Αριθμητική Υπερελλειπτικών Καμπυλών

Νικόλαος Βαρδουλάκης

Μεταπτυχιακή Εργασία

Κατεύθυνση: Θεωρητικά Μαθηματικά

Επιβλέπων Καθηγητής: Ιωάννης Α. Αντωνιάδης

Πανεπιστήμιο Κρήτης
Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών

Εισαγωγή

Κεντρικό πρόβλημα της Θεωρίας Αριθμών είναι η επίλυση διοφαντικών εξισώσεων, δηλαδή η εύρεση όλων των ρητών σημείων αλγεβρικών καμπυλών και γενικότερα αλγεβρικών πολλαπλοτήτων. Δίνεται μία αφινική καμπύλη C ορισμένη σε ένα σώμα K και το πρόβλημα είναι η εύρεση όλων των K-ρητών σημείων αυτής. Το σώμα K μπορεί να είναι το σώμα των ρητών αριθμών $\mathbb{Q}$, ένα αλγεβρικό σώμα αριθμών (δηλαδή μία πεπερασμένη επέκταση του $\mathbb{Q}$), ένα σώμα p-αδικών αριθμών $\mathbb{Q}_p$, $p \in \mathbb{P}$ ή ένα τοπικό σώμα (δηλαδή πεπερασμένη επέκταση κάποιου p-αδικού σώματος αριθμών), ή, ακόμη, ένα αλγεβρικό σώμα συναρτήσεων.

Οι καμπύλες διαιρούνται σε τρεις κατηγορίες, ανάλογα με το αν το γένος τους είναι $g = 0$, $g = 1$ ή $g \geq 2$. Κάθε κατηγορία έχει διαφορετική προσέγγιση. Το 1983, ο Faltings απέδειξε ότι αν το K είναι αλγεβρικό σώμα αριθμών και C μία καμπύλη ορισμένη υπέρ το K, τότε το σύνολο των ρητών σημείων της καμπύλης, $C(K)$, είναι πεπερασμένο. Η απόδειξη όμως δεν υποδεικνύει αλγόριθμο υπολογισμού αυτών.

Στην παρούσα εργασία, εξετάζονται διάφορες μέθοδοι καθορισμού του συνόλου όλων των ρητών σημείων δοθείσας υπερελλειπτικής καμπύλης. Βασικά, λοιπόν, επιθυμούμε να καθορίσουμε το σύνολο όλων των ρητών λύσεων $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ της τετραγωνικής εξίσωσης $Y^2 = f(X)$ όπου $f(X) \in \mathbb{Z}[X]$ ένα ανάγωγο πολυώνυμο υπέρ το $\mathbb{Q}$ βαθμού $\deg(f) \geq 5$.

Στο πρώτο κεφάλαιο, αναπτύσσονται σημαντικές έννοιες Αλγεβρικής Γεωμετρίας (Θεωρίας Αλγεβρικών Καμπυλών), χρήσιμες στα επόμενα.

Στο δεύτερο κεφάλαιο, αναπτύσσονται βασικές έννοιες της θεωρίας των p-αδικών σωμάτων, τρεις διαφορετικές μεταξύ τους εκφράσεις του Λήμματος του Hensel, καθώς και το τοπικό-γενικό αξίωμα.

Το τρίτο, τέταρτο και πέμπτο κεφάλαιο αποτελούν το κύριο μέρος της εργασίας. Σημαντικότατο βοήθημα στην επεξεργασία του αντικειμένου αποτέλεσαν οι παραδόσεις-σημειώσεις του Michael Stoll στο Πανεπιστήμιο του Bayreuth το 2014 και το 2019.

Στο τρίτο κεφάλαιο εφαρμόζουμε τα θεωρήματα του πρώτου στην ειδική περίπτωση των υπερελλειπτικών καμπυλών. Τα K-ρητά σημεία της υπερελλειπτικής καμπύλης C, εμφυτεύονται στα K-ρητά σημεία της Ιακωβιανής, $J(K)$. Επομένως το πρόβλημα

ανάγεται στην εύρεση όλων των ρητών σημείων της Ιακωβιανής. Η $J(K)$ είναι πεπερασμένα παραγόμενη αβελιανή ομάδα.

