Γιάννη Α. Αντωνιάδη
Τμήμα Μαθηματικών,
Πανεπιστήμιο Κρήτης

Αριθμητική Ελλειπτικών Καμπυλών

Το Θεώρημα του Mordell

Έκδοση ΕΠΕΑΕΚ "ΠΡΟΜΗΘΕΑΣ"
Πανεπιστήμιο Κρήτης
Ηράκλειο, 1999

Στην Κατερινιώ,
την μοναχοκόρη μας.

Περιεχόμενα

Εισαγωγή

Το περιεχόμενο του βιβλίου αποτελεί εισαγωγή στην αριθμητική των ελλειπτικών καμπυλών. Το κύριο θέμα το οποίο διαπραγματεύεται είναι η απόδειξη του Θεωρήματος του Mordell. Η διαπραγμάτευση της ύλης γίνεται με στοιχειώδη, κατά το δυνατό, μέσα. Έτσι το περιεχόμενό του θεωρείται ότι βρίσκεται στο μεταίχμιο μεταξύ προπτυχιακού και μεταπτυχιακού επιπέδου. Σε μερικές μόνο περιπτώσεις αφήνουμε ερωτήματα σαν άσκηση στον αναγνώστη.

Στο πρώτο κεφάλαιο περιγράφονται, χωρίς αυστηρότητα, βασικές έννοιες και τεχνικές και διατυπώνεται το θεώρημα του Mordell.

Στο δεύτερο κεφάλαιο ακολουθεί η αναγκαία για τα παρακάτω ύλη από την θεωρία των επίπεδων αλγεβρικών καμπυλών. Στοιχεία από την Άλγεβρα χρήσιμα για την κατανόηση του κεφαλαίου αυτού έχουν προστεθεί σαν παράρτημα στο τέλος του βιβλίου.

Στο τρίτο κεφάλαιο ορίζεται η πρόσθεση ρητών σημείων μη-ιδιαζουσών κυβικών καμπυλών και αποδεικνύεται, αυστηρά πλέον, ότι ως προς αυτή την πράξη αποτελούν **ομάδα**.

Στο τέταρτο κεφάλαιο αποδεικνύεται το Θεώρημα των Lutz-Nagell. Το θεώρημα αφορά στα ρητά σημεία **πεπερασμένης** τάξης μιάς ελλειπτικής καμπύλης.

Τέλος, στο πέμπτο κεφάλαιο αποδεικνύεται το Θεώρημα του Mordell και δίνονται παραδείγματα υπολογισμού του **βαθμού (rank)** ελλειπτικών καμπυλών καθώς και παραδείγματα με μεγάλο βαθμό (rank).

Σημαντικώτατο βοήθημα για μας υπήρξαν οι πολυγραφημένες, κάποτε δυσεύρετες, σημειώσεις των διαλέξεων του J. Tate, στο Haverford College [28]. Αργότερα, έχουν χρησιμοποιηθεί και στα βιβλία [7], [10], [25].

Το περιεχόμενο του βιβλίου διδάχθηκε είτε σαν μεταπτυχιακό μάθημα είτε σαν μάθημα μελέτης σε μεταπτυχιακούς φοιτητές του Τμήματος Μαθηματικών του Πανεπιστημίου Κρήτης. Σημαντικές και χρήσιμες ήταν οι παρατηρήσεις και τα σχόλια των φοιτητών που το παρακολούθησαν.

Το βιβλίο εκδίδεται στα πλαίσια του ΕΠΕΑΕΚ "ΠΡΟΜΗΘΕΑΣ" του Πανεπιστημίου Κρήτης. Θερμές ευχαριστίες χρωστώ στον υπεύθυνο του προγράμματος Αν. Καθηγητή Γιώργο Τζιρίτα. Θερμές επίσης ευχαριστίες χρωστώ στον μεταπτυχιακό φοιτητή του Τμήματος Επιστήμης Υπολογιστών David J. M^{c}Clurkin για την εξαιρετικά επιμελημένη ηλεκτρονική επεξεργασία του κειμένου.

Γιάννης Α. Αντωνιάδης, Καθηγητής

Ηράκλειο, 10 Οκτωβρίου 1999

Κεφάλαιο 1

Ρητά σημεία επιπέδων καμπυλών

Ένα σημείο στο (x, y)-επίπεδο καλείται **ρητό σημείο** αν και μόνο αν οι συντεταγμένες του x και y είναι ρητοί αριθμοί.

Μία ευθεία θα λέγεται **ρητή** αν η εξίσωσή της μπορεί να γραφεί με ρητούς συντελεστές, δηλαδή όταν η εξίσωσή της είναι της μορφής

$$ax + by + c = 0, \quad a, b, c \in \mathbb{Q}.$$

Παρατήρηση:

(i) Αν $(x_1, y_1), (x_2, y_2)$ είναι ρητά σημεία του επιπέδου τότε και η ευθεία που ορίζουν είναι επίσης ρητή.

(ii) Δύο ρητές ευθείες τέμνονται σε ρητό σημείο.

Σκοπός του κεφαλαίου είναι μία πρώτη εισαγωγή σε αποτελέσματα και προβλήματα που συνδέονται με την περιγραφή των ρητών σημείων επίπεδης καμπύλης.

Εξετάζουμε εν συντομία το πρόβλημα της ύπαρξης ενός ρητού σημείου, ενώ το κύριο ενδιαφέρον μας στρέφεται στην δυνατότητα εύρεσης παραμετρικής μορφής του συνόλου όλων των ρητών σημείων όταν μας δοθεί ένα από αυτά.

Αυτό γίνεται εύκολα στις κωνικές τομές. Στόχος μας θα είναι η μελέτη των ρητών σημείων μη ιδιόμορφων (non-singular) κυβικών καμπυλών.

1. Κωνικές τομές με δοσμένο ρητό σημείο

Μία κωνική τομή

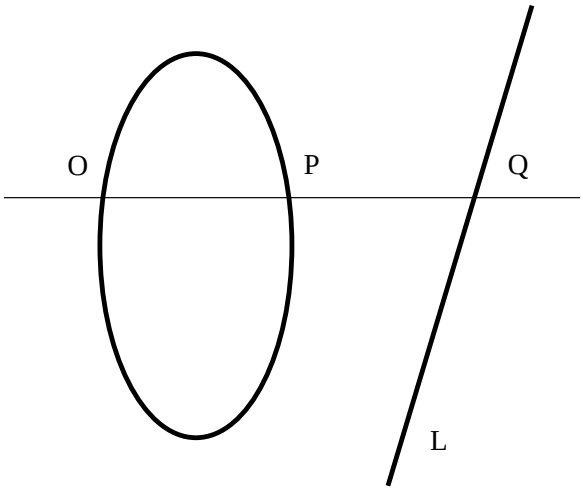
$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

θα λέγεται **ρητή** αν η εξίσωσή της μπορεί να γραφεί με συντελεστές a, b, c, d, e, f ρητούς αριθμούς.

Αν ένα από τα δύο σημεία τομής μιάς **ρητής** κωνικής τομής με **ρητή** ευθεία είναι ρητό σημείο τότε και το άλλο σημείο τομής είναι επίσης ρητό.

Αυτό το βλέπουμε λύνοντας το σύστημα κωνικής τομής και ευθείας (αντικαθιστώ το y της ευθείας στην κωνική τομή). Έτσι βρίσκουμε μία δευτεροβάθμια εξίσωση ως προς x, έστω $Ax^2 + Bx + C = 0$. Αν η κωνική τομή και η ευθεία είναι ρητές, τότε $A, B, C \in \mathbb{Q}$. Το x είναι εν γένει άρρητη ποσότητα δευτέρου βαθμού. Προφανώς αν x είναι ρητός τότε και ο y είναι ρητός. Το πρόβλημα λοιπόν είναι ισοδύναμο με το ότι αν μία δευτεροβάθμια εξίσωση με **ρητούς** συντελεστές έχει μία ρητή λύση τότε και **η άλλη** λύση της θα είναι **ρητή**.

Εγκαταλείπουμε προς στιγμήν το ερώτημα της ύπαρξης ενός ρητού σημείου, υποθέτουμε ότι το O είναι ένα ρητό σημείο κωνικής τομής και θα δούμε πως μπορούμε να βρούμε όλα τα ρητά σημεία αυτής.



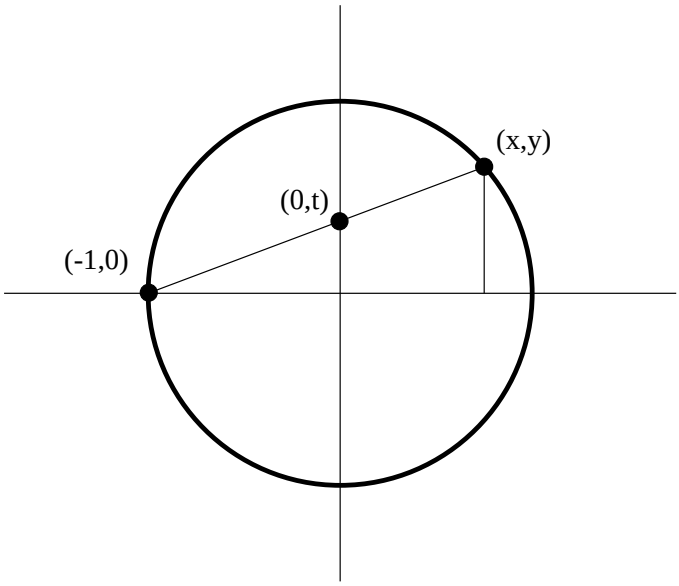
Σχήμα 1.1: Ρητό σημείο κωνικής τομής

Παίρνουμε μία ρητή ευθεία L και προβάλλουμε την κωνική τομή C πάνω στην ευθεία L από το σημείο O. Έτσι έχουμε μία ένα προς ένα αντιστοιχία ανάμεσα στα σημεία της

κωνικής τομής P που είναι διάφορα του O και στα σημεία της ευθείας L. Αφού το O είναι εξ υποθέσεως ρητό σημείο, το P είναι ρητό αν και μόνο αν το Q είναι ρητό. (Διότι αν κατ' αρχήν το P είναι ρητό, η ευθεία OP είναι ρητή και επομένως η τομή των ευθειών OP και L είναι ρητό σημείο. Αν τώρα το Q είναι ρητό σημείο, η ευθεία OQ είναι ρητή και επειδή η κωνική τομή C είναι ρητή και το ένα σημείο τομής, το O είναι ρητό έπεται ότι και το άλλο σημείο τομής, το Q θα είναι επίσης ρητό.)

Ώστε, τα ρητά σημεία της κωνικής τομής C, τα διάφορα του O, βρίσκονται σε ένα προς ένα αντιστοιχία με τα ρητά σημεία της γραμμής L.

Παράδειγμα 1. *Έστω η κωνική τομή (κύκλος)* $x^2 + y^2 = 1$.



Σχήμα 1.2: Κωνική τομή

Προβάλλουμε κάθε σημείο (x, y) *του κύκλου στον άξονα των* y, *από το ρητό σημείο* $(-1, 0)$. *Η ευθεία που περνάει από τα σημεία* $(-1, 0)$ *και* $(0, t)$ *έχει εξίσωση* $y = t(1 + x)$, *οπότε το σύστημα των εξισώσεων*

$$x^2 + y^2 = 1 \quad \text{και} \quad y = t(1 + x),$$

μας δίνει ότι $t^2(1+x)^2 + x^2 = 1$, *δηλαδή* $t^2(x^2+2x+1)+x^2 = 1$ *και επομένως* $(1+t^2)x^2 + 2t^2x + t^2 - 1 = 0$. *Το πολυώνυμο αυτό έχει διακρίνουσα* $\Delta = 4t^4 - 4(t^2 - 1)(t^2 + 1) = 4$.

Συνεπώς παίρνουμε τις λύσεις:

$$x = \frac{1-t^2}{1+t^2} \quad \textit{και} \quad x = -1.$$

Η δεύτερη λύση αντιστοιχεί στο σημείο $(-1, 0)$.

Άρα οι λύσεις (x, y) *του παραπάνω συστήματος δίνονται από την παραμετρική μορφή*

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}.$$

Παρατηρούμε ότι το t *είναι ρητός τότε και μόνο τότε όταν το* (x, y) *είναι ρητό σημείο του κύκλου.*

Αν θέλουμε να πάρουμε και το σημείο $(-1, 0)$ *θα πρέπει να «αντικαταστήσουμε» το* t *με το άπειρο.*

2. Ύπαρξη ρητών σημείων σε κωνικές τομές και κυβικές εξισώσεις

Είδαμε στην προηγούμενη παράγραφο, πως μπορούμε να βρούμε όλα τα ρητά σημεία μιάς κωνικής τομής αν γνωρίζουμε τουλάχιστο ένα από αυτά. Υπάρχουν όμως κωνικές τομές που δεν έχουν καθόλου ρητά σημεία. Έτσι ενώ οι κύκλοι $x^2+y^2=1$ και $x^2+y^2=2$ έχουν ρητά σημεία (ο δεύτερος π.χ. το $(x, y) = (1, 1)$). Ο κύκλος $x^2 + y^2 = 3$ **δεν** έχει ρητά σημεία.

Απόδειξη: Έστω ότι έχει το ρητό σημείο $(x, y) = \left(\frac{a}{c}, \frac{b}{c}\right)$, όπου $a, b, c \in \mathbb{Z}$ και ο μέγιστος κοινός διαιρέτης των a, b, c είναι 1. Επομένως $a^2 + b^2 = 3c^2$. Παρατηρούμε ότι ούτε ο a ούτε ο b διαιρούνται με 3, γιατί αν ο 3 διαιρούσε τον a τότε ο 3 θα διαιρούσε τον b^2 άρα και τον b. Επομένως, οι a και b γράφονταν αντίστοιχα στην μορφή $3s$ και $3t$, δηλαδή $3^2s^2 + 3^2t^2 = 3c^2$ και επομένως ο 3 θα διαιρούσε τον c, δηλαδή ο 3 θα διαιρούσε τον $(a, b, c) = 1$, που είναι άτοπο. Άρα $a, b \equiv \pm 1 \pmod 3$, δηλαδή $a^2, b^2 \equiv 1 \pmod 3$, συνεπώς $a^2 + b^2 \equiv 2 \pmod 3$, άτοπο, διότι αν υπήρχε λύση θα είχαμε $a^2 + b^2 \equiv 0 \pmod 3$. □

Θέτουμε τώρα το πρόβλημα της ύπαρξης ενός ρητού σημείου.

Ο τρόπος που το κάναμε για την εξίσωση του κύκλου $x^2 + y^2 = 3$ μας δείχνει την μέθοδο στην γενική περίπτωση. Υπάρχει ένας αλγόριθμος που, σε πεπερασμένο πλήθος βημάτων, μας δίνει το αν μία **ρητή** κωνική τομή έχει τουλάχιστο ένα **ρητό** σημείο. Χρειάζεται να εξετασθεί αν πληρούται μία ισοδυναμία. Είναι το περίφημο θεώρημα του Legendre.

Θεώρημα 2 (Θεώρημα του Legendre) *Έστω a, b, c ακέραιοι, διάφοροι του μηδενός, των οποίων το γινόμενο abc δεν διαιρείται με το τετράγωνο πρώτου αριθμού. Υποθέτουμε ότι δεν είναι και οι τρείς ομόσημοι και ότι $(a, b) = (a, c) = (b, c) = 1$. Τότε η εξίσωση $ax^2+by^2+cz^2 = 0$ έχει μία μη-τετριμμένη* **ακέραια** *λύση αν και μόνο αν*

(i) $-abRc$

(ii) $-acRb$

(iii) $-bcRa$

όπου $-abRc$ σημαίνει ότι η ισοδυναμία $x^2 \equiv -ab \pmod{c}$ έχει λύση. (Δες [1].)

Το θεώρημα του Legendre είναι ειδική περίπτωση του **τοπικού-γενικού αξιώματος** (**Hasse**):

> **''Η τοπική επιλυσιμότητα μιάς εξίσωσης συνεπάγεται την γενική επιλυσιμότητα αυτής.''**

Τοπική επιλυσιμότητα σημαίνει ότι η εξίσωση έχει μία μη-τετριμμένη λύση $\pmod{p^m}$ για όλους τους πρώτους p και για όλους τους εκθέτες m και επιπλέον έχει μία πραγματική (δηλαδή μέσα στο σώμα των πραγματικών αριθμών $\mathbb{R}$) λύση.

Το τοπικό-γενικό αξίωμα του Hasse ισχύει για τετραγωνικές μορφές.

Για κυβικές καμπύλες δεν είναι γνωστή μέθοδος που να μας καθορίζει, σε πεπερασμένο αριθμό βημάτων, αν υπάρχει κάποιο ρητό σημείο πάνω σε δοθείσα κυβική καμπύλη. Φαίνεται ότι η απάντηση σ' αυτό το θέμα είναι ένα πολύ δύσκολο πρόβλημα.

Η ιδέα να εφαρμοστεί το τοπικό-γενικό αξίωμα δεν είναι σωστή γιατί το αξίωμα δεν ισχύει.

Στα 1950 ο Selmer έδωσε το παράδειγμα της καμπύλης

$$3X^3 + 4Y^3 + 5W^3 = 0$$

στην οποία η τοπική επιλυσιμότητα **δεν** συνεπάγεται την γενική επιλυσιμότητα αυτής.

Στα επόμενα θα **υποθέτουμε** ότι η κυβική καμπύλη που θεωρούμε **έχει πάντοτε ένα ρητό σημείο** $\mathcal{O}$.

3. Ρητά σημεία κυβικών καμπυλών και μία πρώτη μορφή του θεωρήματος του Mordell

Η γενική κυβική εξίσωση έχει τη μορφή:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Υποθέτουμε ότι είναι **ρητή**, δηλαδή ότι οι συντελεστές $a, b, c, d, e, f, g, i, j$ είναι ρητοί αριθμοί.

Το πιό απλό παράδειγμα κυβικής καμπύλης χωρίς ρητό σημείο είναι ίσως η καμπύλη $x^3 + y^3 = 1$. Η ύπαρξη ρητού σημείου στην καμπύλη $x^3 + y^3 = 1$ είναι ισοδύναμη με την ύπαρξη ακεραίου σημείου στην εξίσωση $X^3 + Y^3 = Z^3$. Το ότι η τελευταία εξίσωση δεν έχει, μη-τετριμμένη ακεραία λύση (Εικασία του Fermat για εκθέτη 3) είναι ήδη γνωστό.

Σκοπός μας είναι να περιγράψουμε τα ρητά σημεία ρητής κυβικής καμπύλης όταν μας δίνεται ένα ρητό σημείο αυτής.

Ξαναχρησιμοποιούμε το ίδιο γεωμετρικό αξίωμα θεωρώντας την τομή κωνικής τομής με ευθεία.

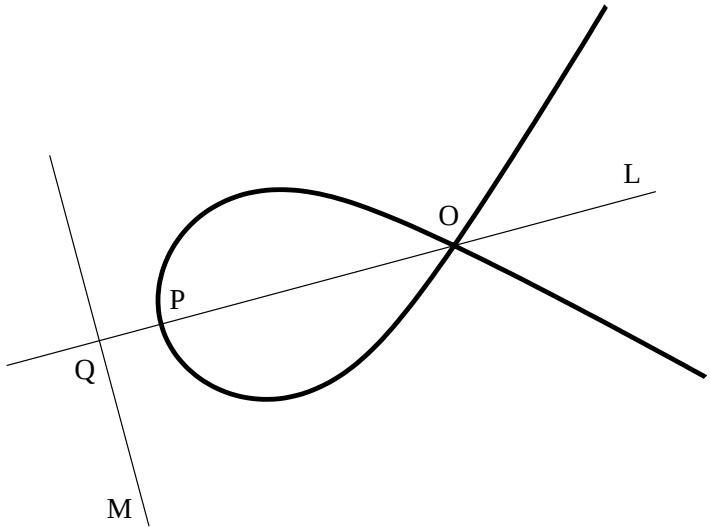
Κυβικές εξισώσεις μιάς μεταβλητής μπορούν να έχουν πολλαπλές ρίζες. Τι σημαίνει αυτό γεωμετρικά σαν σημείο τομής κυβικής καμπύλης και ευθείας;

Αφού η x-συνιστώσα του σημείου τομής πληροί μία κυβική εξίσωση ως προς x, έπεται ότι θα υπάρχουν τρία σημεία τομής. Εδώ δεν ισχύει ότι τα σημεία τομής ρητής κυβικής καμπύλης και ρητής ευθείας η οποία περνάει από ρητό σημείο της καμπύλης είναι επίσης ρητά. Ισχύει όμως ότι αν δύο από τα τρία σημεία τομής μιάς ρητής κυβικής καμπύλης με μία ρητή ευθεία είναι ρητά, τότε και το τρίτο είναι ρητό.

Ορισμός 3. *Έστω $\mathcal{C}$* **ανάγωγη** *(δεν αναλύεται σε γινόμενο πολυωνύμων μικρότερου βαθμού) κυβική καμπύλη. Ένα σημείο $\mathcal{O}$ αυτής θα λέγεται* **ιδιάζον** *(singular) όταν* **κάθε** *ευθεία που περνάει από το $\mathcal{O}$ τέμνει την $\mathcal{C}$ σε* **ακριβώς** *ένα ακόμη σημείο.*

Ας πάρουμε το παράδειγμα μιάς κυβικής καμπύλης που είναι **ιδιάζουσα**.
Η καμπύλη $y^2 = x^2(x + a)$, είναι ιδιάζουσα. Το $O = (0, 0)$ είναι ρητό και ιδιάζον σημείο αυτής.

Έστω L ρητή ευθεία που περνάει από το O και τέμνει την καμπύλη σε ακριβώς ένα σημείο, έστω P. Προφανώς το P επίσης ρητό σημείο της καμπύλης.
Έτσι, όπως και στις κωνικές τομές, προβάλλουμε την $\mathcal{C}$ σε κάποια **ρητή** ευθεία M τα ρητά



Σχήμα 1.3: Ιδιάζουσα καμπύλη

σημεία της οποίας αντιστοιχούν ένα προς ένα στα ρητά σημεία της καμπύλης τα διάφορα του O.

Έστω τώρα $\mathcal{C}$ **μη-ιδιάζουσα** (non-singular) ρητή κυβική καμπύλη. Δεν μπορούμε να χαρακτηρίσουμε τα ρητά σημεία αν μας δίνεται μόνο ένα ρητό σημείο.

Προσεγγίζουμε λοιπόν το θέμα μας αλλιώς. Παρατηρούμε ότι, αν βρούμε δύο ρητά σημεία πάνω στην καμπύλη, τότε βρίσκουμε και το τρίτο. Αρκεί να συνδέσουμε τα δύο σημεία με την ευθεία που ορίζουν. Το τρίτο σημείο θα είναι το τρίτο σημείο τομής της ευθείας αυτής με την κυβική καμπύλη

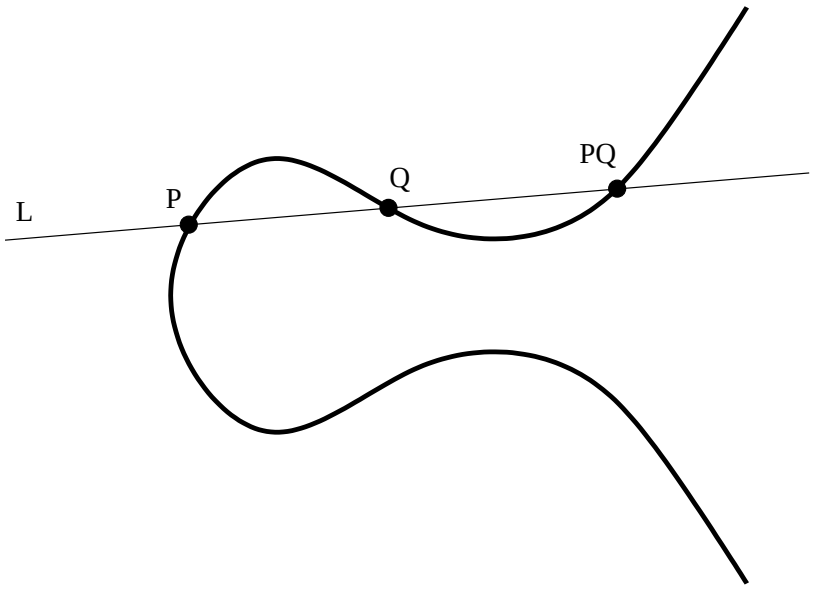
Προφανώς η ευθεία L είναι ρητή και τέμνει την καμπύλη σε ένα ακόμη σημείο, έστω PQ, που είναι επίσης **ρητό**. Αυτό είναι κάποιο «είδος» σύνθεσης δύο σημείων.

Ακόμη και ένα ρητό σημείο να έχει η καμπύλη, P, φέρνουμε την εφαπτομένη στο P και έχουμε ένα άλλο ρητό σημείο, το PP (δηλαδή συνδέουμε το P με τον εαυτό του). Ομοια το PP είναι επίσης ρητό.

Από λίγα λοιπόν ρητά σημεία παράγουμε πολλά.

Μία, κάπως γενική, αναφορά τώρα του περιεχομένου του θεωρήματος του Mordell (1921), είναι:

Σε μία **μη-ιδιάζουσα** (non singular) **ρητή** κυβική καμπύλη υπάρχει ένα **πεπερασμένο** σύνολο ρητών σημείων επί της καμπύλης τέτοιο ώστε **όλα τα ρητά σημεία** αυτής να παράγονται από



Σχήμα 1.4: κυβική καμπύλη

τα πεπερασμένου πλήθους, μέσω του παραπάνω **γεωμετρικού νόμου σύνθεσης**.

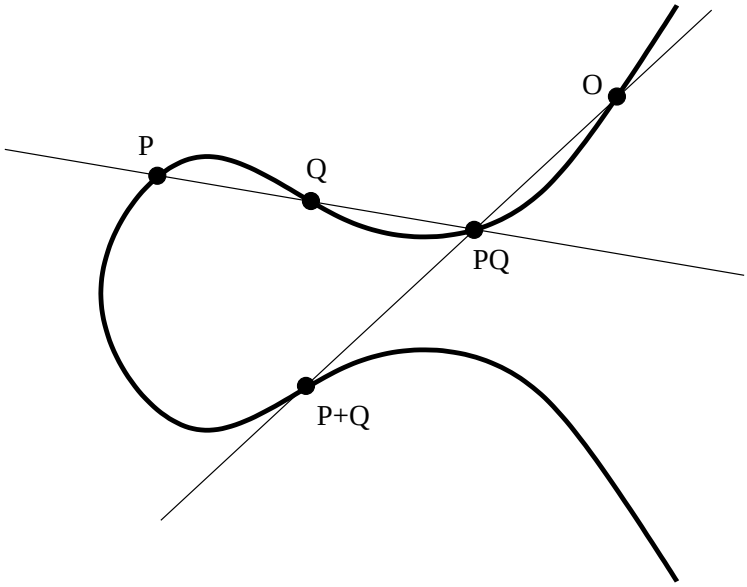
Ο νόμος αυτής της σύνθεσης λέγεται **μέθοδος της χορδής και της εφαπτομένης (chord-tangent)**. Δυστυχώς με τον παραπάνω τρόπο σύνθεσης, δεν μπορούμε να εφοδιάσουμε το σύνολο των ρητών σημείων της καμπύλης με κάποια δομή. Εύκολα βλέπουμε ότι δεν αποτελεί, παραδείγματος χάριν, ομάδα, διότι δεν υπάρχει ουδέτερο στοιχείο, O τέτοιο ώστε $OP = P$ για όλα τα P. Αυτό μπορούμε να το επιτύχουμε με κατάλληλη τροποποίηση της μεθόδου της χορδής και της εφαπτομένης.

Ορισμός 4. *Έστω O ένα ρητό σημείο της κυβικής καμπύλης. Αν P και Q δύο οποιαδήποτε ρητά σημεία αυτής τότε «άθροισμα» των P και Q ορίζεται να είναι το τρίτο σημείο τομής της ευθείας O, PQ με την καμπύλη, όπως στο σχήμα 1.5.*

Εύκολα διαπιστώνει κανείς ότι η παραπάνω ορισθείσα πρόσθεση είναι αντιμεταθετική, ότι το O είναι ουδέτερο στοιχείο ως προς την πρόσθεση

και ότι κάθε ρητό σημείο της καμπύλης έχει επίσης ρητό αντίθετο (Η ευθεία O, OO είναι εφαπτόμενη της κυβικής καμπύλης στο O).

Ο **προσεταιρισμός** είναι δύσκολος και θα γίνει στο επόμενο κεφάλαιο.



Σχήμα 1.5: Άθροισμα δύο σημείων κυβικής καμπύλης

Σημείωση 5. *Αν* P, Q, R *τρία σημεία πάνω σε μία ευθεία τότε* $P + Q + R = 0$.

Ορισμός 6. *Μία* **ελλειπτική** *καμπύλη είναι μία μη-ιδιάζουσα (non-singular) κυβική καμπύλη με συντελεστές ακεραίους αριθμούς η οποία έχει ένα ρητό σημείο (ουδέτερο στοιχείο) και είναι εφοδιασμένη με την παραπάνω πράξη ομάδας.*

Θεώρημα 7 (Θεώρημα του Mordell) *Η ομάδα των ρητών σημείων μιάς ρητής ελλειπτικής καμπύλης είναι πεπερασμένα παραγόμενη αβελιανή ομάδα.*

Η απόδειξη του θεωρήματος είναι ο κύριος σκοπός αυτού εδώ του βιβλίου.

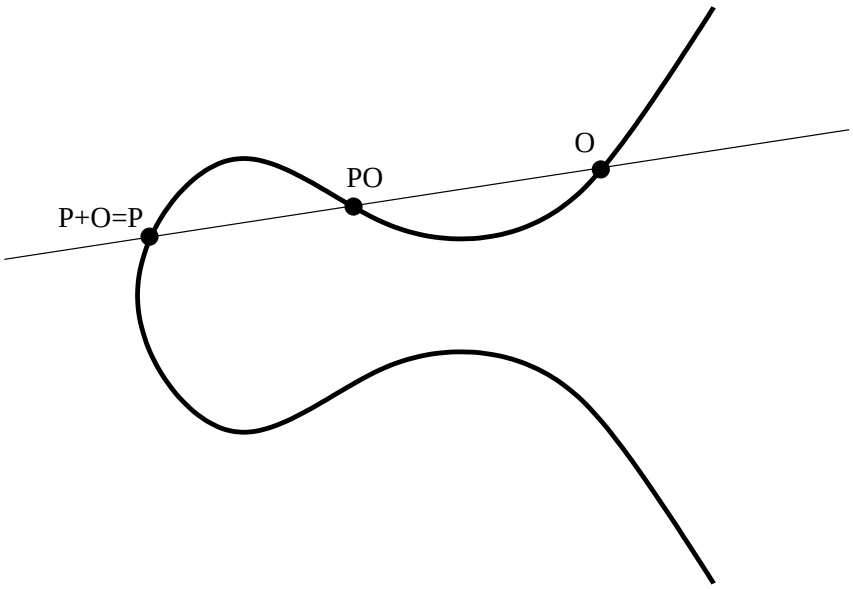
4. Παραδείγματα

(α′) Το γινόμενο τριών διαδοχικών ακεραίων είναι ίσο με το γινόμενο δύο άλλων διαδοχικών ακεραίων.

Η εξίσωση που σχηματίζουμε είναι

$$y(y+1) = x(x-1)(x+1), \quad \text{δηλαδή} \quad y^2 + y = x^3 - x.$$

Προφανώς το σημείο $A = (0, 0)$ είναι ένα ρητό σημείο αυτής.



Σχήμα 1.6: Ουδέτερο ρητό στοιχείο κυβικής καμπύλης

Θεωρούμε το «επ΄ άπειρο» σημείο της καμπύλης σαν ουδέτερο στοιχείο και με την μέθοδο της χορδής και της εφαπτομένης κατασκευάζουμε και άλλα ρητά σημεία αυτής.

Παρατηρούμε ότι αν $P = (x, y)$ τότε $-P = (x, -1 - y)$.

Σημείωση: Μπορεί να αποδείξει κανείς ότι η ομάδα των ρητών σημείων είναι άπειρη, παραγόμενη από το $A = (0, 0)$.

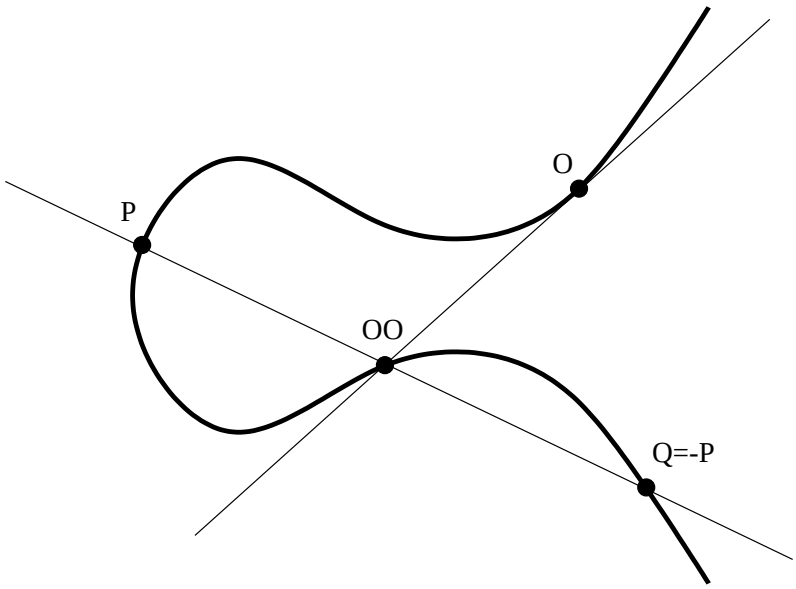
(β΄) Θεωρούμε την ελλειπτική καμπύλη $y^2 + y = x^3 - x^2$.
Προφανώς το σημείο $P = (1, 0)$ είναι ρητό σημείο αυτής.

Παρατηρούμε ότι $5P = \mathcal{O}$, το «επ΄ άπειρο» σημείο αυτής. Η ομάδα των ρητών σημείων της καμπύλης είναι πεπερασμένη και μάλιστα κυκλική τάξης 5.

(γ΄) Η ερώτηση, πότε ο $y^2 + k$ είναι τέλειος κύβος είναι πολύ παλιά και έχει τις ρίζες της στο έργο του Διόφαντου.
Εδώ το πρόβλημά μας είναι η εύρεση ακεραίων λύσεων της $y^2 = x^3 + k$.

(δ΄) Θεωρούμε την ελλειπτική καμπύλη

$$9y^2 = x^3 - 25x.$$



Σχήμα 1.7: Αντίθετα ρητά σημεία κυβικής καμπύλης

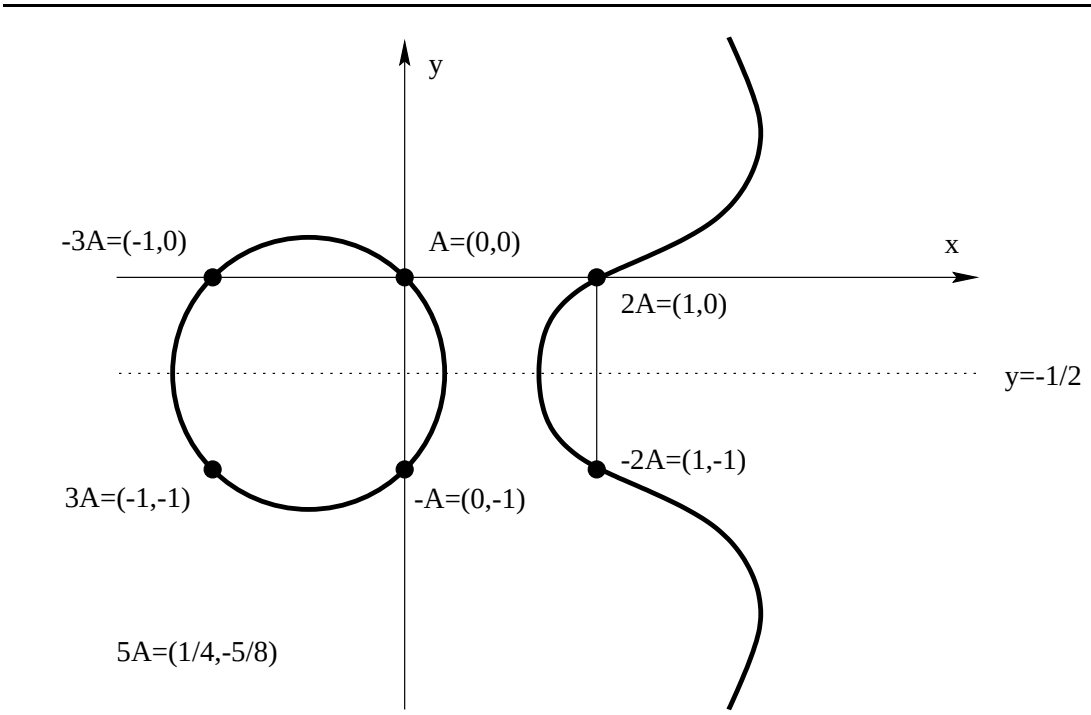
Το σημείο $P = (-4, -2)$ είναι ένα ρητό σημείο της καμπύλης. Υπολογίζουμε το $2P$, (το πως θα το δούμε αργότερα), και βρίσκουμε σχετικά μεγάλους ρητούς αριθμούς σαν συνιστώσες.

(ε′) **Διοφάντου Αριθμητικά**, άσκηση 14, Βιβλίο IV:
Δίνεται ακέραιος αριθμός, π.χ. ο 6. Να αναλυθεί σε δύο μέρη, ώστε το γινόμενό τους να είναι κάποιος κύβος ρητού αριθμού x μείον τον αριθμό x.
Ουσιαστικά ζητούμε να βρούμε ρητές λύσεις της ελλειπτικής καμπύλης $y(6-y) = x^3 - x$. Έστω $x = ky - 1$, π.χ. $x = 2y - 1$. Τότε $6y - y^2 = 8y^3 - 12y^2 + 4y$. Η τελευταία θα ήταν **επιλύσιμη** στους ρητούς αν 6 ήταν ίσο με το 4. Το 6 υπάρχει στην εξίσωση και το 4 προκύπτει από τον συντελεστή της $x = 2y - 1$. Γράφουμε $x = 3y - 1$ και βρίσκουμε

$$6y - y^2 = 27y^3 - 27y^2 + 6y, \quad \text{δηλαδή} \quad y = \frac{26}{27},\ x = \frac{17}{9}.$$

5. Ακέραια σημεία σε καμπύλες

Μερικές φορές ζητούμε ακέραια σημεία. Όπως θα δούμε αργότερα, όλα τα σημεία πεπερασμένης τάξης της ομάδας των ρητών σημείων δοθείσης ελλειπτικής καμπύλης έχουν ακέραιες



Σχήμα 1.8: Παράδειγμα πρόσθεσης ρητών σημείων

συντεταγμένες. Θα πρέπει βέβαια εδώ να επισημάνουμε ότι **δεν** ισχύει το αντίστροφο.

Παράδειγμα: Έστω η ελλειπτική καμπύλη $y^2 + k = x^3$.

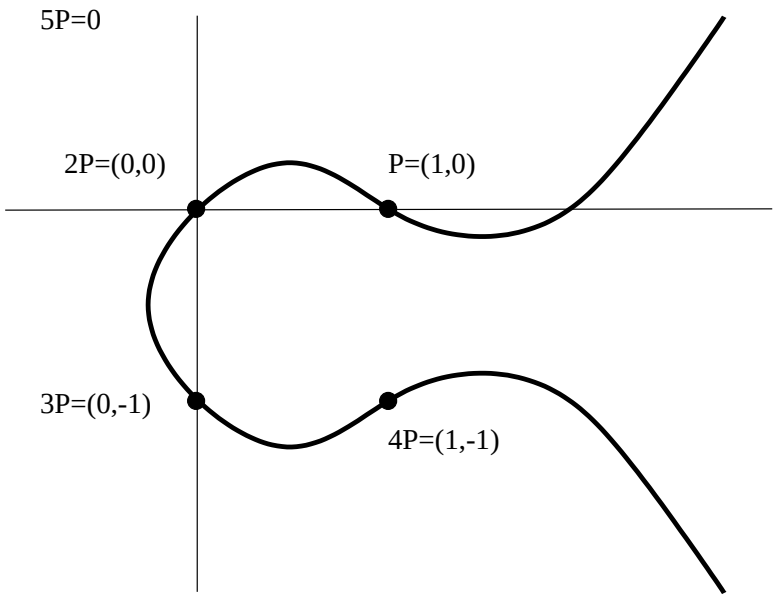
Για $k = 2$, οι μόνες λύσεις είναι όταν $(y = \pm 5, x = 3)$.

Το πρόβλημα αυτό ανάγεται πίσω στον Διόφαντο και λύθηκε από τον Bachet στα 1621. Η παραπάνω εξίσωση γράφεται υπό την μορφή

$$(y + \sqrt{-k})(y - \sqrt{-k}) = x^3,$$

όπου x και y πρέπει να είναι και οι δύο περιττοί για να ισχύει η εξίσωση modulo 4.
Αν p πρώτος που διαιρεί τον x, τότε ο p^3 θα διαιρεί το γινόμενο $(y + \sqrt{-2})(y - \sqrt{-2})$ (για $k = 2$). Αν ο p διαιρεί το $y + \sqrt{-2}$ και το $y - \sqrt{-2}$ τότε ο p διαιρεί το $2y$ και επειδή $p \neq 2$ έπεται ότι ο p διαιρεί το y, επομένως θα διαιρεί το $-y^2 + x^3 = 2$ που είναι άτοπο.
Άρα ο μέγιστος κοινός διαιρέτης των $y + \sqrt{-2}$, $y - \sqrt{-2}$ στον δακτύλιο $\mathbb{Z}[\sqrt{-2}]$ είναι 1. Συνεπώς ο $y + \sqrt{-2}$, γράφεται

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3,$$



$$E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$$

Σχήμα 1.9: Παράδειγμα πρόσθεσης ρητών σημείων

δηλαδή

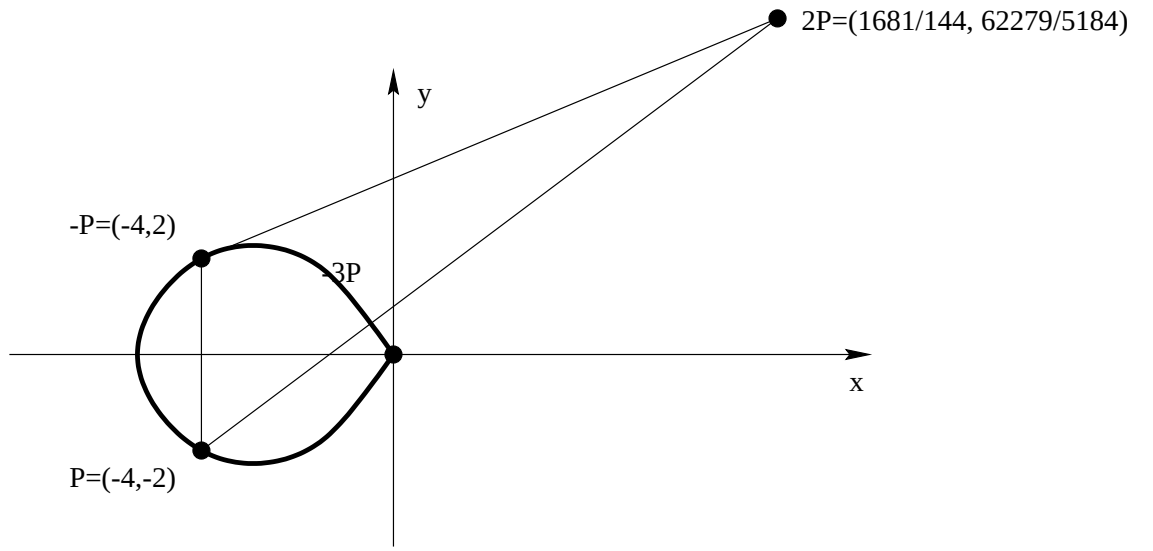
$$y = a^3 - 6ab^2 = a(a^2 - 6b^2) \quad \text{και} \quad 1 = b(3a^2 - 2b^2).$$

Επομένως, $b = \pm 1$ οπότε $a = \pm 1$. Συνεπώς $y = \pm 5$ και $x = 3$. Οι A. Baker και J. Coates απέδειξαν ότι αν (x, y) ακέραια λύση της $y^2 + k = x^3$, τότε ισχύει:

$$\max(|x|, |y|) \leq \exp(2^{7 \cdot 2^4} k^{109 \cdot 23}).$$

Το φράγμα αυτό έχει καλυτερεύσει αρκετά τα τελευταία χρόνια, συνεχίζει όμως να είναι αρκετά μεγάλο για να είμαστε σε θέση να καλύψουμε με ηλεκτρονικό υπολογιστή τον έλεγχο επιλυσιμότητας για όλες τις ενδιάμεσες τιμές.

