ακόμα και το να αποφανθούμε αν είναι 0 ή όχι. Το να βρούμε όμως μια ισογένια δεδομένης μιας καμπύλης είναι αρκετά εύκολο όπως είδαμε από τον τύπο του Velu.

Πρόταση 7.2.1. *(**) Έστω ισογενείς ελλειπτικές καμπύλες E_1, E_2 ορισμένες πάνω στο $\mathbb{Q}$ με $\phi : E_1 \to E_2$. Τότε αν $r = 0$ και $E_1(\mathbb{Q}) \geq E_2(\mathbb{Q})$ ισχύει ότι: $E_1(\mathbb{Q})/E_2(\mathbb{Q}) \leq deg(\phi)$.*

Απόδειξη. *Έστω $\phi : E_1 \to E_2$ τότε $E_1(\mathbb{Q})/ker(\phi) \leq E_2(\mathbb{Q}) \implies |E_1(\mathbb{Q})|/|ker(\phi)| \leq |E_2(\mathbb{Q})|$ και το ζητούμενο έπεται άμεσα.*

8 ΠΑΡΑΡΤΗΜΑ: Επίλυση Εξισώσεων στο $\mathbb{Q}$ με αναγωγή σε Ελλειπτικές Καμπύλες

Σε αυτό το κεφάλαιο θα εξετάσουμε διάφορες διφαντικές εξισώσεις και θα αναζητήσουμε λύσεις στους ρητούς για άλλες με την αναγωγή αυτών στο πρόβλημα εύρεσης ρητών σημείων σε κάποια ελλειπτική καμπύλη. Το βασικό θεώρημα που θα χρησιμοποιήσουμε είναι η εξίσωση του Euler.

Θεώρημα 8.0.1. *Η ελλειπτική καμπύλη $y^2 = x^3+1$ έχει ακριβώς τα ακόλουθα ρητά σημεία: $(x, y) \in \{(0, \pm 1), (-1, 0), (2, \pm 3)\}$.*

Ας δούμε λοιπόν μια σχετικά εύκολη αναγωγή στην εξίσωση του Euler:

Θεώρημα 8.0.2. *(**Legendre**) Η διοφαντική εξίσωση $x^3 + y^3 = 2z^3$ έχει λύσεις μόνο τις $(x, y, z) = (a, a, a), (a, -a, 0)$.*

Απόδειξη. *Θέτοντας $t = 4z^3 - y^3 = 2x^3 + y^3$ έχουμε $\frac{t+y^3}{2} = 2z^3, \frac{t-y^3}{2} = x^3$ και επομένως $t^2 - y^6 = (2xz)^3 \implies (\frac{t}{y^3})^2 = (\frac{2xz}{y^2})^3 + 1$ (αφού $y \neq 0$). Ψάχνουμε επομένως $(\frac{2xz}{y^2}, \frac{t}{y^3}) \in \mathbb{Q}$ τέτοιο ώστε να ισχύει η εξίσωση του Euler. Άρα $(\frac{2xz}{y^2}, \frac{t}{y^3}) = \{(0, \pm 1), (-1, 0), (2, \pm 3)\}$. Από το $(0, \pm 1)$ προκύπτει $z = 0$ αφού $x, y \neq 0$ και άρα $(x, y, z) = (a, -a, 0)$. Για το $(-1, 0)$ παρατηρούμε ότι δίνει $t = 0$ και άρα $4z^3 = y^3 \implies 4 = u^3, u \in \mathbb{Q}$ που είναι άτοπο. Από τη $(2, 3)$ παρατηρούμε ότι προκύπτει $xz = y^2$ και $t = 3y^3$ επομένως $z^3 = \frac{3y^3+y^3}{4} = y^3$ και $x^3 = y^3$ και άρα $(x, y, z) = (a, a, a)$.Από το $(2, -3)$ προκύπτει $-2 = \frac{y^3}{z^3}$ που είναι άτοπο.*

Παρατήρηση. *Η ίδια ακριβώς απόδειξη μας επιτρέπει να συμπεράνουμε ότι η $x^3+y^3 = 2z^3$ έχει ακριβώς τις λύσεις $(x, y, z) = (a, a, a), (a, -a, 0)$ και στο $\mathbb{Q}$.*