Στο τέταρτο κεφάλαιο, επιτυγχάνεται η εύρεση ενός άνω φράγματος του rank αυτής, μέσω της έννοιας της 2-ομάδας του Selmer. Η ομάδα αυτή ορίζεται εδώ με τέτοιο τρόπο ώστε να είναι βολική σε υπολογισμούς. Γενικά, η 2-ομάδα του Selmer, ορίζεται μέσω της θεωρίας της συνομολογίας του Galois. Παρουσιάζει όμως δυσχέρεια στους υπολογισμούς.

Τέλος, στο πέμπτο κεφάλαιο περιγράφεται η μέθοδος του Chabauty, η οποία έγινε effective από τον Coleman, ο οποίος όρισε μία p-αδική θεωρία ολοκλήρωσης και μέσω της οποίας, όταν ο Mordell-Weil βαθμός (rank) της $J(\mathbb{Q})$ είναι αυστηρά μικρότερος του γένους $g = g(C)$, έδωσε ένα άνω φράγμα του $C(\mathbb{Q})$.

Συνδυάζοντας όλα τα παραπάνω είναι δυνατόν σε αρκετές περιπτώσεις να λύσουμε δοθείσα διοφαντική εξίσωση.

Ας σημειωθεί ότι οι υπερελλειπτικές καμπύλες μικρού γένους (2 ή 3), χρησιμοποιούνται και στην κρυπτογραφία.

Introduction

One of the main problems in Number Theory is the solution of Diophantine equations, which means finding all the rational points of algebraic curves and more generally, of algebraic varieties. Given an affine curve C defined over a field K, the problem is finding all of its K-rational points. The field K can be the field of rational numbers $\mathbb{Q}$, an algebraic number field (i.e. a finite extension of $\mathbb{Q}$), the field of p-adic numbers $\mathbb{Q}_p$ for some $p \in \mathbb{P}$ or a local field (i.e. a finite extension of some $\mathbb{Q}_p$, $p \in \mathbb{P}$), or even an algebraic function field.

Curves are divided in three main categories, depending on their genus being $g = 0$, $g = 1$ or $g \geq 2$. A different approach is needed for each category. In 1983, Faltings proved that if K is an algebraic number field and C is a curve defined over K, then the set of its rational points, $C(K)$, is finite. However, the proof is not effective, which means that it does not provide an algorithm for finding $C(K)$.

In this thesis, different methods for finding the set of rational points of a curve are studied. Basically, we want to find the set of rational points $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ of the quadratic equation $Y^2 = f(X)$ where $f(X) \in \mathbb{Z}[X]$ is an irreducible polynomial over $\mathbb{Q}$ and of degree $\deg(f) \geq 5$.

In the first chapter, we develop a number of facts from Algebraic Geometry (Theory of Algebraic Curves), usefull in the next chapters.

In the second chapter, we develop some basic facts about p-adic fileds, three different versions of Hensel's Lemma and the local-global principle.

The third, fourth and fifth chapters are the main part of the thesis. They are based on notes from the lectures of Michael Stoll at the University of Bayreuth in 2014 and 2019.

In the third chapter, we apply the theorems of the first chapter in the case of hyperelliptic curves. The K-rational points of the hyperelliptic curve C are embedded in the K-rational points of the Jacobian, $J(K)$. Thus, our problem becomes finding the rational points of the Jacobian. The Jacobian $J(K)$ is a finitely generated abelian group.

In the fourth chapter, we calculate an upper rank of $J(K)$ by using the 2-Selmer

group. This group is defined here in a way that favors calculations. Generally, the 2-Selmer group is defined by using Galois Cohomology but this approach makes calculations harder to achieve.

Finally, in the fifth chapter, we describe Chabauty's Method, which became effective by Coleman. The latter, defined a p-adic theory of integration, which is used to provide an upper bound for $|C(\mathbb{Q})|$ in the case that the Mordell-Weil rank of $J(\mathbb{Q})$ of the curve is strictly less than its genus.