Γενικά για πολυωνυμικές εξισώσεις $f(x, y) = 0$ με ρητούς συντελεστές, παίρνουμε το γράφημά τους και προσθέτουμε μερικά σημεία (πεπερασμένου πλήθους). Κατασκευάζουμε έτσι μία συμπαγή **πολλαπλότητα** (manifold) $\mathcal{X}_f$ όπου οι μερικές παράγωγοι $D_x f$ και $D_y f$ δεν μηδενίζονται συγχρόνως επί της $f(x, y) = 0$. Τοπολογικά το σύνολο των μιγαδικών σημείων της $\mathcal{X}_f$ είναι μία κλειστή προσανατολισμένη επιφάνεια με g τρύπες.



Σχήμα 1.10: Παράδειγμα πρόσθεσης ρητών σημείων

Η αναλλοίωτη αυτή g της καμπύλης λέγεται **γένος** της καμπύλης. Ευθείες και κωνικές τομές έχουν γένος 0, ενώ οι μη-ιδιάζουσες κυβικές έχουν γένος $g = 1$.

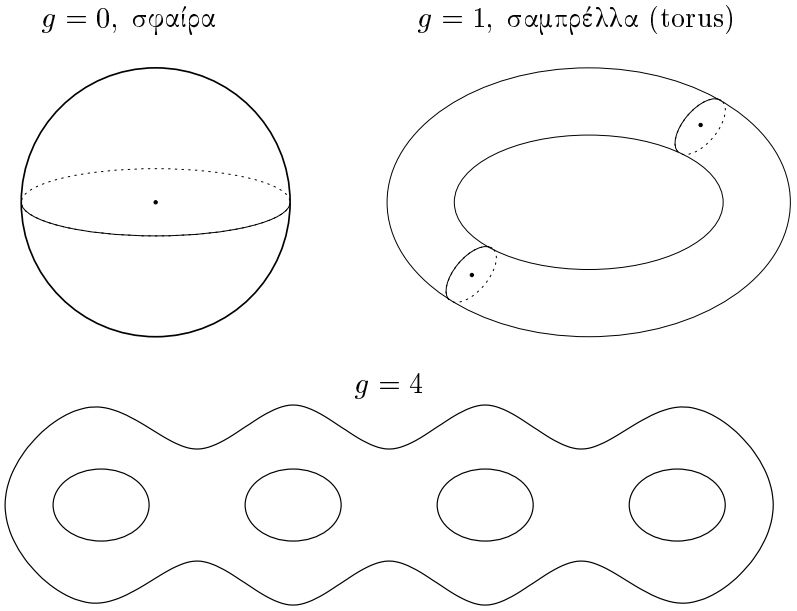
Θεώρημα 8 (Θεώρημα του Seigel) *Τα* **ακέραια** *σημεία της μη-ιδιάζουσας (non-singular) καμπύλης* $f(x, y) = 0$, *γένους* $g \geq 1$ *είναι* **πεπερασμένου πλήθους**.

Αυτό ισχύει φυσικά για μη-ιδιάζουσε κυβικές, δεν ισχύει όμως για ιδιάζουσες κυβικές καμπύλες. Η καμπύλη $y^2 = x^3$ έχει, προφανώς, τις, άπειρες στο πλήθος, λύσεις $(x, y) = (n^2, n^3)$, $n \in \mathbb{N}$.

6. Αλγεβρικά σώματα αριθμών και η αριθμητική των ελλειπτικών καμπυλών

Η μελέτη της εύρεσης των ακεραίων σημείων της κωνικής τομής $x^2 - Ay^2 = \pm 1$, για A θετικό και όχι τέλειο τετράγωνο, έχει παίξει πολύ σημαντικό ρόλο στην ανάπτυξη της Θεωρίας των Αριθμών. Είναι μία εξίσωση, η λεγόμενη εξίσωση του Pell, και η καμπύλη που ορίζει έχει άπειρα στο πλήθος ακέραια σημεία.

Μελετούμε τον δακτύλιο $\mathbb{Z}[\sqrt{A}]$ σαν υποδακτύλιο του σώματος $\mathbb{Q}(\sqrt{A})$.
Για $u = x + y\sqrt{A} \in \mathbb{Z}[\sqrt{A}]$ ορίζουμε $\bar{u} = x - \sqrt{A}$ και την $norm$ του u, $N(u) = u\bar{u} =$



Σχήμα 1.11: Γένος καμπύλης

$x^2 - y^2A$. Η norm είναι μία πολλαπλασιαστική συνάρτηση από το $\mathbb{Z}[\sqrt{A}]$ στο $\mathbb{Z}$. Δηλαδή η εξίσωση του Pell γράφεται

$$\pm 1 = N(u) = u\bar{u} = x^2 - Ay^2.$$

Οι ακέραιες λύσεις της εξίσωσης του Pell βρίσκονται σε αμφιμονότιμη αντιστοιχία με την ομάδα των μονάδων του δακτυλίου $\mathbb{Z}[\sqrt{A}]$.

Γενικά, υπάρχει μία αναλογία μεταξύ της

1) ομάδας των ρητών σημείων ελλειπτικής καμπύλης E και

2) της ομάδας των μονάδων $U(F)$ αλγεβρικού σώματος αριθμών F.

Και οι δύο είναι **πεπερασμένα παραγόμενες** των οποίων οι υποομάδες των σημείων πεπερασμένης τάξης είναι γνωστές αρκετά καλά. Αργότερα θα μελετήσουμε τα σημεία πεπερασμένης τάξης ελλειπτικής καμπύλης. Στα σώματα αριθμών το torsion τμήμα (στοιχεία πεπερασμένης τάξης) της ομάδας των μονάδων είναι οι ρίζες της μονάδας.

Το ερώτημα για τον βαθμό (rank) αυτών των ομάδων και την εύρεση ελεύθερων γεννητόρων οδηγεί σε πολλά άλυτα προβλήματα.

Για τα σώματα αριθμών $r = r_1 + r_2 - 1$ είναι ο βαθμός (rank) όπου $[F : \mathbb{Q}] = r_1 + 2r_2$. Το πρόβλημα της κατασκευής ελευθέρων γεννητόρων για την ${}^{U(F)}\!/_{U(F)_{\text{torsion}}}$ είναι δύσκολο πρόβλημα. Αν $F = \mathbb{Q}(\sqrt{A})$ με $A > 0$ το πρόβλημα ξαναγυρίζει πίσω στην εξίσωση του Pell.

Στις ελλειπτικές καμπύλες ακόμα και η εύρεση του βαθμού (rank) της ομάδας ρητών σημείων είναι πολύ δύσκολο πρόβλημα.

Κεφάλαιο 2

Επίπεδες αλγεβρικές καμπύλες

Στο προηγούμενο κεφάλαιο περιγράψαμε την πρόσθεση ρητών σημείων κυβικών καμπυλών μέσω των ''ιδιοτήτων τομής'' αυτών. Χρησιμοποιήσαμε ιδιότητες τομής, χωρίς να τις αποδείξουμε, όπως ότι δύο διακεκριμένες μεταξύ τους ευθείες τέμνονται σε **ακριβώς** ένα σημείο ή ότι μία ευθεία και μία κυβική καμπύλη τέμνονται πάντοτε σε τρία **ακριβώς** σημεία. Οι ιδιότητες αυτές ισχύουν μόνο εφ' όσον εργαζόμαστε στον προβολικό και όχι στον αφινικό χώρο.

Σκοπός του παρόντος κεφαλαίου είναι η μελέτη των ιδιοτήτων τομής επιπέδων αλγεβρικών καμπυλών. Ειδική περίπτωση αποτελούν οι κυβικές καμπύλες. Ιδιαίτερα χρήσιμο είναι το αποτέλεσμα ότι δύο επίπεδες κυβικές καμπύλες τέμνονται σε ακριβώς 9 σημεία. Το αποτέλεσμα αυτό είναι χρήσιμο για την απόδειξη της προσεταιριστικής ιδιότητας της πρόσθεσης ρητών σημείων.

1. Απαλείφουσα δύο πολυωνύμων

Η μελέτη της παρούσης παραγράφου προϋποθέτει τη γνώση στοιχείων θεωρίας δακτυλίων και θεωρίας σωμάτων. Για να διευκολύνουμε τον αναγνώστη έχουμε προσθέσει, στο τέλος του παρόντος βιβλίου, ένα παράρτημα με αντίστοιχο περιεχόμενο.

Κατ' αρχάς αποδεικνύουμε την ακόλουθη

Πρόταση 1. *Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες*

(1) Το σώμα K είναι αλγεβρικά κλειστό.

(2) Κάθε πολυώνυμο $f(x) \in K[x]$ με $\deg f(x) > 0$ αναλύεται στο K σε γινόμενο γραμμικών παραγόντων.

(3) Κάθε ανάγωγο πολυώνυμο $f(x) \in K[x]$ *με* $\deg f(x) > 0$ *είναι γραμμικό.*

(4) Αν L/K *είναι αλγεβρική επέκταση τότε, κατ' ανάγκη,* $L = K$.

Απόδειξη: (1)⇒(2): Αφού K αλγεβρικά κλειστό, έπεται ότι το $f(x)$ έχει μία ρίζα στο K, έστω a. Το $f(x)$ επομένως γράφεται $f(x) = (x-a)g(x)$, όπου $g(x) \in K[x]$. Αν $\deg g(x) > 0$, επαναλαμβάνουμε την ίδια διαδικασία για το $g(x)$ και συνεχίζουμε επαγωγικά.
(2)⇒(3): Προφανές.
(3)⇒(4): Έστω L/K μία αλγεβρική επέκταση και a οποιοδήποτε στοιχείο του L. Τότε το a είναι αλγεβρικό υπέρ του K. Αν $f(x)$ είναι το ανάγωγο πολυώνυμο του a υπεράνω του K τότε, λόγω της υπόθεσης (3), το $f(x)$ θα είναι της μορφής $f(x) = x - a \in K[x]$, δηλαδή $a \in K$. Αυτό σημαίνει ότι $L \subseteq K$ και επομένως $L = K$.
(4)⇒(1): Έστω $f(x) \in K[x]$ με $\deg f(x) > 0$. Σύμφωνα με γνωστή πρόταση (βλέπε παράρτημα), υπάρχει επέκταση L/K στην οποία το $f(x)$ έχει μία ρίζα, έστω a. Η επέκταση $K(a)/K$ είναι πεπερασμένη, συνεπώς είναι αλγεβρική και, λόγω της υπόθεσης (4), $K(a) = K$, δηλαδή $a \in K$. Επομένως το $f(x)$ έχει τουλάχιστο μία ρίζα στο K δηλαδή αποδείξαμε την (1). □

Αποδεικνύουμε τώρα την παρακάτω

Πρόταση 2. *Κάθε αλγεβρικά κλειστό σώμα περιέχει* **άπειρο** *πλήθος στοιχείων.*

Απόδειξη: 1η περίπτωση: Υποθέτουμε ότι η χαρακτηριστική του σώματος K είναι μηδέν. Επομένως υπάρχει ένας μονομορφισμός $\varphi : \mathbb{Q} \to K$, δηλαδή το $\varphi(\mathbb{Q})$ περιέχεται ισόμορφα μέσα στο K. Το $\mathbb{Q}$ όμως έχει άπειρο πλήθος στοιχείων, άρα και το K.
2η περίπτωση: Έστω ότι η χαρακτηριστική του σώματος K είναι p, όπου p πρώτος αριθμός. Τότε το K περιέχει ισόμορφα το **πρώτο σώμα** $\mathbb{F}_p = \mathbb{Z}/(p)$ των κλάσεων υπολοίπων $(\mathrm{mod} p)$. Αν το K είχε πεπερασμένου πλήθους στοιχεία τότε ο βαθμός της επέκτασης $K/\mathbb{F}_p$ θα ήταν πεπερασμένος, έστω m, οπότε το K θα είχε p^m στοιχεία. Τότε όμως η επέκταση του K $L = K(a)$ όπου a ρίζα του $x^{p^{m+1}} - x$ είναι πεπερασμένη και επομένως αλγεβρική. Επειδή το a δεν είναι ρίζα του πολυωνύμου $x^{p^m} - x$, έπεται ότι $L \supsetneq K$ το οποίο είναι άτοπο διότι το σώμα K είναι αλγεβρικά κλειστό. Επομένως το K είναι άπειρο. □

Από εδώ και μέχρι το τέλος της παραγράφου με R θα συμβολίζουμε οποιοδήποτε δακτύλιο μονοσήμαντης ανάλυσης.

Ορισμός 3. *Η* **απαλείφουσα** *δύο πολυωνύμων*

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \ (a_m \neq 0) \quad \textit{και} \quad g(x) = b_0 + b_1 x + \cdots + b_n x^n \ (b_n \neq 0)$$

με συντελεστές από τον δακτύλιο $R[x]$, *ορίζεται σαν η ορίζουσα του* $(m+n)\times(m+n)$ *πίνακα*

$$[R(f,g)] = \begin{pmatrix} a_0 & a_1 & \dots & a_m & 0 & \dots\dots & 0 \\ 0 & a_0 & \dots & a_{m-1} & a_m & \dots\dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_0 & a_1 & \dots\dots & a_m \\ b_0 & b_1 & \dots & b_{n-1} & b_n & 0 \ \dots & 0 \\ 0 & b_0 & \dots\dots & b_{n-1} & b_n & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & b_0 & b_1 & \dots\dots & \dots & b_n \end{pmatrix}.$$

Συμβολισμός: $R(f,g) := det([R(f,g)])$.

Ορισμός 4. *Η* **διακρίνουσα** $D(f)$ *ενός πολυωνύμου* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *ορίζεται από τη σχέση*

$$R(f,f') = (-1)^{\frac{n(n-1)}{2}} a_n D(f),$$

όπου f' *είναι η παράγωγος του* f.

Άσκηση: Υπολογίστε την διακρίνουσα των πολυωνύμων ax^2+bx+c και x^3+px+q.

Πρόταση 5. *Έστω* $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$, $a_n \neq 0$ *και* $g(x) = b_0 + b_1 x + \cdots + b_m x^m \in R[x]$, $b_m \neq 0$, *όπου* R *δακτύλιος μονοσήμαντης ανάλυσης. Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες:*

(1) Τα πολυώνυμα f *και* g *έχουν κοινό παράγοντα διάφορο σταθεράς,*

(2) $R(f,g) = 0$.

Απόδειξη: Χρησιμοποιούμε το παρακάτω:

Λήμμα 6. *Ισχύουν ισοδύναμα*

(α′) Το (1) της πρότασης 5

(β′) Υπάρχουν μη μηδενικά πολυώνυμα φ *και* ψ *βαθμού μικρότερου από* n *και* m *αντίστοιχα, έτσι ώστε* $\psi f = \varphi g$.

Απόδειξη: "$\Rightarrow$":

Έστω $f = h\varphi,\ g = h\psi$. Τότε $fg = fg$, δηλαδή $fh\psi = h\varphi g$ και επομένως $f\psi = \varphi g$. Αφού $\deg h > 0$ έπεται ότι $\deg\varphi < n$ και $\deg\psi < m$.

"$\Leftarrow$": Έστω ότι $\psi f = \varphi g$. Αναλύουμε το g σε γινόμενο πρώτων παραγόντων. Οι διάφοροι σταθεράς παράγοντες του g, ή οι συνεταιρικοί τους, περιέχονται στους πρώτους παράγοντες του ψf. Όμως δεν μπορούν να εμφανίζονται όλοι σαν παράγοντες του ψ διότι $\deg\psi < \deg g$. Συνεπώς υπάρχει τουλάχιστο ένας **πρώτος παράγοντας** του g που είναι και παράγοντας του f. Άρα $g = hg'$ και $f = hf'$. □

Απόδειξη της πρότασης 5: $\Longrightarrow$: Από το λήμμα έχουμε $\psi f = \varphi g$. Έστω

$$\varphi(x) = \alpha_1 + \alpha_2 x + \cdots + \alpha_n x^{n-1} \in R[x] \text{ και } \psi(x) = \beta_1 + \beta_2 x + \cdots + \beta_m x^{m-1} \in R[x]$$

όπου ένα τουλάχιστο $\alpha_i \neq 0$ και ένα τουλάχιστο $\beta_j \neq 0$.

Η εξίσωση $\psi f = \varphi g$ τότε γράφεται

$$\left\{\begin{array}{rcl} a_0\beta_1 & = & b_0\alpha_1 \\ a_1\beta_1 + a_0\beta_2 & = & b_1\alpha_1 + b_0\alpha_2 \\ \cdots\cdots\cdots\cdots\cdots & & \\ a_n\beta_m & = & b_m\alpha_n \end{array}\right\} \ (1).$$

Έχουμε δηλαδή ένα ομογενές και γραμμικό σύστημα ως προς τις $(n+m)$-μεταβλητές

$$\beta_1,\ \beta_2,\ \ldots,\ \beta_m,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n$$

τό οποίο έχει **μη-τετριμμένη** λύση. Συνεπώς η ορίζουσα των συντελεστών πρέπει να είναι 0. Άρα $R(f,g) = 0$.

$\Longleftarrow$: Αν $R(f,g) = 0$ τότε το σύστημα (1) έχει **μη-τεριμμένη** λύση στο σώμα πηλίκων F του R. Πολλαπλασιάζουμε με τον κοινό παρονομαστή όλων των όρων των εξισώσεων του συστήματος και σχηματίζουμε σύστημα στον R που έχει τουλάχιστο ένα από τα α_i, ή ένα από τα β_j διάφορο του μηδενός. Αν $\alpha_i \neq 0$, τότε $\varphi \neq 0$ οπότε, από τη σχέση $f\psi = g\varphi$, έπεται ότι και $\psi \neq 0$ και το ζητούμενο προκύπτει από το παραπάνω λήμμα. □

Ορισμός 7. *Αν $f(x_0, x_1, \cdots, x_n) \in R[x_0, x_1, \cdots, x_n]$ ομογενές πολυώνυμο βαθμού d τέτοιο ώστε το x_0 να μην διαιρεί το f, τότε το πολυώνυμο*

$$g(x_1, x_2, \cdots, x_n) := f(1, x_1, x_2, \cdots, x_n)$$

θα λέγεται **συνεταιρικό** *του f. Προφανώς $\deg g = d$.*

Πρόταση 8. *Κάθε παράγοντας ομογενούς πολυωνύμου*

$$f(x_0, x_1, \cdots, x_n) \in R[x_0, x_1, \ldots, x_n]$$

είναι ομογενές πολυώνυμο.

Απόδειξη: Ας υποθέσουμε ότι το f αναλύεται σε γινόμενο $f = h_1 h_2$ και ότι το h_1 δεν είναι ομογενές. Αναλύουμε τα h_1 και h_2 σε αθροίσματα ομογενών

$$h_1 = H_i + H_{i+1} + \cdots + H_{i+j},\ H_i \neq 0,\ H_{i+j} \neq 0,\ j > 0.$$

$$h_2 = H'_k + H'_{k+1} + \cdots + H'_{k+l},\ H'_k \neq 0,\ H'_{k+l} \neq 0,\ l \geq 0.$$

Τότε

$$f = h_1 h_2 = H_i H'_k + (H_{i+1} H'_k + H_i H'_{k+1}) + \cdots + H_{i+j} H'_{k+l},$$

$$H_i H'_k \neq 0 \quad \text{και} \quad H_{i+j} H'_{k+l} \neq 0.$$

$$\text{Αλλά} \quad \deg H_i H'_k = i + k < i + j + k + l = \deg H_{i+j} H'_{k+l}.$$

Επομένως, αν κάποιος παράγοντας του f δεν είναι ομογενές πολυώνυμο τότε και το f δεν θα ήταν ομογενές, άτοπο. □

Άμεση συνέπεια της πρότασης 8 είναι το

Πόρισμα 9. *Αν f και g είναι συνεταιρικά πολυώνυμα τότε κάθε παράγοντας του f είναι συνεταιρικός με κάποιο παράγοντα του g και αντιστρόφως.*
Ειδικά: Το f είναι ανάγωγο αν και μόνο αν το g είναι ανάγωγο.

Πρόταση 10. *Τα ομογενή πολυώνυμα*

$$F_1(x_0, x_1) = a_0 x_0^n + a_1 x_0^{n-1} x_1 + \cdots + a_n x_1^n \in R[x_0, x_1]$$

$$F_2(x_0, x_1) = b_0 x_0^m + b_1 x_0^{m-1} x_1 + \cdots + b_m x_1^m \in R[x_0, x_1]$$

έχουν κοινό παράγοντα διάφορο σταθεράς ακριβώς τότε όταν η απαλείφουσα $R(F_1, F_2) = 0$.

Απόδειξη: Αν $a_n = b_m = 0$ τότε $R(F_1, F_2) = 0$. Επειδή λοιπόν η τελευταία στήλη του πίνακα της απαλείφουσας θα έχει όλο μηδενικά, έπεται ότι τα F_1 και F_2 θα έχουν κοινό παράγοντα το x_0.
Αν $a_n b_m \neq 0$ παίρνουμε τα συνεταιρικά τους g_1 και g_2. Η πρόταση 5 και το πόρισμα 9 μας

δίνουν και σ΄ αυτή την περίπτωση την ζητούμενη ισοδυναμία.

Αν τώρα $a_n = 0$ και $b_m \neq 0$ τότε $F_1(x_0, x_1) = x_0^r F_1^*(x_0, x_1)$, όπου το x_0 δεν διαιρεί το F_1^*. Εφαρμόζουμε ξανά την πρόταση 5 και το πόρισμα II.1.9 για τα F_1^* και F_2 και έχουμε ότι τα F_1^* και F_2 έχουν κοινό παράγοντα διάφορο σταθεράς ακριβώς τότε όταν $R(F_1^*, F_2) = 0$. Παρατηρούμε ότι $R(F_1, F_2) = \pm b_m^r R(F_1^*, F_2)$ και συνεπώς ξανά προκύπτει το ζητούμενο.

Όμοια να $a_n \neq 0$ και $b_m = 0$. □

Πρόταση 11. *Αν K αλγεβρικά κλειστό σώμα και $f(x_0, x_1) \in K[x_0, x_1]$ ομογενές πολυώνυμο βαθμού d, τότε υπάρχουν d ζευγάρια σταθερών $a_i, b_i \in K$ τέτοια ώστε*

$$f(x_0, x_1) = \alpha \prod (a_i x_1 - b_i x_0), \quad \alpha \neq 0.$$

Κάθε ζευγάρι είναι μοναδικό με την έννοια ότι ταυτίζουμε το (a_i, b_i) με το (ca_i, cb_i), όπου $c \in K^*$.

Απόδειξη: Επειδή το $f(x_0, x_1)$ είναι ομογενές πολυώνυμο βαθμού d, γράφεται στην μορφή $f(x_0, x_1) = x_0^r f^*(x_0, x_1)$ όπου $f^*(x_0, x_1)$ ομογενές πολυώνυμο βαθμού $d - r$ και $x_0 \nmid f^*$. Το πολυώνυμο $f^*(1, x_1)$ είναι πολυώνυμο μιάς μεταβλητής βαθμού $d - r$ ως προς x_1 και, αφού K αλγεβρικά κλειστό, $f^*(1, x_1) = \alpha \prod_{j=1}^{d-r} (x_1 - b_j)$. Επομένως

$$f^*(x_0, x_1) = \alpha \prod_{j=1}^{d-r} (x_1 - b_j x_0)$$

οπότε

$$f(x_0, x_1) \;=\; x_0^r f^*(x_0, x_1) \;=\; \alpha \prod_{j=1}^{d} (a_j x_1 - b_j x_0).$$

Η μοναδικότητα είναι αποτέλεσμα του μονοσήμαντου της ανάλυσης. □

Θεώρημα 12. *Έστω*

$$F_n(x_1, x_2, \cdots, x_{r-1}, x_r) = A_n + A_{n-1} x_r + \cdots + A_0 x_r^n \quad \textit{και}$$

$$G_m(x_1, x_2, \cdots, x_{r-1}, x_r) = B_m + B_{m-1} x_r + \cdots + B_0 x_r^m$$

*όπου A_i, B_i, **ομογενή** πολυώνυμα βαθμού i ως προς τις μεταβλητές $x_1, x_2, \cdots, x_{r-1}$ και $A_0 B_0 \neq 0$. Αν $R(x_1, x_2, \cdots, x_{r-1})$ είναι η **απαλείφουσα** των F_n και G_m ως προς x_r τότε*

$$\textit{ή} \;\; R(x_1, x_2, \cdots, x_{r-1}) = 0 \;\; \textit{ή}$$

$$R(x_1, x_2, \cdots, x_{r-1}) \;\; \textit{είναι ομογενές πολυώνυμο βαθμού} \;\; nm.$$

Απόδειξη: Υπολογίζουμε την απαλείφουσα

$$R(tx_1, tx_2, \cdots, tx_{r-1}) = \begin{pmatrix} t^nA_n & t^{n-1}A_{n-1} & \ldots\ldots & A_0 & & \\ & t^nA_n & \ldots\ldots\ldots & A_0 & & \\ & & \ldots\ldots\ldots\ldots & & & \\ & & t^nA_n & \ldots\ldots\ldots & A_0 & \\ t^mB_m & t^{m-1}B_m & \ldots\ldots & tB_1 & B_0 & \\ & t^mB_m & \ldots\ldots\ldots & tB_1 & B_0 & \\ & & \ldots\ldots\ldots\ldots\ldots & & & \\ & & t^mA_m & \ldots\ldots\ldots\ldots & & B_0 \end{pmatrix}.$$

Πολλαπλασιάζουμε την i-γραμμή του A με t^{m-i+1} και την j-γραμμή του B με t^{n-j+1} και βρίσκουμε $t^pR(tx_1, tx_2, \cdots, tx_{r-1}) =$

$$= \begin{pmatrix} t^{m+n}A_n & t^{m+n-1}A_{n-1} & \ldots\ldots\ldots & t^mA_0 & & \\ & t^{m+n-1}A_n & \ldots\ldots\ldots\ldots & t^{m-1}A_0 & & \\ & & \ldots\ldots\ldots\ldots\ldots\ldots & & & \\ & & t^{n+1}A_n & \ldots\ldots\ldots\ldots & tA_0 & \\ t^{m+n}B_m & t^{n+m-1}B_{m-1} & \ldots\ldots\ldots & t^{n+1}B_1 & t^nB_0 & \\ & t^{m+n-1}B_m & \ldots\ldots\ldots\ldots\ldots\ldots & & t^{n-1}B_0 & \\ & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \\ & & t^{m+1}B_m & \ldots\ldots\ldots\ldots\ldots\ldots & & tB_0 \end{pmatrix}.$$

όπου $p = \dfrac{m(m+1)}{2} + \dfrac{n(n+1)}{2}$ $(t^{1+2+\cdots+m} = t^{\frac{m(m+1)}{2}})$. Δηλαδή

$$\begin{aligned} t^pR(tx_1, tx_2, \cdots, tx_r) &= t^{m+n} \cdot t^{m+n-1} \cdots t \cdot R(x_1, x_2, \cdots, x_{r-1}) \\ &= t^q \cdot R(x_1, x_2, \cdots, x_{r-1}) \end{aligned}$$

όπου $q = \dfrac{(m+n)(m+n+1)}{2}$. Επειδή $q - p = mn$ έχουμε ότι

$$R(tx_1, tx_2, \cdots, tx_{r-1}) = t^{mn} \cdot R(x_1, x_2, \cdots, x_{r-1})$$

δηλαδή το ζητούμενο. □

Τέλος αποδεικνύουμε την παρακάτω

Πρόταση 13. *Αν*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x], \quad a_n \neq 0$$

και

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m \in R[x], \quad b_m \neq 0,$$

τότε υπάρχουν πολυώνυμα A *και* B *βαθμού το πολύ* $m-1$ *και* $n-1$ *αντίστοιχα, έτσι ώστε*

$$R(f,g) = Af + Bg.$$

Απόδειξη: Έχουμε

$$\begin{array}{lllllll}
f & = & a_0 + & a_1 x + & \dots\dots\dots & a_n x^n & \\
xf & = & & a_0 x + & \dots\dots\dots & a_{n-1} x^n + & a_n x^{n+1} \\
\dots & & & & & & \\
x^{m-1} f & = & & & a_0 x^{m-1} + & \dots\dots\dots & + a_n x^{m+n-1} \\
g & = & b_0 + & b_1 x + & \dots\dots\dots & + b_m x^m & \\
xg & = & & b_0 x + & \dots\dots\dots & + b_{m-1} x^m & + b_m x^{m+1} \\
\dots & & & & & & \\
x^{n-1} g & = & & & b_0 x^{n-1} + & \dots\dots\dots & + b_m x^{m+n-1}
\end{array}$$

Έστω A_i τα αλγεβρικά συμπληρώματα των στοιχείων της πρώτης στήλης του πίνακα του συστήματος ο οποίος είναι ο η απαλείφουσα των f και g.
Πολλαπλασιάζουμε την i-οστή εξίσωση με το A_i και προσθέτουμε κατά μέλη για $i = 1, 2, \cdots, m+n$. Βρίσκουμε

$$(A_1 + A_2 x + \cdots + A_m x^{m-1}) f + (A_{m+1} + A_{m+2} x + \cdots + A_{m+n} x^{m+n-1}) g = R(f,g).$$

□

2. Προβολικοί χώροι

Επεκτείνουμε το αφινικό (x,y)-επίπεδο με την **επ' άπειρο ευθεία** και σχηματίζουμε το προβολικό επίπεδο. Κάθε ευθεία του αφινικού επιπέδου συμπληρώνεται σε μία ευθεία του προβολικού επιπέδου με την πρόσθεση ενός επ' άπειρον σημείου, του σημείου τομής της δοσμένης ευθείας με την επ' άπειρο ευθεία. Μπορούμε να θεωρήσουμε την επ' άπειρο ευθεία σαν παραμετρικοποιητή της κλίσης των αφινικών ευθειών. Κάθε σημείο της επ' άπειρο ευθείας αντιστοιχεί σε μία οικογένεια παραλλήλων ευθειών και είναι ακριβώς τα ζευγάρια εκείνα των ευθειών τα οποία είναι παράλληλα στον αφινικό μας χώρο, τα οποία τέμνονται επί της επ' άπειρο ευθείας.

Μία βασική γεωμετρική σχέση ανάμεσα στα σημεία και τις ευθείες του προβολικού επιπέδου αποτελεί η παρακάτω ιδιότητα.

(P) Δύο διακεκριμένα σημεία ορίζουν μοναδική ευθεία και δύο διακεκριμένες ευθείες τέμνονται σε ακριβώς ένα σημείο.

Ας ρίξουμε τώρα μία ματιά στην αναλυτική περιγραφή του προβολικού επιπέδου.

Θεωρούμε τον τρισδιάστατο χώρο με συντεταγμένες (w, x, y). Μία ευθεία γραμμή που περνάει από την αρχή των αξόνων $(0, 0, 0)$ ορίζεται μονοσήμαντα από οποιοδήποτε σημείο (w, x, y) διάφορο του $(0, 0, 0)$. Επιπλέον δύο σημεία (w, x, y) και (w', x', y') ορίζουν την ίδια ευθεία που περνάει από την αρχή $(0, 0, 0)$ τότε και μόνο τότε όταν υπάρχει μία σταθερά a, $a \neq 0$, τέτοια ώστε

$$w' = aw, \quad x' = ax \quad \text{και} \quad y' = ay. \tag{2.1}$$

Έστω $\mathbb{P}_2$ το σύνολο όλων των ευθειών που περνούν από την αρχή $(0, 0, 0)$. Τα σημεία του $\mathbb{P}_2$ μπορούν να παραμετρικοποιηθούν από τις κλάσεις ισοδύναμίας των τριάδων (w, x, y) μέσω της σχέσης ισοδυναμίας 2.1 (λέγονται ομογενείς συντεταγμένες). Την κλάση ισοδυναμίας του σημείου (w, x, y) την συμβολίζουμε με $[w, x, y]$.

Το ερώτημα που προκύπτει είναι από ποιό σύνολο (σώμα) παίρνουμε τις συντεταγμένες w, x, y.

(α′) Στην κλασική αναλυτική γεωμετρία είναι το $\mathbb{R}$.

(β′) Σε προβλήματα ρητών σημείων είναι το $\mathbb{Q}$.

(γ′) Στην κλασική αλγεβρική γεωμετρία είναι το $\mathbb{C}$.

Γενικά τα w, x, y θα είναι στοιχεία ενός σώματος k και το προβολικό επίπεδο

$$\mathbb{P}_2(k) := \big\{[w, x, y] \;\big|\; w, x, y \in k\big\}.$$

Εμφυτεύουμε το αφινικό (x, y)-επίπεδο k^2 στο προβολικό $\mathbb{P}_2(k)$ ως εξής

$$(x, y) \longmapsto [1, x, y].$$

Κάθε σημείο $[w, x, y] \in \mathbb{P}_2(k)$ με $w \neq 0$ παριστά το σημείο $\left(\frac{x}{w}, \frac{y}{w}\right)$ του k^2 διότι

$$[w, x, y] = \left[1, \frac{x}{w}, \frac{y}{w}\right] \quad \text{στο} \quad \mathbb{P}_2(k).$$

Ορίζουμε **ευθεία** στο $\mathbb{P}_2(k)$

$$E = \{[w,x,y] \mid aw+bx+cy=0, \text{ όπου } (a,b,c) \neq (0,0,0)\}.$$

Για $a=1,b=0,c=0$ έχουμε $w=0$ την **επ' άπειρο** ευθεία, η οποία αποτελείται από όλα τα σημεία της μορφής $[0,x,y]$.

Για $w=1$ παίρνουμε $a+bx+cy=0$ που είναι μία συνηθισμένη αφινική ευθεία όταν $bc \neq 0$.

Δύο σύνολα συντελεστών a,b,c και a',b',c' ορίζουν την ίδια ευθεία τότε και μόνο τότε όταν υπάρχει $u \in k, u \neq 0$ τέτοιο ώστε $a'=ua$, $b'=ub$, $c'=uc$.

Με βάση τους παραπάνω ορισμούς σημείου και ευθείας αποδεικνύεται τώρα εύκολα η αλήθεια της πρότασης (Ρ) που αναφέραμε προηγουμένως. Η απόδειξη αφήνεται σαν άσκηση στον αναγνώστη.

Για ένα μοντέλο του προβολικού χώρου ανεξάρτητου από το σύστημα συντεταγμένων, παίρνουμε έναν τρισδιάστατο διανυσματικό χώρο V υπέρ το k και συμβολίζουμε με $\mathbb{P}(V)$ το σύνολο όλων των **μονοδιάστατων** υποχώρων του V. Ας σημειωθεί ότι $\mathbb{P}_2(k) = \mathbb{P}(k^3)$.

Κάθε **γραμμικό συναρτησιοειδές** $U: V \to k$ ορίζει μία **ευθεία**

$$L = \{P \in \mathbb{P}(V) \mid U(P) = 0\}.$$

Έστω L^+ ο πυρήνας του U. Τότε $dim L^+ = 2$ και για κάθε σημείο P του $\mathbb{P}(V)$ ισχύει $P \in L$ ακριβώς τότε όταν $P \subset L^+$.

Αφού κάθε 2-διάστατος διανυσματικός υπόχωρος του V είναι ο πυρήνας κάποιου μη μηδενικού συναρτησιοειδούς, έπεται ότι είναι της μορφής L^+ για μία μοναδική ευθεία L.

Έστω P και Q δύο διακεκριμένα σημεία του $\mathbb{P}(V)$. Η μοναδική ευθεία L που περνάει από τα P και Q είναι αυτή για την οποία ισχύει $L^+ = P \oplus Q$. Η απόδειξη αφήνεται σαν άσκηση στον αναγνώστη. Για δύο διαφορετικές ευθείες L και M το μοναδικό σημείο τομής είναι $P = L^+ \cap M^+$. Η απόδειξη αφήνεται επίσης σαν άσκηση στον αναγνώστη.

Όμοια μπορούμε να θεωρήσουμε τον $r-$διάστατο προβολικό χώρο $\mathbb{P}_r(k)$ υπέρ το k

$$(y_0, y_1, \cdots, y_r) \sim (y_0', y_1', \cdots, y_r') \Leftrightarrow \exists \lambda \in k - \{0\} \; y_i' = \lambda y_i, \; y_i \text{ όχι όλα } 0.$$

Ορισμός 14. **Υπερεπίπεδο** *του* $\mathbb{P}_r(k)$ *θα καλείται το σύνολο λύσεων της γραμμικής εξίσωσης*

$$a_0 y_0 + \cdots + a_r y_r = 0, \;\; a_i \text{ όχι όλα } \mu\eta\delta\acute{\epsilon}\nu.$$

Αν H_i είναι το υπερεπίπεδο $y_i = 0$ τότε έχουμε την εξής αντιστοιχία

$$k^r \ni (x_1, x_2, \cdots, x_r) \longmapsto (x_1, x_2, \cdots, x_i, 1, x_{i+1}, \cdots, x_r) \in \mathbb{P}_r(k) - H_i.$$

Προφανώς ισχύει

$$\mathbb{P}(k) = (\mathbb{P}_r(k) - H_0) \cup \cdots \cup (\mathbb{P}_r(k) - H_r).$$

Το H_0 λέγεται το **επ' άπειρο** υπερεπίπεδο.

3. Εισαγωγή στις επίπεδες αλγεβρικές καμπύλες και στις υπερεπιφάνειες

Μέχρι στιγμής μελετήσαμε τις ευθείες στον προβολικό χώρο και είδαμε ότι έχουν εξίσωση $l(w, x, y) = 0$ όπου $l(w, x, y)$ ομογενές πολυώνυμο πρώτου βαθμού.

Μία **επίπεδη αλγεβρική καμπύλη** C_f **βαθμού** d είναι το σύνολο όλων των σημείων $[w, x, y] \in \mathbb{P}_2(k)$ τέτοιων ώστε $f(w, x, y) = 0$ όπου το f είναι ομογενές πολυώνυμο βαθμού d.

Αφού για κάθε ομογενές πολυώνυμο βαθμού d ισχύει $f(\lambda w, \lambda x, \lambda y) = \lambda^d f(w, x, y)$, αν για κάποιο αντιπρόσωπο (w, x, y) της κλάσης $[w, x, y]$ ισχύει $f(w, x, y) = 0$, το ίδιο θα ισχύει και για κάθε στοιχείο της κλάσης.

Την αντίστοιχη **αφινική καμπύλη** την παίρνουμε για $w = 1$. Έστω $g(x, y) = f(1, x, y)$. Προφανώς $\deg g(x, y) \leq d$.

$$\text{Ορίζουμε } C_g^{\text{aff}} = \{(x, y) \in k^2 \mid g(x, y) = 0\}.$$

$$\text{Προφανώς, ισχύει } \quad C_g^{\text{aff}} = C_f \cap k^2.$$

Αντίστροφα αν $g(x, y)$ πολυώνυμο βαθμού μικρότερου ή ίσου με d τότε το πολυώνυμο $f(w, x, y) = w^d g\left(\frac{x}{w}, \frac{y}{w}\right)$ είναι ομογενές βαθμού d και $f(1, x, y) = g(x, y)$.

Αφού $f(w, x, y) = 0 \Leftrightarrow f(w, x, y)^2 = 0$ το σύνολο των σημείων της C_f **δεν** ορίζει μονοσήμαντα την εξίσωση $f(w, x, y) = 0$. Αν το f έχει την ανάλυση $f = f_1 f_2 \cdots f_r$ τότε προφανώς ισχύει:

$$C_f = C_{f_1} \cup C_{f_2} \cup \cdots \cup C_{f_r}.$$

Αν πάλι $f \mid f'$ τότε $C_f \subset C_{f'}$.

Δεδομένου ότι η απάντηση στο ερώτημα πότε το πολυώνυμο f αναλύεται σε γινόμενο παραγόντων και πότε όχι εξαρτάται από το σώμα k, θα μιλάμε για την επίπεδη αλγεβρική καμπύλη υπέρ το σώμα k. Τέλος, για να είμαστε σίγουροι ότι υπάρχουν αρκετά σημεία πάνω στην καμπύλη, θα παίρνουμε τις συντεταγμένες των σημείων κάθε φορά από συγκεκριμένη επέκταση K του k.

Ορισμός 15. *Μία* **ανάγωγη επίπεδη αλγεβρική καμπύλη** C_f **βαθμού** d **ορισμένη υπέρ το σώμα** k *ορίζεται από ένα ανάγωγο ομογενές πολυώνυμο* $f(w,x,y) \in k[w,x,y]$ *βαθμού* d *και είναι μία συνάρτηση η οποία, για κάθε επέκταση* K *του* k *μας δίνει το σύνολο*

$$C_f(K) = \big\{[w,x,y] \in \mathbb{P}_2(K) \;\big|\; f(w,x,y) = 0\big\}.$$

Αν η $f = f_1^{a(1)} f_2^{a(2)} \cdots f_r^{a(r)}$ είναι η ανάλυση του ομογενούς πολυωνύμου f βαθμού d του $k[w,x,y]$ σε γινόμενπο πρώτων παραγόντων τότε ισχύει:

$$C_f(K) = C_{f_1}(K) \cup \cdots \cup C_{f_r}(K).$$

Η καμπύλη C_{f_i} λέγεται (ανάγωγη) **συνιστώσα** της C_f και ο φυσικός αριθμός $a(i)$ **πολλαπλότητα** της C_{f_i}.

- Καμπύλες πρώτου βαθμού είναι οι ευθείες.
- Καμπύλες δευτέρου βαθμού λέγονται κωνικές τομές.
- Καμπύλες τρίτου βαθμού λέγονται κυβικές καμπύλες.
- Καμπύλες τετάρτου βαθμού λέγονται τετραδικές καμπύλες, και ούτω καθ' εξής.

Αν $K \subset K'$ επεκτάσεις του k τότε ισχύει $\mathbb{P}_2(K) \subset \mathbb{P}_2(K')$ και $C_f(K) \subset C_f(K')$.

Ορισμός 16. *Μία* **υπερεπιφάνεια** H_f *στον προβολικό χώρο* $\mathbb{P}_n$ *ορίζεται μέσω ενός ομογενούς πολυωνύμου* $f(Y_0, Y_1, \cdots, Y_n) \in k[Y_0, Y_1, \cdots, Y_n]$ *βαθμού* d, *όπου για μία επέκταση* K/k, *το σύνολο* $H_f(K)$ *ορίζεται ως εξής*

$$H_f(K) = \big\{(y_0, y_1, \cdots, y_n) \in \mathbb{P}_n(K) \;\big|\; f(y_0, y_1, \cdots, y_n) = 0\big\}.$$

Παρατηρούμε ότι το επ' άπειρο υπερεπίπεδο $y_0 = 0$ περιέχεται στο H_f αν και μόνο αν $f(0, y_1, \cdots, y_n) = 0$ για κάθε $y_i \in K$, δηλαδή αν και μόνο αν $y_0 | f$, το οποίο συμβάινει

ακριβώς τότε όταν $\deg g < \deg f$ όπου g το συνεταιρικό του f, δηλαδή $g(x_1, x_2, \cdots, x_n) = f(1, x_1, x_2, \cdots, x_n)$.