Το αξιοσημείωτο είναι όπως θα δούμε παρακάτω ότι ξεκινώντας από την $x^3 + y^3 = 2z^3$ μπορούμε να χαρακτηρίσουμε πλήρως τις ρητές λύσεις της εξίσωσης του Euler. Η λύση του Legendre δεν χρησιμοποιεί μεθόδους ελλειπτικών καμπυλών οπότε μπορούμε να χρησιμοποιήσουμε οποιοδήποτε θεώρημα για να αποδείξουμε το άλλο. Θα ξαναδούμε τώρα την ίδια τεχνική με ένα ακόμα παράδειγμα αυτή τη φορά αναζητώντας λύσεις στο $\mathbb{Q}$:

Πρόταση 8.0.1. *Η εξίσωση $2x^3y - y^2 = 1$ έχει μοναδική λύση στο $\mathbb{Q}$ την $(x, y) = (1, 1)$.*

Απόδειξη. *Θέτοντας ξανά $\frac{t+1}{2} = 2x^3y, \frac{t-1}{2} = y^2$ παίρνουμε $t^2 = (2xy)^3+1$ που συνεπάγεται $(2xy, t) \in \{(0, \pm 1), (-1, 0), (2, \pm 3)\}$. Η $(0, \pm 1)$ δίνει $-y^2 = 1$ ή $0 = 1$. Η $(-1, 0)$ δίνει $y^2 = -\frac{1}{2}$. Η $(2, -3)$ δίνει $y^2 = -2$ και τέλος η $(2, 3)$ δίνει τη λύση $(x, y) = (1, 1)$.*

Στη συνέχεια θα εξετάσουμε την ύπαρξη ρητών σημείων σε μια συγκεκριμένη ελλειπτική καμπύλη που θα μας βοηθήσει στα επόμενα προβλήματα μας.

Πρόταση 8.0.2. *Η ελλειπτική καμπύλη $y^2 + y = x^3$ έχει σημεία με ρητές συντεταγμένες μόνο τα $(0, 0), (0, -1)$.*

Απόδειξη. *Έστω $y = \frac{y_1}{y_2}, x = \frac{x_1}{x_2}$ με $gcd(y_1, y_2) = gcd(x_1, x_2) = 1$. Έχουμε τότε: $\frac{y_1(y_1+y_2)}{{y_2}^2} = \frac{{x_1}^3}{{x_2}^3}$ και επειδή $gcd(y_1, y_1 + y_2) = gcd(y_2, y_1 + y_2) = gcd(y_1, y_2) = 1$ θα πρέπει: $y_1(y_1 + y_2) = {x_1}^3$ και ${y_2}^2 = {x_2}^3$ και επομένως $y_1 = a^3, y_1 + y_2 = b^3$ με $x_1 = ab$ και $y_2 = (\sqrt{x_2})^3$ με $\sqrt{x_2} \in \mathbb{N}$. Έχουμε δηλαδή $a^3 + (\sqrt{x_2})^3 = b^3$ και άρα αφού $x_2 \neq 0$ θα έχουμε $a = 0, x_2 = b^2$ ή $b = 0, x_2 = a^2$ και στις δύο περιπτώσεις δηλαδή θα προκύψει $x_1 = 0$ και άρα $y_1(y_1 + y_2) = 0$ και το αποτέλεσμα έπεται άμεσα.*

Περνάμε έτσι στην εξέταση της ύπαρξης λύσης στο $\mathbb{Q}$ πιο ενδιαφέροντων εξισώσεων που διέπονται από συμμετρία όπως η ακόλουθη.

Θεώρημα 8.0.3. *Η εξίσωση $xy^2 - x^2y = 1$ δεν έχει λύση στο $\mathbb{Q}$.*

Απόδειξη. *Θέτοντας $\frac{t+1}{2} = xy^2$ και $\frac{t-1}{2} = x^2y$ όπως πριν προκύπτει $t^2 = 4(xy)^3 + 1$ και με την αντικατάσταση $(xy, t) \to (a, 2b + 1)$ αναζητούμε ισοδύναμα ρητές λύσεις της $b^2 + b = a^3$.Από την Πρόταση 8.0.2 $(a, b) \in \{(0, 0), (0, -1)\} \implies (xy, t) \in \{(0, 1), (0, -1)\}$ και επομένως $x = 0$ ή $y = 0$ που δεν επαληθεύει την αρχική.*