By combining all the above, it is possible to solve a given diophantine equation in many cases.

Finally, it is worth mentioning that hyperelliptic curves of small genus (2 or 3) are used in cryptography.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κύριο Ιωάννη Α. Αντωνιάδη, για όλες τις γνώσεις που μου μετέδωσε κατά την διάρκεια των προπτυχιακών και μεταπτυχιακών σπουδών μου. Ιδιαίτερα, τον ευχαριστώ για το μάθημα μελέτης που μου προσέφερε και για την αδιάκοπη στήριξή του στην περάτωση της παρούσης εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τους καθηγητές Αριστείδη Κοντογεώργη και Αλέξανδρο Κουβιδάκη που μαζί με τον κ. Ιωάννη Α. Αντωνιάδη, αποτέλεσαν την επιτροπή αξιολόγησης.

Τέλος, χρωστάω θερμές ευχαριστίες και στον Καθηγητή του Πανεπιστημίου του Bayreuth, κύριο Michael Stoll, για τη σημαντική του βοήθεια στη διευκρίνηση μερικών σημείων της εργασίας. (Mein herzlicher Dank geht auch an Herrn Prof. Dr. Michael Stoll, Universität Bayreuth, welcher mit wertvollen Hinweisen zur Vollendung der Arbeit beigetragen hat.)

Νίκος Βαρδουλάκης,

Ηράκλειο,
Σεπτέμβριος του 2019

Περιεχόμενα

Κεφάλαιο I

Στοιχεία αλγεβρικής γεωμετρίας

Εισαγωγικά, για λόγους πληρότητας, αναφέρουμε μια σειρά αποτελεσμάτων της θεωρίας αλγεβρικών καμπυλών (κάποια χωρίς αποδείξεις) τα οποία θα χρησιμοποιήσουμε στη συνέχεια. Ο ενδιαφερόμενος αναγνώστης παραπέμπεται σε οποιοδήποτε εισαγωγικό βιβλίο θεωρίας αλγεβρικών καμπυλών, όπως τα [11],[26] και [40] ή αλγεβρικής γεωμετρίας, όπως τα [16] , [27], [33] και [38].

Κάποιες από τις προτάσεις του πρώτου κεφαλαίου θα αποδειχθούν με στοιχειώδεις μεθόδους αργότερα, στο κύριο μέρος της εργασίας, ειδικά για υπερελλειπτικές καμπύλες.

§1 Δακτύλιοι διακριτής εκτίμησης

1.1 Ορισμός. Ένας αντιμεταθετικός δακτύλιος R με μοναδιαίο στοιχείο λέγεται **τοπικός** αν έχει μοναδικό maximal ιδεώδες.

1.2 Πρόταση. *Ένας αντιμεταθετικός δακτύλιος R με μοναδιαίο στοιχείο είναι τοπικός αν και μόνο αν το $R \setminus R^*$ είναι ιδεώδες (που τότε θα είναι το μοναδικό maximal ιδεώδες του R).*

Απόδειξη. Υποθέτουμε ότι ο δακτύλιος R είναι τοπικός και έστω I το μοναδικό maximal ιδεώδες του R.

Αφού το I είναι maximal, το I δεν περιέχει μονάδες (διότι τότε θα είχαμε $I = R$). Άρα $I \subseteq R \setminus R^*$. Για τον αντίστροφο εγκλεισμό, έστω $r \in R \setminus R^*$. Τότε το r ανήκει σε κάποιο maximal ιδεώδες του R. Άρα $r \in I$ (αφού I το μοναδικό maximal ιδεώδες του R), δηλαδή $R \setminus R^* \subseteq I$. Συνεπώς $I = R \setminus R^*$ που σημαίνει ότι το $R \setminus R^*$ είναι ιδεώδες.