Σαν αφινικό κομμάτι της καμπύλης ορίζουμε

$$H_g^{\text{aff}}(K) = \big\{(x_1, x_2, \cdots, x_n) \in K^n \,\big|\, g(x_1, x_2, \cdots, x_n) = 0\big\}.$$

Προφανώς ισχύει

$$H_g^{\text{aff}}(K) = H_f(K) \cap K^n.$$

Έστω $f(X) \in K[X]$. Ο $K[X]$ είναι, ως γνωστό, ευκλείδιος δακτύλιος. Υποθέτουμε ότι $\deg f(X) > 0$. Οι παρακάτω σχέσεις είναι προφανείς.

(i) Το $f(X)$ διαιρούμενο με $X - a$ δίνει υπόλοιπο $f(a)$.

(ii) Ο $a \in k$ είναι ρίζα του πολυνύμου $f(X)$ ακριβώς τότε όταν $X - a \Big|_{k[X]} f(X)$.

(iii) Αν $\deg f(X) = n$, τότε το $f(X)$ έχει το πολύ n ρίζες μέσα στο k.

Πρόταση 17. *Έστω* $f(x_1, x_2, \cdots, x_n) \in k[x_1, x_2, \cdots, x_n]$.
Υποθέτουμε ότι $f(a_1, a_2, \cdots, a_n) = 0$ *για όλα τα στοιχεία* $a_1, a_2, \cdots, a_n$ *ενός* **απείρου** *υποσυνόλου* T *του* k. *Τότε* $f(x_1, x_2, \cdots, x_n) = 0$.

Απόδειξη: Η (iii) ισοδυναμεί με την αλήθεια της πρότασης 17, για $n = 1$. Έστω ότι ισχύει για πολυώνυμα με $n - 1$ μεταβλητές. Γράφουμε

$$f(x_1, x_2, \cdots, x_n) = f_0 + f_1 x_n + \cdots + f_m x_n^m, \; m \geq 0$$

όπου $f_i \in k[x_1, x_2, \cdots, x_{n-1}]$. Αν $f \neq 0$ μπορούμε να υποθέσουμε ότι $f_m \neq 0$.
Από την υπόθεση της μαθηματικής επαγωγής έπεται ότι υπάρχουν στοιχεία $a_1, a_2, \cdots, a_{n-1}$ του T τέτοια ώστε $f_m(a_1, a_2, \cdots, a_{n-1}) \neq 0$. Σύμφωνα με την (iii) όμως τότε θα έχουμε n **το πολύ** δυνατότητες για το a_n έτσι ώστε $f(a_1, a_2, \cdots, a_n) = 0$, άτοπο διότι T άπειρο. Άρα $f = 0$. □

Εύκολα παρατηρούμε ότι αν $f(x_0, x_1, \cdots, x_n), g(x_0, x_1, \cdots, x_n) \in k[x_0, x_1, \cdots, x_n]$ και $f \,|\, g$ τότε $H_f(K) \subset H_g(K)$ για **όλες** τις επεκτάσεις K του k.

Θεώρημα 18. *Έστω* H_f *και* $H_{f'}$ *δύο υπερεπιφάνειες ορισμένες υπέρ το* k *στον* $\mathbb{P}_n$ *και έστω ότι το* f *είναι ανάγωγο υπέρ το* k. *Αν* $H_f(L) \subset H_{f'}(L)$ *για κάποια αλγεβρικά κλειστή επέκταση* L *του* k *τότε το* $f \,|\, f'$ *και συνεπώς* $H_f(K) \subset H_{f'}(K)$ *για όλες τις επεκτάσεις* K *του* k.

Απόδειξη: Άμεση συνέπεια της υπόθεσης $H_f(L) \subseteq H_{f'}(L)$ είναι ότι και $H_f^{\text{aff}}(L) := H_f(L) \cap L^n \subseteq H_{f'}(L) \cap L^n = H_{f'}^{\text{aff}}(L)$ όπου $g(x_1 x_2, \cdots, x_n) = f(1, x_1, x_2, x_n)$ και $g'(x_1 x_2, \cdots, x_n) = f'(1, x_1, x_2, x_n)$ είναι τα αφινικά πολυώνυμα τα συνεταιρικά των f και f' αντίστοιχα. Αναπτύσσουμε το $g(x_1, x_2, \cdots, x_n)$ ως προς τις δυνάμεις του x_n,

$$g(x_1, x_2, \ldots, x_{n-1}, x_n) = \alpha_0(x_1, x_2, \ldots, x_{n-1}) + \ldots + \alpha_d(x_1, x_2, \ldots, x_{n-1}) x_n^d,$$

όπου $d > 0$ και $a_i(x_1, x_2, \ldots, x_{n-1}) \in k[x_1, x_2, \ldots, x_{n-1}]$.

Αν το $f' = 0$ τότε $f \mid f'$. Στην συνέχεια θεωρούμε την περίπτωση όπου $g' \in k[x_1, x_2, \ldots, x_{n-1}]$ και έστω ότι $g' \neq 0$. Δεδομένου ότι το σώμα L είναι άπειρο σύνολο, υπάρχει τουλάχιστο ένα σημείο $(x_1, x_2, \ldots, x_{n-1})$ τέτοιο ώστε $g'(x)\alpha_d(x) \neq 0$, $x := (x_1, x_2, \ldots, x_{n-1})$. Επειδή το L είναι αλγεβρικά κλειστό, η πολυωνυμική εξίσωση $g(x_1, x_2, \ldots, x_{n-1}, t) = 0$ έχει μία λύση $t = x_n$ στο L και συνεπώς το σημείο $(x_1, x_2, \ldots, x_{n-1}) \in H_g^{\text{aff}}(L) - H_{g'}^{\text{aff}}(L)$, άτοπο, διότι $H_g^{\text{aff}}(L) \subseteq H_{g'}^{\text{aff}}(L)$. Επομένως αν $g' \in k[x_1, \ldots, x_{n-1}]$, τότε κατ' ανάγκη $g' = 0$.

Έστω τώρα

$$g(x_1, x_2, \ldots, x_n) = b_0 + b_1 x_n + \cdots + b_l x_n^l$$

όπου $l > 0$ και $b_i \in k[x_1, x_2, \ldots, x_{n-1}]$.

Από την Πρόταση 13, έχουμε ότι η απαλείφουσα $R(x_1, x_2, \ldots, x_{n-1})$ των $g(x)$ και $g'(x)$ ως προς την μεταβλητή x_n έχει την μορφή

$$R(x_1, x_2, \ldots, x_{n-1}) = Ag + Bg',\ A, B \in k[x_1, x_2, \ldots, x_{n-1}, x_n]$$

Επομένως αν $g(x_1, x_2, \ldots, x_n) = 0$, τότε λόγω της υπόθεσης και $g'(x_1, x_2, \ldots, x_n) = 0$ και επομένως $R(x_1, x_2, \ldots, x_{n-1}) = 0$, $(x_1, x_2, \ldots, x_n) \in L^n$. Δηλαδή $H_g^{\text{aff}}(L) \subset H_{R(g,g')}^{\text{aff}}$. Όμως επειδή $R(g, g') \in k[x_1, x_2, \ldots, x_{n-1}]$ έπεται ότι $R(g, g') = 0$. Η απόδειξη είναι εντελώς ανάλογη με την απόδειξη για το g που κάναμε πιό πάνω.

Το Θεώρημα 18 δίνει τώρα ότι g και g' έχουν κοινή συνιστώσα και, επειδή g ανάγωγο, θα πρέπει $g \mid_{k[X]} g'$ οπότε και $f \mid_{k[X]} f'$. □

Πόρισμα 19. *Έστω f και f' δύο ομογενή ανάγωγα πολυώνυμα του $k[x_1, x_2, \ldots, x_n]$, $\deg f > 0$ και $\deg g > 0$.*

Αν για κάποιο αλγεβρικά κλειστό σώμα $L, k \subset L$ ισχύει $H_f(L) = H_{f'}(L)$ τότε $f' = cf$ όπου $c \in k \setminus \{0\}$ και $H_f(K) = H_g(K)$ για κάθε επέκταση K του k.

Παρατήρηση 20. *Η υπόθεση ότι το* L *είναι αλγεβρικά κλειστό είναι ουσιώδης. Αν π.χ. πάρουμε* $K = \mathbb{Q}$ *και* $L = \mathbb{R}$ *τότε για τα πολυώνυμα*

$$f(W, X, Y) = W^2 + X^2 + Y^2, \quad f'(W, X, Y) = W^2 + 2X^2 + Y^2$$

έχουμε $H_f(\mathbb{R}) = H_g(\mathbb{R}) = \phi$ *αλλά* **δεν** *είναι το* g *πολλαπλάσιο του* f *επί σταθερά.*

Πόρισμα 21. *Έστω* $f = f_1^{a(1)} f_2^{a(2)} \cdots f_r^{a(r)}$ *και* $f' = f_1'^{b(1)} f_2'^{b(2)} \cdots f_r'^{b(r)}$ *οι αναλύσεις των* f *και* f' *σε γινόμενο πρώτων παραγόντων, στον δακτύλιο* $k[x_0, x_1, \ldots, x_n]$. *Αν* $H_f(L) = H_{f'}(L)$ *για κάποιο αλγεβρικά κλειστό σώμα* L, $L \supset k$ *τότε* $r = s$ *και* $g_i = c_i f_i$ *όπου* $c_i \in k \setminus \{0\}$.

Ορισμός 22. *Ο εκθέτης* $a(i)$ *του* f_i *στην ανάλυση του* f *λέγεται* **βαθμός πολλαπλότητας** *με τον οποίο η συνιστώσα* H_{f_i} *εμφανίζεται στην υπερεπιφάνεια* H_f.

4. Σημεία τομής αλγεβρικών καμπυλών και ο βαθμός πολλαπλότητάς τους

Στην παράγραφο αυτή υποθέτουμε ότι το σώμα k έχει χαρακτηριστική **μηδέν**. Επομένως το k έχει άπειρο πλήθος στοιχείων. Αν στην καμπύλη C_f που ορίζεται από το $f(W, X, Y) \in k[W, X, Y]$ υποθέσουμε ότι $W \nmid f(W, X, Y)$ (δηλαδή ότι η C_f δεν περιέχει σαν συνιστώσα την επ' άπειρο ευθεία) τότε μπορούμε να θεωρήσουμε το $g(X, Y) = f(1, X, Y)$ και να παρατηρήσουμε αμέσως ότι οι λύσεις της $g(X, Y) = 0$ σε κάποια επέκταση K του k είναι το σύνολο των "πεπερασμένων" σημείων της καμπύλης $C_f(K)$.

Η ελευθερία εκλογής της επ' άπειρο ευθείας στο αφινικό επίπεδο θα είναι χρήσιμη στα επόμενα. Αφού το K απειροσύνολο, υπάρχουν άπειρες ευθείες στον προβολικό χώρο $\mathbb{P}_2(K)$, άρα υπάρχει τουλάχιστο μία που δεν είναι συνιστώσα του $C_f(K)$. Αυτήν διαλέγουμε ως επ' άπειρο ευθεία.

Έστω $P_1 = [w_1, x_1, y_1]$ και $P_2 = [w_2, x_2, y_2]$ σημεία του $\mathbb{P}_2(K)$. Η ευθεία που ορίζουν είναι η $L : \lambda P_1 + \mu P_2$ όπου $\lambda, \mu \in K$ όχι συγχρόνως μηδέν. Οι συντεταγμένες κάθε σημείου τομής των L και $C_f(K)$ θα επαληθεύουν την εξίσωση $f(\lambda w_1 + \mu w_2, \lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2) = 0$. Ξεχωρίζουμε δύο περιπτώσεις:

(i) Έστω ότι $f(\lambda w_1 + \mu w_2, \lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2) = 0$ για **όλα** τα $\lambda, \mu \in K$. Διαλέγουμε κατάλληλο σύστημα συντεταγμένων, έτσι ώστε η ευθεία L να είναι η επ' άπειρο ευθεία

$W = 0$. Τότε έχουμε

$$f(0, x, y) = 0, \ \forall x, y \in K.$$

Η πρόταση 17, σελ. 29, δίνει ότι $f(0, X, Y) = 0$. Συνεπώς ο W είναι κοινός παράγοντας των όρων του $f(W, X, Y)$ δηλαδή η ευθεία L $(W = 0)$ είναι συνιστώσα της $C_f(K)$.

(ii) Έστω τώρα ότι το $f(\lambda P_1 + \mu P_2)$ **δεν** είναι το εκ ταυτότητας μηδενικό πολυώνυμο ως προς λ και μ. Τότε το $f(\lambda P_1 + \mu P_2)$ είναι ομογενές πολυώνυμο βαθμού d ως προς λ και μ. Αν K είναι **αλγεβρικά κλειστό** τότε από την πρόταση 11, σελ. 22, συνεπάγεται ότι η εξίσωση $f(\lambda P_1 + \mu P_2) = 0$ επαληθεύεται από ακριβώς d λόγους $\frac{\lambda}{\mu}$ όπου μία ρίζα πολλαπλότητας r μετριέται $r-$φορές. Κάθε λόγος ορίζει **ακριβώς** ένα σημείο της τομής $L \cap C_f(K)$. Ώστε:

Πρόταση 23. *Αν K αλγεβρικά κλειστό σώμα τότε μία ευθεία L ή είναι συνιστώσα της $C_f(K)$ ή έχει ακριβώς d σημεία τομής ($\deg f = d$).*

Πρόταση 24. *Αν η καμπύλη C_f υπέρ το αλγεβρικά κλειστό σώμα K περιέχει μόνο* **απλές** *συνιστώσες τότε από οποιοδήποτε σημείο $P \in \mathbb{P}_2(K)$ $P \notin C_f(K)$, περνάει μία ευθεία που τέμνει την $C_f(K)$ σε d διακεκριμένα σημεία.*

Απόδειξη: Διαλέγουμε κατάλληλα το σύστημα συντεταγμένων έτσι ώστε το σημείο P να είναι το $[0, 0, 1]$ και έστω $g(X, Y) = 0$ η αντίστοιχη αφινική εξίσωση της f. Οι παραμετρικές εξισώσεις μιάς ευθείας L_a διερχομένης από το P είναι

$$x = a, \ a \in K, \quad y = t.$$

Όταν το t διατρέχει όλα τα στοιχεία του K τότε τα ζευγάρια (x, y) διατρέχουν όλα τα πεπερασμένα σημεία της L_a εκτός του επ' άπειρον σημείου P. Η εξαίρεση όμως αυτή δεν μας δημιουργεί πρόβλημα διότι ενδιαφερόμαστε για τα σημεία τομής της ευθείας L_a με την καμπύλη $C_f(K)$ και $P \notin C_f(K)$ εξ υποθέσεως.
Τα σημεία τομής των L_a και $C_f(K)$ δίνονται από τις ρίζες του πολυωνύμου $g(a, t) = 0$. Το σημείο $P = [0, 0, 1]$ δεν ανήκει στην καμπύλη $C_f(K)$. Αυτό σημαίνει ότι $f(0, 0, t) \neq 0$, δηλαδή ότι υπάρχει μονώνυμο που περιέχει μόνο το Y βαθμού d και συνεπώς $\deg_t g(a, t) = d$.
Έστω ότι για όλα τα a η $g(a, t) = 0$ έχει πολλαπλή ρίζα ως προς t. Έστω $D(X)$ η

διακρίνουσα του πολυωνύμου $g(X,Y)$ ως προς Y. Τότε η $D(a)$ είναι η διακρίνουσα του $g(a,t)$ ως προς t. Λόγω της υπόθεσης της ύπαρξης πολλαπλής ρίζας έχουμε:

$$D(a) = 0, \quad \forall a \in K.$$

Το $D(X)$ όμως είναι πολυώνυμο ως προς X και έχει **άπειρες** ρίζες. Συνεπώς το $D(X)$ είναι εκ ταυτότητος 0. Επομένως το $g(X,Y)$ έχει πολλαπλή ρίζα, δηλαδή η $C_f(K)$ έχει πολλαπλή συνιστώσα, άτοπο.

Άρα όλα τα σημεία τομής είναι διαφορετικά και αφού K αλγεβρικά κλειστό, αυτά είναι σε πλήθος ακριβώς d. □

Ορισμός 25. *Έστω C_f αλγεβρική καμπύλη υπέρ το σώμα k η οποία περιέχει μόνο απλές συνιστώσες. Θα καλούμε* **τάξη της** *C_f (ως προς το k) το* **μέγιστο** *αριθμό τομών της C_f με μία οποιαδήποτε ευθεία L.*

Εξετάζουμε τώρα το πρόβλημα των σημείων τομής ευθείας και αλγεβρικής καμπύλης $C_f(K)$ όταν οι ευθείες περνούν από δοσμένο σημείο της καμπύλης $P \in C_f(K)$.

Διαλέγουμε πάλι κατάλληλο σύστημα συντεταγμένων έστι ώστε οι αφινικές συντεταγμένες του P να είναι (a,b), οπότε αμέσως προκύπτει ότι για το συνεταιρικό του f αφινικό πολυώνυμο $g(X,Y)$ ισχύει $g(a,b) = 0$.

Οι παραμετρικές εξισώσεις των ευθειών L που περνούν από το σημείο $P = (a,b)$ γράφονται

$$\left\{ \begin{array}{rcl} x & = & a + \lambda t \\ y & = & b + \mu t \end{array} \right\}$$

και ορίζονται πλήρως από τον λόγο $\dfrac{\lambda}{\mu}$.

Τα σημεία τομής δίνονται από την σχέση

$$g(a + \lambda t, b + \mu t) = 0.$$

Αναπτύσσουμε το αριστερό μέλος σε σειρά του Taylor ως προς t. Έχουμε

$$\big(g_x\lambda + g_y\mu\big)t + \frac{1}{2}\big(g_{xx}\lambda^2 + 2g_{xy}\lambda\mu + g_{yy}\mu^2\big)t^2 + \cdots = 0$$

όπου g_x, g_y σημαίνει την πρώτη παράγωγο ως προς X, Y στο σημείο P κ.ο.κ.

Πρώτη περίπτωση: Υποθέτουμε ότι τα g_x και g_y δεν είναι συγχρόνως μηδέν. Αυτό σημαίνει ότι $t = 0$ είναι απλή. Συνεπώς κάθε ευθεία που περνάει από το P έχει **απλή** τομή με την C_f

στο P. Μοναδική εξαίρεση αποτελεί η ευθεία που έχει τέτοιες τιμές στα λ και μ έτσι ώστε $g_x\lambda + g_y\mu = 0$.

Ορισμός 26. *Η ευθεία αυτή θα λέγεται* **εφαπτομένη** *της C_f στο P.*

Δεύτερη περίπτωση: Υποθέτουμε ότι $g_x = g_y = 0$ αλλά όχι όλες οι g_{xx}, g_{xy}, g_{yy} ίσες με μηδέν.

Τότε κάθε ευθεία που περνάει από το P έχει σημείο τομής το P με βαθμό πολλαπλότητας τουλάχιστο 2 και το **πολύ** 2 ευθείες που αντιστοιχούν στις ρίζες της $g_{xx}\lambda^2 + 2g_{xy}\lambda\mu + g_{yy}\mu^2 = 0$ έχουν βαθμό πολλαπλότητας μεγαλύτερο του 2. Οι δύο αυτές εξαιρέσεις λέγονται εφαπτόμενες της C_f στο P (αν η παραπάνω εξίσωση έχει διπλή ρίζα τότε λέμε ότι συμπίπτουν).
r-οστή περίπτωση: Υποθέτουμε ότι όλες οι παράγωγοι της g, μεχρι και $(r-1)$-τάξεως συμπεριλαμβανομένης, μηδενίζονται στο P, αλλά **τουλάχιστο** μία παράγωγος r-τάξεως **δεν** μηδενίζεται στο P. Τότε κάθε ευθεία περνάει από το P έχει σημείο τομής με την καμπύλη το P με βαθμό πολλαπλότητας τουλάχιστον r και υπάρχουν **ακριβώς** r ευθείες που έχουν πιο πολλά από r σημεία τομής. Οι εξαιρέσιμες αυτές ευθείες λέγονται **εφαπτόμενες της** C_f στο P, αντιστοιχούν στις ρίζες του πολυωνύμου

$$g_{x^r}\lambda^r + \binom{r}{1} g_{x^{r-1}y}\lambda^{r-1}\mu + \cdots + \binom{r}{r} g_{y^r}\mu^r = 0$$

και μετριούνται με πολλαπλότητα ίση προς την πολλαπλότητα της αντίστοιχης ρίζας της παραπάνω εξίσωσης.

Ορισμός 27. *Στην περίπτωση r θα λέμε ότι το P είναι ένα σημείο της καμπύλης C_f* **βαθμού πολλαπλότητας** *r.*

Σημείωση 28. *Αφού το $g(X,Y)$ δεν είναι εκ ταυτότητας μηδέν έπεται ότι η r-οστή περίπτωση θα συμβαίνει για κάποιο $1 \leq r \leq d$.*

- Ένα σημείο βαθμού πολλαπλότητας 1, θα λέγεται **απλό**.

- Ένα σημείο βαθμού πολλαπλότητας 2, θα λέγεται **διπλό**, κ.ο.κ.

Ορισμός 29. *Κάθε σημείο της C_f βαθμού πολλαπλότητας μεγαλύτερου του 1, θα λέγεται* **ιδιάζον**.

Προφανώς $P = (a, b)$ ιδιάζον σημείο, ακριβώς τότε όταν $g(a, b) = g_x(a, b) = g_y(a, b) = 0$.

Ορισμός 30. *Η C_f θα λέγεται* **μη-ιδιάζουσα** *όταν κάθε σημείο της είναι μη-ιδιάζον.*

Πρόταση 31. *Έστω ότι το $g(X, Y)$ δεν έχει όρους βαθμού μικρότερου του r και έχει μερικούς βαθμού r. Τότε η αρχή των συντεταγμένων είναι ένα σημείο βαθμού πολλαπλότητας r της καμπύλης $g(X, Y) = 0$ και η καμπύλη που ορίζεται από την εξίσωση $g_r(X, Y) = 0$ όπου $g_r(X, Y)$ οι όροι της g βαθμού r έχει σαν συνιστώσες τις εφαπτομένες της g στην αρχή των συντεταγμένων.*

Σε προβολικές συντεταγμένες ισχύει η

Πρόταση 32. *Ένα σημείο P είναι βαθμού πολλαπλότητας r της $f(W, X, Y) = 0$ ακριβώς τότε όταν όλες οι παράγωγοι τάξεως $(r-1)$ του f μηδενίζονται στο P αλλά αυτό δεν συμβαίνει για όλες τις παραγώγους τάξεως r.*

Απόδειξη: Αλλάζοντας, αν χρειαστεί, το σύστημα συντεταγμένων, υποθέτουμε ότι $P = [w, x, y]$ με $w \neq 0$, δηλαδή το P δεν ανήκει στην επ΄ άπειρο ευθεία $W = 0$. Αν $W \mid f(W, X, Y)$ τότε η f δεν έχει αντίστοιχη αφινική εξίσωση, αλλά

$$g(x, y) = f(1, x, y) = 0$$

είναι η αφινική εξίσωση μιάς καμπύλης που διαφέρει από την f μόνο ως προς την έλλειψη μιάς συνιστώσας, της $W = 0$.
Εφ΄ όσον η συνιστώσα αυτή δεν έχει επίδραση στον βαθμό πολλαπλότητας του σημείου P, μπορούμε να θεωρήσουμε την $g(x, y) = 0$ σαν αφινική εξίσωση της $f(w, x, y) = 0$.
Επομένως

$$g(a, b) = 0 \text{ τότε και μόνο τότε όταν } f(1, a, b) = 0.$$

$$\text{Ακόμη έχουμε } g_x(X, Y) = f_x(1, X, Y)$$

$$\text{και } g_y(X, Y) = f_y(1, X, Y).$$

Δηλαδή

$$g_x(a, b) = g_y(a, b) = 0 \text{ τότε και μόνο τότε όταν } f_x(1, a, b) = f_y(1, a, b).$$

Αλλά τότε ο **τύπος του Euler**, η απόδειξη του οποίου αφήνεται σαν άσκηση στον αναγνώστη,

$$wf_w + xf_x + yf_y = d \cdot f$$

μας δίνει ότι

$$f(1,a,b) = f_x(1,a,b) = f_y(1,a,b) = 0$$

$$\text{ακριβώς τότε όταν} \quad f_w(1,a,b) = f_x(1,a,b) = f_y(1,a,b) = 0.$$

Συνεχίζοντας όμοια βρίσκουμε ότι

$$g(a,b) = g_x(a,b) = g_y(a,b) = g_{x^2}(a,b) = \cdots = g_{y^r}(a,b) = 0$$

τότε και μόνο τότε, όταν

$$f_{w^r}(1,a,b) = f_{w^{r-1}x}(1,a,b) = \cdots = f_{y^r}(1,a,b) = 0.$$

Από τον ορισμό του βαθμού πολλαπλότητας r ενός σημείου προκύπτει τώρα η πρόταση. □

Παρατήρηση 33. *Προφανώς το σημείο* $P = [1,a,b]$ *είναι ιδιάζον σημείο της καμπύλης*

$$f(w,x,y) = 0$$

αν και μόνο αν

$$f_w(P) = f_x(P) = f_y(P) = 0.$$

Για τα μη-ιδιάζοντα σημεία της καμπύλης, έχουμε

Πρόταση 34. *Έστω* C_f *και* $C_{f'}$ *δύο επίπεδες αλγεβρικές καμπύλες βαθμού* m *και* n *αντίστοιχα, ορισμένες υπέρ το σώμα* k. *Αν για κάποια επέκταση* K *του* k *το σύνολο* $C_f(K) \cap C_{f'}(K)$ *έχει* **πιό πολλά** *από* mn *σημεία τότε οι* C_f *και* C_g *έχουν* **κοινή συνιστώσα**.

Απόδειξη: Παίρνουμε $mn+1$ από τα σημεία τομής. Κάθε ζευγάρι από τα σημεία αυτά ορίζει μία ευθεία. Το σύνολο των ευθείων που μπορούμε να σχηματίσουμε είναι πεπερασμένου πλήθους. Άρα υπάρχει σημείο P που να **μην** ανήκει σε καμμία από τις ευθείες ούτε στις καμπύλες C_f και C_g. Διαλέγουμε το σύστημα συντεταγμένων κατά τέτοιο τρόπο ώστε οι συντεταγμένες του P να είναι $[0,0,1]$. Γράφουμε

$$f(W,X,Y) = A_0Y^m + A_1Y^{m-1} + \cdots + A_m$$

$$f'(W,X,Y) = B_0Y^n + B_1Y^{n-1} + \cdots + B_n$$

όπου $A_0B_0 \neq 0$, σταθερές και A_i, B_i, για $i > 0$ ομογενή πολυώνυμα βαθμού i ως προς W, X. Από το θεώρημα 12, σελ. 22 έχουμε ότι η απαλείφουσα των f και f' ως προς Y,

$R(f,f')(W,X)$ είναι πολυώνυμο βαθμού mn ως προς W,X, ή το μηδενικό πολυώνυμο. Για δύο στοιχεία $w,x \in K$ ισχύει:

$$R(f,g)(w,x)=0 \text{ ακριβώς τότε όταν } \exists y \in \tilde{K}, \text{ τέτοιο ώστε } f(w,x,y)=f'(w,x,y)=0$$

όπου $\tilde{K}$ μία αλγεβρική θήκη του K.

Αφού $P=[0,0,1] \notin C_f$ έπεται ότι $A_0 \neq 0$ διότι αν $A_0=0$ θα είχαμε $f([0,0,1])=0$, δηλαδή $P \in C_f$ το οποίο είναι άτοπο.

Ομοίως $B_0 \neq 0$. Άρα $A_0B_0 \neq 0$.

Αφού τώρα υπάρχουν $mn+1$ σημεία

$$(w_i,x_i,y_i) \in C_f(K) \cap C_{f'}(K), \quad i=0,1,2,\ldots,mn$$

έπεται ότι το πολυώνυμο $\prod_{0\leq i\leq mn}(x_iW-w_iX)$ το οποίο είναι βαθμού $mn+1$ διαιρεί το πολυώνυμο $R(f,f')(W,X)$ βαθμού mn. Επομένως κατ' ανάγκη $R(f,f')(w,x)=0$.

Από την πρόταση 10, σελ. 21, παίρνουμε το ζητούμενο, ότι δηλαδή f και f' έχουν κοινή συνιστώσα $C_h \subset C_f \cap C_{f'}$. □

Πρόταση 35. *Αν K αλγεβρικά κλειστό σώμα, f και f' όπως στην προηγούμενη πρόταση, $P=[w,x,y]$ ένα σημείο της $C_f(K)$ βαθμού πολλαπλότητας r και συγχρόνως σημείο της $C_{f'}(K)$ βαθμού πολλαπλότητας s, τότε η απαλείφουσα $R(f,f')(w,x)$ δεν είναι μηδενική, έχει το λόγο $\frac{w}{x}$ ρίζα βαθμού πολλαπλότητας* **τουλάχιστο** *rs, υπό την προϋπόθεση βέβαια ότι $R(f,f')(w,x)\neq 0$.*

Απόδειξη: Όπως και στην πρόταση 34 το σημείο $P_0=[0,0,1]$ δεν ανήκει ούτε στην $C_f(K)$ ούτε στην $C_{f'}(K)$. Επομένως τουλάχιστο μία από τις συνιστώσες w,x είναι διάφορη του μηδενός. Χωρίς περιορισμό της γενικότητας, υποθέτουμε ότι $w\neq 0$. Κάνουμε αλλαγή συντεταγμένων

$$W'=\frac{W}{w}, \quad X'=X-\frac{x}{w}W, \quad Y'=Y.$$

Το P τώρα έχει συντεταγμένες $P=[1,0,y]$ και η απαλείφουσα ως προς $Y'=Y$ της μετασχηματισθείσης εξίσωσης, $R(wW',X'+xW')$ έχει σαν ρίζα τον λόγο $1:0$ στον ίδιο βαθμό πολλαπλότητας που έχει η ρίζα $w:x$ του $R(W,X)$. Συνεπώς, χωρίς περιορισμό της γενικότητας, υποθέτουμε και πάλι ότι $w=1$ και $x=0$.

Θα δείξουμε ότι μπορούμε να υποθέσουμε ότι $y = 0$.

Προς τούτο θεωρούμε την απαλείφουσα των

$$f(W, X, Y + \lambda W) \text{ και } f'(W, X, Y + \lambda W) \text{ ως προς } Y \ (\lambda \in K).$$

Αυτή είναι ένα πολυώνυμο

$$R(W, X, \lambda) = c_0 + c_1\lambda + \cdots + c_N\lambda^N, \ N \geq 0 \text{ όπου } c_i \in K[W, X].$$

Η σταθερά $c_0 = R(f, f')(W, X)$ είναι διάφορη του μηδενός.

Έστω $N > 0$ και $c_N \neq 0$. Υπάρχουν προφανώς τιμές $w, x \in K$ τέτοιες ώστε

$$c_0(w, x)c_N(w, x) \neq 0.$$

Λόγω της υπόθεσης ότι το K είναι αλγεβρικά κλειστό συνεπάγεται η ύπαρξη $\lambda_0 \in K$ ώστε να ισχύει $R(w, x, \lambda_0) = 0$ οπότε τα πολυώνυμα $f(w, x, Y + \lambda_0 w)$ και $f'(w, x, Y + \lambda_0 w)$ έχουν κοινή ρίζα έστω $y \in K$. Επομένως τα $f(w, x, Y)$ και $g(w, x, Y)$ έχουν μία κοινή ρίζα $y + \lambda_0 w$, κάτι το οποίο όμως είναι αδύνατο διότι $R(w, x, 0) = c_0 \neq 0$. Επομένως το $R(W, X, \lambda)$ δεν περιέχει το λ.

Αλλάζουμε συντεταγμένες

$$W' = W, \ \ X' = X, \ \ Y' = Y - yW.$$

Το P τώρα έχει την μορφή $[1, 0, 0]$ και η απαλείφουσα της καινούργιας εξίσωσης είναι όπως και της παλιάς $R(W', X') = R(W, X)$ (ως προς Y' και Y αντίστοιχα).

Περνούμε σε **αφινικές συντεταγμένες**.

Αφού, λόγω της υπόθεσης του θεωρήματος, το σημείο $P = (0, 0)$ είναι r-οστού βαθμού πολλαπλότητας σημείο της $C_f(K)$ και s-οστού βαθμού πολλαπλότητας σημείο της $C_{f'}(K)$ μπορούμε να γράψουμε

$$f(X, Y) = f_0X^r + f_1X^{r-1}Y + \cdots + f_rY^r + f_{r+1}Y^{r+1} + \cdots$$

και

$$g(X, Y) = g_0X^s + g_1X^{s-1}Y + \cdots + g_sY^s + g_{s+1}Y^{s+1} + \cdots$$

όπου $f_i, g_i \in K$.

$$R(X) = \left(\begin{array}{ccccccccc} f_0X^r & f_1X^{r-1} & \dots & f_r & f_{r+1} & \dots & f_m & & \\ & f_0X^r & \dots & f_{r-1}X & f_r & \dots & f_{m-1} & f_m & \\ & & \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & & & & & & \\ & & & f_0X^r & \dots\dots\dots\dots\dots\dots & & & f_m & \\ g_0X^s & g_1X^{s-1} & \dots & g_s & g_{s+1} & \dots & g_{n-1} & g_n & \\ & & \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & & & & & & \\ & & & & g_0X^s & \dots\dots\dots\dots & & g_n & \end{array} \right) \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} s \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} r \end{array}$$

Πολλαπλασιάζουμε την πρώτη γραμμή με X^s, την δεύτερη με X^{s-1}, $\cdots$ και την $s-$στή με X. Επίσης την πρώτη γραμμή της g με X^r, την δεύτερη με X^{r-1}, $\dots$ και την $r-$στή με X. Από την i-στήλη βγαίνει κοινός παράγοντας το $X^{r+s+1-i}$ οπότε η απαλείφουσα διαιρείται με X στην δύναμη

$$\sum_{i=1}^{r+s} i - \sum_{i=1}^{r} i = \frac{(r+s)(r+s+1)}{2} - \frac{r(r+1)}{2} - \frac{s(s+1)}{2} = rs.$$

□

Πρόταση 36. *Αν δύο αλγεβρικές καμπύλες C_f και $C_{f'}$ ορισμένες στο σώμα k βαθμού m και n αντίστοιχα* **δεν έχουν κοινή συνιστώσα** *στην επέκταση K του k και τα σημεία τομής τους έστω P_i $(i = 1, 2, \dots)$ έχουν βαθμό πολλαπλότητας r_i και s_i ως προς τις δύο καμπύλες αντίστοιχα τότε*

$$\sum_i r_i s_i \leq mn.$$

Απόδειξη: Όπως και στην πρόταση 34 (σελ. 36) διαλέγουμε έτσι το σύστημα συντεταγμένων ώστε οι f και f' να γράφονται ως εξής:

$$\begin{aligned} f(W, X, Y) &= A_0Y^m + A_1Y^{m-1} + \cdots + A_m, \\ f'(W, X, Y) &= B_0Y^n + B_1Y^{n-1} + \cdots + B_n \end{aligned}$$

όπου $A_0B_0 \neq 0$ και A_i, B_i για κάθε $i > 0$ είναι ομογενή πολυώνυμα βαθμού i ως προς W, X και έτσι ώστε δύο διαφορετικά σημεία τομής να μην βρίσκονται πάνω σε κάποια ευθεία της μορφής

$$xW - wX = 0.$$

Τότε, σύμφωνα με την πρόταση 35, σε κάθε σημείο (w, x, y) τομής των καμπυλών βαθμού πολλαπλότητας r_i και s_i αντίστοιχα, αντιστοιχεί μία ρίζα $\frac{w}{x}$ της απαλείφουσας $R(W, X)$ βαθμού πολλαπλότητας **τουλάχιστο** $r_i s_i$. Αφού, λόγω εκλογής του συστήματος συντεταγμένων, διαφορετικά σημεία δίνουν διαφορετικό λόγο $\frac{w}{x}$ έπεται ότι οι ρίζες της απαλείφουσας $R(W, X)$ που αντιστοιχούν σε διαφορετικά σημεία τομής είναι μεταξύ τους διαφορετικές.
Ώστε η $R(W, X)$ έχει τουλάχιστο $\sum_i r_i s_i$ ρίζες μετρημένες βέβαια με την πολλαπλότητά τους, οπότε

$$\sum_i r_i s_i \leq mn.$$

□

Παρατήρηση 37. *Η τελευταία πρόταση είναι χρήσιμη στην διαπίστωση ότι μερικές καμπύλες με «αρκετά» στο πλήθος ιδιάζοντα σημεία, δεν μπορούν να είναι ανάγωγες π.χ. μία κυβική καμπύλη με δύο διπλά σημεία θα πρέπει να έχει σαν συνιστώσα την ευθεία που τα συνδέει, διότι αλλιώς τα σημεία τομής της κυβικής καμπύλης και της ευθείας θα έδιναν* $\sum_i r_i s_i = 4 > 3 \cdot 1$. *Ώστε, μία* **ανάγωγη** *κυβική καμπύλη περιέχει το πολύ ένα ιδιάζον σημείο. Μία ανάγωγη κωνική τομή δεν έχει κανένα.*

Πρόταση 38. *Αν* C_f *και* $C_{f'}$ *είναι δύο αλγεβρικές καμπύλες υπεράνω του σώματος* k *και οι δύο βαθμού* n*, υποθέτουμε ότι για κάποιο* $K \supset k$ *ισχύει*

$$\#(C_f(K) \cap C_{f'}(K)) = n^2$$

και ότι **ακριβώς** mn *σημεία τομής ανήκουν σε μία* **ανάγωγη** *καμπύλη βαθμού* m*. Τότε τα υπόλοιπα* $n(n-m)$ *σημεία τομής βρίσκονται πάνω σε καμπύλη βαθμού* $n-m$*.*

Απόδειξη: Έστω C_h η ανάγωγη καμπύλη βαθμού m που περιέχει ακριβώς τα $m \cdot n$ σημεία τομής των C_f και $C_{f'}$. Βρίσκουμε δύο σταθερές λ_1 και $\lambda_2 \in \mathbb{C}$ έστι ώστε $\lambda_1 f + \lambda_2 f'$ να περνάει από τυχόν δοσμένο σημείο $P = [w, x, y]$. Στη συνέχεια διαλέγουμε το σημείο P να βρίσκεται πάνω στην $C_h(K)$.
Άρα η C_h και η $\lambda_1 f + \lambda_2 f'$ έχουν **τουλάχιστο** $mn + 1$ σημεία κοινά. Συνεπώς, από την πρόταση 34, έπεται ότι έχουν κοινή συνιστώσα. Αυτή όμως είναι η C_h, διότι C_h ανάγωγη. Άρα

$$C_{\lambda_1 f + \lambda_2 f'} = C_h \cdot C_H \text{ όπου η } C_H \text{ είναι βαθμού } n - m.$$

Η $\lambda_1 f + \lambda_2 f'$ όμως περνάει από n^2 σημεία τομής των C_f και $C_{f'}$. Άρα, αφού η C_h περνάει από mn σημεία η C_H θα περνάει από τα υπόλοιπα $(n-m)n$. □

Πρόταση 39. *Αν C_0 και C_1 είναι δύο κωνικές τομές με* **ακριβώς** *4 (P_1, P_2, P_3, P_4) διακεκριμένα σημεία μεταξύ τους ορισμένες υπεράνω του απείρου σώματος K. Κάθε άλλη κωνική τομή που περνάει από τα σημεία P_1, P_2, P_3, P_4 είναι της μορφής*

$$b_0 C_0 + b_1 C_1, \quad \text{όπου} \quad b_0, b_1 \in K.$$

Απόδειξη: Προφανώς δεν υπάρχει τριάδα από τα παραπάνω σημεία P_1, P_2, P_3, P_4 που να κείνται επ' ευθείας, διότι αλλιώς, σύμφωνα με την πρόταση 34, σελίδα 36, οι C_0 και C_1 θα είχαν μία ευθεία σαν κοινή συνιστώσα.

Αφού το K άπειρο, υπάρχει ένα πέμπτο σημείο της C έστω P διαφορετικό από τα P_i (στην περίπτωση που η C είναι γινόμενο δύο ευθειών, σαν P παίρνουμε το σημείο τομής τους).

Διαλέγουμε τώρα τα b_0 και b_1 έτσι ώστε η κωνική τομή $b_0 C_0 + b_1 C_1$ να περνάει από το P. Ώστε οι C και $b_0 C_0 + b_1 C_1$ έχουν 5 διακεκριμένα σημεία κοινά. Άρα έχουν κοινή συνιστώσα.

Αν η C είναι ανάγωγη τότε προφανώς, όπως και στην πρόταση 36, ισχύει $C = b_0 C_0 + b_1 C_1$.

Αν η C δεν είναι ανάγωγη τότε έχουμε:

$$C = L_0 \cup L_1 \text{ και } b_0 C_0 + b_1 C_1 = L_0 \cup L_2.$$

Η L_0 περιέχει το πολύ δύο σημεία τομής. Από τα υπόλοιπα τρία της L_1 το πολύ ένα μπορεί να ανήκει στην L_0, διότι αλλιώς η C θα ήταν ευθεία. Άρα L_1 και L_2 έχουν τουλάχιστο δύο κοινά σημεία. Επομένως οι L_1 και L_2 ταυτίζονται και συνεπώς και σ' αυτή την περίπτωση $C = b_0 C_0 + b_1 C_1$. □

Το επόμενο θεώρημα είναι **βασικό** για την απόδειξη της προσεταιριστικότητας στη δομή ομάδος της πρόσθεσης των ρητών σημείων ελλειπτικής καμπύλης.

Θεώρημα 40. *Έστω Γ_0 και Γ_1 δύο κυβικές καμπύλες, οι οποίες τέμνονται σε* **ακριβώς** *9 σημεία του $\mathbb{P}_2(K)$, όπου K* **άπειρο** *σώμα. Αν μία επίπεδη κυβική καμπύλη Γ περνάει από οκτώ από τα σημεία τομής των δύο καμπυλών Γ_0 και Γ_1, τότε περνάει και από το ένατο και έχει την μορφή*

$$\Gamma = b_0 \Gamma_0 + b_1 \Gamma_1, \quad b_0, b_1 \in K.$$

Απόδειξη: Ας υποθέσουμε ότι $P_1, P_2, \ldots, P_9$ είναι τα σημεία τομής των δυο καμπυλών Γ_0 και Γ_1 και ότι η καμπύλη Γ περνάει από τα σημεία $P_1, P_2, \ldots, P_8$. Θα αποδείξουμε ότι κατ'

ανάγκη θα περνάει και από το P_9. Δεν υπάρχει τετράδα των σημείων τομής που να βρίσκεται πάνω σε μία ευθεία, ούτε επτάδα σημείων που να βρίσκεται πάνω σε μία κωνική τομή. Αυτό ισχύει διότι, σύμφωνα με την πρόταση 34, η ευθεία ή η κωνική τομή θα ήταν συνιστώσα των καμπυλών Γ_0 και Γ_1 κάτι το οποίο δεν ισχύει, διότι έχουμε υποθέσει ότι οι Γ_0 και Γ_1 έχουν ακριβώς εννέα σημεία τομής.