Έχουμε τώρα ένα νέο εργαλείο στη διάθεσή μας επομένως:

Πρόταση 8.0.3. *Η ελλειπτική καμπύλη $y^2 = 4x^3+1$ έχει λύσεις στο $\mathbb{Q}$ ακριβώς τις $(0, \pm 1)$.*

Απόδειξη. *Αποδείχθηκε στο παραπάνω θεώρημα.*

Παρατήρηση. *Παρατηρούμε ότι τώρα είμαστε γενικά σε θέση να λύσουμε στο $\mathbb{Q}$ εξισώσεις τις μορφής $F(x_1, \dots, x_n) - G(x_1, \dots, x_n) = u^3$ με $F(x_1, \dots, x_n)G(x_1, \dots, x_n) = H(x_1, \dots, x_n)^3$ ή $F(x_1, \dots, x_n)G(x_1, \dots, x_n) = 2H(x_1, \dots, x_n)^3$. Πράγματι θέτοντας $\frac{t+u^3}{2} = F(x_1, \dots, x_n)$, $\frac{t-u^3}{2} = G(x_1, \dots, x_n)$ παίρνουμε: $t^2 = 4F(x_1, \dots, x_n)G(x_1, \dots, x_n) + 1$ που έχει είτε τη μορφή $y^2 = 4x^3 + 1$ είτε $y^2 = x^3 + 1$.*

Παράδειγμα 8.0.1. *Η ειδική περίπτωση του FLT $x^3 + y^3 = 1$ προφανώς δεν έχει μη τετριμμένη λύση στο $\mathbb{Q}$ και αυτό ισχύει διότι θα έχουμε μέσω της $(x, y) \to (x, -y)$ την ισοδύναμη εξίσωση $x^3 - y^3 = 1$ και άρα όπως παραπάνω $t^2 = 4(xy)^3 + 1$ που σημαίνει ότι $(xy, t) \in \{(0, 1), (0, -1)\}$ και άρα $x = 0$ ή $y = 0$.*

Ας δούμε τώρα ένα παράδειγμα μιας άλλης τεχνικής:

Πρόταση 8.0.4. *Η εξίσωση $x^2y^2 + x + y = 0$ έχει λύση στο $\mathbb{Q}$ μόνο το $(0, 0)$.*

Απόδειξη. *Ας δούμε την εξίσωση σαν δυώνυμο του x, τότε για να έχει λύση στο $\mathbb{Q}$ πρέπει η διακρίνουσά της να είναι τέλειο τετράγωνο στο $\mathbb{Q}$, δηλαδή $\Delta = q^2$,$q \in \mathbb{Q}$. Έχουμε δηλαδή λύση ανν $q^2 = 1 - 4x^3$ και μέσω του μετασχηματισμού $(x, y) \to (-x, y) : q^2 = 4x^3 + 1$. Άρα $(x, q) = (0, \pm 1) \implies x = 0 \implies y = 0$.*

Παρατήρηση. *Έστω η εξίσωση $y^2+x+x^2y = 0$. Τότε έχουμε μια λύση την $(x, y) = (0, 0)$, ενώ αν $x \neq 0$ τότε θέτοντας $(x, y) \to (\frac{1}{x}, y)$ θα έχουμε $x^2y^2 + x + y = 0$ και άρα η λύση $(0, 0)$ είναι μοναδική στο $\mathbb{Q}$. Αυτό που πρέπει ουσιαστικά να κρατήσουμε από αυτά τα παραδείγματα είναι η μορφή των εξισώσεων: το γινόμενο των όρων τους είναι της μορφής $(xy)^3$.*

Θεώρημα 8.0.4. *Έστω $f \in Q[X, Y]$ με $deg(f(x)) = deg(f(y)) = 2$ ή 3 και το γινόμενο των όρων της f είναι της μορφής $A[X, Y]^3 \in \mathbb{Q}[X, Y]$, τότε η $f(x, y) = 0$ έχει το πολύ δύο μη τετριμμένες λύσεις στο $\mathbb{Q}$.*

Απόδειξη.