Αντίστροφα, υποθέτουμε ότι το $R \setminus R^*$ είναι ιδεώδες του R. Τότε το $R \setminus R^*$ είναι maximal: Έστω I ένα άλλο ιδεώδες του R. Τότε το I δεν περιέχει μονάδες (αλλιώς θα είχαμε $I = R$). Άρα $I \leq R \setminus R^*$.

Για την μοναδικότητα: Έστω I άλλο ένα maximal ιδεώδες. Δεν μπορεί να ισχύει κάποιος από τους εγκλεισμούς $I \leq R \setminus R^*$ ή $R \setminus R^* \leq I$ διότι τότε κάποιο από τα

ιδεώδη I και $R \setminus R^*$ δεν θα ήταν maximal. Άρα το I περιέχει στοιχείο του συμπληρώματος του $R \setminus R^*$, δηλαδή περιέχει μονάδα. Αυτό σημαίνει ότι $I = R$ που είναι άτοπο.

Συνεπώς ο R είναι τοπικός δακτύλιος με μοναδικό maximal ιδεώδες το $R \setminus R^*$. ■

1.3 Πρόταση. *Έστω R ακέραια περιοχή που δεν είναι σώμα. Τα ακόλουθα είναι ισοδύναμα:*
1) Ο R είναι τοπικός δακτύλιος της Noether και το maximal ιδεώδες του είναι κύριο.
2) Υπάρχει ανάγωγο στοιχείο $t \in R$ τέτοιο ώστε κάθε μη μηδενικό $z \in R$ να γράφεται κατά μοναδικό τρόπο στη μορφή $z = ut^n$ με $u \in R^*$ και $n \in \mathbb{N}_0$.

Απόδειξη. (1) $\Rightarrow$ (2): Έστω $\mathfrak{m} := R \setminus R^*$ το maximal ιδεώδες του R και t ένας γεννήτοράς του. Έστω $z \in R$, $z \neq 0$. Αν $z \in R^*$ τότε $z = zt^0$ και τελείωσαμε. Αν $z \notin R^*$ τότε $z \in \mathfrak{m}$ οπότε $z = z_1 t$ για κάποιο $z_1 \in R$. Αν $z_1 \in R^*$ τελειώσαμε ενώ αν $z_1 \notin R^*$ τότε $z_1 = z_2 t$ για κάποιο $z_2 \in R$. Θεωρούμε την ακολουθία $z = z_0, z_1, \ldots$ με $z_i \notin R^*$ και $z_i = t z_{i+1}$ με $i = 0, 1, \ldots$. Θεωρούμε και την αντίστοιχη αλυσίδα ιδεωδών

$$\langle z_0 \rangle \subseteq \langle z_1 \rangle \subseteq \langle z_2 \rangle \cdots .$$

Θα δείξουμε ότι αυτή η ακολουθία γίνεται σταθερή έπειτα από κάποιον δείκτη n. Έστω ότι δεν γινόταν σταθερή. Από την υπόθεση ότι ο R είναι δακτύλιος της Noether, η παραπάνω ακολουθία έχει maximal στοιχείο. Αυτό σημαίνει ότι $\langle z_n \rangle = \langle z_{n+1} \rangle$ για κάποιον φυσικό n, οπότε θα είχαμε $z_{n+1} = v z_n$ για κάποιο $v \in R$, οπότε $z_{n+1} = v t z_{n+1}$, δηλαδή $z_{n+1} = 0$ ή $vt = 1$. Αν $z_{n+1} = 0$ τότε από τη σχέση $z_i = t z_{i+1}$, έπεται ότι $z = 0$, άτοπο. Επίσης, η ισότητα $vt = 1$ είναι αδύνατη διότι $t \notin R^*$.

Συνεπώς η ακολουθία $z_1, z_2, \ldots$ γίνεται σταθερή από για κάποιον δείκτη n και πέρα, για τον οποίο ισχύει ότι $z_n = u z_{n-1}$ με $u \in R^*$. Όμως τότε $z = ut^n$.