Αν τώρα η $\Gamma = b_0\Gamma_0 + b_1\Gamma_1,\ b_0, b_1 \in K$, τότε τελειώσαμε, διότι η Γ θα περνάει και από το ένατο κοινό σημείο τομής P_9 αφού Γ_0 και Γ_1 κάνουν το ίδιο.
Έστω ότι οι Γ, Γ_0 και Γ_1 είναι γραμμικά ανεξάρτητες. Μπορούμε να διαλέξουμε πάντοτε συντελεστές b, b_0 και b_1 ώστε η καμπύλη

$$b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$$

να περνάει από δύο **οποιαδήποτε** δοσμένα σημεία.
Θα αποδείξουμε ότι αυτό οδηγεί σε άτοπο. Διακρίνουμε διάφορες περιπτώσεις:

(α′) Όπως κάναμε και στην πρόταση 38, βλέπουμε αμέσως ότι πέντε σημεία, εδώ τα P_4, P_5, P_6, P_7 και P_8, ορίζουν **μοναδική** κωνική τομή που περνάει απ′ αυτά. Ας ονομάσουμε αυτή την κωνική τομή C. Επίσης P_1, P_2, P_3, ανήκουν σε ευθεία L. Παίρνουμε δύο σημεία $A \in L, B \notin C \cup L$ και διαλέγουμε τα b, b_0, b_1 έτσι ώστε η καμπύλη $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$ να περνάει από τα σημεία A και B. Η καμπύλη $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$ περνάει επιπλέον και από τα σημεία $P_1, \ldots, P_8$. Επομένως έχει με την ευθεία L τέσσερα κοινά σημεία, τα P_1, P_2, P_3, A. Άρα η ευθεία L είναι συνιστώσα της $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$. Η άλλη συνιστώσα θα είναι (πρόταση 38, σελ. 40) μία κωνική τομή η οποία θα έχει 5 κοινά σημεία $(P_4, \ldots, P_8)$ με την C και συνεπώς θα συμπίπτει με την C.
Αυτό όμως είναι άτοπο διότι το σημείο B δεν ανήκει στην C.

(β′) Υποθέτουμε ότι έξι σημεία, π.χ., τα $P_1, \ldots, P_6$, βρίσκονται σε κωνική τομή C και ονομάζουμε L την ευθεία που ορίζουν τα P_7 και P_8. Έστω A κάποιο σημείο της C διάφορο των $P_i,\ i = 1, \ldots, 6$ και $B \notin C \cup L$. Διαλέγουμε πάλι τα b, b_0, b_1 έτσι ώστε η κυβική καμπύλη $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$ να περνάει από τα A και B. Η κωνική τομή C και η κυβική καμπύλη $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$ έχουν τώρα επτά κοινά σημεία, τα $P_1, P_2, P_3, P_4, P_5, P_6$ και A, άρα έχουν κοινή συνιστώσα. Αυτή είναι η ίδια η C, αν η C είναι ανάγωγη.

$$\text{Επομένως,}\quad b\Gamma + b_0\Gamma_0 + b_1\Gamma_1 = C \cup L'$$

όπου L' ευθεία. Αλλά οι ευθείες L και L' ταυτίζονται διότι έχουν δύο κοινά σημεία, τα P_7 και P_8.

Αυτό όμως είναι πάλι άτοπο, διότι $B \notin C \cup L$, ενώ $B \in b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$.

Αν η C δεν είναι ανάγωγη θα είναι ένωση δύο ευθειών, $C = L_1 \cup L_2$. Σ' αυτή την περίπτωση μία τουλάχιστο από τις δύο ευθείες θα είχε τέσσερα κοινά σημεία με την $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$, άτοπο.

(γ') Υποθέτουμε τώρα ότι δεν υπάρχει τριάδα σημείων από τα $P_1, \ldots, P_8$ τα οποία να ανήκουν σε ευθεία, ούτε εξάδα σημείων τα οποία να ανήκουν σε κάποια κωνική τομή. Ονομάζουμε L την ευθεία που ορίζουν τα P_1, P_2 και C την κωνική τομή που ορίζουν τα $P_3, \ldots, P_7$. Στην συνέχεια επιλέγουμε δύο σημεία A και B διαφορετικά των P_i, $(i = 1, \ldots, 8)$ τα οποία ανήκουν στην ευθεία L αλλά όχι στην κωνική τομή C. Διαλέγουμε τα b, b_0, b_1 ώστε η κυβική καμπύλη $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$ να περνάει από τα A και B. Όπως και παραπάνω, η καμπύλη $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$ έχει σαν συνιστώσα την ευθεία L (τέσσερα κοινά σημεία) και την κωνική τομή C διότι $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1 = L \cup C'$ όπου $C' \cap C = \{P_3, \ldots, P_7\}$ δηλαδή $C' = C$. Το άτοπο και αυτή τη φορά είναι ότι το P_8 ανήκει στην $b\Gamma + b_0\Gamma_0 + b_1\Gamma_1$ ενώ δεν ανήκει στην L (αλλιώς θα είχαμε τρία κοινά σημεία με την L) ούτε ανήκει στην C (διότι θα είχαμε και πάλι έξι σημεία τομής πάνω στην κωνική τομή C.

5. Σημεία καμπής (inflections ή flexes)

Ορισμός 41. *Ένα σημείο $P = [w, x, y]$ μιάς αλγεβρικής καμπύλης C_f θα λέγεται* **σημείο καμπής** *της C_f ακριβώς τότε όταν*

(i) το P είναι μη-ιδιάζον, και

(ii) ο βαθμός πολλαπλότητας της εφαπτομένης στο P είναι μεγαλύτερος ή ίσος του 3.

Σημείωση 42. *Από τον ορισμό έπεται ότι αν μία καμπύλη έχει σαν συνιστώσα κάποια ευθεία τότε κάθε μη-ιδιάζον σημείο της είναι σημείο καμπής.*
Αυτή η περίπτωση δεν μας ενδιαφέρει, έτσι στα επόμενα θα θεωρούμε μόνο καμπύλες που δεν έχουν ευθεία σαν συνιστώσα (δές πρόταση 31, σελίδα 35).

Λόγω της πρότασης 31, σελ. 35, για να είναι η αρχή των συντεταγμένων $[1, 0, 0]$ ένα

σημείο καμπής με εφαπτομένη την ευθεία

$$bX - aY = 0$$

θα πρέπει το πολυώνυμο $f(1, X, Y)$ να έχει την εξής μορφή:

$$f(1, X, Y) = (bX - aY) + g_2(X, Y) + \cdots + g_d(X, Y), \tag{2.2}$$

όπου το $g_i(X, Y)$ είναι ομογενές πολυώνυμο βαθμού i για $i = 2, 3, \ldots, d$ και

$$g_2(at, bt) = t^2 g_2(a, b) = 0.$$

Έστω τώρα μία κωνική τομή C υπέρ το σώμα k.

Υποθέτουμε ότι έχει ένα ιδιάζον σημείο. Μία ευθεία L που περνάει από το σημείο αυτό τέμνει (μέσα στην αλγεβρική θήκη του k, $\tilde{k}$) την κωνική τομή και σε ένα άλλο σημείο. Αφού $1 \cdot 2 + 1 \cdot 1 = 3 > 2$ η πρόταση 36, σελ. 39 δίνει ότι L και C έχουν κοινή συνιστώσα δηλαδή η L είναι συνιστώσα της C, και επομένως η C δεν είναι ανάγωγη. Από την άλλη μεριά αν η C δεν είναι ανάγωγη τότε αποτελείται από ένα ζευγάρι διακεκριμένων ευθειών, οπότε το σημείο τομής τους είναι ιδιάζον ή από το γινόμενο μιάς ευθείας με τον εαυτό της, οπότε όλα τα σημεία είναι ιδιάζοντα.

Ώστε: η κωνική τομή C είναι **ανάγωγη** ακριβώς τότε όταν δεν έχει κανένα ιδιάζον σημείο.

Πρόταση 43. *Η κωνική τομή C_f όπου*

$$f(X_0, X_1, X_2) = \sum_{i,j=0}^{2} a_{ij} X_i X_j \quad (\mu\epsilon\ a_{ij} = a_{ji})$$

είναι **μη-ανάγωγη** *τότε και μόνο τότε όταν η ορίζουσα $det(a_{ij}) = 0$.*

Απόδειξη: Η C_f είναι μη-ανάγωγη ακριβώς τότε όταν έχει ένα ιδιάζον σημείο, έστω $P = [x_0, x_1, x_2]$. Το τελευταίο όμως είναι ισοδύναμο με το ότι

$$\left.\frac{\partial f}{\partial x_0}\right|_P = \left.\frac{\partial f}{\partial x_1}\right|_P = \left.\frac{\partial f}{\partial x_2}\right|_P = 0 \quad (\text{πρότ. } 32, \text{ σελ. } 35)$$

δηλαδή με το ότι το παραπάνω σύστημα έχει μία μη τετριμμένη λύση. Επειδή

$$\frac{\partial f}{\partial x_i} = 2 \sum_{j=0}^{2} a_{ij} x_j, \quad (i = 0, 1, 2),$$

το σύστημα έχει μη-τετριμμένη λύση τότε και μόνο τότε όταν $det\big(a_{ij}\big)_{i,j=0,1,2} = 0$. □

Πρόταση 44. *Έστω τώρα* C_f *μία αλγεβρική καμπύλη,* $f(X_0, X_1, X_2) \in k[X_0, X_1, X_2]$. *Τα σημεία καμπής είναι ακριβώς τα μη ιδιάζοντα σημεία της καμπύλης τα οποία είναι σημεία τομής με την Hessian*

$$H(X_0, X_1, X_2) := det \begin{pmatrix} \frac{\partial^2 f}{\partial X_0^2} & \frac{\partial^2 f}{\partial X_1 \partial X_0} & \frac{\partial^2 f}{\partial X_2 \partial X_0} \\ \frac{\partial^2 f}{\partial X_0 \partial X_1} & \frac{\partial^2 f}{\partial X_1^2} & \frac{\partial^2 f}{\partial X_2 \partial X_1} \\ \frac{\partial^2 f}{\partial X_0 \partial X_2} & \frac{\partial^2 f}{\partial X_1 \partial X_2} & \frac{\partial^2 f}{\partial X_2^2} \end{pmatrix}.$$

Απόδειξη: Έστω $a = [a_0, a_1, a_2]$ ένα απλό (σελ. 34) σημείο της καμπύλης και $b = [b_0, b_1, b_2]$ κάποιο άλλο σημείο. Με $f_i(a)$ συμβολίζουμε την μερική παράγωγο της f ως προς X_i στο σημείο a. Ανάλογα ορίζεται το $f_{ij}(a) = \left.\frac{\partial^2 f}{\partial X_i \partial X_j}\right|_a$.
Από τον τύπο του Taylor προκύπτει

$$f(as + bt) = f(a)s^d + \sum_{i=0}^{2} f_i(a) b_i s^{d-1} t + \frac{1}{2} \sum_{i,j=0}^{2} f_{ij}(a) b_i b_j s^{d-2} t^2 + \cdots$$

Έστω L η ευθεία $\sum_{i=0}^{2} f_i(a) X_i = 0$ και Q η κωνική τομή $\sum_{i,j=0}^{2} f_{ij}(a) X_i X_j = 0$. Προφανώς το a είναι σημείο καμπής ακριβώς τότε όταν η L είναι συνιστώσα της Q δηλαδή ακριβώς τότε όταν $\sum_{i,j=0}^{2} f_{ij}(a) b_i b_j = 0$ εφ' όσον $\sum_{i=0}^{2} f_i(a) b_i = 0$.
Επομένως αν το a είναι σημείο καμπής τότε η Q δεν είναι ανάγωγη και συνεπώς (πρόταση 43, σελ. 44) $H(a) = 0$.

Αντίστροφα, αν $H(a) = 0$, τότε από την πρόταση 43, σελ. 44, έπεται ότι η Q δεν είναι ανάγωγη. Το σημείο a ανήκει στην Q, διότι

$$\sum_{i,j=0}^{2} f_{ij}(a) a_i a_j = d(d-1) f(a) = 0 \text{ (γενικευμένο θεώρημα του Euler).}$$

Η εφαπτομένη της Q στο σημείο a είναι $\sum_{i,j=0}^{2} f_{ij}(a) a_i X_j = 0$. Το αριστερό μέλος όμως, λόγω του θεωρήματος του Euler, γράφεται $(d-1) \sum_{j=0}^{2} f_j(a) X_j = 0$, δηλαδή $\sum_{j=0}^{2} f_j(a) X_j = 0$. Ώστε η εφαπτόμενη της Q στο a είναι η ευθεία L. Η Q όμως δεν είναι ανάγωγη. Επομένως η L είναι συνιστώσα της Q, δηλαδή το σημείο a είναι σημείο καμπής. □

Παρατήρηση: Αφού f είναι ομογενές πολυώνυμο βαθμού d έπεται ότι η H είναι ομογενές πολυώνυμο βαθμού $3(d-2)$.
Ώστε:

Πόρισμα 45. *Κάθε μη-ιδιάζουσα καμπύλη τάξεως μεγαλύτερης ή ίσης του 3 έχει τουλάχιστο ένα σημείο καμπής. Μια κωνική τομή δεν έχει κανένα σημείο καμπής.*

Έστω τώρα οτι μία μη-ιδιάζουσα κυβική καμπύλη έχει το σημείο καμπής $[1,0,0]$ με εφαπτομένη ευθεία την $Y=0$, δηλαδή τον άξονα των X. Η καμπύλη μας θα έχει την μορφή (δες σελ. 44)

$$f(1,X,Y) = Y + f_2(X,Y) + f_3(X,Y) = Y + bXY + aY^2 + f_3(X,Y)$$

διότι, για $Y=0$, θα πρέπει $f_2(X,0)=0$. Άρα

$$f(W,X,Y) = W^2Y + aY^2W + bWXY + f_3(X,Y).$$

Αν κάνουμε τώρα το ίδιο και πάρουμε το επ΄ άπειρο σημείο $[0,0,1]$ σαν σημείο καμπής, με εφαπτομένη την επ΄ έπειρο ευθεία $W=0$, τότε καταλήγουμε στην εξίσωση του παρακάτω ορισμού.

Ορισμός 46. *Η εξίσωση μιάς μη-ιδιάζουσας κυβικής καμπύλης C στην* **κανονική** *της* **μορφή** *είναι*

$$WY^2 + a_1WXY + a_3W^2Y = X^3 + a_2X^2W + a_4XW^2 + a_6W^3.$$

(Μερικές φορές λέγεται και **γενικευμένη μορφή του Weierstrass***).*

Ώστε, για να πάρουμε την κανονική μορφή πρέπει να μεταφέρουμε ένα σημείο καμπής στο άπειρο έτσι ώστε η εφαπτομένη να είναι η επ΄ άπειρο ευθεία.

Αν η χαρακτηριστική του σώματος k είναι διαφορετική του 2, τότε μπορούμε να γράψουμε την κανονική μορφή ως εξής:

$$W\left[Y^2 + 2\left(\frac{a_1X + a_3W}{2}\right)Y + \left(\frac{a_1X + a_3W}{2}\right)^2\right] = X^3 + \frac{b_2}{4}X^2W + \frac{b_4}{2}XW^2 + \frac{b_6}{4}W^3$$

όπου

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6.$$

Θέτουμε

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2.$$

και βρίσκουμε

$$4b_8 = b_2b_6 - b_4.$$

Για $\nu = Y + \dfrac{a_1 + a_3 W}{2}$ η κανονική μορφή γίνεται

$$W\nu^2 = X^3 + \frac{b_2}{4}X^2W + \frac{b_4}{2}XW^2 + \frac{b_6}{4}W^3.$$

Αν η χαρακτηριστική του σώματος k είναι διάφορη των 2 και 3 τότε για

$$c_4 = b_2^2 - 24b_4 \text{ και } c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

και $\xi = x + \dfrac{b_2}{12}$ η κανονική μορφή γίνεται

$$W\nu^2 = \xi^3 - \frac{c_4}{48}\xi W^2 - \frac{c_6}{864}W^3.$$

Παρατηρούμε ότι τα b_2, b_4, b_6, b_8 και c_4, c_6 είναι ακέραιοι αν a_1, a_2, a_3, a_4, a_6 είναι ακέραιοι.

Ορισμός 47. *Θα λέμε ότι μία μη-ιδιάζουσα κυβική καμπύλη C έχει εξίσωση στη* **μορφή** *του* **Weierstrass** *όταν έχει την μορφή*

$$WY^2 = X^3 + bW^2X + cW^3$$

Σε αφινικές συντεταγμένες γράφεται

$$Y^2 = f(X), \quad f(X) \in K[X],$$

κυβικό, εναδικό πολυώνυμο του οποίου το άθροισμα των ριζών είναι ίσο με μηδέν.

Το πολυώνυμο $f(X) = X^3 + bX + c$ έχει διπλή ρίζα, σε κάποια επέκταση του K, ακριβώς τότε όταν $D(f) = 4b^3 + 27c^2 = 0$.

Πρόταση 48. *Ένα σημείο $[1, a, 0]$ της C με εξίσωση $WY^2 = X^3 + bXW^2 + cW^3$ είναι* **μη-ιδιάζον** *ακριβώς τότε όταν το a είναι* **απλή** *ρίζα του $X^3 + bX + c$.*

Απόδειξη: Κατ' αρχήν παρατηρούμε ότι το σημείο $[w, x, y]$ της C είναι ιδιάζον αν και μόνο αν το σημείο $[w, x, -y]$ είναι επίσης ιδιάζον. Γνωρίζουμε όμως ότι μία ανάγωγη (δες σημείωση 42, σελίδα 43) κυβική καμπύλη έχει το πολύ ένα ιδιάζον σημείο, άρα πρέπει $y = 0$, δηλαδή το σημείο θα είναι της μορφής $[w, x, 0]$. Ένα σημείο $P = [1, x, 0]$ τώρα της καμπύλης είναι ιδιάζον ακριβώς τότε όταν

$$\left.\frac{\partial F}{\partial X}\right|_P = 0 \wedge \left.\frac{\partial F}{\partial Y}\right|_P = 0, \quad \text{όπου} \quad F(X, Y) = Y^2 - X^3 - bX - C.$$

Η $\dfrac{\partial F}{\partial Y}$ είναι πάντοτε ίση με μηδέν στο $P = [1, x, 0]$. Όμως $\left.\dfrac{\partial F}{\partial X}\right|_P = 0$ ακριβώς τότε όταν το x είναι διπλή ρίζα του $f(X) = X^3 + bX + c$ δηλαδή ακριβώς τότε όταν $D(f) = 0$. □

Ώστε η κυβική καμπύλη $Y^2 = X^3 + bX + c$ είναι μη-ιδιάζουσα αν και μόνο άν $D(f) \neq 0$.

Κεφάλαιο 3

Ρητά σημεία κυβικών καμπυλών

Στο κεφάλαιο αυτό αποδεικνύουμε ότι το σύνολο των ρητών σημείων μιάς ελλειπτικής καμπύλης με πράξη την πρόσθεση που θα ορίσουμε αποτελεί αβελιανή ομάδα. Επί πλέον μελετούμε ρητά σημεία P μιάς ελλειπτικής καμπύλης τάξεως 2 ή 3.

1. Δομή ομάδας πάνω σε μη-ιδιάζουσες κυβικές καμπύλες

Στην εισαγωγή περιγράψαμε την μέθοδο της χορδής και εφαπτομένης στην σύνθεση PQ δύο σημείων P και Q μιάς κυβικής καμπύλης υπέρ το k. Δηλαδή το PQ είναι το τρίτο σημείο τομής της ευθείας L που περνάει από τα P και Q. Για κάθε επέκταση K του k ο νόμος σύνθεσης είναι μία συνάρτηση

$$\Gamma(K)\times\Gamma(K) \longrightarrow \Gamma(K).$$

$$(P,Q) \longmapsto PQ.$$

Από αυτά που αναπτύχθηκαν στο προηγούμενο κεφάλαιο έχουμε τις εξής περιπτώσεις:

Έστω L μία ευθεία και C μία κυβική καμπύλη ορισμένες πάνω στο k. Έστω $\tilde{k}$ η αλγεβρική θήκη του k. Για τα σημεία τομής λοιπόν $L(\tilde{k})\cap C(\tilde{k})$ έχουμε

(α′) Αν $L(\tilde{k})\cap C(\tilde{k}) = \{P_1, P_2, P_3\}$ τρία σημεία όπου ή πολλαπλότητα τομής $i(P_i, L, C) = 1$ για $i = 1, 2, 3$. Η σύνθεση δίνεται λοιπόν από τη σχέση $P_iP_j = P_k$ και αν δύο από τα τρία σημεία είναι ρητά υπέρ το k τότε το ίδιο είναι και το τρίτο.

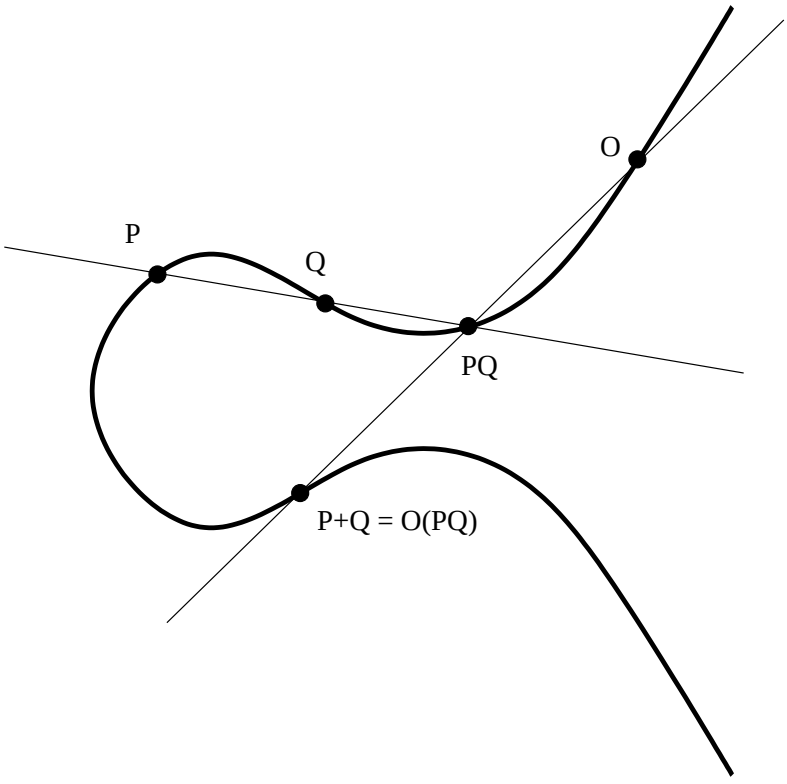
(β′) Αν $L(\tilde{k})\cap C(\tilde{k}) = \{P, P')\}$ δύο σημεία, όπου $i(P, L, C) = 2$ και $i(P', L, C) = 1$. Ώστε η L είναι εφαπτομένη της C στο P ή το P είναι ιδιάζον σημείο της C, και η σύνθεση

δίνεται από τη σχέση $PP = P'$ και $PP' = P$ και, αν το P είναι ρητό υπέρ το k, το ίδιο ισχύει και για το P'.

(γ') $L(\tilde{k}) \cap C(\tilde{k}) = \{P\}$ ένα σημείο όπου η πολλαπλότητα τομής $i(P, L, C) = 3$ οπότε $PP = P$ και το P είναι σημείο καμπής.

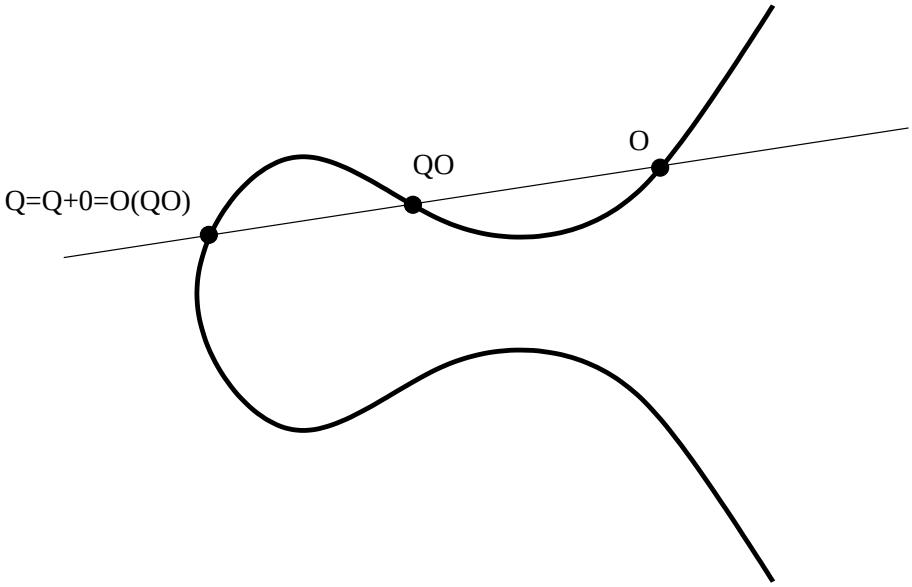
Θεώρημα 1. *Έστω Γ μία κυβική καμπύλη που ορίζεται πάνω στο σώμα k και K μία επέκταση του k και έστω $\mathcal{O} \in \Gamma(K)$. Ο νόμος σύνθεσης $P + Q = \mathcal{O}(PQ)$ κάνει το $\Gamma(K)$ αβελιανή ομάδα με $\mathcal{O}$ το μηδενικό στοιχείο και $-P = P(\mathcal{O}\mathcal{O})$. Επιπλέον το $\mathcal{O}$ είναι σημείο καμπής αν και μόνο αν $P + Q + R = \mathcal{O}$ όπου P, Q, R είναι τα τρία σημεία τομής της Γ με μία ευθεία. Σ' αυτήν την περίπτωση $-P = P\mathcal{O}$.*

Απόδειξη: Προφανώς $P+Q = Q+P$ διότι $PQ = QP$, δηλαδή ισχύει η αντιμεταθετικότητα. Γενικά ισχύει $P(PQ) = Q$. Για $P = \mathcal{O}$ βρίσκουμε $Q = \mathcal{O}(\mathcal{O}Q) = \mathcal{O} + Q$. Ώστε το $\mathcal{O}$ είναι το ουδέτερο στοιχείο, δες σχήμα 3.2.



Σχήμα 3.1: Πρόσθεση ρητών σημείων

Για το αντίθετο θεωρούμε την εφαπτομένη της Γ στο $\mathcal{O}$.



Σχήμα 3.2: Πρόσθεση ρητών σημείων

Η ευθεία αυτή τέμνει την καμπύλη στο σημείο $\mathcal{OO}$. Αν τώρα P κάποιο ρητό σημείο της καμπύλης, η ευθεία $P(\mathcal{OO})$ τέμνει την καμπύλη σε κάποιο τρίτο σημείο, το οποίο είναι το $-P$, δηλαδή $P = P(\mathcal{OO})$.

Προτού αποδείξουμε τον προσεταιρισμό, αποδεικνύουμε την τελευταία απαίτηση του θεωρήματος.

Αν P, Q, R είναι τρία σημεία τομής της Γ με μία ευθεία, τότε $R = PQ$. Τώρα $-R = P + Q$ αν και μόνο αν $-R = (\mathcal{OO})R = \mathcal{O}(PQ) = P + Q$. Αυτό όμως ισχύει ακριβώς τότε όταν $(\mathcal{OO})R = \mathcal{O}R$ ή αλλιώς $\mathcal{O} = \mathcal{OO}$ δηλαδή ακριβώς τότε όταν το $\mathcal{O}$ είναι σημείο καμπής.

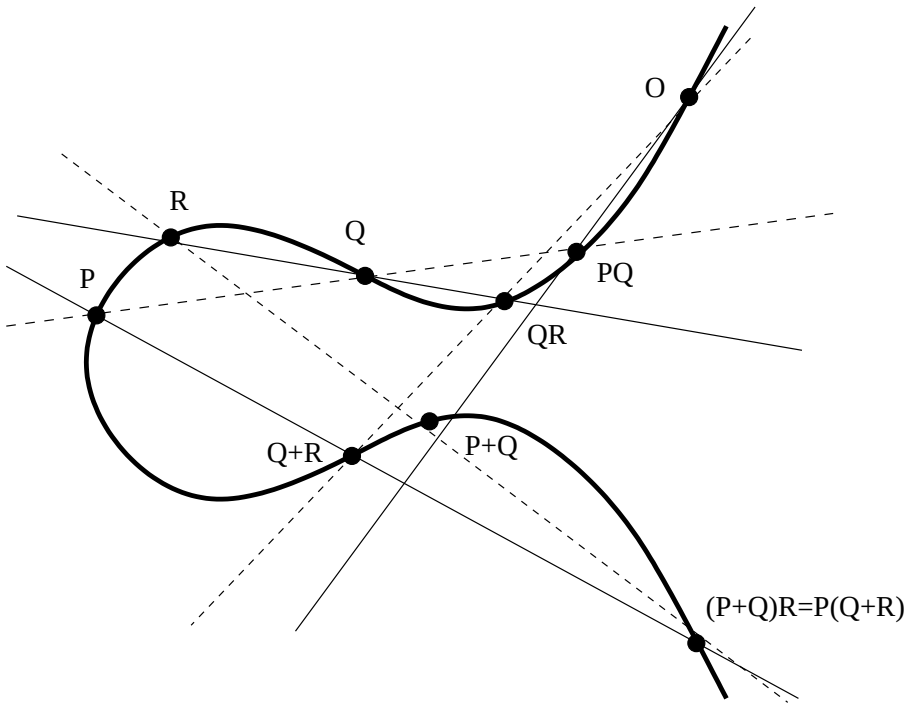
Για τον προσεταιριστικό νόμο αρκεί να δείξουμε ότι $P(Q + R) = (P + Q)R$, δες σχήμα 3.3.

Έστω ότι P, Q και R διακεκριμένα μεταξύ τους σημεία της καμπύλης Γ.

Έχουμε τα ακόλουθα 8 σημεία πάνω στην καμπύλη

$$\mathcal{O},\ P,\ Q,\ R,\ PQ,\ RQ,\ P{+}Q,\ R{+}Q.$$

Καθένα απ' αυτά τα 8 σημεία είναι σημείο μιάς **κόκκινης** και μιάς **μπλέ** ευθείας γραμμής. Το γινόμενο των εξισώσεων των κόκκινων ευθειών δίνει μία κυβική καμπύλη. Το ίδιο και το γινόμενο των μπλέ.



Σχήμα 3.3: Προσεταιρισμός πρόσθεσης ρητών σημείων

Το σημείο τομής των ευθειών $R, P+Q$ και $P, R+Q$ είναι το ένατο σημείο τομής των δύο κυβικών καμπυλών. Η δοθείσα κυβική καμπύλη Γ έχει 8 κοινά σημεία και με τις δύο, άρα θα έχει και το ένατο, δηλαδή οι ευθείες που ορίζονται από τα σημεία $R, P+Q$ και $P, R+Q$ τέμνονται πάνω στη Γ, δηλαδή τα σημεία $R(P+Q)$ και $P(R+Q)$ ταυτίζονται, οπότε $(P+Q)+R = P+(Q+R)$.

Οταν τα P, Q και R δεν είναι διακεκριμένα βλέπουμε ότι, εφαρμόζοντας την αντιμεταθετικότητα, απομένει να εξεταστεί η περίπτωση

$$P+(P+Q) = (P+P)+Q.$$

Η απόδειξη της τελευταίας ισότητας αφήνεται σαν άσκηση στον αναγνώστη. □

Ορισμός 2. *Μία* **ελλειπτική καμπύλη** *E υπέρ το k είναι μία μη-ιδιάζουσα κυβική καμπύλη ωρισμένη υπέρ το σώμα k μαζί με ένα* **μηδενικό (ουδέτερο) σημείο** *$\mathcal{O} \in E(k)$ και τον αντίστοιχο νόμο σύνθεσης στο $E(K)$ (για κάθε επέκταση K του k) που ορίζεται από το προηγούμενο θεώρημα.*

Παρατήρηση: Αν $K \xrightarrow{\varphi} K'$, ένας k-ομομορφισμός σωμάτων, τότε αυτός επάγει έναν ομομορφισμό ομάδων

$$E(K) \xrightarrow{\tilde{\varphi}} E(K').$$

2. Παραδείγματα και μέθοδοι υπολογισμού

Έστω μία κυβική καμπύλη στην κανονική της μορφή

$$C : WY^2 + a_1WXY + a_3W^2Y \ = \ X^3 + a_2X^2W + a_4XW^2 + a_6W^3$$

ορισμένη πάνω στο σώμα k.

Η τομή της καμπύλης C με την επ΄ άπειρο ευθεία $W = 0$ δίνεται από τη σχέση $X^3 = 0$. Δηλαδή το σημείο $P = [0, 0, 1]$ είναι το **μοναδικό** σημείο τομής της ευθείας $W = 0$ και της καμπύλης C. Επομένως το σημείο αυτό έχει βαθμό πολλαπλότητας $i(L, C, P) = 3$ δηλαδή είναι σημείο καμπής. Αυτό το σημείο παίρνουμε σαν ουδέτερο στοιχείο $\mathcal{O}$.

Τα μη-μηδενικά σημεία της καμπύλης είναι λύσεις της αφινικής εξίσωσης

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

Οι ευθείες τώρα που διέρχονται από το επ΄ άπειρο σημείο $P = [0, 0, 1]$ είναι ακριβώς οι κάθετες στον άξονα των x στο αφινικό $xy-$επίπεδο και η επ΄ άπειρο ευθεία.

Άρα, αν $P = (x, y)$ τότε $-P = (x, y^*)$ διότι και τα δύο σημεία βρίσκονται πάνω σε μία ευθεία που περνάει από το $\mathcal{O}$, δηλαδή μία ευθεία κάθετη προς τον άξονα των x.

Αφού τώρα και τα δύο y και y^* είναι ρίζες της εξίσωσης

$$Y^2 + (a_1x + a_3)Y = x^3 + a_2x^2 + a_4x + a_6$$

η οποία είναι δευτέρου βαθμού ως προς Y, βρίσκουμε ότι $y + y^* = -a_1x - a_3$.

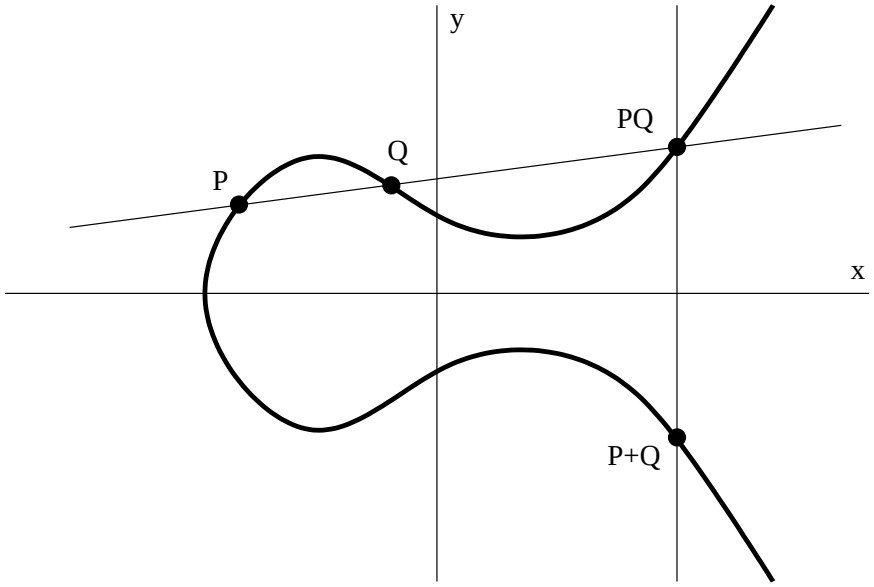
Ώστε: Πάνω σε μία ελλειπτική καμπύλη E δοσμένη σε κανονική μορφή

$$WY^2 + a_1WXY + a_3W^2Y = X^3 + a_2X^2W + a_4XW^2 + a_6W^3$$

το αντίθετο του $(x, y) \in E(k)$ δίνεται από τη σχέση

$$-P = -(x, y) = (x, -y - a_1x - a_3).$$

Σημείωση 3. *Αν $a_1 = 0$ τότε $-P = -(x, y) = (x, -y - a_3)$ και αν $a_1 = a_3 = 0$ τότε $-P = -(x, y) = (x, -y)$.*



Σχήμα 3.4: Πρόσθεση ρητών σημείων

Στην συνέχεια θα προθέσουμε δύο σημεία P και Q μιάς ελλειπτικής καμπύλης E.

Αν $a_1 = a_3 = 0$ τότε το $P + Q$ είναι το συμμετρικό του PQ ως προς τον άξονα των x.

Στην γενική περίπτωση γράφουμε $P_1P_2 = P_3$ όπου (x_i, y_i) είναι οι συντεταγμένες του P_i, $i = 1, 2, 3$. Θα βρούμε τις συντεταγμένες του σημείου P_3 συναρτήσει αυτών των P_1 και P_2.

Περίπτωση 1η: Αν $x_1 \neq x_2$ τότε η ευθεία που περνάει από τα P_1 και P_2 έχει εξίσωση

$$Y = \lambda X + \nu, \text{ όπου } \lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

Περίπτωση 2η: Αν $P_1 = P_2 = P$ τότε η εφαπτομένη στο P έχει εξίσωση

$$Y = \lambda X + \nu, \text{ όπου } \lambda = \frac{f'(x_1) - a_1 y - 1}{2y_1 + a_1 x_1 + a_3}.$$

Αντικαθιστούμε το Y στην εξίσωση της καμπύλης και βρίσκουμε

$$(\lambda X + \nu)^2 + a_1 X(\lambda X + \nu) + a_3(\lambda X + \nu) = X^3 + a_2 X^2 + a_4 X + a_6$$

$$\Longrightarrow X^3 + (a_2 - \lambda^2 - \lambda a_1)X^2 + (a_4 - 2\lambda\nu - a_1\nu - \lambda a_3)X + (a_6 - \nu^2 - a_3\nu) = 0.$$

Οι τρεις ρίζες της κυβικής εξίσωσης x_1, x_2, x_3 είναι οι X-συντεταγμένες των τριών σημείων τομής. Επομένως

$$x_1 + x_2 + x_3 = -a_2 + \lambda^2 + \lambda a_1,$$

δηλαδή

$$x_3 = \lambda^2 + \lambda a_1 - a_2 - x_1 - x_2 \tag{3.1}$$

και $y_3 = \lambda x_3 + \nu$. Τελικά παίρνουμε

$$(x_1, y_1) + (x_2, y_2) \;=\; (x_3, -y_3 - a_1 x_3 - a_3) \;=\; (x_3, -(\lambda + a_1)x_3 - \nu - a_3).$$

Παρατήρηση 4. *Ένα σημείο $P = (x, y)$ είναι τάξης 2 μέσα στην ομάδα $E(k)$ ακριβώς τότε όταν*

$$2P = \mathcal{O} \iff P = -P \iff (x, y) = (x_3, -y_3 - a_1 x_1 - a_3).$$

$$Αν \quad ch(k) \neq 2 \quad τότε \quad y = -\frac{a_1 x + a_3}{2}.$$

Αν η E έχει τη μορφή $Y^2 = f(X) = X^3 + aX^2 + bX + c$ τότε το σημείο $P = (x, y)$ είναι τάξης 2 τότε και μόνο τότε όταν $(x, y) = (x, -y)$, δηλαδή ακριβώς τότε όταν $y = 0$.

Ώστε τα σημεία τάξεως 2 είναι ακριβώς εκείνα της μορφής $(x, 0)$ όπου x λύση της κυβικής εξίσωσης

$$X^3 + aX^2 + bX + c = 0 \tag{3.2}$$

Αυτό σημαίνει ότι η 2-ομάδα στρέψεως $E(K)_{\text{2-torsion}}$ έχει τάξη ένα, άν καμμία ρίζα της (3.2) δεν ανήκει στο k.

$E(k)_{\text{2-torsion}}$ έχει τάξη δύο, άν μία ρίζα της (3.2) ανήκει στο k.

$E(k)_{\text{2-torsion}}$ έχει τάξη 4, άν όλες οι ρίζες της (3.2) ανήκουν στο k.

Στην τελευταία περίπτωση η $E(k)_{\text{2-torsion}}$ είναι ισόμορφη με την τετραδική ομάδα του Klein.

3. Μερικές παρατηρήσεις στα σημεία διαίρεσης

Ξαναθυμόμαστε τώρα ότι τα 2-σημεία διαίρεσης, τα «ρητά» δηλαδή σημεία τάξης 2 μιάς ελλειπτικής καμπύλης E στην κανονική μορφή του Weierstrass

$$Y^2 = f(X)$$

όταν η χαρακτηριστική του σώματος k είναι διάφορη του 2 είναι τα $(\alpha_1, 0)$, $(\alpha_2, 0)$ και $(\alpha_3, 0)$ όπου $\alpha_1, \alpha_2, \alpha_3$ είναι διακεκριμένες ρίζες της κυβικής εξίσωσης $f(X) = 0$. Επί πλέον ισχύει για $\{1, 2, 3\} = \{i, j, k\}$ ότι

$$(\alpha_i, 0) + (\alpha_j, 0) = (\alpha_k, 0).$$

Ώστε η ομάδα των 2-σημείων διαίρεσης της E πάνω από το σώμα $K = k(\alpha_1, \alpha_2, \alpha_3)$ είναι ισόμορφη με την **τετραδική** ομάδα του Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Κάνοντας τώρα έναν κατάλληλο αφινικό μετασχηματισμό $X \mapsto \alpha X + \beta$, στέλνουμε τα σημεία $(\alpha_1, 0), (\alpha_2, 0)$ στα $(0,0)$ και $(1,0)$ αντίστοιχα, οπότε η εξίσωση παίρνει την παρακάτω **μορφή του Legendre**:

$$Y^2 = X(X-1)(X-\lambda), \quad \lambda \neq 0, 1.$$

Τι γίνεται τώρα όταν η χαρακτηριστική του k είναι 2;

Γράφουμε την εξίσωση στη μορφή

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

Είναι ήδη γνωστό ότι αν $P = (x, y)$ τότε $-P = (x, -y - a_1x - a_3)$, οπότε $2P = \mathcal{O}$ στην $E(k)$ τότε και μόνο τότε όταν $a_1x + a_3 = 0$. Στη συνέχεια ξεχωρίζουμε δύο περιπτώσεις.

(i) Αν $a_1 \neq 0$. Στην αλγεβρική θήκη του k, $\tilde{k}$ η ομάδα των 2-σημείων διαίρεσης έχει δύο ακριβώς στοιχεία $\mathcal{O}$ και (x, y) όπου $x = \dfrac{a_3}{a_1}$ και $y^2 = f\left(\dfrac{a_3}{a_1}\right)$.
Άρα είναι κυκλική τάξεως 2.

(ii) Αν $a_1 = 0$ τότε αντικαθιστούμε το Y με a_3Y και έχουμε

$$a_3^2Y^2 + a_3Y = f(X) \Longrightarrow Y^2 + Y = f'(X)$$

οπότε το μοναδικό 2-σημείο διαίρεσης είναι το $\mathcal{O}$.

Θα κλείσουμε την παρούσα παράγραφο με τη μελέτη των ρητών σημείων τάξεως 3 μιάς ελλειπτικής καμπύλης.
Έστω E ελλειπτική καμπύλη στη μορφή του Weierstrass

$$Y^2 = X^3 + aX^2 + bX + c$$

Αν $P = (x, y) \in E(k)$ τότε αν $3P = \mathcal{O}$ έχουμε $2P = -P$, δηλαδή $2P = -(x, y) = (x, -y)$. Με άλλα λόγια η εφαπτομένη $Y = \lambda X + \nu$ της E στο $P = (x, y)$ έχει τομή βαθμού πολλαπλότητας 3 και συνεπώς θα πρέπει να είναι σημείο καμπής. Άρα θα έχουμε

$$(\lambda X + \nu)^2 = x^3 + ax^2 + bx + c \Rightarrow x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + c - \nu^2 = 0$$

με τριπλή ρίζα το x. Επομένως

$$3x = \lambda^2 - a = (\frac{f'(x)}{2y})^2 - a$$

διότι $\lambda = \frac{f'(x)}{2y}$. Λύνουμε την εξίσωση ως προς $f'(x)$ και βρίσκουμε

$$f'(x)^2 = (3x + a)4y^2 = 2f(x)(6x + 2a) = 2f(x)f''(x)$$

$$\text{δηλαδή} \quad g(x) := f'(x)^2 - 2f(x)f''(x) = 0.$$

Πρόταση 5. *Έστω E ελλειπτική καμπύλη στη μορφή του Weierstrass*

$$Y^2 = f(X) = X^3 + aX^2 + bX + c$$

(i) Αν η χαρακτηριστική του k είναι διάφορη του 3 τότε η ομάδα $E(\tilde{k})$ έχει 9 σημεία (x, y) τάξεως 3 όπου το x είναι λύση της εξίσωσης $4^{ου}$ βαθμού

$$g(X) = f'(X)^2 - 2f(X)f''(X) = 0.$$

Η ομάδα αυτών των σημείων τάξεως 3 είναι ισόμορφη προς την $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(ii) Αν η χαρακτηριστική του σώματος k είναι 3 και $a \neq 0$, τότε η $E(\tilde{k})$ έχει 3 σημεία $(x, \pm y)$ και $\mathcal{O}$ όπου x είναι η πλήρως μη-διαχωρίσιμη ρίζα του

$$\frac{4ac - b^2}{4a}.$$

Η ομάδα είναι ισόμορφη προς την $\mathbb{Z}/3\mathbb{Z}$.