- *αν $f(x, y)$ είναι δυώυμο ως προς x ή y τότε (έστω ότι είναι ως προς x ΧΒΓ) έχουμε: $a_yx^2 + b_yx + c_y = 0 \iff \Delta = q^2 \in \mathbb{Q}$ ή ισοδύναμα: $q^2 = {b_y}^2 - 4a_yc_y$. Όμως $a_yb_yc_yx^3 = z^3 \implies a_yb_yc_y = (\frac{z}{x})^3 \implies a_yc_y = u^3/b_y$. Έτσι έχουμε: $(q/b_y)^2 = 1 + 4(-\frac{u}{b_y})^3, (b_y \neq 0)$ και επομένως $(a_yc_y, q) = (0, \pm 1)$. Από το $q = \pm 1$ παίρνουμε λύσεις τις $x = 0, -\frac{b_y}{a_y}$ και άρα και στις δύο περιπτώσεις $y \in \mathbb{Q} : c_y = 0$. Επειδή $c_y = y^3 + c', c' \in \mathbb{Q}$ ή $c_y = a'y^2 + b'y + c'$ που έχει το πολύ δύο ρίζες στο $\mathbb{Q}$. Αν $b_y = 0$ τότε ισχύουν ακριβώς τα αντίστοιχα.*

- *αν η $f(x,y)$ δεν είναι δυώνυμο ως προς x ούτε y τότε έχει είτε μόνο όρους βαθμού 3 και άρα έχουμε την $a(xy)^3 = c$ που είναι τετριμμένη ή την $ax^3+by^3 = c$ με $abc = z^3$ για την οποία θέτοντας $(a',b') = (a/c, b/c)$ παρατηρούμε ότι $a'b' = ab/c^2 = abc/c^3 = (z/c)^3 = z'^3$ και άρα θέτοντας $\frac{t+1}{2} = a'x^3$, $\frac{t-1}{2} = b'y^3$ καταλήγουμε στην $t^2 = 4(z'xy)^3 + 1$ και επομένως $x = 0$ ή $y = 0$.*

Παρατήρηση. *Την ίδια τεχνική μπορούμε να εφαρμόσουμε και όταν το γινόμενο των όρων είναι της μορφής $2q^3$ καταλήγοντας στην $y^2 = x^3+1$ όμως. Μπορούμε επίσης να διατυπώσουμε το ίδιο θεώρημα στη περίπτωση που η μια μόνο μεταβλητή έχει βαθμό 2.*

Θα εφαρμόσουμε τώρα μια τεχνική που είδαμε στο προηγούμενο κεφάλαιο αλλά μόνο θεωρητικά: τη χρήση ισογενιών για τη μέτρηση των ρητών σημείων.

Θεώρημα 8.0.5. *Η εξίσωση $y^2+y = x^3-7$ έχει ακριβώς δύο λύσεις στο $\mathbb{Q}$: $(x,y) = (3,4)$ και $(x,y) = (3,-5)$.*

Απόδειξη. *Παρατηρούμε ότι η δοθείσα εξίσωση είναι ισογενής με την $y^3 + y = x^3$ με ισογένια βαθμού 3 και επομένως έχουμε πεπερασμένο πλήθος ρητών σημείων το οποίο είναι ακριβώς η ομάδα στρέψης της καμπύλης. Επειδή $\Delta = -3^9$ έχουμε από Nagell-Lutz: $(x,y) \in \mathbb{Q} \implies y^2|3^9 \implies y|3^4$ και επομένως καταλήγουμε στις δύο παραπάνω ρίζες.*

Θα δείξουμε τώρα τέλος ότι η επίλυση της $y^2 = x^3 + 1$ στο $\mathbb{Q}$ είναι ισοδύναμη με την επίλυση της $x^3 + y^3 = 2$ στο $\mathbb{Q}$. Το ότι οι λύσεις της $x^3 + y^3 = 2$ προκύπτουν από τις λύσεις της $y^2 = x^3 + 1$ έχει αποδειχθεί στο Θεώρημα 8.0.2.