Μοναδικότητα: Έστω $ut^n = vt^m$ όπου $u, v \in R^*$ και $n, m \in \mathbb{N}_0$, $n \geq m$. Τότε $ut^{n-m} = v \in R^*$ και συνεπώς $n = m$ και $u = v$. Συνεπώς κάθε $z \in R$ γράφεται στη μορφή $z = ut^n$, $n \in \mathbb{N}_0$ και $u \in R^*$ με μοναδικό τρόπο.

(2) $\Rightarrow$ (1): Υποθέτουμε την ύπαρξη ενός τέτοιου t. Αφού κάθε στοιχείο $z \in R$, $z \neq 0$ γράφεται στη μορφή $z = ut^n$ με $u \in R^*$, έπεται ότι τα μοναδικά γνήσια ιδεώδη του R είναι αυτά της μορφής $\langle t^n \rangle$ με $n \in \mathbb{N}$ και ότι το μοναδικό maximal ιδεώδες είναι το $\langle t \rangle$. Άρα ο R είναι περιοχή κυρίων ιδεωδών και συνεπώς δακτύλιος της Noether. ■

1.4 Ορισμός. Μια ακέραια περιοχή R που ικανοποιεί τις συνθήκες της Πρότασης 1.3 λέγεται **δακτύλιος διακριτής εκτίμησης**.

1.5 Ορισμός. Το στοιχείο t της συνθήκης 2 της Πρότασης 1.3 λέγεται **uniformizer** του R.

1.6 Ορισμός. Έστω R μία ακέραια περιοχή. Μία **διακριτή εκτίμηση** στην R είναι μια επί απεικόνιση $v : R \to \mathbb{N}_0 \cup \{\infty\}$ με τις εξής ιδιότητες, που ισχύουν για όλα τα $a, b \in R$:

1. $v(a) = \infty \Leftrightarrow a = 0$.
2. $v(ab) = v(a) + v(b)$.
3. $v(a + b) \geq \min\{v(a), v(b)\}$.

Αν ο R είναι δακτύλιος διακριτής εκτίμησης με σώμα πηλίκων K τότε η v επεκτείνεται σε εκτίμηση στο K κατά μοναδικό τρόπο θέτοντας $v(r/s) = v(r) - v(s)$. Έτσι, η v επεκτείνεται σε απεικόνιση $v : K \to \mathbb{Z} \cup \{\infty\}$ και ικανοποιεί τις συνθήκες του παραπάνω ορισμού.

1.7 Παρατήρηση. Έστω R δακτύλιος διακριτής εκτίμησης και t ένας uniformizer του R. Αν $z \in R$ και $z = ut^n$ με $u \in R^*$ και $n \in \mathbb{N}_0$ τότε η $v : K \to \mathbb{N}_0$ με $v(z) = n$ είναι διακριτή εκτίμηση.

1.8 Πρόταση. *Αν K σώμα και v διακριτή εκτίμηση αυτού, το σύνολο $\mathcal{O}_v \coloneqq \{x \in K : v(x) \geq 0\}$ είναι δακτύλιος διακριτής εκτίμησης με σύνολο μονάδων $\mathcal{O}_v^* = \{x \in K : v(x) = 0\}$ και μοναδικό maximal ιδεώδες το $\mathfrak{m}_v \coloneqq \mathcal{O}_v \setminus \mathcal{O}_v^* = \{x \in K : v(x) \geq 1\}$*

Απόδειξη. Πρώτα θα δείξουμε ότι το σύνολο $\mathcal{O}_v$ είναι δακτύλιος. Παρατηρούμε ότι $v(1) = v(1 \cdot 1) = v(1) + v(1)$ και επομένως $v(1) = 0$, οπότε $\mathcal{O}_v \neq \emptyset$. Έστω $a, b \in \mathcal{O}_v$. Τότε $v(a), v(b) \geq 0$ και $ab, a - b \in \mathcal{O}_v$, αφού

$$v(ab) = v(a) + v(b) \geq 0$$

και

$$v(a - b) \geq \min\{v(a), v(-b)\} = \min\{v(a), v(-1) + v(b)\} = \min\{v(a), v(b)\} \geq 0.$$

Συνεπώς το σύνολο $\mathcal{O}_v$ είναι υποδακτύλιος του K, δηλαδή είναι δακτύλιος.