(iii) Αν $chk = 3$ και $a = 0$ τότε $E(k)_{3\text{-}torsion} = \{\mathcal{O}\}$.

Αποδειξη:

(i) Αρκεί να δείξουμε ότι το πολυώνυμο $g(X) = 0$ έχει 4 διακεκριμένες ρίζες στο $\tilde{k}$. Κατ' αρχήν

$$g'(X) = 2f'(X)f''(X) - 2f'(X)f''(X) - 2f(X)f'''(X) = -12f(X).$$

Μια κοινή ρίζα των $g(X)$ και $g'(X)$ θα ήταν κοινή ρίζα και των $f(X)$ και $f'(X)$. Αυτό όμως δεν είναι δυνατό γιατί η $f'(X)$ και $f(X)$ δεν έχουν κοινές ρίζες, εξ ορισμού της E. Ώστε, το $g(X)$ δεν έχει διπλή ρίζα. Επομένως και οι 4 ρίζες του είναι μεταξύ τους διαφορετικές. Δηλαδή έχουμε $(x, \pm y)$, όπου x ρίζα του $g(X)$ συνολικά 8 σημεία τάξεως 3 και το μηδενικό. Το γεγονός ότι $E(\tilde{k}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ είναι προφανές.

(ii) Αν τώρα $\mathrm{ch}k = 3$ έπεται ότι

$$f'(X) = 2aX + b \quad \text{και} \quad f''(X) = 2a$$

$$\text{οπότε} \quad g(X) = f'(X)^2 - 2f(X)f''(X) =$$

$$= (2aX + b)^2 - 2(2a)(X^3 + aX^2 + bX + c) = -4aX^3 + b^2 - 4ac.$$

Αν $a \neq 0$ τότε το x είναι κυβική ρίζα του $\dfrac{4ac - b^2}{4a}$.

(iii) Αν $a = 0$ τότε δεν υπάρχει σημείο του οποίου η τάξη να διαιρεί τον 3 άλλο εκτός από το $\mathcal{O}$.

Παρατήρηση 6. *Αναφέρουμε προς το παρόν ότι αν το k είναι αλγεβρικά κλειστό τότε τα n-σημεία διαίρεσης της $E(k)$, δηλαδή ο πυρήνας του ομομορφισμού*

$$\begin{cases} E(k) & \xrightarrow{\nu} & E(k) \\ P & \longmapsto & nP \end{cases}$$

είναι ισόμορφος προς την $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ υπό την προϋπόθεση ότι $(n, chk) = 1$.

Για τα p-σημεία διαίρεσης σε σώμα k χαρακτηριστικής p έχουμε δύο περιπτώσεις.

(α′) **Κανονικές** καμπύλες (ordinary), όταν τα σημεία αυτά αποτελούν κυκλική υποομάδα της $E(\tilde{k})$ τάξεως p.

(β′) **Υπεριδιάζουσες** καμπύλες E όταν

$$E(\tilde{k})_{p\text{-torsion}} = \{\mathcal{O}\}.$$

Κεφάλαιο 4

Το Θεώρημα των Lutz-Nagell

Στο κεφάλαιο αυτό περιοριζόμαστε, για λόγους ευκολίας, σε ελλειπτικές καμπύλες που είναι ορισμένες πάνω από το σώμα των ρητών αριθμών $\mathbb{Q}$. Στο τέλος του κεφαλαίου ίσως περιγράψουμε τι γίνεται σε γενικότερες περιπτώσεις.

Σκοπός μας είναι να χαρακτηρίσουμε όλα τα σημεία **πεπερασμένης τάξης** (torsion points) της ομάδας των ρητών σημείων $E(\mathbb{Q})$ μιάς ελλειπτικής καμπύλης

$$E : Y^2 = f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X] \quad (1).$$

Ότι τα σημεία πεπερασμένης τάξης μιάς αβελιανής ομάδας αποτελούν υποομάδα αυτής είναι γνωστό και η απόδειξή του αφήνεται σαν άσκηση στον αναγνώστη.

Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι οι συντελεστές του πολυωνύμου $f(X)$ είναι **ακέραιοι** αριθμοί. Αν δεν είναι, πολλαπλασιάζουμε με Z^6 και αντικαθιστούμε το Y με το Z^3Y και το X με το Z^2X, οπότε έχουμε

$$Y^2 = X^3 + Z^2aX^2 + Z^4bX + Z^6c.$$

Με κατάλληλη επιλογή του Z τώρα μπορούμε να εξαλείψουμε τους παρονομαστές. Επομένως μπορούμε να υποθέσουμε ότι

$$Y^2 = f(X) = X^3 + aX^2 + bX + c \in \mathbb{Z}[X].$$

1. Το θεώρημα των Lutz-Nagell

Το κύριο αποτέλεσμα του κεφαλαίου διατυπώνεται ως εξής:

Θεώρημα 1 (Θεώρημα των Lutz-Nagell) *Όλα τα σημεία πεπερασμένης τάξης* $P = (x, y)$ *της* $E(\mathbb{Q})$ *έχουν* **ακέραιες συντεταγμένες** x *και* y *και μάλιστα ή* $y = 0$ *(σημεία τάξης 2) ή* $y \mid D(f)$ *την διακρίνουσα του* $f(X)$

$$(D(f) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2).$$

Παρατήρηση 2. *Λόγω της πρότασης 13, σελίδα 23, ισχύει*

$$D(f) = R(f, f') = A(X)f(X) + B(X)f'(X) \quad \text{όπου} \quad A(X), B(X) \in \mathbb{Z}[X].$$

Αν μπορούμε να αποδείξουμε ότι τα ρητά σημεία πεπερασμένης τάξης έχουν ακέραιες συνιστώσες τότε, με χρήση του παραπάνω τύπου της διακρίνουσας, μπορούμε να αποδείξουμε ότι $y = 0$ *ή* $y \mid D(f)$*, οπότε, μετά από πεπερασμένου πλήθους βημάτων βρίσκουμε όλα τα δυνατά* $y \mid D(f)$*, τα αντικαθιστούμε στην εξίσωση* $Y^2 = f(X)$*. Αφού* $f(X)$ *έχει ακέραιους συντελεστές και συντελεστή μεγαλύτερης δύναμης του* X *την μονάδα έπεται ότι αν το* $f(X)$ *έχει κάποια ακεραία ρίζα, αυτή θα διαιρεί το σταθερό όρο του πολυωνύμου* $f(X)$*.*

Έτσι είμαστε εξασφαλισμένοι ότι μπορούμε να βρούμε όλα τα σημεία πεπερασμένης τάξης μετά από πεπερασμένο πλήθος βημάτων.

Προσοχή! Δεν ισχυριζόμαστε ότι κάθε σημείο $P = (x, y)$ με ακέραιες συντεταγμένες και $y \mid D(f)$ είναι σημείο πεπερασμένης τάξης.

Απόδειξη: Υποθέτουμε κατ' αρχήν ότι τα σημεία πεπερασμένης τάξης έχουν ακέραιες συντεταγμένες. Έστω $P = (x_1, y_1)$ ένα τέτοιο σημείο. Θα αποδείξουμε ότι $y_1 = 0$ ή $y_1 \mid D(f)$. Είναι γνωστό, από το προηγούμενο κεφάλαιο, ότι

$$2P = \mathcal{O} \iff y_1 = 0.$$

Έστω τώρα $2P \neq \mathcal{O}$. Το $2P$ θα είναι τότε κι αυτό πεπερασμένης τάξης και, σύμφωνα με την υπόθεση, θα έχει ακέραιες συντεταγμένες. Έστω $2P = (x_2, y_2)$. Ο τύπος (3.1) της σελίδας 55 τώρα δίνει

$$x_2 = \lambda^2 - a - 2x_1 \quad \text{όπου} \quad \lambda = \frac{f'(x_1)}{2y_1}.$$

Αφού $a, x_1, x_2 \in \mathbb{Z}$ έπεται ότι $\lambda^2 \in \mathbb{Z}$.

Από τη σχέση $\lambda = \dfrac{f'(x_1)}{2y_1}$ έπεται ότι ο λ είναι ρητός αριθμός, ενώ από τη σχέση $x_2 = \lambda^2 - a - 2x_1$ και, δεδομένου ότι a, x_1, x_2 είναι ακέραιοι, έπεται ότι ο λ είναι κατ' ανάγκη ακέραιος. Επομένως $2y_1 \mid f'(x_1)$ οπότε και $y_1 \mid f'(x_1)$. Επιπλέον $y_1 \mid y_1^2 = f(x_1)$. Συνεπώς,

$$y_1 \mid D(f) = A(x_1)f(x_1) + B(x_1)f'(x_1).$$

Ερχόμαστε τώρα στο δύσκολο κομμάτι της απόδειξης. Θα αποδείξουμε ότι τα ρητά σημεία πεπερασμένης τάξης μιάς ελλειπτικής καμπύλης έχουν ακέραιες συντεταγμένες. Για να αποδείξουμε ότι κάποιος ρητός αριθμός, γραμμένος σε μορφή αναγώγου κλάσματος, είναι ακέραιος, αρκεί να αποδείξουμε ότι ο παρονομαστής του είναι ίσος με ένα. Ένας τρόπος να αποδείξουμε ότι κάποιος ακέραιος αριθμός είναι ίσος με 1 είναι να αποδείξουμε ότι δεν διαιρείται με κανένα πρώτο. Ώστε, μπορούμε να σπάσουμε το πρόβλημα σε άπειρα κομμάτια και να δείξουμε ότι όταν μία συνιστώσα του σημείου x μπορεί να γραφεί σε **ανάγωγο** κλάσμα $\frac{A}{B}$ τότε ο παρονομαστής B δεν διαιρείται ούτε με το 2, ούτε με το 3, ούτε μέ κανένα άλλο πρώτο αριθμό.

Αν αποδείξουμε λοιπόν αυτό για τους παρονομαστές των x και y τότε θα έχουμε τελειώσει, δηλαδή θα έχουμε αποδείξει ότι $x, y \in \mathbb{Z}$.

Ξαναθυμίζουμε ότι αν ο x γράφεται $x = p^r \cdot \frac{a}{b}$ όπου $p \nmid ab$ τότε έχουμε $\mathrm{ord}_p(x) = r$. Προφανώς λοιπόν το p διαιρεί τον παρονομαστή ρητού αριθμού x ακριβώς τότε όταν $\mathrm{ord}_p(x) < 0$ και p διαιρεί τον αριθμητή του x ακριβώς τότε όταν $\mathrm{ord}_p(x) > 0$.

Ο p δεν διαιρεί ούτε τον αριθμητή ούτε τον παρονομαστή αν και μόνο αν $\mathrm{ord}_p(x) = 0$.

Έστω $P = (x, y)$ κάποιο ρητό σημείο της E με

$$x = \frac{m}{np^r} \quad \text{και} \quad y = \frac{d}{ep^s} \quad \text{όπου} \quad r > 0 \quad \text{και} \quad p \nmid mnde.$$

Η εξίσωση της ελλειπτικής καμπύλης μας δίνει

$$\frac{d^2}{e^2p^{2s}} = \frac{m^3 + am^2np^r + bmn^2p^{2r} + cn^3p^{3r}}{n^3p^{3r}}$$

οπότε $\mathrm{ord}_p\left(\frac{d^2}{e^2p^{2s}}\right) = -2s$. Αφού $r > 0$ και $p \nmid m$ έπεται ότι

$$p \nmid (m^3 + am^2np^r + bmn^2p^{2r} + cn^3p^{3r}).$$

Επομένως

$$\mathrm{ord}_p\left(\frac{m^3 + am^2np^r + bmn^2p^{2r} + cn^3p^{3r}}{n^3p^{3r}}\right) = -3r.$$

Άρα $2s = 3r$ και επομένως $s > 0$ (αφού $r > 0$). Αυτό σημαίνει ότι το p διαιρεί και τον παρονομαστή του y.

Ακόμη $3 \mid s$ και αν $s = 3q$ έπεται ότι $r = 2q$, $q \in \mathbb{Z}$ $(q > 0)$.

Αν τώρα υποθέσουμε ότι ο p διαιρεί τον παρονομαστή του y, τότε, όμοια βρίσκουμε ότι $p \mid x$, $r = 2q$ και $s = 3q$, $q \in \mathbb{Z}$, $q > 0$, και φυσικά p διαιρεί και τον παρονομαστή του x.

Ώστε: Αν κάποιος πρώτος αριθμός διαιρεί έναν από τους παρονομαστές των x και y θα διαιρεί και τον άλλο και μάλιστα οι ακριβείς δυνάμεις διαρέσεως θα έχουν την μορφή $2q$ και $3q$ αντίστοιχα.

Για οποιοδήποτε ρητό σημείο $P = (x(P), y(P))$ της ελλειπτικής καμπύλης E, ορίζουμε

$$A(p^r) := \left\{P \in E(\mathbb{Q}) \middle| \operatorname{ord}_p(\operatorname{denom}(x(P))) \geq 2r \text{ και } \operatorname{ord}_p(\operatorname{denom}(y(P))) \geq 3r\right\} \cup \{\mathcal{O}\}.$$

$$\text{Προφανώς} \quad E(\mathbb{Q}) \supset A(p) \supset A(p^2) \supset \cdots$$

Σκοπός μας είναι να δείξουμε ότι ένα σημείο πεπερασμένης τάξης δεν μπορεί να ανήκει στο $A(p)$. Πρώτα απ' όλα όμως θα αποδείξουμε ότι τα $A(p^r)$ αποτελούν υποομάδες της $E(\mathbb{Q})$.

Κατ' αρχήν θα αλλάξουμε συντεταγμένες και θα φέρουμε το $\mathcal{O}$ σε κάποια «πεπερασμένη» θέση.
Θέτουμε $t = \dfrac{X}{Y}$ και $s = \dfrac{1}{Y}$ οπότε η εξίσωση της καμπύλης

$$Y^2 = X^3 + aX^2 + bX + c \quad \text{μετασχηματίζεται στην}$$

$$s = t^3 + at^2 s + bts^2 + cs^3 \quad \text{στο } (t,s)\text{-επίπεδο.}$$

Στο (t,s)-επίπεδο έχουμε τώρα όλα τα σημεία του (x,y)-επιπέδου εκτός εκείνων για τα οποία $y = 0$. Το επ' άπειρο σημείο της καμπύλης το έχουμε τώρα στην θέση $(0,0)$.

Σχηματικά λοιπόν θα μπορέσουμε να σχεδιάσουμε την καμπύλη στα δύο συστήματα συντεταγμένων.

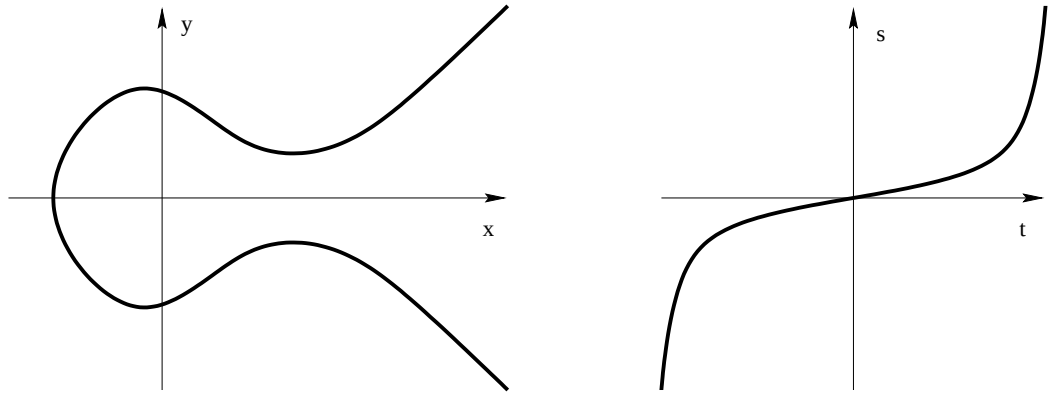
Στο αριστερό σχήμα βλέπουμε όλα τα σημεία της καμπύλης εκτός του $\mathcal{O}$. Στο δεξιό βλέπουμε όλα τα σημεία της καμπύλης (και το $\mathcal{O}$) εκτός των σημείων τάξεως 2, δηλαδή εκτός των σημείων τομής με τον άξονα των x. Αν λοιπόν εξαιρέσουμε το επ' άπειρον σημείο $\mathcal{O}$ και τα σημεία τάξεως 2, όλα τα υπόλοιπα ρητά σημεία βρίσκονται σε αμφιμονοσήμαντη αντιστοιχία μεταξύ τους.

Μία ευθεία $y = \lambda x + \nu$ του (x,y)-επιπέδου αντιστοιχεί σε μία ευθεία του (t,s)-επιπέδου. Πράγματι, αν διαιρέσουμε την $\lambda x + \nu$ με την νy έχουμε

$$\frac{1}{\nu} = \frac{\lambda}{\nu}\frac{x}{y} + \frac{1}{y}$$

η οποία στο (t,s)-επίπεδο μας δίνει

$$s = \frac{-\lambda}{\nu}t + \frac{1}{\nu}.$$



Σχήμα 4.1: Μετασχηματισμός

Επομένως στο (t,s)-επίπεδο μπορούμε να προσθέσουμε σημεία όπως και στο (x,y)-επίπεδο.

Θεωρούμε τον **τοπικό** δακτύλιο

$$R := R_p = \big\{x \in \mathbb{Q} \,\big|\, \mathrm{ord}_p(x) \geq 0\big\}$$

ο οποίος έχει ως γνωστό (μοναδικό) μέγιστο ιδεώδες το

$$\mathfrak{m} = \big\{x \in \mathbb{Q} \,\big|\, \mathrm{ord}_p(x) > 0\big\} \quad \text{και ομάδα μονάδων} \quad R^* = \big\{x \in \mathbb{Q} \big|\mathrm{ord}_p(x) = 0\big\}.$$

Έστω $(x,y) \in E(\mathbb{Q})$ του (x,y)-επιπέδου με

$$x = \frac{m}{np^{2q}}, \quad y = \frac{d}{ep^{3q}}.$$

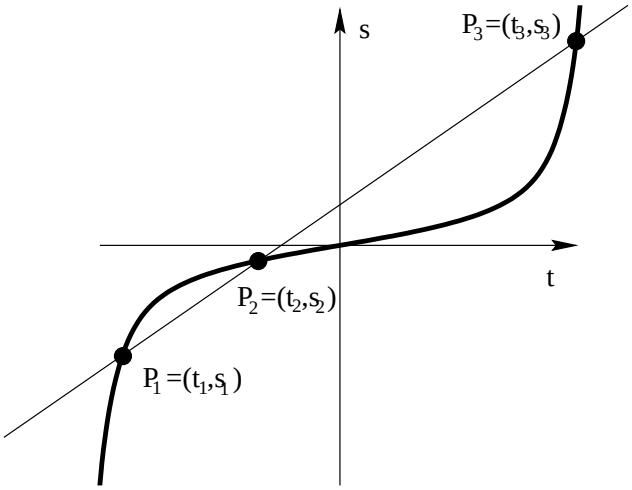
$$\text{Τότε} \quad t = \frac{x}{y} = \frac{em}{dn}p^q \quad \text{και} \quad s = \frac{1}{y} = \frac{e}{d}p^{3q}.$$

Συνεπώς:

$$(x,y) \in A(p^r) \iff (t \in p^r R \ \text{ και } \ s \in p^{3r}R).$$

Για να δείξουμε ότι το σύνολο $A(p^r)$ είναι υποομάδα της ομάδας $E(\mathbb{Q})$ αρκεί να δείξουμε ότι είναι κλειστό ως προς την πρόσθεση, δηλαδή αν κάποια δύναμη του p διαιρεί τις t-συνιστώσες δύο ρητών σημείων της καμπύλης θα διαιρεί και την t-συνιστώσα και του αθροίσματος.

Έστω $P_1 = (t_1, s_1)$ και $P_2 = (t_2, s_2)$ δύο διακεκριμένα σημεία της καμπύλης. Αν $t_1 = t_2$, τότε $P_1 = -P_2$, οπότε $P_1 + P_2 \in A(p^r)$. Υποθέτουμε λοιπόν ότι $t_1 \neq t_2$ και έστω $s = \rho t + \sigma$ η ευθεία που τα συνδέει.



Σχήμα 4.2: Πρόσθεση ρητών σημείων μετασχηματισμένης καμπύλης

Τα σημεία $P_1 = (t_1, s_1)$ και $P_2 = (t_2, s_2)$ επαληθεύουν την εξίσωση της ελλειπτικής καμπύλης $s = t^3 + at^2 s + b + s^2 + cs^3$. Επομένως έχουμε

$$\begin{aligned} & s_1 &=& \ t_1^3 + at_1^2 s_1 + bt_1 s_1^2 + cs_1^3 \\ \text{και} \qquad & s_2 &=& \ t_2^3 + at_2^2 s_2 + bt_2 s_2^2 + cs_2^3 \end{aligned}$$

Αφαιρούμε τις τελευταίες δύο ισότητες κατά μέλη

$$s_2 - s_1 \ = \ \left(t_2^3 - t_1^3\right) + a\left[(t_2^2 - t_1^2)s_2 + t_1^2(s_2 - s_1)\right] + b\left[(t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)\right] + c\left(s_2^3 - s_1^3\right).$$

Συνεπώς

$$(s_2 - s_1) - at_1^2(s_2 - s_1) - bt_1(s_2^2 - s_1^2) - c(s_2^3 - s_1^3) \ = \ t_2^3 - t_1^3 + a(t_2^2 - t_1^2)s_2 + b(t_2 - t_1)s_2^2.$$

Η κλίση της ευθείας που συνδέει τα δύο σημεία P_1 και P_2 είναι

$$\rho \ = \ \frac{s_2 - s_1}{t_2 - t_1} \ = \ \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)} \tag{4.1}$$

Ομοίως, αν $P_1 = P_2$, η κλίση της εφαπτομένης της καμπύλης στο P_1 είναι

$$\rho = \frac{ds}{dt}(P_1) = \frac{3t_1^2 + 2at_1 s_1 + bs_1^2}{1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2},$$

κάτι το οποίο προκύπτει και από την παραπάνω σχέση, αν θέσουμε $t_2 = t_1$ και $s_2 = s_1$. Επομένως θα εργασθούμε με την σχέση (4.1).

Έστω $P_3 = (t_3, s_3)$ το τρίτο σημείο τομής της ευθείας $s = \rho t + \sigma$ με την καμπύλη. Στην εξίσωση της καμπύλης, αντικαθιστούμε το s με $\rho t + \sigma$ και παίρνουμε:

$$\rho t + \sigma = t^3 + at^2(\rho t + \sigma) + bt(\rho t + \sigma)^2 + c(\rho t + \sigma)^3$$

$$\Longrightarrow 0 = t^3(1 + a\rho + b\rho^2 + c\rho^3) + t^2(a\sigma + 2b\rho\sigma + 3c\rho^2\sigma) + \cdots$$

Από τις σχέσεις ριζών συντελεστών προκύπτει:

$$t_1 + t_2 + t_3 = -\frac{a\sigma + 2b\rho\sigma + 3c\rho^2\sigma}{1 + a\rho + b\rho^2 + c\rho^3}.$$

Αφού η ευθεία περνάει από το σημείο $P_1 = (t_1, s_1)$ έπεται ότι $\sigma = s_1 - \rho t_1$.

Τώρα πρέπει να βρούμε το $P_1 + P_2$. Φέρουμε την ευθεία που περνάει από το σημείο (t_3, s_3) και το μηδενικό σημείο $(0, 0)$. Το τρίτο σημείο τομής θα είναι το $(-t_3, -s_3)$. Ας κυττάξουμε το ρ. Ο αριθμητής του ρ ανήκει στο $p^{2r}R$ διότι $t_1, s_1, t_2, s_2 \in p^rR$. Ο παρονομαστής είναι μονάδα του R. Άρα $\rho \in p^{2r}R$.

$$\text{Από τις σχέσεις} \quad \left.\begin{array}{l} s_1 \in p^{3r}R \\ \rho \in p^{2r}R \\ t_1 \in p^rR \end{array}\right\} \Longrightarrow \sigma = s_1 - \rho t_1 \in p^{3r}R.$$

Ο παρονομαστής $1 + a\rho + b\rho^2 + c\rho^3$ του $t_1 + t_2 + t_3$ είναι επίσης μονάδα του R. Συνεπώς

$$t_1 + t_2 + t_3 \in p^{3r}R.$$

Αφού $t_1, t_2 \in p^rR$ έπεται ότι $t_3 \in p^rR$, οπότε και $-t_3 \in p^rR$. Αποδείξαμε λοιπόν ότι η t-συνιστώσα του $P_1 + P_2$ ανήκει στο p^rR.

Αφού για $P = (t, s)$, $-P = (-t, -s)$ έπεται ότι, αν $P_1, P_2 \in A(p^r)$ τότε $P_1 \pm P_2 \in A(p^r)$, και συνεπώς η $A(P^r)$ είναι **υποομάδα** της $E(\mathbb{Q})$.

Με την βοήθεια των παραπάνω θα τελειώσουμε την απόδειξη του θεωρήματος των Lutz-Nagell.

Την t-συνιστώσα ενός σημείου I της καμπύλης θα την θεωρούμε σαν συνάρτηση του σημείου και θα την συμβολίζουμε με $t(P)$. Σε κάθε σημείο λοιπόν P θα αντιστοιχούμε κάποιο ρητό αριθμό $t(P)$.

$$\text{Αν} \quad P_1, P_2 \in A(p^r) \quad \text{τότε} \quad t_1 + t_2 + t_3 \in p^{3r}R, \quad \text{δηλαδή}$$

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3r}R}.$$

Επομένως η απεικόνιση t είναι ένας ομομορφισμός της ομάδας $A(p^r)$ στην ομάδα πηλίκων $p^rR/p^{3r}R$:

$$A(p^r) \xrightarrow{t} p^rR/p^{3r}R.$$

Ο πυρήνας της t είναι η ομάδα $A(p^{3r})$, διότι $t(P) \in p^{3r}R$ αν και μόνο αν $P \in A(p^{3r})$.
Η απεικόνιση t επάγει έναν μονομορφισμό ομάδων,

$$A(p^r)/A(p^{3r}) \xrightarrow{t} p^rR/p^{3r}R.$$

Έστω τώρα $P \in E(\mathbb{Q})_{\text{torsion}}$, σημείο της καμπύλης πεπερασμένης τάξης, έστω m. Υποθέτουμε ότι $P \neq \mathcal{O}$, δηλαδή ότι $m \neq \pm 1$.
Αν p είναι οποιοσδήποτε πρώτος αριθμός, θα αποδείξουμε ότι $P \notin A(p)$.

Αν $P \in A(p)$, τότε υπάρχει $r \in \mathbb{N}$ τέτοιος ώστε $P \in A(p^r) - A(p^{r+1})$. Ξεχωρίζουμε δύο περιπτώσεις, ανάλογα με το αν $p \nmid m$ ή $p \mid m$. Ας υποθέσουμε, κατ' αρχάς, ότι $p \nmid m$. Από τη γνωστή σχέση

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3r}R}$$

με επαγωγή βρίσκουμε ότι

$$0 = t(mP) \equiv mt(P) \pmod{p^{3r}R}.$$

Αφού όμως $p \nmid m$, έπεται ότι

$$t(P) \equiv 0 \pmod{p^{3r}R} \quad \text{και συνεπώς} \quad P \in A(p^{3r})$$

άτοπο, διότι $P \notin A(p^{r+1})$.

Αν πάλι $p \mid m$, τότε γράφουμε $m = pn$ και έστω P' το σημείο $n \cdot P$. Η τάξη του στοιχείου P' είναι p. Αν $P \in A(p)$ τότε και $P' \in A(p)$ και έστω πάλι $P' \in A(p^r) - A(p^{r+1})$. Όπως παραπάνω έχουμε

$$0 \equiv t(pP') \equiv p \cdot t(P') \pmod{p^{3r}R}$$

Αυτό σημαίνει ότι

$$t(P') \equiv 0 \pmod{p^{3r-1}R} \quad \text{δηλαδή ότι} \quad P' \in A(p^{3r-1}),$$

το οποίο όμως είναι άτοπο διότι $3r - 1 \geq r + 1$ και $P' \notin A(p^{r+1})$.

Αποδείξαμε ότι αν P ρητό σημείο της καμπύλης πεπερασμένης τάξης τότε το

$$P \notin A(p), \quad \text{για κάθε πρώτο αριθμό } p,$$

δηλαδή το θεώρημα. □

Σημείωση 3. *Μπορεί κανείς γενικότερα να αποδείξει ότι, όταν $y \neq 0$, τότε όχι μόνον το $y|D(f)$, αλλά ότι $y^2|D(f)$ (δες [24], σελίδα 221).*

Αναφέρουμε την τάξη της $E(\mathbb{Q})_{\text{torsion}}$ από μερικές ελλειπτικές καμπύλες:

- $y^2 = x^3 - 2$, η τάξη της είναι ένα, μόνο το μηδενικό στοιχείο.
- $y^2 = x^3 + 8$, η τάξη της είναι 2, $(\mathcal{O}, (-2, 0))$.
- $y^2 = x^3 - 432$, η τάξη της είναι 3.
- $y^2 = x^3 + 4x$, είναι κυκλική, τάξης 4.
- $y^2 = x^3 - 4x$, είναι τάξης 4 με ομάδα την τετραδική ομάδα του Klein.
- $y^2 = x^3 - 16 \cdot 27x + 19 \cdot 16 \cdot 27$, έχει τάξη 5 με γεννήτορα το σημείο $P = (-12, 108)$.
- $y^2 = x^3 + 1$, η τάξη της είναι 6.
- $y^2 = x^3 - 43x + 166$, με τάξη 8 και ομάδα $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Το πρόβλημα της εύρεσης όλων των δυνατών αβελιανών ομάδων που είναι υλοποιήσιμες σαν ομάδες ρητών σημείων πεπερασμένης τάξης ελλειπτικής καμπύλης ορισμένης πάνω από το $\mathbb{Q}$ λύθηκε τελικά από τον **Mazur** το 1976.

Συγκεκριμένα απέδειξε το εξής

Θεώρημα 4 (Θεώρημα του Mazur) *Έστω E ελλειπτική καμπύλη ωρισμένη πάνω από το $\mathbb{Q}$. Οι δυνατότητες της ομάδας $E(\mathbb{Q})_{torsion}$ είναι οι εξής*

$$E(\mathbb{Q})_t \cong \mathbb{Z}/m\mathbb{Z} \quad \text{για} \quad m \leq 10 \quad \text{ή} \quad m = 12$$

$$\text{ή} \quad E(\mathbb{Q})_t \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \quad \text{για} \quad m \leq 4.$$

Η απόδειξη του θεωρήματος είναι πολύ δύσκολη και, σύμφωνα με την γνώμη πολλών Μαθηματικών αποτελεί ένα από τα σπουδαιότερα στα Μαθηματικά επιτεύγματα κατά την δεκαετία του εβδομήντα.

Κεφάλαιο 5

Το Θεώρημα του Mordell

Σκοπός του κεφαλαίου αυτού είναι η απόδειξη του **Θεωρήματος του Mordell** ότι

> **η αβελιανή ομάδα $E(\mathbb{Q})$ των ρητών σημείων, μιάς ελλειπτικής καμπύλης E ορισμένης πάνω από το $\mathbb{Q}$, είναι πεπερασμένα παραγόμενη.**

Αυτό σημαίνει ότι υπάρχουν πεπερασμένου πλήθους σημεία της αβελιανής ομάδας $E(\mathbb{Q})$, έστω $Q_1, Q_2, \ldots, Q_n$, τέτοια ώστε κάθε σημείο P της $E(\mathbb{Q})$ να γράφεται στην μορφή

$$P = k_1 Q_1 + \cdots + k_n Q_n + T$$

όπου $k_1, k_2, \cdots, k_n \in \mathbb{Z}$ και το T να ανήκει σε κάποιο **πεπερασμένο** υποσύνολο της $E(\mathbb{Q})$.

Μία πολύ χρήσιμη έννοια για τα επόμενα είναι η έννοια του **ύψους** (height, Höhe) ενός ρητού αριθμού. Αν $x = \dfrac{m}{n}$ ρητός, γραμμένος σε μορφή αναγώγου κλάσματος, τότε σαν ύψος του x, **ορίζουμε** το $H(x) = \max\{|m|, |n|\}$.

Μία πολύ βασική ιδιότητα του ύψους είναι ότι, για κάθε θετικό πραγματικό αριθμό M, το σύνολο

$$\#\{x \in \mathbb{Q} \mid H(x) \leq M\} < \infty$$

είναι πεπερασμένο. Η απόδειξη αφήνεται σαν άσκηση στον αναγνώστη. Έστω τώρα $Y^2 = f(X) = X^3 + aX^2 + bX + c \in \mathbb{Z}[X]$ μία ελλειπτική καμπύλη και $P = (x, y) \in E(\mathbb{Q})$. **Ύψος του σημείου** P θα καλείται το ύψος της συνιστώσας x αυτού.

Για κάθε θετικό πραγματικό αριθμό M, το σύνολο

$$\{P \in E(\mathbb{Q}) \mid H(P) \leq M\}$$

είναι πεπερασμένο διότι υπάρχουν πεπερασμένου πλήθους δυνατότητες για το x και σε κάθε x αντιστοιχούν το πολύ δύο σημεία (το πολύ δύο y).

Για το επ΄ άπειρο τώρα σημείο της καμπύλης ορίζουμε $H(\mathcal{O}) = 1$.

1. Απόδειξη του θεωρήματος του Mordell

Για να αποδειχθεί το θεώρημα, χρειάζονται τρία λήμματα.

Λήμμα 1. *Για κάθε ρητό σημείο $P_0 \in E(\mathbb{Q})$ υπάρχει μία θετική σταθερά c_0 (εξαρτωμένη από το P_0) έτσι ώστε*

$$H(P + P_0) \leq c_0 H(P)^2, \quad \textit{για όλα τα } P \in E(\mathbb{Q}).$$

Λήμμα 2. *Υπάρχει μία θετική σταθερά $c > 0$ τέτοια ώστε*

$$H(P)^4 \leq cH(2P), \quad \textit{για όλα τα σημεία } P \in E(\mathbb{Q}).$$

Λήμμα 3. *Ο δείκτης $[E(\mathbb{Q}):2E(\mathbb{Q})]$ είναι πεπερασμένος.*

Σημείωση 4. *Είναι προφανές ότι το σύνολο*

$$2E(\mathbb{Q}) = \{P \in E(\mathbb{Q}) \mid \exists Q \in E(\mathbb{Q}) : P = 2Q\}$$

είναι υποομάδα της $E(\mathbb{Q})$.

Γενικά, για κάθε φυσικό αριθμό $m \in \mathbb{N}$, ορίζουμε την συνάρτηση

$$E(\mathbb{Q}) \ni P \stackrel{m}{\longmapsto} mP \in E(\mathbb{Q}),$$

η οποία είναι ομομορφισμός ομάδων. Η εικόνα της m είναι η υποομάδα $mE(\mathbb{Q})$ της $E(\mathbb{Q})$.

Υποθέτουμε προς το παρόν την αλήθεια των τριών λημμάτων, και θα αποδείξουμε την αλήθεια του θεωρήματος του Mordell.

Η απόδειξη είναι γενική. Θα μπορούσαμε να υποθέσουμε ότι έχουμε μία προσθετική αβελιανή ομάδα G και μία συνάρτηση $H : G \to N$ έτσι ώστε να ισχύουν τα τρία λήμματα. Τότε η G είναι πεπερασμένα παραγόμενη.

Απόδειξη του Θεωρήματος:

Έστω $A = \{Q_1, Q_2, \cdots, Q_n\}$ ένα πλήρες σύστημα αντιπροσώπων των πλευρικών κλάσεων της $E(\mathbb{Q})/2E(\mathbb{Q})$. Αυτό σημαίνει ότι για κάθε $P \in E(\mathbb{Q})$ υπάρχει $i_1 \in \mathbb{N}_n$ (εξαρτώμενος από το P) τέτοιος ώστε

$$P - Q_{i_1} = 2P_1, \quad P_1 \in E(\mathbb{Q}).$$

Συνεχίζουμε τώρα την ίδια διαδικασία με το P_1, με το P_2 που θα βρούμε, και έχουμε:

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\cdots\cdots\cdots\cdots \\ P_{m-1} - Q_{i_m} &= 2P_m \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

όπου $Q_{i_1}, Q_{i_2}, \cdots, Q_{i_m} \in A$ και $P_i \in E(\mathbb{Q})$.

Τελικά βρίκουμε

$$\begin{aligned} P &= Q_{i_1} + 2P_1 = Q_{i_1} + 2(Q_{i_2} + 2P_2) = \\ &= Q_{i_1} + 2Q_{i_2} + 4P_2 = \cdots \\ &= Q_{i_1} + 2Q_{i_2} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m. \end{aligned}$$

Από την τελευταία σχέση έπεται ότι το P ανήκει στην υποομάδα της $E(\mathbb{Q})$ που παράγεται από τα Q_{i_λ}, $\lambda = 1, 2, \cdots, m$ και το P_m. Η ιδέα τώρα είναι να χρησιμοποιήσουμε τα λήμματα 1 και 2 και να δείξουμε ότι, για αρκετά μεγάλο m, το P_m έχει ύψος μικρότερο από κάποιο σταθερό φράγμα, οπότε δεν έχει σημασία από ποιό P αρχίσαμε. Το σημείο P_m θα είναι στοιχείο ενός συγκεκριμένου πεπερασμένου συνόλου στοιχείων της $E(\mathbb{Q})$ τα οποία μαζί με τα $Q_1, Q_2, \cdots, Q_m$ θα παράγουν την $E(\mathbb{Q})$.

Ας εξετάσουμε την σχέση των υψών των P_{m-1} και P_m. Θα δείξουμε ότι το $H(P_m)$ είναι αρκετά μικρότερο του $H(P_{m-1})$.

Εφαρμόζουμε το **Λήμμα 1** για $P_0 = -Q_i$, $i = 1, 2, \cdots, n$, και έχουμε

$$H(P - Q_i) \leq c_i H(P)^2, \quad \text{για κάθε } P \in E(\mathbb{Q}).$$

Για $c' := \max\{c_i \mid i = 1, 2, \cdots, n\}$ έπεται ότι

$$H(P - Q_i) \leq c' H(P)^2, \quad \text{για κάθε } P \in E(\mathbb{Q}) \text{ και κάθε } i = 1, 2, \ldots, n.$$

Εφαρμόζουμε τώρα το **Λήμμα 2** και βρίσκουμε ότι

$$H(P_m)^4 \leq cH(2P_m) = cH(P_{m-1} - Q_{i_m}) \leq cc'H(P_{m-1})^2$$

Την παραπάνω ανισότητα γράφουμε ως εξής:

$$H(P_m)^4 \leq \frac{16cc'}{H(P_{m-1})^2} \cdot \left(\frac{H(P_{m-1})}{2}\right)^4$$

$$\Longrightarrow H(P_m) \leq \sqrt[4]{\frac{16cc'}{H(P_{m-1})^2}} \cdot \frac{H(P_{m-1})}{2}$$

Αν τώρα υποθέσουμε ότι

$$H(P_{m-1})^2 > 16cc' \quad \text{θα έχουμε} \quad \Longrightarrow H(P_m) < \frac{H(P_{m-1})}{2}.$$

Αυτό όμως είναι άτοπο γιατί η ακολουθία των σημείων $P_1, P_2, \cdots, P_m, \cdots$ μας δίνει ακολουθία υψών που τείνει στο μηδέν.

$$\text{Άρα, για αρκετά μεγάλο } m, \text{ ισχύει} \quad H(P_m)^2 \leq 16cc'$$

οπότε τα σημεία $Q_1, Q_2, \ldots, Q_n$ μαζί με τα σημεία P για τα οποία $H(P) < 4\sqrt{cc'}$ παράγουν την $E(\mathbb{Q})$, δηλαδή έχουμε αποδείξει την αλήθεια του Θεωρήματος του Mordell.

Σημείωση 5. *Συχνά, για πρακτικούς κυρίως λόγους, ορίζουμε σαν ύψος ενός σημείου P της $E(\mathbb{Q})$ τον λογάριθμο του ύψους του P, $h(P) := \log H(P)$.*

Προτού τώρα αποδείξουμε τα λήμματα θα κάνουμε δύο παρατηρήσεις.

Παρατήρηση 6. *Αν $P = (x, y) \in E(\mathbb{Q})$ τότε*

$$x = \frac{m}{e^2} \quad \textit{και} \quad y = \frac{n}{e^3}$$

όπου m, n και $e \in \mathbb{Z}$, $e > 0$ και $(m, e) = (n, e) = 1$.

Απόδειξη της παρατήρησης 6: Έστω $x = \frac{m}{M}$ και $y = \frac{n}{N}$ όπου τα κλάσματα είναι ανάγωγα και $M > 0$ και $N > 0$. Η $Y^2 = f(X)$ δίνει

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c$$

$$\Rightarrow M^3n^2 = N^2m^3 + aN^2m^2M + bN^2mM^2 + cN^2M^3 \tag{5.1}$$

Επομένως, $N^2|M^3n^2$, οπότε $N^2|M^3$, διότι $(N,n)=1$.

Θα αποδείξουμε και το αντίστροφο, δηλαδή ότι $M^3|N^2$.

Κατ' αρχήν από την (5.1) παίρνουμε ότι $M|N^2m^3$, δηλαδή $M|N^2$ αφού $(M,m)=1$. Με βάση την τελευταία διαιρετότητα ξαναγυρίζουμε πίσω στην (5.1) και βρίσκουμε ότι $M^2|N^2m^3$, οπότε $M^2|N^2$. Και πάλι ξαναγυρίζουμε πίσω στην (5.1) και βρίσκουμε ότι $M^2|N^2m^3$, επομένως $M^3|N^2$.

Ώστε $M^3=N^2$, οπότε για $e=\dfrac{N}{M}$ έχουμε την επιθυμητή έκφραση της παρατήρησης. □

Παρατήρηση 7. *Το ύψος σημείου ορίστηκε μέσω της x-συνιστώσας του. Αν γράψουμε τώρα το σημείο P στην μορφή $P=\left(\frac{m}{e^2},\frac{n}{e^3}\right)$, με $(m,e)=(n,e)=1$, το ύψος $H(P)=max(|m|,e^2)$, συνεπώς $|m|\le H(P)$ και $e^2\le H(P)$.*

Ισχυρίζομαι ότι το ύψος δίνει ένα **ανώτερο φράγμα και για το** n. Συγκεκριμένα ότι υπάρχει $k>0$ τέτοιο ώστε $|n|\le kH(P)^{3/2}$.

Από την εξίσωση

$$\frac{n^2}{e^6}=\frac{m^3}{e^6}+a\frac{m^2}{e^4}+b\frac{m^2}{e^4}+c$$

έπεται ότι

$$n^2=m^3+am^2e^2+be^4m+e^6.$$

Επομένως

$$|n|^2\le H(P)^3+|a|H(P)^3+|b|H(P)^3+|c|H(P)^3,$$

οπότε μπορουμε να πάρουμε

$$k:=\sqrt{1+|a|+|b|+|c|}.$$

Από τα παραπάνω συμπεραίνουμε ότι το ύψος ενός σημείου $P=(x,y)$ μας δίνει φράγμα και της y-συνιστώσας αυτού.

Στην συνέχεια θα αποδείξουμε τα τρία λήμματα.