Θεώρημα 8.0.6. *Έστω ότι η $x^3 + y^3 = 2$ έχει λύσεις στο $\mathbb{Q}$ ακριβώς τις $(x,y) = (a,a)$. Τότε η εξίσωση του Euler $y^2 = x^3+1$ έχει λύσεις στο $\mathbb{Q}$ ακριβώς τις $(-1,0), (0,\pm1), (2,\pm3)$.*

Απόδειξη. *Θέτοντας $y = y_1/y_2, x = x_1/x_2$ έχουμε ότι $\frac{{y_1}^2-{y_2}^2}{{y_2}^2} = \frac{{x_1}^3}{{x_2}^3}$ και $gcd({y_1}^2 - {y_2}^2, {y_2}^2) = gcd(y_1,y_2)^2 = 1$. Έτσι προκύπτει ότι: ${y_1}^2 - {y_2}^2 = {x_1}^3, {y_2}^2 = {x_2}^3$ και άρα:*

- *Αν ${y_1}^2 = {y_2}^2$ τότε παίρνουμε τη λύση $(x,y) = (0,\pm1)$.*
- *Αν $gcd(y_1+y_2, y_1-y_2) = 1$ τότε $y_2 = \sqrt{x_2}^3, y_1-y_2 = a^3, y_1+y_2 = b^3$ με $ab = x_1$. Και άρα έχουμε $2\sqrt{x_2}^3 = b^3+(-a)^3 \implies -a = b = \sqrt{x_2}$ και επομένως $y_1 = (a^3+b^3)/2 = 0, x = -a^2/a^2 = -1$ άρα $(x,y) = (-1,0)$.*
- *Αν $gcd(y_1+y_2, y_1-y_2) = 2$ τότε $y_2 = \sqrt{x_2}^3, \frac{(y_1+y_2)}{2}\frac{(y_1-y_2)}{2} = 2(x_1/2)^3$ και $gcd(\frac{(y_1+y_2)}{2}, \frac{(y_1-y_2)}{2}) = 1$ επομένως $\frac{(y_1-y_2)}{2} = 2a^3, \frac{(y_1+y_2)}{2} = b^3 \implies y_2 = b^3 - 2a^3 \implies \sqrt{x_2}^3 + (-b)^3 = 2(-a)^3 \implies \sqrt{x_2} = -b = -a \implies {y_1}^2 - {y_2}^2 = 8a^3 \implies x^3 = 8a^3/a^3 \implies x = 2$ και άρα έχουμε τη λύση $(x,y) = (2,\pm3)$. (Αν είχαμε $\frac{(y_1+y_2)}{2} = 2b^3, \frac{(y_1-y_2)}{2} = a^3$ τότε αντίστοιχα προκύπτει $a = b = \sqrt{x_2}$ και άρα πάλι η ίδια λύση.)*

Βιβλιογραφία

[1] Joseph H. Silverman [The Arithmetic of Elliptic Curves]. Springer, ISBN 978-0-387-09493-9, 2009.

[2] Alexandru Gica,[Rational Points on Elliptic Curves]. http://www.imar.ro/~sergium/ens/Rational.pdf

[3] MIT,[Introduction to Arithmetic Geometry, Lecture 25]. https://ocw.mit.edu/courses/mathematics/18-782-introduction-to-arithmetic-geometry-fa lecture-notes/MIT18_782F13_lec25.pdf

[4] Tate, [Endomorphisms of abelian varieties over finite fields], Invent.Math., 2:134–144, 1966.

[5] MIT, [Elliptic Curves Lecture 3] http://math.mit.edu/classes/18.783/2017/LectureNotes16.pdf

[6] J.S.Milne, [Elliptic Curves] https://www.jmilne.org/math/Books/ectext5.pdf

[7] Josep M. Miret, Ramiro Moreno and Anna Rio, [Generalization of Velus Formulae for Isogenies between Elliptic Cuves] https://pdfs.semanticscholar.org/5abe/24623f165f8b27b734e2d272025c802223e7.pdf

[8] R.Hartshorne [Algebraic Geometry, Graduate Texts in Mathematics 52]. Springer.

[9] J.Silverman and J.Tate [Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag]. Springer.

[10] BRIAN OSSERMAN, [THE WEIL CONJECTURES] http://www.wiskundemeisjes.nl/wp-content/uploads/2008/12/weil.pdf

[11] Prof.Dr.Uwe Jannsen, [Deligne's Proof of the Weil-conjecture] http://www.mathematik.uni-regensburg.de/Jannsen/home/Weil-gesamt-eng.pdf

[12] Igor Tolkov, [Counting points on elliptic curves: Hasse's theorem and recent developments] https://sites.math.washington.edu/~morrow/336_09/papers/Igor.pdf