Έπειτα, θα δείξουμε ότι $\mathcal{O}_v^* = \{x \in K : v(x) = 0\}$. Αφού $v(1) = 0$ έχουμε $1 \in \mathcal{O}_v^*$. Επίσης, αν $a \in \mathcal{O}_v^*$ τότε

$$v(a^{-1}) = v(\frac{1}{a}) = v(1) - v(a) = -v(a).$$

Αν $a \in K$ με $v(a) > 0$ τότε $v(a^{-1}) = -v(a) < 0$, δηλαδή $a^{-1} \notin \mathcal{O}_v$, που σημαίνει ότι το a δεν είναι αντιστρέψιμο. Άρα αν το a είναι αντιστρέψιμο τότε αναγκαστικά $v(a) = 0$. Αντίστροφα, αν $v(a) = 0$ τότε $v(a^{-1}) = -v(a) = 0$, δηλαδή $a^{-1} \in \{x \in K : v(x) = 0\}$. Συνεπώς, $\mathcal{O}_v^* = \{x \in K : v(x) = 0\}$.

Τώρα, θα δείξουμε ότι το $\mathfrak{m}_v \coloneqq \mathcal{O}_v \setminus \mathcal{O}_v^* = \{x \in K : v(x) \geq 1\}$ είναι ιδεώδες του $\mathcal{O}_v$, οπότε από την Πρόταση 1.2, θα είναι το μοναδικό maximal ιδεώδες του $\mathcal{O}_v$. Έστω $a, b \in \mathfrak{m}_v$ και $r \in \mathcal{O}_v$, δηλαδή $v(a), v(b) \geq 1$ και $v(r) \geq 0$. Τότε $a - b, ra \in \mathcal{O}_v$ αφού

$$v(a - b) \geq \min\{v(a), v(-b)\} = \min\{v(a), v(b)\} \geq 1$$

και

$$v(ra) = v(r) + v(a) \geq 1.$$

Στη συνέχεια, θα δείξουμε ότι ο δακτύλιος $\mathcal{O}_v \coloneqq \{x \in K : v(x) \geq 0\}$ είναι δακτύλιος διακριτής εκτίμησης. Αφού η $v : K \to \mathbb{Z} \cup \{\infty\}$ είναι επί, υπάρχει $t \in \mathcal{O}_v$ τέτοιο ώστε $v(t) = 1$. Το t είναι ανάγωγο στον $\mathcal{O}_v$ (αν δεν ήταν τότε θα είχαμε $t = t_1 t_2$ με $t_1, t_2 \in \mathcal{O}_v \setminus \mathcal{O}_v^*$, οπότε $v(t) = v(t_1 t_2) = v(t_1) + v(t_2) > 1$, άτοπο). Έστω $z \in \mathcal{O}_v \setminus \{0\}$ με $v(z) = n \in \mathbb{N}$ (που υπάρχει αφού η εκτίμηση είναι επί του $\mathbb{N}_0 \cup \{\infty\}$). Τότε αφού $v(t^n) = n$, για το στοιχείο $\frac{z}{t^n}$ ισχύει ότι $v(\frac{z}{t^n}) = 0$, άρα $\frac{z}{t^n} \in \mathcal{O}_v^*$, δηλαδή υπάρχει $u \in \mathcal{O}_v^*$ τέτοιο ώστε $\frac{z}{t^n} = u$, δηλαδή $z = ut^n$. Αφού κάθε $z \in \mathcal{O}_v \setminus \{0\}$ γράφεται σε αυτή τη μορφή, σύμφωνα με την Πρόταση 1.3, ο $\mathcal{O}_v$ είναι δακτύλιος διακριτής εκτίμησης. ■

1.9 Παρατήρηση. Στην δεύτερη παράγραφο της παραπάνω απόδειξης, δείξαμε ότι ένα στοιχείο t για το οποίο $v(t) = 1$ είναι uniformizer.