2. Αποδείξεις των τριών λημμάτων

Απόδειξη του λήμματος 1:

Αν το $P_0=0$ τότε το λήμμα προφανώς ισχύει. Έστω ότι $P_0\neq 0$, $P_0=(x_0,y_0)$. Η σταθερά c_0 θα εξαρτάται από το P_0. Είναι αρκετό να δείξουμε την ύπαρξη τέτοιας σταθεράς για **σχεδόν**

όλα τα P, εκτός δηλαδή πεπερασμένου πλήθους σημείων. Και αυτό γιατί, απλούστατα, μπορούμε να πάρουμε τους λόγους $\frac{H(P+P_0)}{H(P)^2}$ για το σύνολο αυτό των πεπερασμένου πλήθους σημείων και να διαλέξουμε τελικά το c_0 να είναι μεγαλύτερο και από τους πεπερασμένους στο πλήθος αυτούς λόγους.

Συνεπώς μπορούμε, χωρίς περιορισμό της γενικότητας, να υποθέσουμε ότι $P \neq P_0, -P_0, \mathcal{O}$. Αν $P=(x,y)$, τότε $P \neq P_0, -P_0$ σήμαινει $x \neq x_0$. Έστω $P+P_0=(\xi,\eta)$. Ξαναθυμίζουμε ότι, από τους τύπους του αθροίσματος δύο σημείων, έχουμε:

$$\xi = \lambda^2 - a - x - x_0, \quad \text{όπου} \quad \lambda = \frac{y-y_0}{x-x_0}.$$

Επομένως

$$\xi = \frac{(y-y_0)^2 - x(x-x_0)^2 - x_0(x-x_0)^2 - a(x-x_0)^2}{(x-x_0)^2}.$$

Αν αντικαταστήσουμε το y^2 από την εξίσωση $y^2 = x^3 + ax^2 + bx + c$, βρίσκουμε

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

όπου A, B, C, D, E, F και G ρητοί αριθμοί δοσμένοι συναρτήσει των a, b, c και των συντεταγμένων του σημείου $P_0=(x_0,y_0)$. Χωρίς περιορισμό της γενικότητας, πολλαπλασιάζοντας, αν χρειαστεί τους όρους του κλάσματος με το ελάχιστο κοινό πολλαπλάσιο των A, B, C, D, E, F, G, μπορουμε να υποθέσουμε ότι A, B, C, D, E, F και G είναι ακέραιοι.

Αφού το $P=(x,y) \in E(\mathbb{Q})$ **τυχαίο** ρητό σημείο της καμπύλης έπεται ότι οι σταθερές A, B, C, D, E, F και G είναι ίδιες για όλα τα ρητά σημεία της καμπύλης, $P \neq P_0, -P_0, \mathcal{O}$, δηλαδή ότι η σταθερά c_0 θα εξαρτάται από τις σταθερές και όχι από το σημείο P.

Στην συνέχεια γράφουμε $x = \frac{m}{e^2}$ και $y = \frac{n}{e^3}$ (δες παρατήρηση 6) και βρίσκουμε

$$\xi = \frac{Aen + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Έτσι έχουμε το ξ σαν έκφραση ενός πηλίκου δύο ακεραίων. Δεν γνωρίζουμε βέβαια ότι το κλάσμα είναι ανάγωγο, αλλά, τυχόν διαγραφή κοινού παράγοντα αριθμητή και παρονομαστή, θα έκανε το ύψος μικρότερο.

Έστω $H := H(P) = H(x)$. Χρησιμοποιούμε τις ανισότητες

$$e \leq H^{1/2}, \quad n \leq KH^{3/2}, \quad m \leq H$$

όπου K σταθερά που εξαρτάται από τα a, b, c και έχουμε

$$\begin{aligned} \left|(Aen + Bm^2 + Cme^2 + De^4)\right| &\leq (|AK| + |B| + |C| + |D|)H^2 \\ \text{και} \quad \left|(Em^2 + Fme^2 + Ge^4)\right| &\leq (|E| + |F| + G|)H^2. \end{aligned}$$

Επομένως

$$H(\xi) \leq c_0 H^2 \quad \text{όπου } c_0 = \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}.$$

□

Απόδειξη του Λήμματος 2:

Δεδομένου ότι υπάρχει μόνο πεπερασμένο πλήθος ρητών σημείων με την ιδιότητα $2P = \mathcal{O}$, μπορούμε να υποθέσουμε ότι $2P \neq \mathcal{O}$. Αν $P = (x, y)$ και $2P = (\xi, \eta)$, τότε $\xi = \lambda^2 - 2x - a$ όπου $\lambda = \dfrac{f'(x)}{2y}$. Επομένως

$$\xi = \frac{(f'(x))^2 - 8xf(x) - 4af(x)}{4f(x)} = \frac{x^4 + \cdots}{4x^3 + \cdots}$$

όπου $f(x) \neq 0$, αφού $2P \neq \mathcal{O}$. Ώστε το ξ είναι πηλίκο δύο πολυωνύμων ως προς x με συντελεστές ακεραίους. Αφού η κυβική καμπύλη είναι μη-ιδιάζουσα, τα πολυώνυμα $f(x)$ και $f'(x)$ είναι πρώτα μεταξύ τους, συνεπώς αριθμητής και παρονομαστής του ξ δεν έχουν κοινές ρίζες. Καταφέραμε λοιπόν να αναγάγουμε το πρόβλημα στο παρακάτω λήμμα για τα ύψη. Το λήμμα αυτό είναι γενικό και δεν έχει καμμία σχέση με κυβικές καμπύλες. □

Λήμμα 2′. *Έστω $\varphi(X)$ και $\psi(X)$ δύο πολυώνυμα με ακεραίους συντελεστές, τα οποία δεν έχουν κοινή (μιγαδική) ρίζα. Με d θα συμβολίζουμε το μέγιστο των βαθμών των φ και ψ.*

1. *Υπάρχει ακέραιος $R \geq 1$, ο οποίος εξαρτάται από τα φ και ψ, τέτοιος ώστε για όλους τους ρητούς αριθμούς m/n ο μέγιστος κοινός διαιρέτης των ακεραίων $n^d\varphi(m/n)$ και $n^d\psi(m/n)$ διαιρεί τον R.*

2. *Υπάρχουν θετικές σταθερές c_1 και c_2 τέτοιες ώστε*

$$c_1 \left(H\Big(\frac{m}{n}\Big)^d\right) \leq H\left(\frac{\varphi(m/n)}{\psi(m/n)}\right) \leq c_2 \left(H\Big(\frac{m}{n}\Big)\right)^d$$

για όλους τους ρητούς m/n οι οποίοι δεν είναι ρίζα του πολυωνύου $\psi(X)$.

Απόδειξη:

1. Από τον ορισμό του d έπεται ότι οι ποσότητες $n^d\varphi(m/n)$ και $n^d\psi(m/n)$ είναι ακέραιοι αριθμοί. Επομένως έχει νόημα η έννοια του μεγίστου κοινού διαιρέτη αυτών. Χωρίς περιορισμό της γενικότητας, υποθέτουμε ότι $\deg\varphi = d$ και $\deg\psi = r \leq d$. Μπορούμε επομένως να

γράψουμε

$$\begin{aligned} n^d\varphi\left(\frac{m}{n}\right) &= a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d \\ n^d\psi\left(\frac{m}{n}\right) &= b_0m^rn^{d-r} + b_1m^{r-1}n^{d-r+1} + \cdots + b_rn^d \end{aligned}$$

Συμβολίζουμε

$$\begin{aligned} F(m,n) &:= n^d\varphi\left(\frac{m}{n}\right) \\ \text{και} \qquad G(m,n) &:= n^d\psi\left(\frac{m}{n}\right) \end{aligned}$$

Στην συνέχεια θα **προσπαθήσουμε να** εκτιμήσουμε τον μέγιστο κοινό διαιρέτη των $F(m,n)$ και $G(m,n)$ ανεξάρτητα των τιμών m και n.

Τα πολυώνυμα $\varphi(X)$ και $\psi(X)$ δεν έχουν κοινές ρίζες μεταξύ τους. Επομένως είναι πρώτα μεταξύ τους στον δακτύλιο $\mathbb{Q}[X]$. Αυτό σημαίνει ότι υπάρχουν πολυώνυμα $k(X) \in \mathbb{Q}[X]$ και $l(X) \in \mathbb{Q}[X]$ τέτοια ώστε

$$k(X)\varphi(X) + l(X)\psi(X) = 1 \tag{5.2}$$

Έστω $A \in \mathbb{Z}$ αρκετά μεγάλος ώστε τα πολυώνυμα $Ak(X)$ και $Al(X)$ να έχουν ακεραίους συντελεστές. Αν πάλι D είναι ο μέγιστος των βαθμών των πολυωνύμων $k(X)$ και $l(X)$, πολλαπλασιάζουμε και τα δύο μέλη της εξίσωσης (5.2) με $A \cdot n^{D+d}$ και θέτουμε $X = m/n$, οπότε προκύπτει η ισότητα:

$$\left\{n^D \cdot Ak(m/n)\right\} \cdot F(m,n) + \left\{n^D \cdot A \cdot l(m/n)\right\} \cdot G(m,n) \;=\; A \cdot n^{D+d}$$

Παρατηρούμε ότι οι ποσότητες μέσα στις αγκύλες είναι ακέραιοι αριθμοί. Αυτό σημαίνει ότι αν $\gamma := \gamma(m,n)$ είναι ο μέγιστος κοινός διαιρέτης των $F(m,n)$ και $G(m,n)$ τότε $\gamma \,\big|\, A \cdot n^{D+d}$. Το αποτέλεσμα αυτό δεν είναι ικανοποιητικό διότι θέλουμε το γ να διαιρεί κάποιο ακέραιο που να **μην εξαρτάται από το** n. Θα δείξουμε ότι $\gamma \,\big|\, A \cdot a_0^{D+d}$.

Το $\gamma | F(m,n)$, άρα θα διαιρεί και το

$$An^{D+d-1}F(m,n) = Aa_0m^d \cdot n^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \cdots + Aa_dn^{D+2d-1}$$

Το γ επομένως διαιρεί το $An^{D+d-1}F(m,n)$ και το An^{D+d}. Επομένως θα διαιρεί και το $Aa_0m^d \cdot n^{D+d-1}$ και συνεπώς και το μέγιστο κοινό διαιρέτη των $Aa_0m^dn^{D+d-1}$ και An^{D+d}. Επειδή δε $(m,n) = 1$ έπεται ότι $\gamma | Aa_0n^D + d - 1$.

Κατεβάσαμε την δύναμη του n κατά ένα και πολλαπλασιάσαμε την ποσότητα με a_0. Συνεχίζοντας όμοια καταλήγουμε στο συμπέρασμα ότι $\gamma|A \cdot a_0^{D+d} =: R$.

2. Η δεξιά ανισότητα του προς απόδειξη 2. του λήμματος 2 δεν μας χρειάζεται για την απόδειξη του θεωρήματος του Mordell και είναι αρκετά πιο εύκολη από την αριστερά. Την αφήνουμε σαν άσκηση στον αναγνώστη.

Κατ΄ αρχήν παρατηρούμε ότι αν α ρητός αριθμός τότε $H(\alpha) = H(1/\alpha)$. Αυτό σημαίνει ότι μπορούμε, αν χρειαστεί, να αλλάξουμε τους ρόλους των φ και ψ, να υποθέσουμε και πάλι ότι $\deg\varphi = d$ και ότι $\deg\psi = r \leq d$.

Αν τώρα m/n ρητός ο οποίος δεν είναι ρίζα του πολυωνύμου ψ θα προσπαθήσουμε να εκτιμήσουμε το ύψος του αριθμού

$$\xi := \frac{\varphi(m/n)}{\psi(m/n)} = \frac{n^d\varphi(m/n)}{n^d\psi(m/n)} = \frac{F(m,n)}{G(m,n)}.$$

Το ύψος του ξ είναι, εξ ορισμού, το μέγιστο των ακεραίων $|F(m,n)|$ και $|G(m,n)|$ αν είμαστε σίγουροι ότι το κλάσμα $F(m,n)/G(m,n)$ είναι ανάγωγο. Η μεγαλύτερη δυνατή απλοποίηση που θα μπορούσε να γίνει είναι ο μέγιστος κοινός διαιρέτης των $F(m,n)$ και $G(m,n)$. Κάνοντας χρήση του ισχυρισμού του πρώτου μέρους του λήμματος, έχουμε:

$$\begin{aligned} H(\xi) &\geq \frac{1}{R}\max\{|F(m,n)|,\ |G(m,n)|\} \\ &= \frac{1}{R}\max\left\{|n^d\varphi(m/n)|,\ |n^d\psi(m/n)|\right\} \\ &\geq \frac{1}{2R}\left(|n^d\varphi(m/n)| + |n^d\psi(m,n)|\right). \end{aligned}$$

Στην τελευταία ανισότητα χρησιμοποιήσαμε την γνωστή σχέση $\max\{a,b\} \geq \frac{1}{2}(a+b)$. Στόχος μας είναι να συγκρίνουμε το ύψος $H(\xi)$ με το $H(m/n)^d = \max\{|m^d|,\ |n^d|\}$.

Επομένως έχουμε

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{1}{2R}\cdot\frac{|n^d\varphi(m/n)| + |n^d\psi(m/n)|}{\max\{|m^d|,\ |n^d|\}} = \frac{1}{2R}\cdot\frac{|\varphi(m/n)| + \psi(m/n)|}{\max\{|m/n|^d,\ 1\}}.$$

Θεωρούμε τώρα την συνάρτηση

$$f(t) := \frac{|\varphi(t)| + |\psi(t)|}{\max\{|t|^d,\ 1\}}$$

και παρατηρούμε ότι υπάρχει το όριο της $f(t)$ και είναι διάφορο του μηδενός όταν το $|t|$ τείνει στο άπειρο. Το όριο αυτό είναι $|a_0|$ αν $\deg\psi = r < d$ και είναι $|a_0| + |b_0|$ αν $\deg\psi = r = d$.

Αυτό σημαίνει ότι η συνάρτηση $f(t)$ είναι, έξω από κάποιο κλειστό διάστημα, φραγμένη και θετική. Και μέσα στο κλειστό διάστημα έχουμε μία συνεχή συνάρτηση η οποία δεν μηδενίζεται

πουθενά διότι $\varphi(X)$ και $\psi(X)$ δεν έχουν κοινές ρίζες. Η $f(t)$ είναι επομένως συνεχής σε κάποιο κλειστό διάστημα και άρα εκεί θα παίρνει τις ακρότατες τιμές. Επειδή σ' αυτό το διάστημα δεν μηδενίζεται, έπεται ότι υπάρχει μία σταθερά $c_1 > 0$ τέτοια ώστε $f(t) > c_1$ για κάθε $t \in \mathbb{R}$. Επομένως,

$$H(\xi) \geq \frac{c_1}{2R} \cdot H(m/n)^d.$$

□

Σειρά τώρα έχει το τρίτο λήμμα. Για να αποφύγουμε την χρήση στοιχείων Αλγεβρικής Θεωρίας Αριθμών, κάνουμε την επιπλέον υπόθεση ότι το πολυώνυμο $f(x) = x^3 + ax^2 + bx + c$ έχει τουλάχιστο μία ρητή ρίζα, το οποίο ισοδυναμεί με το ότι έχει ένα ρητό σημείο P τάξης δύο $2P = \mathcal{O}$.

Η μέθοδος αυτή δουλεύει γενικά. Στην περίπτωση που η υπόθεση δεν ισχύει πρέπει να πάρουμε μία ρίζα του $f(x)$ να την επισυνάψουμε στο $\mathbb{Q}$ και να δουλέψουμε στο σώμα $\mathbb{Q}(\alpha)$, όπου α η ρίζα.

Απόδειξη του Λήμματος 3:

Έστω $f(x)$ έχει μία ρητή ρίζα x_0. Αυτή θα πρέπει να είναι ακέραιος διότι το $f(x)$ είναι **εναδικό**, δηλαδή ο συντελεστής της μεγαλύτερης δύναμης του x είναι 1. Αλλάζουμε το σύστημα συντεταγμένων και στέλνουμε το x_0 στην αρχή των αξόνων. Η καινούργια εξίσωση έχει τώρα την μορφή $E : y^2 = x^3 + ax^2 + bx = f(x)$ όπου a, b πάλι ακέραιοι.
Ώστε το σημείο $(0,0) = P_0$ είναι ρητό σημείο της ελλειπτικής καμπύλης. Η διακρίνουσα του $f(x)$ είναι $D(f) = b^2(a^2 - 4b) \neq 0$. Επομένως $b \neq 0$ και $a^2 - 4b \neq 0$.

Ενδιαφερόμαστε για τον δείκτη $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$. Θα αναλύσουμε την απεικόνιση

$$\begin{cases} E(\mathbb{Q}) & \xrightarrow{2} & E(\mathbb{Q}) \\ P & \longmapsto & 2P \end{cases}$$

σε δύο άλλες απεικονίσεις. Η παραπάνω απεικόνιση είναι, κατά κάποιο τρόπο, βαθμού 4 διότι η συνάρτηση που δίνει την x-συνιστώσα του $2P$ είναι βαθμού 4 ως προς την x-συνιστώσα του P. Θα αναλύσουμε λοιπόν την απεικόνιση αυτή σε 2 άλλες βαθμού 2 η καθεμία. Μάλιστα οι απεικονίσεις αυτές δεν θα είναι από την καμπύλη στον εαυτό της, αλλά από την καμπύλη E σε μία άλλη καμπύλη $\bar{E}$ και από αυτήν στην αρχική.

Μαζί με την ελλειπτική καμπύλη E θεωρούμε και την $\bar{E}$ που ορίζεται από την E, συγκεκριμένα

$$\bar{E} | y^2 = x^3 + \bar{a}x^2 + \bar{b}x \quad \text{όπου} \quad \bar{a} = -2a,\ \bar{b} = a^2 - 4b.$$

Για λόγους που θα δούμε σε λίγο, οι δύο ελλειπτικές καμπύλες είναι στενά συνδεδεμένες μεταξύ τους και θεωρείται πολύ φυσικό όταν μελετούμε την μία να μελετούμε και την άλλη.
Μπορούμε τώρα να ξανακάνουμε το ίδιο για την $\bar{E}$. Βρίσκουμε την

$$\bar{\bar{E}} : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x, \quad \text{όπου} \quad \begin{cases} \bar{\bar{a}} &= -2\bar{a} = 4a \\ \bar{\bar{b}} &= \bar{a}^2 - 4\bar{b} \\ &= 4a^2 - 4(a^2 - 4b) = 16b \end{cases}$$

$$\text{Ώστε} \quad \bar{\bar{E}} : y^2 = x^3 + 4ax^2 + 16bx.$$

Η $\bar{\bar{E}}$ είναι όμως ουσιαστικά η ίδια η E: αρκεί να αντικαταστήσουμε το y με το $8y$, το x με το $4x$, και να διαιρέσουμε με το 64. Ώστε $\bar{\bar{E}}(\mathbb{Q}) \overset{\lambda}{\cong} E(\mathbb{Q})$ μέσω της $\lambda(x, y) = \left(\frac{x}{4}, \frac{y}{8}\right)$.

Ορίζουμε τώρα μία συνάρτηση $\varphi : E(\mathbb{C}) \to \bar{E}(\mathbb{C})$ η οποία θα είναι ομομορφισμός ομάδων και θα στέλνει την $E(\mathbb{Q})$ στην $\bar{E}(\mathbb{Q})$. Όμοια θα ορίσουμε στην συνέχεια την $\psi : \bar{E}(\mathbb{C}) \to \bar{\bar{E}}(\mathbb{C})$. Αφού $\bar{\bar{E}}(\mathbb{Q}) \overset{\lambda}{\cong} E(\mathbb{Q})$ το τελικό αποτέλεσμά μας θα είναι η $\psi \circ \varphi$ που θα είναι πολλαπλασιασμός με 2.

Ορισμός 8. *Έστω*

$$\varphi : E(\mathbb{C}) \ni (x, y) \longmapsto (\bar{x}, \bar{y}) \in \bar{E}(\mathbb{C}),$$

όπου για $x \neq 0$

$$\bar{x} = x + a + \frac{b}{x} = \frac{y^2}{x^2}, \quad \bar{y} = y(\frac{x^2 - b}{x^2}).$$

Ορίζουμε ακόμα $\varphi(\mathcal{O}) = \bar{\mathcal{O}}$ *και* $\varphi(P_0) = \bar{\mathcal{O}}$.

Ο ορισμός μας θα μπορούσε να δικαιολογηθεί αν όλη η θεωρία είχε συνδεθεί με την πραγματική της πηγή τις ελλειπτικές συναρτήσεις.

Κατ' αρχήν, η απεικόνιση φ είναι καλά ωρισμένη πράγματι, εύκολα υπολογίζει κανείς ότι $\bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} = \bar{y}^2$. Θα αποδείξουμε ότι η φ είναι ομομορφισμός ομάδων

$$\varphi(P_1 + P_2) = \varphi(P_1) + \varphi(P_2).$$

Αν P_1 ή $P_2 = \mathcal{O}$ τότε δεν έχουμε να αποδείξουμε τίποτα.
Αν τώρα ένα από τα P_1 ή P_2 είναι το P_0, έστω $P_1 = P_0$, τότε θα δείξουμε ότι

$$\varphi(P_0 + P_2) = \varphi(P_2).$$

Έστω (ξ, η) το τρίτο σημείο τομής της ευθείας P_0P_2 με την καμπύλη E. Τότε $P_0 + P_2 = (\xi, -\eta)$ οπότε

$$\varphi(P_0 + P_2) = (\bar{x}(P_0 + P_2), \bar{y}(P_0 + P_2))$$

όπου $\bar{x}(P_0 + P_2) = \left(\frac{\eta}{\xi}\right)^2$, αλλά $\eta = \frac{y}{x}\xi$ $(\lambda = \frac{y}{x},\ v = 0)$, οπότε

$$\bar{x}(P_0 + P_2) = \left(\frac{\eta}{\xi}\right)^2 = \left(\frac{y}{x}\right)^2 = \bar{x}(P_2).$$

Όμοια αποδεικνύουμε ότι $\bar{y}(P_0 + P_2) = \bar{y}(P_2)$.
Αν φυσικά ήταν και το $P_2 = P_0$ η μέθοδος δεν δουλεύει αλλά τότε

$$\varphi(P_0 + P_0) = \varphi(P_0) + \varphi(P_0) = \mathcal{O}$$

εξ ορισμού διότι $2P_0 = \mathcal{O}$, δηλαδή $\varphi(P_0 + P_2) = \bar{\mathcal{O}}$ και $\varphi(P_0) = \bar{\mathcal{O}}$.

Έστω τώρα ότι κανένα από τα σημεία P_1, P_2, P_3 δεν είναι το $\mathcal{O}$ ή το P_0. Αρκεί να δείξουμε ότι

$$\text{αν} \quad P_1 + P_2 + P_3 = \mathcal{O} \quad \text{τότε} \quad \varphi(P_1) + \varphi(P_2) + \varphi(P_3) = \bar{\mathcal{O}} \tag{5.3}$$

Εξ ορισμού της φ ισχύει $\varphi(x, -y) = (\bar{x}, -\bar{y}) = -(\bar{x}, \bar{y}) = -\varphi(x, y)$, δηλαδή $\varphi(-P) = -\varphi(P)$, οπότε αν η (5.3) είναι αληθής θα έχουμε πράγματι αυτό που ζητούμε διότι έχουμε

$$P_1 + P_2 + P_3 = \mathcal{O},$$

οπότε

$$\begin{aligned} \varphi(P_1 + P_2) &= \varphi(\mathcal{O} - P_3) = \varphi(-P_3) \\ &= -\varphi(P_3) = \varphi(P_1) + \varphi(P_2), \end{aligned}$$

διότι

$$\varphi(P_1) + \varphi(P_2) + \varphi(P_3) = \bar{\mathcal{O}}.$$

Αρκεί λοιπόν να αποδείξουμε την (5.3).

Ας πάρουμε την ευθεία $y = \lambda x + \nu$ και έστω P_1, P_2, P_3 τα σημεία τομής με την $E(\mathbb{C})$. Θα αποδείξουμε ότι τα $\varphi(P_1), \varphi(P_2), \varphi(P_3)$ είναι σημεία τομής της $\bar{E}(\mathbb{C})$ με κάποια ευθεία.

Παρατηρούμε ότι $\nu \neq 0$, διότι αν ήταν $\nu = 0$ η ευθεία θα περνούσε από το P_0.

Αν τώρα $\nu \neq 0$ μπορούμε πάλι να επαληθεύσουμε ότι τα σημεία $\varphi(P_1), \varphi(P_2), \varphi(P_3)$ βρίσκονται πάνω στην ευθεία

$$y = \bar{\lambda}x + \bar{\nu}, \quad \text{όπου} \quad \bar{\lambda} = \frac{\nu\lambda - b}{\nu}, \ \ \bar{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}.$$

Αυτό που θα πρέπει να δείξουμε είναι ότι $\bar{x}(P_1), \bar{x}(P_2)$ και $\bar{x}(P_3)$ είναι οι τρείς ρίζες της εξίσωσης

$$(\bar{\lambda}x + \bar{\nu})^2 = f(x) = x^3 + ax^2 + bx.$$

Η απόδειξη αυτή αφήνεται σαν άσκηση στον αναγνώστη.

Λόγω ορισμού του φ, είναι $\ker(\varphi) = \{\mathcal{O}, P_0\}$ και φαίνεται αμέσως ότι $\varphi : E(\mathbb{Q}) \to \bar{E}(\mathbb{Q})$. Ζητούμε την εικόνα $\mathrm{Im}\varphi$ της $E(\mathbb{Q})$ μέσω του φ. Προφανώς $\bar{\mathcal{O}} \in Im\varphi$. Ισχυρίζομαι ότι αν $\bar{x} \neq 0$ τότε το σημείο

$$(\bar{x}, \bar{y}) \in Im\varphi \Longleftrightarrow \bar{x} \text{ είναι τέλειο τετράγωνο ρητού}$$

και ότι $P_0' = (0,0) \in Im\varphi$ αν και μόνο αν $\bar{b} = a^2 - 4b$ είναι τέλειο τετράγωνο ρητού. Ας αποδείξουμε κατ' αρχήν το τελευταίο:

$$(0,0) \in Im\varphi \Longleftrightarrow \exists (x,y) \in E(\mathbb{Q}) : \bar{x} = \frac{y^2}{x^2} = 0.$$

Το x όμως είναι διάφορο του μηδενός γιατί αν $x = 0$ τότε και $y = 0$ και συνεπώς θα έπρεπε $\varphi(P_0) = P_0'$ κάτι το οποίο δεν ισχύει διότι, εξ ορισμού, $\varphi(P_0) = \mathcal{O}$. **Ώστε**

$$(0,0) \in \mathrm{Im}\varphi \iff \exists (x,y) \in E(\mathbb{Q}), x \neq 0 \text{ και } y = 0.$$

Αν όμως $y = 0$, τότε $0 = x^3 + ax^2 + bx = x(x^2 + ax + b)$ και το x θα πρέπει να είναι μία μη μηδενική ρίζα του δεξιού μέλους, δηλαδή ρίζα του $x^2 + ax + b$. Το τελευταίο όμως συμβαίνει ακριβώς τότε όταν $\bar{b} = a^2 - 4b$ είναι τέλειο τετράγωνο στο $\mathbb{Q}$.

Έστω τώρα $(\bar{x}, \bar{y}) \in E(\mathbb{Q})$, $(\bar{x}, \bar{y}) \neq P_0' = (\bar{0}, \bar{0})$ δηλαδή $\bar{x} \neq \bar{0}$. Αν $(\bar{x}, \bar{y}) \in \mathrm{Im}\,\varphi$ τότε $\bar{x} = \left(\frac{y}{x}\right)^2$ δηλαδή τέλειο τετράγωνο ρητού.
Αντιστρόφως, έστω ότι $\bar{x} = w^2$, $w \in \mathbb{Q}$. Θέτουμε

$$\begin{aligned} x_1 &= \frac{1}{2}\left(w^2 - a + \frac{\bar{y}}{w}\right), \quad y_1 = x_1 w, \\ x_2 &= \frac{1}{2}\left(w^2 - a - \frac{\bar{y}}{w}\right), \quad y_2 = -x_2 w. \end{aligned}$$

Θα δείξουμε ότι για $i = 1, 2$ ισχύουν

(α′) $P_i = (x_i, y_i) \in E(\mathbb{Q})$,

(β′) $\varphi(P_i) = (\bar{x}, \bar{y})$.

Απόδειξη: (α′) Παίρνουμε

$$\begin{aligned} x_1 x_2 &= \frac{1}{4}\left[(w^2-a)^2 - \frac{\bar{y}^2}{w^2}\right] = \frac{1}{4}\left[(\bar{x}-a)^2 - \frac{\bar{y}^2}{\bar{x}}\right] \\ &= \frac{1}{4\bar{x}}(\bar{x}^3 - 2a\bar{x}^2 + a^2\bar{x} - \bar{y}^2) = b, \end{aligned}$$

διότι

$$\bar{y}^2 = \bar{x}^3 - 2a\bar{x}^2 + (a^2 - 4b)\bar{x},$$

οπότε έχουμε

$$\begin{aligned} (x_i, y_i) \in E(\mathbb{Q}) &\iff y_i^2 = x_i^3 + a x_i^2 + b x_i \\ &\iff \left(\frac{y_i}{x_i}\right)^2 = x_i + a + \frac{b}{x_i} \\ \iff w^2 = x_1 + a + x_2, &\quad \text{διότι } b = x_1 x_2. \end{aligned}$$

Η τελευταία σχέση όμως ισχύει λόγω της εκλογής των x_1 και x_2 και συνεπώς αποδείξαμε την (α′).

(β′) Έχουμε

$$\begin{aligned} \varphi(P_i) &= \left(\left(\frac{y_i}{x_i}\right)^2,\, y_i\left(\frac{x_i^2 - x_1 x_2}{x_i^2}\right)\right) \\ &= \begin{cases} \big(w^2, w(x_1 - x_2)\big), & \text{για} \quad i = 1 \\ \big(w^2, -w(x_2 - x_1)\big), & \text{για} \quad i = 2 \end{cases} \\ &= (\bar{x}, \bar{y}) \end{aligned}$$

(δες σελίδα 81 για τους ορισμούς των x_1 και x_2). Ορίζουμε τώρα, όπως ακριβώς και τον φ, ένα μορφισμό $\psi' : \bar{E}(\mathbb{Q}) \to \bar{\bar{E}}(\mathbb{Q})$ και θεωρούμε την σύνθεση $\psi = \lambda \circ \psi' : \bar{E}(\mathbb{Q}) \to E(\mathbb{Q})$ όπου λ ο γνωστός από τα προηγούμενα ισομορφισμός

$$\bar{\bar{E}}(\mathbb{Q}) \ni (x, y) \overset{\lambda}{\longmapsto} \left(\frac{x}{4}, \frac{y}{8}\right) \in E(\mathbb{Q}).$$

Θα αποδείξουμε ότι ισχύει $(\psi \circ \varphi)(P) = 2P$, **για κάθε** $P \in E(\mathbb{Q})$. Έχουμε

$$\begin{aligned} \varphi(P) &= \bar{P} = (\bar{x}, \bar{y}) = \left((\frac{y}{x})^2, y\frac{x^2 - b}{x^2}\right), \\ \psi'(\bar{P}) &= (\bar{\bar{x}}, \bar{\bar{y}}), \end{aligned}$$

όπου

$$\begin{aligned} \bar{\bar{x}} &= \left(\frac{\bar{y}}{\bar{x}}\right)^2 = \frac{y^2\left(\frac{x^2-b}{x^2}\right)^2}{\left(\frac{y}{x}\right)^4} = \left(\frac{x^2-b}{y}\right)^2 \\ \text{και} \quad \lambda(\bar{\bar{x}}) &= \left(\frac{x^2-b}{2y}\right)^2. \end{aligned}$$

Από την άλλη μεριά η x-συνιστώσα του $2P$ είναι

$$\begin{aligned} x' &= \lambda^2 - a - 2x = \frac{(3x^2+2ax+b)^2}{4y^2} - a - 2x \\ &= \frac{9x^4+4a^2x^2+b^2+12ax^3+6bx^2+4abx-4a(x^3+ax^2+bx)-8x(x^3+ax^2+bx)}{4y^2} \\ &= \frac{x^4-2bx^2+b^2}{4y^2} = \left(\frac{x^2-b}{2y}\right)^2 = \lambda(\bar{\bar{x}}). \end{aligned}$$

Για τις y-συνιστώσες έχουμε

$$\begin{aligned} \bar{\bar{y}} &= \bar{y}\frac{\bar{x}^2-\bar{b}}{\bar{x}^2} = \frac{y(x^2-b)}{x^2}\cdot\frac{y^4-(a^2-4b)x^4}{y^4} \\ &= \frac{(x^2-b)\left[(x^2+ax+b)^2-(a^2-4b)x^2\right]}{y^3} \\ &= \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{y^3} \\ &= \frac{x^6+2ax^5+5bx^4-5b^2x^2-2ab^2x-b^3}{y^3} \quad \text{και} \quad \lambda(\bar{\bar{y}}) = \frac{\bar{\bar{y}}}{8}. \end{aligned}$$

Από την άλλη μεριά η y-συνιστώσα του σημείου $2P$ είναι

$$\begin{aligned} y' &= -y + \frac{f'(x)}{2y}(x-x') = -y + \frac{3x^2+2ax+b}{2y}\left[x - \left(\frac{x^2-b}{2y}\right)^2\right] \\ &= -y + \frac{3x^2+2ax+b}{2y}\cdot\frac{3x^4+4ax^3+6bx^2-b^2}{4y^2} \\ &= \frac{-8(x^3+ax^2+bx)^2+(3x^2+2ax+b)(3x^4+4ax^3+6bx^2-b^2)}{8y^3} \\ &= \frac{x^6+2ax^5+5bx^4-5b^2x^2-2ab^2x-b^3}{8y^3} = \lambda(\bar{\bar{y}}). \end{aligned}$$

Ώστε

$$(\psi\circ\varphi)(P) = 2P \quad \text{για κάθε} \quad P\in E(\mathbb{Q}).$$

Στην συνέχεια θα αποδείξουμε ότι $[\bar{E}(\mathbb{Q}):\varphi(E(\mathbb{Q}))]<\infty$ και μάλιστα $[\bar{E}(\mathbb{Q}):\varphi(E(\mathbb{Q}))]\leq 2^{s+1}$ όπου s ο αριθμός των διακεκριμένων πρώτων παραγόντων του $\bar{b}=a^2-4b$.

Ομοίως $[E(\mathbb{Q}) : \psi(\bar{E}(\mathbb{Q}))] \leq 2^{r+1}$ όπου r το πλήθος των διακεκριμένων πρώτων παραγόντων του b. Προφανώς αρκεί να αποδείξουμε μόνο μία από αυτές. Εντελώς ανάλογα αποδεικνύεται και η δεύτερη. Από τα προηγούμενα προκύπτει ότι

$$\psi(\bar{E}(\mathbb{Q})) = \big\{(x,y) \in E(\mathbb{Q}) \big| x = w^2 \neq 0, w \in \mathbb{Q}\big\} \cup \{\mathcal{O}\} \cup \begin{cases} \{P_0\}, & \text{αν } b \text{ τέλειο τετράγωνο} \\ \phi, & \text{αν } b \text{ όχι τέλειο τετράγωνο} \end{cases}$$

Η ιδέα της απόδειξης είναι να βρούμε έναν αμφιμονοσήμαντο ομομορφισμό της

$$\frac{E(\mathbb{Q})}{\psi(\bar{E}(\mathbb{Q}))}$$

σε μία πεπερασμένη ομάδα. Έστω $\mathbb{Q}^*$ η πολλαπλασιαστική ομάδα των ρητών και $\mathbb{Q}^{*2}$ η υποομάδα των τελείων τετραγώνων του $\mathbb{Q}^*$. Ορίζουμε

$$\alpha : E(\mathbb{Q}) \longrightarrow {}^{Q^*}\!/_{\mathbb{Q}^{*2}}$$

$$\begin{aligned} \alpha(\mathcal{O}) &\equiv 1 \,(\mathrm{mod}\, \mathbb{Q}^{*2}) \\ \alpha(P_0) &\equiv b \,(\mathrm{mod}\, \mathbb{Q}^{*2}) \\ \alpha(x,y) &\equiv x \,(\mathrm{mod}\, \mathbb{Q}^{*2}), \quad \text{αν } x \neq 0. \end{aligned}$$

Θα αποδείξουμε ότι ο α είναι ομομορφισμός ομάδων και ότι

$$\ker \alpha = \mathrm{Im}\psi = \psi(\bar{E}(\mathbb{Q})).$$

Απόδειξη: Αρκεί να αποδείξουμε ότι

$$P_1 + P_2 + P_3 = \mathcal{O} \Longrightarrow \alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \,(\mathrm{mod}\, \mathbb{Q}^{*2}).$$

Αφού για $P = (x,y)$, $-P = (x,-y)$ έχουμε $\alpha(-P) = \alpha(P)$ και αφού $x \equiv \frac{1}{x} \,(\mathrm{mod}\, \mathbb{Q}^{*2})$ ισχύει $\alpha(P)^{-1} = \alpha(P)$ οπότε η αλήθεια της πρότασης, μέσα στις παρενθέσεις δίνει

$$\alpha(P_3) = \alpha(-(P_1 + P_2)) = \alpha(P_1 + P_2) \equiv \alpha(P_1) \cdot \alpha(P_2) \,(\mathrm{mod}\, \mathbb{Q}^{*2}).$$

Έστω ότι $P_1, P_2, P_3 \notin \{\mathcal{O}, P_0\}$ δηλαδή $x_1 x_2 x_3 \neq 0$.
Το γεγονός ότι $P_1 + P_2 + P_3 = \mathcal{O}$ σημαίνει ότι τα σημεία P_1, P_2, P_3 βρίσκονται πάνω σε μία ευθεία έστω $y = \lambda x + \nu$. Από τον τύπο 3.1 στην σελίδα 55 έχουμε ότι x_1, x_2, x_3 είναι ρίζες του

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x - \nu^2 = 0.$$

Επομένως το γινόμενο $x_1x_2x_3 = \nu^2 \in \mathbb{Q}^{*2}$ δηλαδή

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = \nu^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

Έστω τώρα ότι ένα από τα σημεία π.χ. το $P_1 = \mathcal{O}$. Τότε αν $P_1 + P_2 + P_3 = \mathcal{O}$ έπεται ότι $P_2 + P_3 = \mathcal{O}$, δηλαδή $P_3 = -P_2$, που σημαίνει ότι $x_2 = x_3$ οπότε $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1 \cdot x_2x_3 \equiv 1 \pmod{\mathbb{Q}^{*2}}$.

Έστω πάλι ότι το $P_1 = P_0 = (0,0)$. Τότε η ευθεία που ορίζεται από τα P_1, P_2, P_3 έχει την μορφή $y = \lambda x$, δηλαδή $\nu = 0$. Επομένως $x_2x_3 = x_1x_2 + x_2x_3 + x_1x_3 = b$. Συνεπώς

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = bx_2x_3 = b^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

Άρα ο α είναι ομομορφισμός ομάδων. Η σχέση τώρα $\ker\alpha = \mathrm{Im}\psi$ είναι προφανής διότι έχουμε ήδη δείξει ότι $(x,y) \in \mathrm{Im}\psi$ αν και μόνο αν $x = w^2,\ w \in \mathbb{Q}^*$.

Τέλος εξετάζουμε την εικόνα $\alpha(E(\mathbb{Q}))$.

Το ερώτημα είναι ποιοί ρητοί αριθμοί x αποτελούν x-συνιστώσα ενός σημείου της $E(\mathbb{Q})$. Είδαμε πιό μπροστά ότι αν $(x,y) \in E(\mathbb{Q})$ τότε $x = \frac{m}{e^2},\ y = \frac{n}{e^3}$ όπου $(m,e) = (n,e) = 1$, οπότε η $y^2 = x^3 + ax^2 + bx$ μας δίνει ότι

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4).$$

Έστω $d = (m, m^2 + ame^2 + be^4)$. Τότε $m = dm_1$ και $d|be^4$ οπότε $d|b$ διότι $(m,e) = 1$. Γράφουμε $b = db_1$ και έχουμε

$$n^2 = d^2 \cdot m_1(m_1^2d + am_1 + b_1e^4).$$

και

$$(m_1, m_1^2b + am_1 + b_1e^4) = 1.$$

Συνεπώς το m_1 είναι, κατ' απόλυτη τιμή, τέλειο τετράγωνο, οπότε αν $m = \prod_{p\in\mathbb{P}} p^{a_p}$ τότε το m είναι το γινόμενο ενός τελείου τετραγώνου και του $(\pm p_1^{\varepsilon_1}p_2^{\varepsilon_2}\cdots p_r^{\varepsilon_r})$ όπου τα ε_i θα είναι 0 ή 1 και τα $p_1, p_2, \cdots, p_r$ οι πρώτοι διαιρέτες του b.

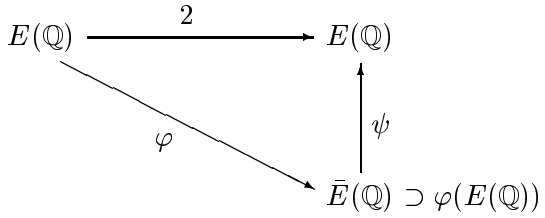
Το πλήθος τώρα των δυνατοτήτων για το $m \pmod{\mathbb{Q}^{*2}}$ είναι 2^{r+1}.

Αν βέβαια $x = 0$, οπότε και $m = 0$ το παραπάνω επιχείρημα δεν δουλεύει, αλλά ο ορισμός της α σαν $\alpha(P_0) \equiv b \pmod{\mathbb{Q}^{*2}}$ δείχνει ότι το συμπέρασμα για την τάξη της $\alpha(E(\mathbb{Q}))$ ισχύει.