1.10 Πρόταση. *Έστω R δακτύλιος διακριτής εκτίμησης με σώμα πηλίκων το K. Αν ο R' είναι δακτύλιος τέτοιος ώστε $R \leq R' \leq K$ τότε $R' = R$ ή $R' = K$.*

Απόδειξη. Έστω $R' \neq R$. Θα αποδείξουμε ότι $R' = K$. Αφού $R' \neq R$ τότε υπάρχει $x \in R' \setminus R$. Όμως $R' \leq K$, οπότε $x \in K = \mathrm{Quot}(R)$. Από το (2) της Πρότασης 1.3, $x = ut^{-n}$ με $u \in R^*$ και $n > 0$ (αν ήταν $n \leq 0$ τότε θα είχαμε $x \in R$ που είναι άτοπο). Άρα, $t^{-1} = u^{-1}t^{n-1}x \in R'$ (αφού $x \in R'$ και $u^{-1}t^{n-1} \in R'$) και επομένως, $K = R[t^{-1}] \leq R'$. Συνεπώς $R' = K$. ■

1.11 Ορισμός. Έστω R ακέραια περιοχή, $K = \mathrm{Quot}(R)$ και P ένα πρώτο ιδεώδες του R. Ο δακτύλιος

$$R_P \coloneqq \left\{\frac{a}{b} \in R : b \notin P\right\}$$

είναι λέγεται **τοπικοποίηση** του R στο P. Το maximal ιδεώδες του είναι το $P \cdot R_P$.

Με αυτόν τον τρόπο, μπορούμε να κατασκευάσουμε από περιοχές κυρίων ιδεωδών, δακτυλίους διακριτής εκτίμησης.

1.12 Παράδειγμα. Για κάθε $p \in \mathbb{P}$, ο δακτύλιος

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$$

είναι δακτύλιος διακριτής εκτίμησης στο $\mathbb{Q}$ με διακριτή εκτίμηση την **p-αδική εκτίμηση** v_p ($v_p(a/b) = v_p(a) = \max\{n : p^n | a\}$). Το maximal ιδεώδες του $\mathbb{Z}_{(p)}$ είναι το $\langle p \rangle$ και το σύνολο των μονάδων του τα κλάσματα της μορφής $\frac{a}{b}$ με $p \nmid a$ και $p \nmid b$. □

1.13 Παράδειγμα. Έστω K σώμα. Με $K[\![t]\!]$ συμβολίζουμε τον δακτύλιο των τυπικών δυναμοσειρών ως προς t υπέρ το K. Τα στοιχεία του είναι δυναμοσειρές της μορφής $\sum_{n=0}^{\infty} a_n t^n$ με $a_n \in K$. Ο $K[\![t]\!]$ είναι δακτύλιος διακριτής εκτίμησης με εκτίμηση

$$v\left(\sum_{n=0}^{\infty} a_n t^n\right) = \min\{n \in \mathbb{N}_0 : a_n \neq 0\}$$

(δηλαδή η εκτίμιση ισούται με τη μικρότερη δύναμη του t που εμφανίζεται στο ανάπτυγμα.) Το maximal ιδεώδες είναι το $\langle t\rangle$ ενώ το σύνολο των μονάδων είναι οι δυναμοσειρές που έχουν μη μηδενικό σταθερό όρο. □

1.14 Παράδειγμα. Έστω K σώμα και R ο δακτύλιος διακριτής εκτίμησης του $K(X)$, με $X \in R$. Τότε $K[X] \leq R \leq K(X)$ και για κάθε ανάγωγο (μονικό) πολυώνυμο $p(X) \in K[X]$, ο R είναι της μορφής

$$R = K[X]_{p(X)} \coloneqq \left\{ \frac{a(X)}{b(X)} : a(X), b(X) \in K[X], p(X) \nmid b(X) \right\}.$$

Αν το K είναι αλγεβρικά κλειστό τότε το ανάγωγο πολυώνυμο $p(X) \in K[X]$ είναι της μορφής $p(X) = X - \alpha$, $\alpha \in K$, οπότε ο περιορισμός $p(X) \nmid b(X)$ είναι ισοδύναμος με την συνθήκη $b(\alpha) \neq 0$.