Από την ισομορφία

$$E(\mathbb{Q})\big/_{\psi(\bar{E}(\mathbb{Q}))} = E(\mathbb{Q})\big/_{\ker\alpha} \equiv \alpha(E(\mathbb{Q})) \tag{5.4}$$

βρίσκουμε: $[E(\mathbb{Q}) : \psi(\bar{E}(\mathbb{Q}))] \leq 2^{r+1}$. Όμοια έχουμε $[\bar{E}(\mathbb{Q}) : \varphi(E(\mathbb{Q}))] \leq 2^{s+1}$.
Τελικά



$$2E(\mathbb{Q}) = (\psi\circ\varphi)(E(\mathbb{Q})) \leq \psi(\bar{E}(Q)) \leq E(\mathbb{Q})$$

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = [E(\mathbb{Q}) : \psi(\bar{E}(\mathbb{Q}))] \cdot [\psi(\bar{E}(\mathbb{Q})) : \psi(\varphi(E(\mathbb{Q})))].$$

Από την Θεωρία Ομάδων δανειζόμαστε το παρακάτω

Λήμμα 9. *Έστω A και C αβελιανές ομάδες, B υποομάδα της A και $\psi : A \to C$ ομομορφισμός ομάδων. Τότε*

$$\psi A\big/_{\psi B} \equiv \Big(A\big/_B\Big)\Big/\Big(\ker\psi\big/_{\ker\psi\cap B}\Big).$$

Η απόδειξη αφήνεται σαν άσκηση στον αναγνώστη.
Έστω τώρα $A = \bar{E}(\mathbb{Q})$ και $B = \varphi(E(\mathbb{Q}))$. Έχουμε

$$\psi(\bar{E}(\mathbb{Q}))\big/_{2E(\mathbb{Q})} = \psi(\bar{E}(\mathbb{Q}))\big/_{\psi(\varphi(E(\mathbb{Q})))} \cong \Big(\bar{E}(\mathbb{Q})\big/_{\varphi(E(\mathbb{Q}))}\Big)\Big/\Big(\ker\psi\big/_{\ker\psi\cap\varphi(E(\mathbb{Q}))}\Big),$$

οπότε

$$\big[\bar{E}(\mathbb{Q}) : \varphi(E(\mathbb{Q}))\big] = \big[\psi(\bar{E}(\mathbb{Q})) : \psi(\varphi(E(\mathbb{Q})))\big]\ \big[\ker\psi : \ker\psi\cap\varphi(E(\mathbb{Q}))\big]$$

$$\Longrightarrow\quad [\psi(\bar{E}(\mathbb{Q})) : \psi(\varphi(E(\mathbb{Q})))] \leq [\bar{E}(\mathbb{Q}) : \varphi(E(\mathbb{Q}))] \leq 2^{s+1}$$

$$\Longrightarrow\quad [E(\mathbb{Q}) : 2E(\mathbb{Q})] \leq 2^{r+1}\cdot 2^{s+1} = 2^{r+s+2},$$

δηλαδή η πλήρης απόδειξη του Θεωρήματος του Mordell. □

3. Εφαρμογές και παραδείγματα

Το Θεώρημα του Mordell μας λέει ότι η ομάδα των ρητών σημείων $\Gamma = E(\mathbb{Q})$ μιάς ελλειπτικής καμπύλης E είναι πεπερασμένα παραγόμενη αβελιανή ομάδα. Συνεπώς υπάρχουν $r, s \in \mathbb{N}_0,\ p_i \in \mathbb{P},\ \nu_i \in \mathbb{N} (i = 1, 2, \ldots, s)$ τέτοιοι ώστε

$$\Gamma \ \cong\ \mathbb{Z}^r \oplus \left(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right) \oplus \cdots \oplus \left(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z}\right) \tag{5.5}$$

$$\text{οπότε} \qquad 2\Gamma \ \cong\ (2\mathbb{Z})^r \oplus \left(2\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right) \oplus \cdots \oplus \left(2\mathbb{Z}/p_s^{\nu_s}\mathbb{Z}\right)$$

$$\Longrightarrow\ \Gamma/2\Gamma \ \cong\ \left(\mathbb{Z}/2\mathbb{Z}\right)^r \oplus \left(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right)\Big/\left(2\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right) \oplus \cdots \oplus \left(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z}\right)\Big/\left(2\mathbb{Z}/p_s^{\nu_s}\mathbb{Z}\right).$$

Αν p περιττός, τότε $2\mathbb{Z}/p^\nu\mathbb{Z} \cong \mathbb{Z}/p^\nu\mathbb{Z}$.
Αν $p = 2$ τότε $2\mathbb{Z}/2^\nu\mathbb{Z} \cong \mathbb{Z}/2^{\nu-1}\mathbb{Z}$.
Επομένως για p περιττό ο προσθετέος $\left(\mathbb{Z}/p^\nu\mathbb{Z}\right)\Big/\left(2\mathbb{Z}/p^\nu\mathbb{Z}\right)$ δίνει το μοναδιαίο και εξαφανίζεται από την άθροιση.
Αν $p = 2$ τότε το πηλίκο $\left(\mathbb{Z}/2^\nu\mathbb{Z}\right)\Big/\left(2\mathbb{Z}/2^\nu\mathbb{Z}\right)$ δίνει $\mathbb{Z}/2\mathbb{Z}$.

Έστω $t = \#\left\{j \in \{1, 2, \cdots, s\} \,\middle|\, p_j = 2\right\}$. Επομένως

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^{r+t}.$$

Ισχυρίζομαι ότι αν Γ_2 συμβολίζει την ομάδα των $\mathbb{Q}$-ρητών σημείων τάξεως 2 της E τότε

$$|\Gamma_2| = 2^t.$$

Λόγω της (5.5) υπάρχουν $P_1, P_2, \cdots, P_r, Q_1, Q_2, \cdots, Q_s \in \Gamma = E(\mathbb{Q})$ τέτοια ώστε

$$\forall P \in \Gamma,\ P = n_1P_1 + \cdots + n_rP_r + m_1Q_1 + m_2Q_2 + \cdots m_sQ_s.$$

Οι ακέραιοι n_i είναι μονοσήμαντα ορισμένοι και οι m_j ορίζονται $\bmod p_j^{\nu_j}$.

Έστω Q ένα σημείο τάξεως 2, δηλαδή $2Q = \mathcal{O}$.

$$Q \ =\ n_1P_1 + n_2P_2 + \cdots n_rQ_r + m_1Q_1 + \cdots + m_sQ_s.$$

$$2Q = \mathcal{O} \Longrightarrow \left\{ \begin{array}{ll} n_i = 0 & \forall i = 1, 2, \cdots, r \\ 2m_j \equiv 0 \ (\mathrm{mod}\, p_j^{\nu_j}) & (j \in \{1, 2, \cdots, s\}) \end{array} \right\}.$$

Αν p_j περιττός, τότε $m_j \equiv 0 \pmod{p_j^{\nu_j}}$ ενώ αν $p_j = 2$ τότε $m_j \equiv 0 \pmod{2^{\nu_j - 1}}$.
Επειδή δε m_j είναι μονοσήμαντα ορισμένο $\pmod{2^{\nu_j}}$ έπεται ότι $m_j \equiv 0$ ή $2^{\nu_j - 1} \pmod{2^{\nu_j}}$.
Παρατηρούμε ότι για κάθε m_j έχουμε δύο δυνατότητες και συνεπώς υπάρχουν 2^t σημεία Q με $2Q = \mathcal{O}$ δηλαδή $|\Gamma_2| = 2^t$.

Συμπέρασμα:

$$2^r = \frac{\left|\Gamma/2\Gamma\right|}{\left|\Gamma_2\right|}.$$

Προφανώς

$$\left|\Gamma_2\right| = \begin{cases} 2, & \text{όταν } a^2 - 4b \text{ δεν είναι τέλειο τετράγωνο} \\ 4, & \text{όταν } a^2 - 4b \text{ είναι τέλειο τετράγωνο} \end{cases}$$

Το λήμμα 9 της σελίδας 86 δίνει

$$\psi A/\psi B \cong \left(A/B\right) \Big/ \left(\ker\psi/\ker\psi \cap B\right).$$

Για $A = \bar{\Gamma}$ και $B = \varphi\Gamma$ έχουμε

$$\psi\bar{\Gamma}/2\Gamma \cong \left(\bar{\Gamma}/\varphi\Gamma\right) \Big/ \left(\ker\psi/\ker\psi \cap \varphi\Gamma\right), \qquad \ker\psi = \left\{\mathcal{O}, (0,0)\right\}.$$

Επίσης

$$(0,0) \in \varphi\Gamma \quad \Longleftrightarrow \quad \bar{b} = a^2 - 4b \in {\mathbb{Q}^*}^2$$

οπότε

$$\begin{aligned} \left|\ker\psi/\ker\psi \cap \varphi\Gamma\right| &= \begin{cases} 2, & \text{όταν } a^2 - 4b \notin {\mathbb{Q}^*}^2 \\ 1, & \text{όταν } a^2 - 4b \in {\mathbb{Q}^*}^2 \end{cases} \\ &= \frac{4}{\left|\Gamma_2\right|}. \end{aligned}$$

Από τα παραπάνω προκύπτει ότι

$$\left|\Gamma/2\Gamma\right| = \left|\Gamma/\psi\bar{\Gamma}\right| \cdot \left|\bar{\Gamma}/\varphi\Gamma\right| \cdot \frac{1}{4}|\Gamma_2| \qquad \left(\begin{array}{c} \text{όλοι οι δείκτες} \\ \text{είναι πεπερασμένοι} \end{array}\right)$$

$$\text{οπότε} \quad 2^r = \frac{\left|\Gamma/\psi\bar{\Gamma}\right| \cdot \left|\bar{\Gamma}/\varphi\Gamma\right|}{4}, \quad \text{δηλαδή}$$

$$2^r = \frac{[\Gamma : \psi\bar{\Gamma}]\,[\bar{\Gamma} : \varphi\Gamma]}{4}.$$

Από τη σχέση 5.4 της σελίδας 86, έχουμε $[\bar{\Gamma} : \varphi\Gamma] = |\bar{\alpha}\bar{\Gamma}|$. Έχουμε λοιπόν αποδείξει το

Θεώρημα 10. *Αν* $E : y^2 = x^3 + ax^2 + bx$ $(a, b \in \mathbb{Z})$, $\bar{E} : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$ *και αν συμβολίσουμε με* $\Gamma = E(\mathbb{Q}), \bar{\Gamma} = \bar{E}(\mathbb{Q}), r = rank(E(\mathbb{Q})$, *ισχύει*

$$2^r = \frac{|\alpha\Gamma| \cdot |\bar{\alpha}\bar{\Gamma}|}{4}.$$

Υπολογισμός της $\alpha\Gamma$

Αφού $(0,0) \in \Gamma$ έπεται ότι το $b\,\mathbb{Q}^{*2}$ ανήκει πάντα στο $\alpha\Gamma$. Έστω τώρα $(x, y) \in \Gamma$ και $y \neq 0$. Είχαμε πιό μπροστά καταλήξει στο συμπέρασμα ότι θα πρέπει

$$x = \frac{m}{e^2},\ y = \frac{n}{e^3},\ \ (m, e) = (n, e) = 1,\ e > 0,$$

$$n^2 = m(m^2 + ame^2 + be^4).$$

Έστω $b_1 := (m, b)$. Διαλέγουμε το b_1 έτσι ώστε ο

$$m_1 = \frac{m}{b_1} > 0, \quad b_2 := \frac{b}{b_1}, \quad \text{δηλαδή} \quad (m_1, b_2) = 1.$$

Έχουμε $n^2 = b_1 m_1(b_1^2 m_1^2 + ab_1 m_1 e^2 + b_1 b_2 e^4) = b_1^2 m_1(b_1 m_1^2 + am_1 e^2 + b_2 e^4)$

$$\Longrightarrow \quad b_1^2 \,\big|\, n^2 \quad \Longrightarrow \quad b_1 \,\big|\, n.$$

Έστω τώρα $n_1 = \frac{n}{b_1}$. Έχουμε

$$n_1^2 = m_1(b_1 m_1^2 + am_1 e^2 + b_2 e^4).$$

Ο μέγιστος κοινός διαιρέτης $(m_1, b_1 m_1^2 + am_1 e^2 + b_2 e^4) = (m_1, b_2 e^4) = 1$ διότι $(b_2, m_1) = 1$ και $(e, m_1) = 1$ (το τελευταίο διότι $(e, m) = 1$). Επειδή τώρα $m_1 > 0$ έπεται ότι υπάρχει $M \in \mathbb{N}$ τέτοιος ώστε $m_1 = M^2$ και $M \,\big|\, n_1$ (διότι $m_1 \,\big|\, n_1$).
Γράφουμε $N = \frac{n_1}{M} \in \mathbb{N}$ και έχουμε

$$N^2 = b_1 M^4 + a^2 M^2 e^2 + b_2 e^4$$

$$\text{όπου} \quad x = \frac{b_1 M^2}{e^2} \quad \text{και} \quad y = \frac{b_1 MN}{e^3}.$$

Θεώρημα 11 (Θεώρημα του Tate)

$$\alpha\Gamma = \left\{\mathbb{Q}^{*2}, b\mathbb{Q}^{*2}\right\} \cup \left\{b_1\mathbb{Q}^{*2},\ \text{όπου } b_1|b,\ b = b_1 b_2\right.$$
$$\left.\text{και ή}\ \ z^2 = b_1 x^4 + ax^2 y^2 + b_2 y^4 \ \text{έχει λύση στο}\ \ \mathbb{Z}\ \ \text{με}\ \ xy \neq 0\right\}.$$

Απόδειξη:

"$\subseteq$": Έστω $c\,\mathbb{Q}^{*2} \in \alpha\Gamma$. Τότε υπάρχει $P \in \Gamma$ τέτοιο ώστε $\alpha P = c\,\mathbb{Q}^{*2}$.

1^{η} περίπτωση: Αν $P = \mathcal{O}$ τότε $\alpha P = \mathbb{Q}^{*2}$.

2^{η} περίπτωση: Αν $P = (0,0)$ τότε $\alpha P = b\,\mathbb{Q}^{*2}$.

3^{η} περίπτωση: Αν $P = (x,y),\ y \neq 0$ έχουμε ήδη αποδείξει ότι

$$x = \frac{b_1 M^2}{e^2} \Longrightarrow \alpha(P) \equiv b_1 \pmod{\mathbb{Q}^{*2}}.$$

4^{η} περίπτωση: Αν $P = (x,0)$ με $x \neq 0$ τότε $x^2 + ax + b = 0$ όπου $x \in \mathbb{Q}$ και $a, b \in \mathbb{Z}$, δηλαδή $x \in \mathbb{Z}$ και $x|b$. Γράφουμε $b_1 = x,\ b_2 = \dfrac{b}{b_1}$ και επομένως $b_1^2 + ab_1 + b_1 b_2 = 0$. Επειδή $x = b_1 \neq 0$ έχουμε $b_1 + a + b_2 = 0$, συνεπώς η $z^2 = b_1 x^4 + a x^2 y^2 + b_2 y^4$ είναι επιλύσιμη με $(x,y,z) = (1,1,0)$.

"$\supseteq$": Έστω $c\mathbb{Q}^{*2}$.

1^{η} περίπτωση: Έστω $c\,\mathbb{Q}^{*2} = \mathbb{Q}^{*2},\ b\,\mathbb{Q}^{*2}$, ισχύει.

2^{η} περίπτωση: Έστω $c\,\mathbb{Q}^{*2} = b_1\mathbb{Q}^{*2}$ με $b_1|b,\ b = b_1 b_2$ και έστω (M,e,N) λύση της $z^2 = b_1 x^4 + a x^2 y^2 + b_2 y^4$ με $Me \neq 0$ στο $\mathbb{Z}$. Τότε

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4 \Rightarrow b_1 M^2 N^2 = b_1^3 M^6 N^2 + a b_1^2 M^4 e^2 + b b_1 M^2 e^4.$$

Συνεπώς

$$P = \left(\frac{b_1 M^2}{e^2}, \frac{b_1 M N}{e^3}\right) \in \Gamma \quad \text{και} \quad \alpha P = b_1 \mathbb{Q}^{*2} = c\,\mathbb{Q}^{*2}.$$

Παραδείγματα:

(1) Έστω η ελλειπτική καμπύλη $E/y^2 = x^3 - x$.

Έχουμε $a = 0, b = -1$ δηλαδή $-2a = 0, a^2 - 4b = 4$. Επομένως $\bar{E}/y^2 = x^3 + 4x$. Επειδή το $b = -1$ για το b_1 έχουμε δύο δυνατότητες ± 1. Για την α ισχύουν

$$\alpha(\mathcal{O}) \equiv 1 \pmod{\mathbb{Q}^{*2}},\ \ \alpha(P_0) \equiv b \pmod{\mathbb{Q}^{*2}}.$$

$$\Longrightarrow \alpha\Gamma = \{\mathbb{Q}^{*2}, -\mathbb{Q}^{*2}\} \Longrightarrow |\alpha\Gamma| = 2.$$

Επίσης $\bar{b} = 4$, οπότε για το b_1 έχουμε τις δυνατότητες

$$b_1 = \pm 1,\ \pm 2,\ \pm 4.$$

Αλλά $4 \equiv 1 \pmod{\mathbb{Q}^{*2}}$ και $-4 \equiv -1 \pmod{\mathbb{Q}^{*2}}$ οπότε η $\bar{\alpha}(\bar{\Gamma})$ έχει το πολύ τέσσερα στοιχεία:

$$\bar{\alpha}(\bar{\Gamma}) \subseteq \left\{\mathbb{Q}^{*2}, -\mathbb{Q}^{*2}, 2\,\mathbb{Q}^{*2}, -2\,\mathbb{Q}^{*2}\right\}.$$

Οι εξισώσεις για $b_1 = \pm 1, \pm 2$ είναι αντίστοιχα

$$Z^2 = X^4 + 4Y^4,$$
$$Z^2 = -X^4 - 4Y^4,$$
$$Z^2 = 2X^4 + 2Y^4,$$
$$Z^2 = -2X^4 - 2Y^4.$$

Η δεύτερη και τέταρτη προφανώς δεν έχουν ακέραια λύση. Άρα, έχουμε να ελέγξουμε τις $Z^2 = X^4 + 4Y^4$ και $Z^2 = 2X^4 + 2Y^4$.
Η πρώτη αντιστοιχεί στο $b_1 = 1$ και προφανώς το $\mathbb{Q}^{*\,2}$ ανήκει στην $\bar{\alpha}\bar{\Gamma}$. Και η δεύτερη θα πρέπει να έχει λύση διότι από το θεώρημα 10 της σελίδας 89 έπεται ότι $|\alpha\Gamma| \cdot |\bar{\alpha}\bar{\Gamma}|$ είναι τουλάχιστο 4. Συνεπώς

$$|\bar{\alpha}\bar{\Gamma}| = 2 \implies |\bar{\alpha}\bar{\Gamma}| = \{1, 2 \pmod{\mathbb{Q}^{*\,2}}\}$$
$$\implies 2^r = 1 \Rightarrow r = 0.$$

Τέλος, επειδή η $E(\mathbb{Q})$ είναι πεπερασμένη και η $\bar{E}(Q)$ είναι πεπερασμένη, έπεται ότι ο 1 δεν είναι ισοδύναμος αριθμός. Θυμίζουμε ότι ένας φυσικός αριθμός m λέγεται **ισοδύναμος** όταν είναι εμβαδό ενός ορθογωνίου τριγώνου με πλευρές **ρητούς** αριθμούς.

Σημείωση 12. *Λύση της* $Z^2 = 2X^4 + 2Y^4$ *είναι* $2^2 = 2 \cdot 1^4 + 2 \cdot 1^4$.

(2) Έστω $E/y^2 = x^3 + x$, $\bar{E}/y^2 = x^3 - 4x$.
Εύκολα βρίσκουμε ότι $r = 0$ και ότι $\mathcal{O}$ και P_0 είναι τα μόνα σημεία πεπερασμένης τάξης της E.

(3) Έστω $E/y^2 = x^3 - 5x$, $a = 0$, $b = -5$ $\bar{E}/y^2 = x^3 + 20x$. Οι δυνατότητες για το $b_1 = 1, -1, 5, -5$. Συνεπώς πρέπει να ελέγξουμε αν οι παρακάτω εξισώσεις είναι επιλύσιμες:

$$Z^2 = X^4 - 5Y^4, \quad Z^2 = -X^4 + 5Y^4 \tag{5.6}$$

$$Z^2 = 5X^4 - Y^4 \quad Z^2 = -5X^4 + Y^4 \tag{5.7}$$

Οι εξισώσεις (5.6) είναι επιλύσιμες αν και μόνο αν οι εξισώσεις (5.7) είναι επιλύσιμες. Έχουμε

$$1^2 = 3^4 - 5 \cdot 2^4 \;\; 2^2 = (-1)^4 + 5 \cdot 1^4$$

δηλαδή όλες έχουν λύση. Επομένως

$$\alpha\Gamma = \{\pm 1, \pm 5\mathbb{Q}^{*\,2}\} \Longrightarrow |\alpha\Gamma| = 4.$$

Για το $\bar{b}_1$ έχουμε τις εξής δυνατότητες:

$$\pm 1,\ \pm 2,\ \pm 4,\ \pm 5,\ \pm 10,\ \pm 20.$$

Επειδή $\pm 4 \equiv \pm 1 \pmod{\mathbb{Q}^{*\,2}}$ και $\pm 20 \equiv \pm 5 \pmod{\mathbb{Q}^{*\,2}}$ έπεται ότι για το $\bar{b}_1$ έχουμε τις δυνατότητες $\pm 1, \pm 2, \pm 5, \pm 10$. Για $b_1 b_2 = 20 > 0$ έχουμε $b_1 X^4 + b_2 Y^4 = Z^2 > 0$. Για $b_1 = -1, -2, -5, -10$ δεν έχουμε λύση.
Επομένως $\bar{\alpha}\bar{\Gamma} \subseteq \{1, 2, 5, 10 \pmod{\mathbb{Q}^{*\,2}}\}$.

$$\alpha(\bar{\mathcal{O}}) = 1 \quad \Longrightarrow \quad \alpha(P_0') = \bar{b} = 20 \equiv 5 \pmod{\mathbb{Q}^{*\,2}}.$$

Απομένει να ελεγχθεί αν η εξίσωση

$$Z^2 = 2X^4 + 10Y^4, \text{ έχει λύση με } XY \neq 0$$

(η άλλη εξίσωση είναι όμοια, $Z^2 = 10X^4 + 2Y^4$).
Έστω ότι έχει λύση (x_0, y_0, z_0). Προφανώς ο z είναι άρτιος, $z = 2z_1$, συνεπώς $2z_1^2 = x_0^4 + 5y_0^4$. Επειδή $(M, b_2) = (x_0, 5) = 1$ έπεται ότι $x_0^4 \equiv 1 \pmod 5$ δηλαδή $2z_1^2 \equiv 1 \pmod 5$ ή αλλιώς $z_1^2 \equiv 3 \pmod 5$ που σημαίνει ότι $\left(\frac{3}{5}\right) = 1$, άτοπο, διότι $\left(\frac{3}{5}\right) = -1$.

$$\begin{aligned} &\text{Ώστε} \qquad \bar{\alpha}\bar{\Gamma} = \left\{1, 5 \pmod{\mathbb{Q}^{*\,2}}\right\}, \ \left|\bar{\alpha}\bar{\Gamma}\right| = 2 \\ &\Longrightarrow \qquad 2^r = \frac{4 \cdot 2}{4} = 2. \end{aligned}$$

Επομένως ο rank της E είναι ένα.

Σημείωση 13. *Ίσως φαίνεται λίγο περίεργο ότι $y^2 = x^3 - 5x$ έχει άπειρο πλήθος ρητών σημείων ενώ η $y^2 = x^3 - x$ έχει πεπερασμένο. Γενικά, είναι πολύ δύσκολο από την εξίσωση της ελλειπτικής καμπύλης να βγάλουμε συμπέρασμα για το rank αυτής.*

(4) Έστω $p \in \mathbb{P}$, $p \equiv 5 \pmod 8$.
Θεωρούμε την ελλειπτική καμπύλη $E/y^2 = x^3 + p^2 x$. Έχουμε $\bar{E}/y^2 = x^3 - 4p^2 x$. Έστω $r_1 = \log_2 |\alpha\Gamma| - 1$ και $r_2 = \log_2 |\bar{\alpha}\bar{\Gamma}| - 1$ και $r = \text{rank} E(\mathbb{Q})$. Προφανώς $r = r_1 + r_2$.

$b_1 = \pm 1, \pm p$ (διότι $\pm p^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}$)

Αν $b_1 = 1, b = p^2$ τότε $\mathbb{Q}^{*2} \subseteq \alpha\Gamma$.

Οι εξισώσεις $-X^4 - p^2Y^4 = Z^2$ και $-pX^4 - pY^4 = Z^2$, δεν έχουν λύση. Επομένως

$$\alpha\Gamma \subset \{1, p \pmod{\mathbb{Q}^{*2}}\}.$$

Στη συνέχεια εξετάζουμε αν η $pX^4 + pY^4 = Z^2$, δηλαδή αν η $p(X^4 + Y^4) = Z^2$ έχει ακέραια λύση.

Έστω (x, y, z) λύση της εξίσωσης με $xy \neq 0$.

Αν $x \equiv 0 \pmod 2$ τότε $x^4 \equiv 0 \pmod 8$.

Αν $x \equiv 1 \pmod 2$ τότε $x^4 \equiv 1 \pmod 8$ οπότε

$x \pmod 2$	$y \pmod 2$	$x^4+y^4 \pmod 8$
0	0	$*$
0	1	1
1	0	1
1	1	2

Την $*$ δεν την μελετούμε διότι, χωρίς περιορισμό της γενικότητας, μπορούμε να υποθέσουμε ότι $(x, y) = 1$.

Πράγματι, $x = \dfrac{b_1M^2}{e^2}$, $y = \dfrac{b_1MN}{e^3}$ $(b_1|b,\ (M, e) = (N, e) = (b_1, e) = 1)$. Έχουμε $(b_2, M) = 1$ διότι $(m_1, b_2) = 1$ $(b_1 = (m, b)$ και $m_1 = \dfrac{m}{b_1})$.

Επίσης $(N, M) = 1$. Πράγματι, αν $p|(N, M)$ τότε $p|b_2e^4$ επομένως $p|b_2$ δηλαδή $p|(b_2, M) = 1$, άτοπο.

Άρα $x^4 + y^4 \equiv 1, 2 \pmod 8$ συνεπώς $p(x^4 + y^4 \equiv 5, 2 \pmod 8)$. Αλλά $p(x^4 + y^4) = z^2 \equiv 0, 1, 4 \pmod 8$, άτοπο.

Επομένως $\alpha\Gamma = \{\mathbb{Q}^{*2}\}$ δηλαδή $r_1 = -1$.

Μελετούμε στην συνέχεια την ελλειπτική καμπύλη $\bar{E}/y^2 = x^3 - 4p^2x$. Προφανώς,

$$\{1, -1\}\mathbb{Q}^{*2} \subseteq \bar{\alpha}\bar{\Gamma} \subseteq \{1, 2, p, 2p, -1, -2, -p, -2p\}\mathbb{Q}^{*2}.$$

Θεωρούμε την εξίσωση $pX^4 - 4pY^4 = Z^2$ ή αλλιώς την $p(X^4 - 4Y^4) = Z^2$.

Έστω (x, y, z) λύση της τελευταίας με $xy \neq 0$. Τότε $x^4 - 4y^4 \equiv 0 \pmod p$ συνεπώς $\left(\dfrac{x}{y}\right)^4 \cong 4 \pmod p$. (Αν ήταν $y \equiv 0 \pmod p$ τότε και $x \equiv 0 \pmod p$ δηλαδή $p|(x, y)$).

Επομένως $\left(\frac{x}{y}\right)^2 \equiv \pm 2 \pmod p$, που σημαίνει ότι $\left(\frac{\pm 2}{p}\right) = 1$. Αλλά $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{2}{p}\right) = -1$, επομένως $\left(\frac{\pm 2}{p}\right) = -1$, άτοπο. Άρα $p\mathbb{Q}^{*2} \notin \bar{\alpha}\bar{\Gamma}$ οπότε $|\bar{\alpha}\bar{\Gamma}| \leq 4$. Συνεπώς $r_2 = \log_2 |\bar{\alpha}\bar{\Gamma}| - 1 \leq 2 - 1 = 1$. Άρα

$$r_2 \leq 1 \quad \Rightarrow \quad r = r_1 + r_2 \leq -1 + 1 = 0 \quad \Rightarrow \quad r = 0.$$

Πόρισμα 14. *Αν $p \in \mathbb{P}$, $p \equiv 5 \ (mod\, 8)$ τότε η εξίσωση $2(X^4 - p^2Y^4) = Z^2$ έχει υπέρ το $\mathbb{Z}$ μόνο την τετριμμένη λύση.*

Απόδειξη: Η $2p(X^4 - Y^4) = Z^2$ έχει λύση $(1, 1, 0)$ συνεπώς $2p\mathbb{Q}^{*2} \in \bar{\alpha}\bar{\Gamma}$. Αν και $2\mathbb{Q}^{*2} \in \bar{\alpha}\bar{\Gamma}$ έπεται ότι και το γινόμενο $2p\mathbb{Q}^{*2} \cdot 2\mathbb{Q}^{*2} = p\mathbb{Q}^{*2} \in \bar{\alpha}\bar{\Gamma}$, άτοπο διότι στο θεώρημα αποδείξαμε ότι $p\mathbb{Q}^{*2} \notin \bar{\alpha}\bar{\Gamma}$.
Επομένως $2\mathbb{Q}^{*2} \notin \bar{\alpha}\bar{\Gamma}$ δηλαδή η $2(X^4 - p^2Y^4) = Z^2$ έχει μόνο την τετριμμένη λύση. □

Εικασία 15 (Εικασία των Mordell-Selmer) *Αν p πρώτος, $p \equiv 5 \ (mod\, 8)$, η ελλειπτική καμπύλη $E/y^3 = x^3 + px$ έχει rank ένα.*

Για $p < 1000$ επαληθεύτηκε από τους Bremner-Cassels, το 1984. Επίσης,

- 1948 Wiman, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 4$.
- 1974 Penney και Pomerance, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 6$.
- 1975 Penney και Pomerance, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 7$.
- 1977 Grunewald και Zimmert, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 8$.
- 1977 Grunewald και Zimmert, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 9$.
- 1979 Nakata, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 9$.

- 1981 Mestre, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 10, 11, 12$.
- 1984 Kretschmer, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r = 10$ και τετριμμένη torsion.
- 1985 Mestre, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 14$.
- 1993 Nagao, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 20$.
- 1994 Nagao και Kouya, αποδείχτηε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 21$.
- 1998, Fermigier, αποδείχτηκε ότι υπάρχει ελλειπτική καμπύλη με rank $r \geq 22$.
- 1999, Marin, McMillen, αποδείχτηκε ότι η ελλειπτική καμπύλη

  $$\begin{aligned} Y^2 + XY + Y &= X^3 - 1925296640867401282806596461641844172 3X \\ &\quad + 3268550072771637625792334707145204429590744305634561400 6 \end{aligned}$$

  έχει rank $r \geq 23$.

Εικασία 16. *Υπάρχει ελλειπτική καμπύλη ορισμένη υπέρ το $\mathbb{Q}$ με οσοδήποτε μεγάλο rank.*

Πρόσφατα ο Noam Elkies έθεσε το ερώτημα:

> ''Ποιός είναι ο πιο μεγάλος φυσικός αριθμός r για τον οποίο υπάρχουν άπειρες ελλειπτικές καμπύλες της μορφής
>
> $$Y^2 = X^3 + A$$
>
> ορισμένες στο $\mathbb{Q}$ τέτοιες ώστε να έχουν rank $\geq r$; Έχει κατασκευαστεί μία τέτοια οικογένεια καμπυλών;''

Ο Mestre παρέπεμψε στην εργασία του "Rang de courbes elliptiques d' invariant nul", C. R. Acad. Sc. Paris, **321** (1995), 1235-1236 βάσει της οποίας το ρεκόρ μέχρι αυτή τη στιγμή είναι $r = 7$.

Στην συνέχεια θα μελετήσουμε ελλειπτικές καμπύλες της μορφής $E|y^2 = x^3 + d$, $d \in \mathbb{Z}$, d ελεύθερος τετραγώνου. Το σημείο $(-d, 0)$ είναι ρητό σημείο τάξεως 2. Κάνουμε τον μετασχηματισμό

$$x \mapsto x - d, \quad y \mapsto y.$$

και παίρνουμε $y^2 = (x-d)^3 + d^3$, δηλαδή $E/y^2 = x(x^2 - 3dx + 3d^2)$, $A = -3d, B = 3d^2$. Η ισογενής της είναι $\tilde{E}/y^2 = x^3 + \bar{A}x^2 + \bar{B}x$, όπου $\bar{A} = -2A = 6d$, $\bar{B} = A^2 - 4B = 9d^2 - 12d^2 = -3d^2$, δηλαδή

$$\tilde{E}/y^2 = x^3 + 6dx^2 - 3d^2x.$$

Έστω ότι ο d είναι πρώτος αριθμός, $d = p > 3$, $B = 3p^2$, οπότε για το b_1 έχουμε τις ακόλουθες δυνατότητες:

$$b_1 = \pm 1, \pm 3, \pm p, \pm 3p.$$

Ψάχνουμε για λύσεις στην διοφαντική εξίσωση

$$Z^2 = b_1X^4 - 3pX^2Y^2 + b_2Y^4.$$

Έχουμε

$$\{1,3\}\mathbb{Q}^{*\,2} \subseteq \alpha\Gamma \subseteq \{\pm 1, \pm 3, \pm p, \pm 3p\}\mathbb{Q}^{*\,2}.$$

Για $b_1 = -1$ η εξίσωση $-X^4 - 3pX^2Y^2 - 3p^2Y^4 = Z^2$ δεν έχει λύση διότι η τετραγωνική μορφή της παριστά μόνο αρνητικούς ακέραιους. Ομοίως για $b_1 = -3, -p, -3p$.
Ώστε $\{1,3\}\mathbb{Q}^{*\,2} \subseteq \alpha\Gamma \subseteq \{1,3,p,3p\}\mathbb{Q}^{*\,2}$.
Αν $b_1 = p$ τότε $b_2 = 3p$ και αντίστροφα αν $b_1 = 3p$ τότε $b_2 = p$ οπότε αρκεί να εξετάσουμε αν έχει λύση η εξίσωση για $b_1 = p$.

$$|\alpha\Gamma| = \begin{cases} 4, & \text{αν η } Z^2 = pX^4 - 3pX^2Y^2 + 3pY^4 \ (*) \text{ έχει μη-τετριμμένη ακέραια λύση} \\ 2, & \text{αλλιώς} \end{cases}$$

Παίρνουμε τώρα την ισογενή της $\tilde{E}/y^2 = x^3 + 6px^2 - 3p^2x$. Έχουμε

$$\{1,-3\}\mathbb{Q}^{*\,2} \subseteq \bar{\alpha}\bar{\Gamma} \subseteq \{\pm 1, \pm 3, \pm p, \pm 3p\}\mathbb{Q}^{*\,2}.$$

Πρέπει να ελέγξουμε την επιλυσιμότητα της διοφαντικής εξίσωσης $Z^2 = b_1X^4 + 6pX^2Y^2 + b_2Y^4$.
Για $b_1 = \pm 1$ βρίσκουμε $b_2 = \mp 3p$.
Για $b_1 = \pm 3p$ βρίσκουμε $b_2 = \mp p$.
Αν έχει η μία λύση τότε θα έχει και η άλλη.
Τέλος για $b_1 = 3$ έχουμε $b_2 = -p^2 \equiv -1 \pmod{\mathbb{Q}^{*\,2}}$.

Έχουμε λοιπόν να ελέγξουμε την επιλυσιμότητα των διοφαντικών εξισώσεων

$$Z^2 = -3pX^4 + 6pX^2Y^2 + pY^4 \tag{5.8}$$

$$Z^2 = 3pX^4 + 6pX^2Y^2 - pY^4 \tag{5.9}$$

$$Z^2 = 3X^4 + 6pX^2Y^2 - p^2Y^4 \tag{5.10}$$

Έστω (u, v, w) μία μη-τετριμμένη λύση της εξίσωσης μίας, οποιασδήποτε, από τις παραπάνω εξισώσεις. Αν $3|w$ τότε $3|u^2$, δηλαδή $3|u$. Επομένως $3^2|pv^4$, συνεπώς $3|v$. Θέτουμε

$$\left\{ \begin{array}{lcl} u & \to & \frac{u}{3^2} \\ v & \to & \frac{v}{3} \\ w & \to & \frac{w}{3} \end{array} \right\}.$$

Επομένως $\left(\frac{u}{3^2}, \frac{v}{3}, \frac{w}{3}\right)$ είναι επίσης λύση, οπότε, χωρίς περιορισμό της γενικότητας, υποθέτουμε ότι $3 \nmid w$.

Η (5.10) τώρα $(\mathrm{mod}\, 3)$ δίνει

$$Z^2 \equiv -p^2Y^4 \ (\mathrm{mod}\, 3).$$

Όμως, επειδή $\left(\frac{-p^2Y^4}{3}\right) = \left(\frac{-1}{3}\right) = -1$, έπεται ότι η (5.10) δεν έχει λύση.

Αν (u, v, w) όχι τετριμμένη λύση της (5.9) τότε

$$u^2 \equiv -pw^4 \ (\mathrm{mod}\, 3) \Rightarrow p \equiv 2 \ (\mathrm{mod}\, 3).$$

Ανάλογα για την 5.8 βρίσκει κανείς ότι αν έχει μη-τετριμμένη ακεραία λύση τότε $p \equiv 1 \ (\mathrm{mod}3)$. Επομένως

$$\left|\bar{\alpha}\bar{\Gamma}\right| = \left\{ \begin{array}{ll} 4, & \text{αν } p \equiv 2 \ (\mathrm{mod}\, 3) \text{ και η 5.9 έχει μη-τετριμμένη λύση} \\ 4, & \text{αν } p \equiv 1 \ (\mathrm{mod}\, 3) \text{ και η 5.8 έχει μη-τετριμμένη λύση} \\ 2, & \text{σ' όλες τις άλλες περιπτώσεις} \end{array} \right. \tag{5.11}$$

Πολλαπλασιάζουμε την (5.8) με p^3 και βρίσκουμε την ισοδύναμή της

$$pZ^2 = -3X^4 + 6X^2Y^2 + Y^4. \tag{5.8'}$$

Ομοίως

$$pZ^2 = 3X^4 + 6X^2Y^2 - Y^4 \tag{5.9'}$$

είναι ισοδύναμη της (5.9).

Λύνουμε και τις δύο $(\mathrm{mod}\, p)$ ως προς X^2 και βρίσκουμε

$$X^2 \equiv \left(1 \pm \frac{2}{3}\sqrt{3}\right) y^2 \ (\mathrm{mod}\, p).$$

Για να είναι επιλύσιμη θα πρέπει $\sqrt{3} \in \mathbb{Q}_p$ (σώμα των p-αδικών αριθμών). Ισχύει

$$\sqrt{3} \in \mathbb{Q}_p \iff \sqrt{3} = p^m \varepsilon, \quad m \in \mathbb{Z} \text{ και } \varepsilon \ p\text{-αδική μονάδα.}$$

Θα πρέπει λοιπόν το 3 να είναι τέλειο τετράγωνο $(\mathrm{mod} p)$. Αυτό συμβαίνει ακριβώς τότε όταν $\left(\frac{3}{p}\right) = 1$ ή αλλιώς $(-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) = 1$.
Αν $p \equiv 1 \ (\mathrm{mod}\, 4)$ τότε $p \equiv 1 \ (\mathrm{mod}\, 12)$ και
αν $p \equiv 3 \ (\mathrm{mod}\, 4)$ τότε $p \equiv 11 \ (\mathrm{mod}\, 12)$. Έχουμε επομένως αποδείξει το ακόλουθο

Θεώρημα 17 (G. Frey, Manuscripta Mathematica, 1984) *Αν $p \equiv 5 \ (mod\, 12)$ τότε $r = rank(E(\mathbb{Q})) = 0$.*
Αν $p \equiv 7 \ (mod\, 12)$ τότε $r = rank(E(\mathbb{Q})) \leq 1$.
Ισχύει $r = 1$ ακριβώς τότε όταν η εξίσωση 5.11 στην σελίδα 97, έχει μη-τετριμμένη ακέραια λύση.
Αν $p \equiv 11 \ (mod\, 12)$ τότε $rank(E(\mathbb{Q})) \leq 1$ και μάλιστα ισχύει $rank(E(\mathbb{Q})) = 1$ αν και μόνο αν η 5.9′ έχει μη-τετριμμένη λύση.
Αν $p \equiv 1 \ (mod\, 12)$ τότε $rank(E(\mathbb{Q})) \leq 2$ και μάλιστα $rank(E(\mathbb{Q})) = 2$ αν και μόνο αν η 5.8′ και 5.11 έχουν μη τετριμμένες λύσεις.
(Εδώ παρατηρούμε ότι $Z^2 \equiv pX^4 \ (mod\, 3)$ έχει λύση αν και μόνο αν $p \equiv 1 \ (mod\, 3)$ δηλαδή αν και μόνο αν $p \equiv 1, 7 \ (mod\, 12)$.

Επανερχόμαστε τώρα στο θέμα της εύρεσης ελλειπτικών καμπυλών με μεγάλο rank. Έχουμε αποδείξει ότι

$$2^r = \frac{|\Gamma/2\Gamma|}{|\Gamma_2|} \Longrightarrow |\Gamma/2\Gamma| = 2^{r+1} \Longrightarrow$$

$$2^{r+1} = |(\mathbb{Z}/2\mathbb{Z})^{r+1}| = |\Gamma/2\Gamma| \geq |\Gamma/\ker\alpha| = |\alpha\Gamma|$$

διότι $2\Gamma \subseteq \ker\alpha$. Αν λοιπόν γνωρίζουμε το $\alpha\Gamma$, γνωρίζουμε ένα κατώτερο φράγμα για το rank r της E. Θα πρέπει λοιπόν να ψάξουμε για $a, b \in \mathbb{Z}$ τέτοια ώστε το $|\alpha\Gamma|$ να γίνεται μεγάλο. Θα πρέπει δηλαδή το b να έχει όσο πιό πολλούς παράγοντες γίνεται.

Ορίζουμε $S := \{b\} \cup \{b_1 \mid b_2, b_2 = b/b_1,\ b_1 + a + b_2$ είναι τέλειο τετράγωνο.$\}$.

Προφανώς $S\,\mathbb{Q}^{*\,2} \subseteq \alpha\Gamma$.

Έστω B η ομάδα που παράγεται από το $S\,\mathbb{Q}^{*\,2}$, υποομάδα της $\mathbb{Q}^*/\mathbb{Q}^{*\,2}$. Επειδή $S\,\mathbb{Q}^{*\,2} \subseteq \alpha\Gamma$ έπεται ότι $B = \langle S\,\mathbb{Q}^{*\,2}\rangle \subseteq \alpha\Gamma$ συνεπώς $|B| = 2^t,\ t \in \mathbb{N}_0$. Επομένως

$$2^{r+1} \geq |\alpha\Gamma| \geq |B| = 2^t \Rightarrow r \geq t - 1.$$

Αρκεί λοιπόν να φτιάξουμε το t κατά το δυνατό μεγάλο.

Αλγόριθμος 18.

(1) Διαλέγουμε ένα $b \in \mathbb{Z}$ με αρκετούς πρώτους διαιρέτες.

(2) Διαλέγουμε έτσι το a ώστε όσο γίνεται πιό πολλοί από τους ακεραίους $b_1 + a + b_2$ να είναι τέλεια τετράγωνα ($b_i \in \mathbb{Z},\ b_1 b_2 = b$).

(3) Βρίσκουμε ένα κάτω φράγμα του r.

Αλγόριθμος υπολογισμού του t, $|B| = 2^t$: Έστω $p_1, p_2, \cdots, p_s$ $(s \in \mathbb{N})$ οι διακεκριμένοι μεταξύ τους πρώτοι διαιρέτες του b και

$$T = \left\{(-1)^{l_0} p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s} \mid l_i \in \mathbb{N}_0\right\}$$

Ορίζουμε

$$\pi : \begin{cases} T & \longrightarrow \quad (\mathbb{Z}/2\mathbb{Z})^{s+1} \\ (-1)^{l_0} p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s} & \longmapsto \quad \big(l_0 \pmod 2, \cdots, l_s \pmod 2\big) \end{cases}$$

Ο $\pi(S)$ έχει σαν πίνακα $|S| \times (s+1)$ υπέρ το $\mathbb{Z}/2\mathbb{Z}$. Επομένως

$$t = \operatorname{rank} \pi(S).$$

Παράδειγμα: Έστω $y^2 = x^3 + 17x^2 + 15x,\ a = 17, b = 3 \cdot 5$. Έχουμε

$$\begin{aligned} -1 + 17 - 15 &= 1 \\ 3 + 17 + 5 &= 5^2 \\ -3 + 17 - 5 &= 3^2 \end{aligned}$$

Επομένως $S = \{15, -1, 3, -3, -15, 5, -5\}$. Γράφουμε $S' = \{15, -1, 3\} \subset S$ και βρίσκουμε την εικόνα του S μέσω της απεικόνισης π

$$\left\{ \begin{array}{l} \pi(15) = (0,1,1) \\ \pi(-1) = (1,0,0) \\ \pi(3) = (0,1,0) \end{array} \right\} \Longrightarrow \pi(S) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Ο πίνακας έχει rank 3. Συνεπώς $B = \langle -1, 3, 5 \rangle \mathbb{Q}^{*2} \subseteq \alpha\Gamma$.

Άρα $r \geq 2$. (Το b έχει δύο πρώτους παράγοντες, δεν περιμένουμε καλύτερο φράγμα).

Θεώρημα 19. *Αν* $a = 12273038545$ *και*

$$b = 2^{10} \cdot 3^6 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 = 17236434803911308288$$

και $E/Y^2 = X^3 + aX^2 + bX$ *τότε*

$$r = rank(E(\mathbb{Q})) = 10.$$

Απόδειξη: Έχουμε $\bar{E}/Y^2 = X^3 + \bar{a}X^2 + \bar{b}X$,

$$\bar{a} = -2a = -24546077090,$$

$$\bar{b} = a^2 - 4b = 47^2 \cdot 53 \cdot q = 816817359114104838 73$$

$$q := 697675341112349 \in \mathbb{P}.$$

Έστω $\Gamma = E(\mathbb{Q})$, $\bar{\Gamma} = \bar{E}(\mathbb{Q})$, $r_1 = \log_2 |\alpha\Gamma| - 1$ και $r_2 = \log_2 |\bar{\alpha}\bar{\Gamma}| - 1$.

Θα αποδείξουμε ότι $r_1 = 10$ και $r_2 = 0$, άρα $r = r_1 + r_2 = 10$. Έχουμε

$$B = \langle 2 \cdot 41, 3 \cdot 41, 17, 19 \cdot 41, 23 \cdot 41, 29, 31 \cdot 41, 37, 43, 53, -1 \rangle \mathbb{Q}^{*2}.$$

Επομένως $r_1 \geq 10$. Αν $r_1 = 11$ τότε $B = \alpha\Gamma$. Συνεπώς θα έπρεπε η $Y^2 = 41X^4 + aX^2 + \dfrac{b}{41}$ να είναι επιλύσιμη στο $\mathbb{Q}_q$ πράγμα το οποίο δεν συμβαίνει διότι $\left(\dfrac{41}{q}\right) = -1$.

Για το r_2 θα αποδείξουμε ότι

$$\bar{\alpha}\bar{\Gamma} = \{\mathbb{Q}^{*2}, \bar{b}\,\mathbb{Q}^{*2}\}.$$

Έστω $\bar{b}_1 \mathbb{Q}^{*2} \in \bar{\alpha}\bar{\Gamma}$ με $\bar{b}_1 \bar{b}_2 = \bar{b}$.

Αν $\bar{b}_1 < 0$ τότε $\bar{b}_2 < 0$ δεν έχουμε λύση.

Αν $\bar{b}_1 > 0$, $\bar{b}_1 | \bar{b}$ τότε $\bar{b}_1 = 47^{\varepsilon_1} 53^{\varepsilon_2} q^{\varepsilon_3}$, $\varepsilon_1 \in \{0,1,2\}, \varepsilon_2, \varepsilon_3 \in \{0,1\}$.

Αν $\bar{b}_1 \mathbb{Q}^{*2} \in \bar{\alpha}\bar{\Gamma}$ τότε $\left(\dfrac{\bar{b}_1}{19}\right) = \left(\dfrac{\bar{b}_1}{29}\right) = 1$.

Χρησιμοποιούμε το ακόλουθο

Λήμμα 20. *Αν* $p \in \mathbb{P}$, $\mu = v_p(a^2 - 4b) \geq 1$ *και* $p \nmid \varepsilon b$ *τότε η* $Y^2 = g(X)$ *επιλύσιμη στο* $\mathbb{Q}_p$ *ακριβώς τότε όταν*

(i) b_1 *(αντ.* b_2*) τετραγωνικό υπόλοιπο* $(mod\, p)$ *ή*

(ii) μ *άρτιος και* $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{αν } p \equiv 5, 7 \ (mod\, 8) \\ -1, & \text{αν } p \equiv 1, 3 \ (mod\, 8) \end{cases}$

Σημείωση 21. *Έχουμε* $19, 29 \,||\, (\bar{a}^2 - 4\bar{b}) = 16b$ *και* $19, 29 \nmid 6\bar{b}$.

$$x$$

p	47	53	q
19	1	-1	-1
29	-1	1	1

$\left(\frac{x}{p}\right)$.

Συνεπώς $\varepsilon_2 = \varepsilon_3$ *και* $\varepsilon_1 \equiv 0 \ (mod\, 2)$. *Επομένως*

$$\bar{b}_1 \mathbb{Q}^{*2} = \begin{cases} \mathbb{Q}^{*2}, & \text{όταν } \varepsilon_2 = \varepsilon_3 = 0 \\ 53q\mathbb{Q}^{*2} = \bar{b}\mathbb{Q}^{*2}, & \text{όταν } \varepsilon_2 = \varepsilon_3 = 1 \end{cases}$$

Επομένως $|\bar{\alpha}\bar{\Gamma}| = 2$ *συνεπώς* $r_2 = 1 - 1 = 0$. *Άρα*

$$r = r_1 + r_2 = 10.$$

Ερώτημα: Έστω $M \in \mathbb{N}$. Υπάρχει $b \in \mathbb{Z}$ με n διακεκριμένους μεταξύ τους πρώτους παράγοντες και $a \in \mathbb{Z}$ έτσι ώστε:

$$E/y^2 = x^3 + ax^2 + bx, \text{ έχει } \operatorname{rank}(E(\mathbb{Q})) \geq n;$$

Για $n = 1, 2, \cdots, 6$

n	b	a
1	2	7
2	$2^7 \cdot 3^3$	169
3	$2^7 \cdot 3^3 \cdot 7$	997
4	$2^7 \cdot 3^4 \cdot 7 \cdot 13$	6865
5	$2^8 \cdot 3^3 \cdot 7 \cdot 11 \cdot 17$	17905
6	$2^7 \cdot 3^4 \cdot 13 \cdot 23 \cdot 29 \cdot 31$	154465

Σε όλες ο rank είναι ακριβώς n.

Εικασία 22. *Για κάθε $P = \{p_1, p_2, \cdots, p_n\}$ $(n \in \mathbb{N})$ υπάρχει ελλειπτική καμπύλη $E/\mathbb{Q}$ τέτοια ώστε:*

(i) $rank E(\mathbb{Q}) = n$

(ii) $E_{tor}(\mathbb{Q}) \neq \mathcal{O}$

(iii) *Υπάρχει πρώτος p έτσι ώστε η E να έχει το πολύ* **κακή αναγωγή** *στο σύνολο $P \cup \{2, 3, p\}$.*

4. Ρητά σημεία πεπερασμένης τάξης μιάς κλάσης ελλειπτικών καμπυλών

Θα κλείσουμε το κεφάλαιο με τη μελέτη των δυνατοτήτων που έχουμε για την ομάδα των ρητών σημείων πεπερασμένης τάξης ελλειπτικών καμπυλών που έχουν ένα σημείο τάξης 2.

Θεωρούμε την ελλειπτική καμπύλη $E/Y^2 = X^3 + aX^2 + bX,\ a, b \in \mathbb{Z}$. Κατ' αρχήν διατυπώνουμε ένα

Λήμμα 23. *Έστω $P = (x, y)$ ένα torsion σημείο της καμπύλης διάφορο των $\mathcal{O}$ και $(0, 0)$. Τότε*

- $x \mid b$, *και*
- $x + a + \dfrac{b}{x} = n^2,\ n \in \mathbb{N}_0$.

Απόδειξη: Έστω κατ' αρχήν $y \neq 0$, ορίζουμε $(x_2, y_2) = 2P\ (\neq \mathcal{O})$. Επειδή $x, y, x_2, y_2 \in \mathbb{Z}$ έχουμε $x = b_1 M^2$ και $y = b_1 MN$ όπου $b_1,\ N \in \mathbb{N},\ M \in \mathbb{N},\ b_1 | b, b_2 = \dfrac{b}{b_2}$. Συνεπώς

$$\begin{aligned} x_2 &= \lambda^2 - 2x_1 - a = \left(\frac{f'(x_1)}{2y_1}\right)^2 - (2x_1 + a) \\ &= \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right)^2 - 2x_1 - a = \left(\frac{x_1^2 - b}{2y_1}\right)^2 \\ \Longrightarrow \quad x_2 &= \left(\frac{x_1^2 - b}{2y}\right)^2 = \left(\frac{b_1^2 M^4 - b_1 b_2}{2b_1 MN}\right)^2 = \left(\frac{b_1 M^4 - b_2}{2MN}\right)^2. \end{aligned}$$

Πρέπει $x_2 \in \mathbb{Z}$ συνεπώς $M | b_2$. Έχουμε $(M, e) = (N, e) = (b_1, e) = 1$. Επίσης $(b_2, M) = 1$ διότι $(m_1, b_2) = 1$, οπότε, επειδή $(b_2, M) = 1$ και $M | b_2$, συνεπάγεται ότι $M = 1$, δηλαδή

$x = b_1|b$. Συνεπώς

$$b_1^3 + ab_1^2 + bb_1 = (b_1N)^2 = b_1^2N^2 \quad \Rightarrow \quad b_1 + a + b_2 = N^2.$$

Αν τώρα $y = 0$ τότε $2P = \mathcal{O}$, οπότε από το θεώρημα του Tate ισχύει. □

Λήμμα 24. *Έστω $P = (x, y)$ torsion σημείο της E με $2P \neq \mathcal{O}$. Τότε ισχύουν:*

- $x \mid b$
- $x + a + \dfrac{b}{x} = n^2,\ n \in \mathbb{N}$
- $n^2 \mid a^2 - 4b.$

Απόδειξη: Θεωρούμε τις συναρτήσεις $\varphi : E(\mathbb{Q}) \to \bar{E}(\mathbb{Q})$ και $\psi : \bar{E}(\mathbb{Q}) \to E(\mathbb{Q})$ τις οποίες έχουμε ήδη ορίσει σε προηγούμενη παράγραφο. Το $\varphi(P)$ είναι torsion σημείο της $\bar{E}(\mathbb{Q})$. Από την γνωστή σχέση

$$(\psi \circ \varphi)(P) = 2P \neq \mathcal{O}$$

έπεται ότι

$$\varphi(P) \notin \ker \psi = \big\{\mathcal{O}, (0,0)\big\}.$$

Εφαρμόζουμε τώρα το λήμμα 23 της σελίδας 102 για το σημείο $\varphi(P)$ και την ελλειπτική καμπύλη E και παίρνουμε ότι $x(\varphi(P)) \mid \bar{b}$ αν και μόνο αν $x+a+\dfrac{b}{x} \mid a^2-4b$, διότι $\varphi(P) \neq (0,0)$. □

Θεώρημα 25. *Θεωρούμε την ελλειπτική καμπύλη*

$$E/Y^2 = X^3 + aX^2 + bX, \quad a, b \in \mathbb{Z}$$

και υποθέτουμε ότι ο ακέραιος $a^2 - 4b$ είναι ελεύθερος τετραγώνου. Η $E(\mathbb{Q})_{torsion}$ είναι ισόμορφη προς τις ακόλουθες ομάδες:

$$\mathbb{Z}/2\mathbb{Z},\ \ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \ \mathbb{Z}/4\mathbb{Z},\ \ \mathbb{Z}/6\mathbb{Z},\ \ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Πιο συγκεκριμένα,

(i) Έστω $a^2 - 4b = 1$, τότε αν

(α′) $\dfrac{1-a}{2}$ είναι τέλειο τετράγωνο φυσικού έπεται ότι $E(\mathbb{Q})_{tor} \equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

(β′) $A\nu$ $\dfrac{1-a}{2}$ *όχι τέλειο τετράγωνο φυσικού τότε* $E(\mathbb{Q})_{tor} \equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(ii) Έστω $a^2 - 4b \neq 1$, *τότε αν*

(α′) *για κάθε* $b_1 \mid b$, $b_1 + a + b_2 \neq 1$ *ισχύει* $E(\mathbb{Q})_{tor} \equiv \mathbb{Z}/2\mathbb{Z}$.

(β′) $A\nu$ *υπάρχει* $b_1 \mid b$ *όπου* $b_1 + a + b_2 = 1$ *τότε*

(β′1) $A\nu$ $b_1 = b_2$ *έχουμε* $E(Q)_{tor} \equiv \mathbb{Z}/4\mathbb{Z}$.

(β′2) $A\nu$ $b_1 \neq b_2$ *τότε* $E(Q)_{tor} \equiv \mathbb{Z}/2\mathbb{Z}$ *ή* $\mathbb{Z}/6\mathbb{Z}$.

Ιδιαίτερα

$$E(\mathbb{Q})_{tor} \equiv \mathbb{Z}/6\mathbb{Z} \quad \Longleftrightarrow \quad b_i = \frac{4b}{4b-(a-1)(a+3)}, \;\; i = 1 \text{ ή } 2.$$

Απόδειξη:

(i) Έστω $a^2 - 4b = 1$. Το $X^2 + aX + b$ έχει ρίζες τους ακεραίους

$$x_1 = -\frac{1}{2}(a+1), \quad \text{και} \quad x_2 = -\frac{1}{2}(a_1 - 1)$$

$$\Longrightarrow \quad \{\mathcal{O}, (0,0), (x_1,0), (x_2,0)\} \leq E(\mathbb{Q})_{\text{tor}}.$$

Έστω ότι υπάρχουν κι άλλα torsion σημεία, και έστω P ένα από αυτά. Τότε $2P \neq \mathcal{O}$. Αφού $a^2 - 4b = 1$ το προηγούμενο λήμμα 24 δίνει $x(P) = b_1 \mid b$ και $b_1 + a + \dfrac{b}{b_1} = 1$. Επομένως

$$b_1 + a + \frac{a^2-1}{4b_1} = 1 \quad \Longrightarrow \quad b_1^2 + (a-1)b_1 = \frac{1-a^2}{4}$$

$$\Longrightarrow \quad (b_1 + \frac{a-1}{2})^2 = \frac{1-a}{2}.$$

Ισχύει $|a| \neq 1$, διότι αλλιώς $b = 0$, δηλαδή $\Delta = 0$, συνεπώς E όχι ελλειπτική καμπύλη, άτοπο.

Έστω τώρα:

(α′) $\dfrac{1-a}{2} = n^2$ για $n \in \mathbb{N}$ ($n \neq 1$ γιατί αλλιώς $a = -1$). Η ισότητα τώρα $\left(b_1 + \dfrac{a-1}{2}\right)^2 = \dfrac{1-a}{2}$ μας δίνει

$$(b_1 - n^2)^2 = n^2 \Rightarrow b_1^2 - 2n^2 b_1 + n^4 - n^2 = 0$$

$$\Longrightarrow b_1 = \frac{2n^2 \pm 2n}{2} \Longrightarrow b_1 = n^2 \pm n.$$

Παίρνουμε τώρα τα σημεία $P_1 = (n^2+n, n^2+n)$ και $P_2 = (n^2-n, n^2-n)$. Τα σημεία P_i είναι ρητά σημεία της καμπύλης E. Πράγματι, $b_1 + a + \frac{b}{b_1} = 1$, συνεπώς $b_1^2 + ab_1 + b = b_1$ επομένως $b_1^3 + ab_1^2 + bb_1 = b_1^2$, δηλαδή το σημείο (b_1, b_1) είναι ρητό σημείο της E και $b_1 = n^2 \pm n$.

Αφού $2P_1 = (n^2, 0) = (x_2, 0)$ και $2P_2 = (n^2-1, 0) = (x_1, 0)$ έπεται ότι τα P_1 και P_2 είναι torsion σημεία τάξεως 4. Δηλαδή $4P_1 = 4P_2 = \mathcal{O}$. Άρα

$$\begin{aligned} E(\mathbb{Q})_{\text{tor}} &= \{\mathcal{O},\, (0,0),\, P_1,\, P_2,\, 2P_1 = (x_2, 0),\, 2P_2 = (x_1, 0),\, 3P_1, 3P_2\} \\ &\cong \mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{4\mathbb{Z}}. \end{aligned}$$

Ο τελευταίος ισομορφισμός είναι συνέπεια του αποκλεισμού των περιπτώσεων $\mathbb{Z}\!\diagup_{8\mathbb{Z}}$ (αφού δεν υπάρχει στοιχείο τάξης 2) και της $\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}$ (διότι τότε όλα τα στοιχεία θα ήταν τάξης 2).

(β′) Έστω τώρα $\frac{1-a}{2}$ όχι τέλειο τετράγωνο φυσικού αριθμού. Τότε από την σχέση $\left(b_1 + \frac{a-1}{a}\right)^2 = \frac{1-a}{2}$ παίρνουμε $\frac{1-a}{2} = 0$ και επομένως $a = 1$, άτοπο διότι τότε δεν θα είχαμε σημείο τάξης μεγαλύτερης του 2. Επομένως

$$E(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}.$$

(ii) Υποθέτουμε τώρα $a^2 - 4b$ ελεύθερο τετραγώνου και διάφορο του 1. Τότε σημεία τάξης 2 έχουμε μόνο τα $\{\mathcal{O}, (0,0)\}$. Αν P κάποιο άλλο σημείο πεπερασμένης τάξης τότε, σύμφωνα με το προηγούμενο λήμμα 24, $x(P) = b_1 \mid b$ και $b_1 + a + b_2 = n^2$, όπου $n \in \mathbb{N}$, $b_1 b_2 = b$ και $n^2 \mid a^2 - 4b$.

Επειδή $a^2 - 4b$ ελεύθερο τετραγώνου, κατ′ ανάγκη θα έχουμε $n = 1$. Οπότε $P = (b_1, b_1)$ και $-P = (b_1, -b_1) \neq P$. Συνεπώς παίρνουμε το (i) διότι $b_1 + a + b_2 = n^2 = 1$. Προσπαθούμε τώρα να απαντήσουμε αν υπάρχουν και άλλα σημεία πεπερασμένης τάξης εκτός των $\mathcal{O}, (0,0), P, -P$. Έστω $Q \neq \mathcal{O}, (0,0), P, -P$. Τότε, όπως αποδείξαμε παραπάνω και για το P, $Q = (c_1, c_1)$ ή $Q = (c_1, -c_1)$. Συνεπώς

$$b = c_1 c_2,\ \ c_1, c_2 \in \mathbb{Z},\ \ b_1 \neq c_1\ \ c_1 + a + c_2 = 1$$

$$\begin{aligned} &\Longrightarrow\ \ b_1 + a + b_2 = 1 = c_1 + a + c_2 \quad\Longrightarrow\quad b_1 + b_2 = c_1 + c_2 \\ &\Longrightarrow\ \ (b_1 + b_2)^2 = (c_1 + c_2)^2 \quad\Longrightarrow\quad b_1^2 + 2b_1 b_2 + b_2^2 = c_1^2 + 2c_1 c_2 + c_2^2 \\ &\Longrightarrow\ \ b_1 + 2b + b_2^2 = c_1^2 + 2b + c_2^2 \quad\Longrightarrow\quad (b_1 - c_1)(b_1 + c_1) = (c_2 - b_2)(c_2 + b_2) \\ &\Longrightarrow\ \ (b_1 - c_1)(b_1 + c_1) = (b_1 - c_1)(c_2 + b_2). \end{aligned}$$

Επειδή $b_1 \neq c_1$ έπεται $b_1 + c_1 = c_2 + b_2$ και επειδή $b_1 + b_2 = c_1 + c_2$ έχουμε

$$b_2 - c_1 = c_1 - b_2 \quad \Longrightarrow \quad b_2 = c_1$$

οπότε και $b_1 = c_2$, δηλαδή $Q = (b_2, b_2)$ (ή $Q = (b_2, -b_2)$). Καταλήξαμε τώρα ότι αν υπάρχει $b_1 \,|\, b$ με $b_1 + a + b_2 \neq 1$ τα σημεία πεπερασμένης τάξης της E είναι

$$\mathcal{O},\ (0,0),\ P = (b_1, b_1),\ -P,\ Q = (b_2, b_2),\ -Q.$$

Αν $b_1 + a + b_2 = 1$ και $b_1 = b_2$ τότε $P = Q$ και $b = b_1^2 = b_2^2$.
Ακόμα ισχύει $x(2P) = \left(\dfrac{b_1^2 - b}{2b_1}\right)^2 = 0$. Επομένως $2P = (0,0)$ δηλαδή το P είναι torsion σημείο τάξεως 4, οπότε

$$E(\mathbb{Q})_{\text{tor}} \equiv \langle P \rangle \equiv \mathbb{Z}/4\mathbb{Z}.$$

Ομοίως αποδεικνύεται και το (ii, $\beta'2$).

Έστω τώρα $b_1 + a + b_2 = 1$ και $b_1 \neq b_2$. Αυτο σημαίνει ότι $P \neq Q$. Το σημείο $P + Q$ είναι το $(0,0)$, διότι

$$\chi(P+Q) = \frac{1}{b_1 b_2} \cdot \left(\frac{b_1 b_2 - b_2 b_1}{b_2 - b_1}\right)^2 = 0$$

Επομένως

$$P \in E(\mathbb{Q})_{\text{tor}} \quad \Longleftrightarrow \quad Q \in E(\mathbb{Q})_{\text{tor}},$$

δηλαδή η ομάδα $E(\mathbb{Q})_{\text{tor}}$ είναι ισόμορφη με την $\mathbb{Z}/2\mathbb{Z}$ ή με την $\mathbb{Z}/6\mathbb{Z}$. Θα αποδείξουμε ότι

$$E(Q)_{\text{tor}} \cong \mathbb{Z}/6\mathbb{Z} \quad \Longleftrightarrow \quad b_i = \frac{4b}{4b - (a-1)(a+3)} \quad \text{για } i = 1 \text{ ή } 2$$

Ας υποθέσουμε ότι $\text{ord}(P) = 6$. Επειδή, όπως εύκολα διαπιστώνουμε, $2P \neq \mathcal{O}$, $2P \neq (0,0) = P+Q$, $2P \neq -P$, θα έχουμε $2P = Q$ ή $-Q$. Το $Q = (b_2, b_2)$, $-Q = (b_2, -b_2)$. Επομένως, $2P = Q$ ή $-Q$

$$\begin{aligned}
&\Longleftrightarrow && \chi(2P) = b_2 \\
&\Longleftrightarrow && \left(\frac{b_1^2 - b}{2b_1}\right)^2 = b_2 \\
&\Longleftrightarrow && (b_1 - b_2)^2 = 4b_2 \\
&\Longleftrightarrow && -b_1^2 + 2b - b_2^2 + 4b_2 = 0 \\
&\Longleftrightarrow && \big((a-1)b_1 + b\big) + 2b + \big((a-1)b_2 + b\big) + 4b_2 = 0 \qquad (a - 1 = b_1 + b_2) \\
&\Longleftrightarrow && (a-1)b_1 + (a+3)b_2 + 4b = 0
\end{aligned}$$

Αν πολλαπλασιάσουμε την τελευταία ισότητα με b_2 έχουμε την ισοδύναμη της

$$(a+3)\big((1-a)b_2 - b\big) + 4bb_2 + (a-1)b = 0$$

διότι

$$(1-a)b_2 - b = (b_1+b_2)b_2 - b_1b_2 = b_2^2.$$

Επομένως $\chi(2P) = b_2$, τότε και μόνο τότε όταν

$$\begin{aligned} & [(a+3)(1-a)+4b]b_2 - 4b = 0 \\ \iff \quad & (a+3)((1-a)+4b)b_2 - 4b = 0 \\ \iff \quad & b_2 = \frac{4b}{4b-(a-1)(a+3)} \neq 0 \end{aligned}$$

Ας υποθέσουμε τέλος ότι το b_2 επαληθεύει την τελευταία ισότητα. Όπως αποδείξαμε λίγο πιο μπροστά, $2P = Q$ ή $-Q$. Επίσης,

$$\chi(2Q) = \left(\frac{b_2^2 - b}{2b_2}\right)^2 = \left(\frac{b_2 - b_1}{2}\right)^2 = b_2 = \chi(2P) = \chi(Q).$$

Επειδή $Q \neq \mathcal{O}$ έχουμε $2Q = -Q$, επομένως $3Q = \mathcal{O}$ και $6P = \mathcal{O}$. □

ΤΕΛΟΣ

Παράρτημα

Το παράρτημα αυτό χρησιμεύει σαν βοήθημα για την ανάπτυξη της θεωρίας των αλγεβρικών καμπυλών.

1. Δακτύλιοι με μονοσήμαντη ανάλυση

Όλοι οι δακτύλοι που θεωρούμε εδώ θα είναι αντιμεταθετικοί με μοναδιαίο στοιχείο. Έστω R δακτύλιος. Ένα στοιχείο $u \in R$ θα λέγεται **μονάδα** του R αν και μόνον αν υπάρχει $v \in R$ τέτοιο ώστε $uv = 1$.

Το σύνολο των μονάδων του R αποτελεί **ομάδα** ως προς τον πολλαπλασιασμό, συμβολίζεται δε με R^*. Αν R σώμα τότε, προφανώς, $R^* = R \setminus 0$. Αν $a, b \in R$ θα λέμε ότι ο a διαιρεί το b (και γράφουμε $a \,|\, b$) ακριβώς τότε όταν υπάρχει $x \in R$ τέτοιο ώστε $b = ax$. Για κάθε μονάδα $u \in R^*$ ισχύει $u \,|\, a$. Δύο κύρια ιδεώδη $\langle a \rangle$ και $\langle b \rangle$ του δακτυλίου R είναι ίσα ακριβώς τότε όταν $b = u \cdot a$, όπου $u \in R^*$.

Ορισμός 1. *Έστω $p \in R$. Το p λέγεται* **ανάγωγο** *όταν από κάθε ανάλυση του $p = ab$, συνεπάγεται ότι ο a είναι μονάδα ή ο b είναι μονάδα αλλά όχι συγχρόνως και τα δύο.*

Προφανώς αφού $0 = 0 \cdot 0$, έπεται ότι το 0 όχι ανάγωγο και αφού, αν $u \in R^*$, συνεπάγεται ότι $u = u_1 u_2$ δηλαδή τα u_1, u_2 είναι μονάδες, έπεται ότι ένα ανάγωγο στοιχείο δεν είναι μονάδα.

Ορισμός 2. *Ένας δακτύλιος R καλείται δακτύλιος μονοσήμαντης ανάλυσης όταν ισχύουν τα ακόλουθα:*

- *Για κάθε $a \neq 0$, ο a γράφεται $a = up_1p_2 \cdots p_r$ όπου το u είναι μονάδα του R και τα $p_i,\ i = 1, 2, \cdots, r$ είναι ανάγωγα και*

- *Η ανάλυση κάθε στοχείου* $a \in R$ *είναι μοναδική, δηλαδή αν* $a = vq_1q_2\cdots q_s = up_1p_2\cdots p_r$, *τότε* $r = s$ *και, μετά από κάποια μετάθεση των* q_i *ισχύει* $p_i = u_iq_i$ *όπου* u_i *μονάδα του* R.

Κάθε μη-κενό σύνολο κυρίων ιδεωδών ενός δακτυλίου με μονοσήμαντη ανάλυση έχει μέγιστα στοιχεία. Αν p ανάγωγο στοιχείο του R και R δακτύλιος μονοσήμαντης ανάλυσης τότε το p είναι πρώτο, δηλαδή αν ο p διαιρεί το γινόμενο δύο στοιχείων $a\cdot b$ του R τότε θα διαιρεί κατ΄ ανάγκη τουλάχιστον ένα από τα a, b. Αν τώρα p πρώτο στοιχείο του R τότε το $\langle p\rangle = R\cdot p$ είναι πρώτο ιδεώδες του R. Κάθε δακτύλιος κυρίων ιδεωδών είναι δακτύλιος με μονοσήμαντη ανάλυση. Έτσι, ο δακτύλιος των ακεραίων είναι δακτύλιος με μονοσήμαντη ανάλυση. Επίσης ο δακτύλιος των πολυωνύμων $K[X]$, όπου K σώμα, είναι δακτύλιος με μονοσήμαντη ανάλυση.

Θεώρημα 3. *Αν* R *δακτύλιος με μονοσήμαντη ανάλυση, τότε και ο* $R[X]$ *είναι επίσης δακτύλιος με μονοσήμαντη ανάλυση.*

Πόρισμα 4. *Αν* R *δακτύλιος με μονοσήμαντη ανάλυση τότε και ο* $R[X_1, X_2, \ldots, X_n]$ *είναι επίσης δακτύλιος με μονοσήμαντη ανάλυση.*

2. Εκτιμήσεις

Έστω R δακτύλιος με μονοσήμαντη ανάλυση, F τό σώμα πηλίκων αυτού και p ένα πρώτο στοιχείο του R. Κάθε $x \in F$ γράφεται

$$x = p^r\frac{a}{b},\ r \in \mathbb{Z},\ a, b \in R, p \nmid ab$$

με r και $\dfrac{a}{b}$ μονοσήμαντα ωρισμένα.

Ορίζουμε μία συνάρτηση

$$\mathrm{ord}_p : F^* \longrightarrow \mathbb{Z},\ \mathrm{ord}_p(x) = r.$$

Προφανώς ισχύουν

$$\begin{aligned}\mathrm{ord}_p(xy) &= \mathrm{ord}_p(x) + \mathrm{ord}_p(y) \quad \text{και}\\ \mathrm{ord}_p(x+y) &\geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}.\end{aligned}$$

Επιπλέον ισχύει $\mathrm{ord}_p(a) \geq 0$ για όλα τα πρώτα στοιχεία p του R αν και μόνο αν $a \in R$.

Ορισμός 5. *Μία (διακεκριμένη)* **εκτίμηση** *σε κάποιο σώμα* F *είναι μια συνάρτηση*

$$\nu : F \longleftrightarrow \mathbb{Z}, \ \mu\epsilon$$

(i) $\nu(0) = \infty$

(ii) $\nu(xy) = \nu(x) + \nu(y)$ *και*

(iii) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ *για όλα τα ζεύγη* (x, y) *του* F.

Προφανείς ιδιότητες:

(a) $\nu\left(\frac{x}{y}\right) = \nu(x) - \nu(y)$, (οπότε αν θέσουμε $x = y = 1$ και $x = 1, y = -1$ αντίστοιχα παίρνουμε $\nu(1) = \nu(-1) = 0$),

(b) $\nu(x^n) = n \cdot \nu(x)$, και

(c) Αν $\nu(x) < \nu(y)$ τότε $\nu(x) = \nu(x+y)$.
Απόδειξη: Από τον ορισμό έχουμε $\nu(x) \leq \nu(x+y)$. Γράφουμε, $x = (x+y) + (-y)$ δηλαδή $\nu(x) = \nu((x+y) + (-y)) \geq \min\{\nu(x+y), \nu(-y)\} = \min\{\nu(x+y), \nu(y)\}$. Συνεπώς $\nu(x) \geq \nu(x+y)$.

Για κάθε πρώτο αριθμό p ορίζεται μία εκτίμηση ord_p στο $\mathbb{Q}$. Καλείται p-**αδική εκτίμηση** και αποδεικνύεται ότι όλες οι άλλες εκτιμήσεις προκύπτουν κατ' αυτόν τον τρόπο (η απόλυτη τιμή λέμε ότι αντιστοιχεί στον «άπειρο πρώτο»).

Σε κάθε εκτίμηση επισυνάπτουμε ένα δακτύλιο κυρίων ιδεωδών, συνεπώς ένα δακτύλιο με μονοσήμαντη ανάλυση με ένα **μοναδικό** πρώτο στοιχείο.

Ορισμός 6. *Έστω* ν *μία εκτίμηση του σώματος* F. *Θεωρούμε το σύνολο*

$$R_\nu = \{a \in F \mid \nu(a) \geq 0\}$$

O R_ν *είναι δακτύλιος διότι αν* $a, b \in R_\nu$ *τότε* $\nu(a-b) \geq \min\{\nu(a), \nu(b)\} \geq 0$, *επομένως* $a - b \in R_\nu$ *και* $\nu(ab) = \nu(a) + \nu(b) \geq 0$, *δηλαδή* $ab \in R_\nu$.

Ο R_ν λέγεται **δακτύλιος εκτιμήσεως**.
Η ομάδα των μονάδων του είναι $R_\nu^* = \{x \in F \mid \nu(x) = 0\}$, διότι αν $x \in R_\nu$ συνεπάγεται ότι $\nu(x) \geq 0$ και αν x μονάδα $\frac{1}{x} \in R_\nu$ οπότε $\nu\left(\frac{1}{x}\right) = \nu(1) - \nu(x) = -\nu(x) \geq 0$ δηλαδή $\nu(x) \leq 0$ οπότε έχουμε $\nu(x) = 0$.

Το σύνολο $M_\nu = \{x \in F \mid \nu(x) > 0\} = R_\nu - R_\nu^*$ είναι το **μοναδικό μέγιστο ιδεώδες του** R_ν.

Απόδειξη: Κατ' αρχήν το M_ν είναι ιδεώδες του R_ν διότι αν πάρουμε $a, b \in M_\nu$ τότε $\nu(a-b) > 0$ και επομένως $a - b \in M_\nu$. Αν πάλι $r, a \in M_\nu$ τότε $\nu(ra) = \nu(r) + \nu(a) > 0$ δηλαδή $ra \in M_\nu$.

Επίσης το M_ν είναι μέγιστο, διότι αν υπάρχει ιδεώδες I τέτοιο ώστε $M_\nu \subset I$ και $M_\nu \neq I$ τότε υπάρχει $u \in R_\nu^*, u \in I$, δηλαδή $I = R$.

Τέλος το M_ν είναι το **μοναδικό μέγιστο** ιδεώδες του R_ν διότι κάθε ιδεώδες $A \neq R_\nu$ του R_ν περιέχεται στο M_ν καθ' όσον δεν περιέχει μονάδες.

Άσκηση 7. *Έστω R ακέραια περιοχή και $P \neq R$ ένα πρώτο ιδεώδες. Τότε το υποσύνολο $R_P = \{\frac{a}{b} \mid a \in R, b \in R - P\}$ του σώματος πηλίκων K της R αποτελεί* **τοπικό δακτύλιο**, *με μοναδικό μέγιστο ιδεώδες το $P^* = \left\{\frac{a}{b} \,\middle|\, a \in P, b \in R - P\right\}$.*

3. Στοιχεία Θεωρίας Σωμάτων

Έστω K, L σώματα τέτοια ώστε $K \subset L$. Το L θα λέγεται επέκταση του K. Συμβολισμός L/K.

Το L είναι $K-$διανυσματικός χώρος. Η διάσταση του L είναι ο βαθμός της επέκτασης L/K. Προφανώς αν $[L : K] = 1$ τότε $L = K$.

Ισχύει για τις επεκτάσεις L/K και M/L

$$[M : K] = [M : L]\,[L : K].$$

Έστω L/K επέκταση σωμάτων. Ένα στοιχείο $a \in L$ θα λέγεται **αλγεβρικό** αν και μόνο αν υπάρχει $f(x) \in K[x]$, $f(x) \neq 0$ με $f(x) = 0$. Αν $a \in L$ όχι αλγεβρικό θα λέμε ότι το a είναι **υπερβατικό**.

Πρόταση 8. *Αν ο βαθμός $[L : K]$ είναι πεπερασμένος τότε η επέκταση L/K είναι αλγεβρική.*

Απόδειξη: Έστω $[L : K] = n$. Έστω a **τυχαίο** στοιχείο του L. Τα $1, a, a^2, \cdots, a^n$ είναι **γραμμικά εξαρτημένα** υπέρ το K διότι είναι $n+1 > [L : K] = n$. Συνεπώς υπάρχει σχέση $\lambda_0 1 + \lambda_1 a + \cdots \lambda_n a^n$, $\lambda_i \in K$ όπου τουλάχιστο ένα λ_i είναι διάφορο του μηδενός. Επομένως το a είναι αλγεβρικό ως ρίζα του πολυωνύμου $f(x) = \lambda_0 + \lambda_1 x + \cdots \lambda_n x^n$. Άρα η επέκταση L/K είναι αλγεβρική. □

Έστω τώρα L/K όχι πεπερασμένη, και $L' = \{a \in L \mid a \text{ αλγεβρικό υπέρ το } K\}$. Τότε το L' είναι υπόσωμα του L.

Απόδειξη: Έστω $a \neq 0$ και $b \in L'$. Η επέκταση $K(a,b)/K$ είναι πεπερασμένη άρα αλγεβρική. Άρα $a-b, ab$ και a^{-1} αλγεβρικά υπέρ το K. Συνεπώς $a-b, ab$ και $a^{-1} \in L'$. Επομένως το L' είναι **σώμα**.

Ορισμός 9. *Το L' λέγεται* **αλγεβρική θήκη** *του K στο L.*

Ισχύει ακόμη: Αν $a \in L$, a αλγεβρικό υπέρ το L' τότε $a \in L'$.

Απόδειξη: Η επέκταση $L'(a)/L'$ είναι πεπερασμένη άρα και αλγεβρική. Επίσης η L'/K είναι αλγεβρική. Επομένως L'/K είναι αλγεβρική. Συνεπώς το a είναι αλγεβρικό υπέρ το K. Άρα $a \in L'$. □

Δηλαδή, όπως λέμε το L' είναι **αλγεβρικά κλειστό στο** L.

Ορισμός 10. *Έστω Ω σώμα. Το Ω λέγεται* **αλγεβρικά κλειστό** *όταν και μόνο όταν για κάθε $f(x) \in \Omega[x]$ με $degf(x) > 0$, υπάρχει τουλάχιστο μία ρίζα a του $f(x)$ τέτοια ώστε $a \in \Omega$.*

Θεμελιώδες Θεώρημα της Αλγεβρας: *Το $\mathbb{C}$ είναι αλγεβρικά κλειστό.*

Πρόταση 11. *Έστω σώμα $K \subset \Omega$, Ω αλγεβρικά κλειστό. Τότε η* **αλγεβρική θήκη** *$\tilde{K}$ του K στο Ω είναι επίσης* **αλγεβρικά κλειστό** *σώμα.*

Απόδειξη: Έστω $f(x) \in \tilde{K}[x]$, $degf(x) > 0$. Συνεπώς $f(x) \in \Omega[x]$ και επομένως το $f(x)$ έχει όλες τις ρίζες του $a_1, a_2, \cdots, a_n$ στο Ω. Δηλαδή $a_1, a_2, \cdots, a_n \in \Omega$ και είναι αλγεβρική υπέρ το $\tilde{K}$. Άρα $a_i \in \tilde{K}$. □

Ορισμός 12. *Το L λέγεται* **αλγεβρική θήκη** *του K αν και μόνο αν*

(i) Το L είναι αλγεβρικά κλειστό και

(ii) Η επέκταση L/K είναι αλγεβρική.

Τέλος σημειώνουμε ότι για κάθε σώμα K υπάρχει μία αλγεβρική θήκη αυτού L η οποία είναι μοναδική υπεράνω ισομορφίας.

Βιβλιογραφία

[1] Γ. Α. Αντωνιάδη, Θεωρία Αριθμών κατά τον $17^ο$ και $18^ο$ αιώνα, Έκδοση ΕΠΕΑΕΚ "Προμηθέας ", Ηράκλειο 1999.

[2] B. J. Birch, Elliptic Curves, Παραδόσεις, Oxford 1990.

[3] R. Bix, Conics and Cubics, Springer-Verlag, New York 1998.

Πρόσφατο εισαγωγικό βιβλίο γεωμετρίας των κυβικών καμπυλών.

[4] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, J.-P. Serre, Seminar on Complex Multiplication, Springer-Verlag, Berlin 1966.

[5] J. W. S. Cassels, Diophantine Equations with Special Reference to Elliptic Curves, Journal of the L.M.S. **41** (1996), 193-291.

Επισκόπηση της μέχρι τότε βιβλιογραφίας της σχετικής με την περιοχή. Χρησιμοποιεί κυρίως γεωμετρική γλώσσα.

[6] J. W. S. Cassels, Lectures on Elliptic Curves, CUP, Cambridge 1991.

Περιεκτικό και αρκετά συντομογραμμένο κείμενο.

[7] J. S. Chahal, Topics in Number Theory, Plenum Press, New York 1988.

Εισαγωγικό βιβλίο, ανάλογο του επιπέδου αυτού που κρατάτε στα χέρια σας.

[8] W. Fulton, Algebraic Curves, W. A. Benjamin, London 1969.

Κλασικό σύγγραμμα της θεωρίας των αλγεβρικών καμπυλών. Περισσότερο αλγεβρικό και ανωτέρου επιπέδου αυτού του Walker.

[9] B. H. Gross, Arithmetic on Elliptic Curves with Complex Multiplication, Lecture Notes in Mathematics, Springer-Verlag, New York 1980.

[10] D. Husemöller, Elliptic Curves, Springer-Verlag, New York 1987.

[11] H. Kisilevsky, M. Ram Murty, Editors, Elliptic Curves and Related Topics, AMS, Providence 1994.

Πρακτικά Συνεδρίου που έγινε στο Montréal το 1993.

[12] A. W. Knapp, Elliptic Curves, Princeton University Press, Princeton, New Jersey 1992.

Θαυμάσιο βιβλίο μεταπτυχιακού επιπέδου. Πάρα πολύ καλογραμμένο το αναλυτικό μέρος το οποίο εκτείνεται μέχρι και την θεωρία των Eichler-Shimura.

[13] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York 1984.

Παίρνει αφορμή από το πρόβλημα των ισοδυνάμων αριθμών και αναπτύσσει τη θεωρία. Καταπληκτική ιδέα να έχει ο αναγνώστης ένα ακόμη κίνητρο για τη μελέτη των ελλειπτικών καμπυλών.

[14] Th. Kretschmer, Konstruction elliptischer Kurven von hohem Rang, Diplomarbeit, Saarbrücken 1983.

[15] Κ. Λάκκη, Άλγεβρα, Θεσσαλονίκη 1993.

[16] S. Lang, Elliptic Curves, Diophantine Analysis, Springer-Verlag 1978.

[17] S. Lang, Elliptic Functions, Addison Wesley, Reading 1973.

Αρκετά προχωρημένο βιβλίο.

[18] R. Löschel, Kongruente Zahlen, Diplomarbeit, Universität Erlangen-Nürnberg, Erlangen 1990.

[19] H. McKean, V. Moll, Elliptic Curves, CUP, Cambridge 1997.

Το βιβλίο περιέχει κυρίως την κλασική θεωρία των ελλειπτικών συναρτήσεων.

[20] J.-S. Milne, Elliptic Curves, Ann-Arbor, Michigan 1996.

Πρόκειται για σημειώσεις του μαθήματος που διδάσκονται από την συγγραφέα στο Ann-Arbor. Τις έχουμε πάρει από το Internet.

[21] Mordell, Diophantine Equations, Academic Press 1969.

Ο Mordel δίνει, μεταξύ άλλων, την απόδειξη του... θεωρήματός του!

[22] A. Robert, Elliptic Curves, Lecture Notes in Math 326, Springer-Verlag, Berlin 1973.

Θαυμάσιες σημειώσεις. Ένα από τα πρώτα βιβλία θεωρίας ελλειπτικών καμπυλών. Έχει εξαντληθεί.

[23] J. P. Serre, A Course in Arithmetic, Springer-Verlag, New York 1973.

Περιέχει θαυμάσια εισαγωγή στη θεωρία των modular συναρτήσεων απαραίτητη για την μελέτη των ελλειπτικών καμπυλών.

[24] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York 1986.

[25] J. H. Silverman, J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, New York 1992.

Θαυμάσιο εισαγωγικό βιβλίο θεωρίας των ελλειπτικών καμπυλών. Το συνιστούμε ένθερμα σε κάθε ενδιαφερόμενο αναγνώστη.

[26] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, New York 1994.

Το δίτομο έργο του Silverman είναι κατάλληλο για τον προχωρημένο μεταπτυχιακό φοιτητή και τον ειδικό επιστήμονα της περιοχής.

[27] R. J. Stroeker, Aspects of Elliptic Curves, An Introduction, Nieuw Archief voor Wiskunde, XXVI (1978).

[28] J. Tate, Rational Points s on Elliptic Curves, Philips Lectures, Haverford College, April, May 1961.

Η απόδειξη του Θεωρήματος του Mordell του βιβλίου που κρατάτε στα χέρια σας είναι η απόδειξη του Tate στο Haverford College. Η απόδειξη αυτή περιέχεται και στα βιβλία [7], [10], [25].

[29] J. Tate, The Arithmetic of Elliptic Curves, Inventiones Math. **23** (1974), 179-206.

Επισκόπηση της μέχρι τότε βιβλιογραφίας. Χρησιμοποιεί κυρίως αλγεβρική γλώσσα.

[30] J. Tate, Elliptic Curves, Austin, Texas 1992.

Πρόκειται για σημειώσεις που κράτησε ο κύριος Antonios Broumas.

[31] R. Walker, Algeberaic Curves, Dover, New York 1962.

Αρκετά καλό, εισαγωγικό βιβλίο της θεωρίας των αλγεβρικών καμπυλών.

[32] D. B. Zagier, Elliptische Kurven, Παραδόσεις, Max-Planck Institut für Mathematik, Bonn 1987.