Έστω τώρα ότι $X \notin R$. Τότε $X \in R^*$. Σε αυτήν την περίπτωση,

$$R = K[X^{-1}] = \left\{ \frac{a(X)}{b(X)} : b(X) \neq 0, \deg(b) \geq \deg(a) \right\}.$$

□

1.15 Σημείωση. Υπάρχουν τοπικοί δακτύλιοι οι οποίοι δεν είναι δακτύλιοι διακριτής εκτίμησης. Αργότερα θα δούμε τη γεωμετρική σημασία αυτής της αλγεβρικής διαφοροποίησης.

§2 Αλγεβρικές καμπύλες και αλγεβρικά σώματα συναρτήσεων

Σε αυτό το κεφάλαιο υποθέτουμε ότι το K είναι τέλειο σώμα, (δηλαδή $\mathrm{ch}K = 0$ ή $K^p = K$ για κάποιον $p \in \mathbb{P}$), ή, ισοδύναμα, ότι κάθε πεπερασμένη επέκτασή του είναι διαχωρίσιμη. Με $\bar{K}$ θα συμβολίζουμε μια (σταθεροποιημένη) αλγεβρική θήκη του K.

1.16 Ορισμός. Μια **αφινική αλγεβρική καμπύλη** πάνω από το K είναι το σύνολο των λύσεων της εξίσωσης $f(X,Y) = 0$ όπου $f(X,Y) \in K[X,Y]$ ένα μη σταθερό ανάγωγο πολυώνυμο.

1.17 Ορισμός. Έστω $C : f(X,Y) = 0$ μια αφινική αλγεβρική καμπύλη. Ως **δακτύλιο συντεταγμένων** της C ορίζουμε τον δακτύλιο

$$K[C] \coloneqq K[X,Y]/\langle F\rangle \coloneqq K[\bar{x},\bar{y}]$$

όπου $\bar{x} \coloneqq X + \langle f\rangle$ και $\bar{y} \coloneqq Y + \langle f\rangle$.

Αφού το f είναι ανάγωγο υπέρ το K, ο δακτύλιος συντεταγμένων μια καμπύλης είναι ακέραια περιοχή. Επομένως, μπορούμε να ορίσουμε το σώμα πηλίκων του.

1.18 Ορισμός. Το σώμα $K(C) \coloneqq \mathrm{Quot}(K[C])$ θα λέγεται **αλγεβρικό σώμα συναρτήσεων** της C και τα στοιχεία του θα λέγονται **ρητές συναρτήσεις** επί της C.

Μία ρητή συνάρτηση $\phi(X,Y) \in K(C)$ γράφεται στη μορφή

$$\phi(X,Y) = \frac{h_1(X,Y)}{h_2(X,Y)}$$

όπου $h_1, h_2 \in K[X,Y]$ και $h_2(X,Y) \neq 0$.

1.19 Ορισμός. Το $(x,y) \in K \times K$ θα λέγεται K- ρητό σημείο της C αν $f(x,y) = 0$. Το σύνολο των K-ρητών σημείων της C το συμβολίζουμε με $C(K)$, δηλαδή

$$C(K) \coloneqq \{(x,y) \in K \times K : f(x,y) = 0\}.$$

Ανάλογα, αν η L/K είναι επέκταση σωμάτων ορίζουμε

$$C(L) \coloneqq \{(x,y) \in L \times L : f(x,y) = 0\}.$$

1.20 Ορισμός. Έστω $C : f(X,Y) = 0$ μια αφινική αλγεβρική καμπύλη ορισμένη σε ένα σώμα K. Ένα σημείο $P \in C(K)$ θα λέγεται **ιδιάζον** αν $f_X(P) = f_Y(P) = 0$. Διαφορετικά, το P θα λέγεται **ομαλό σημείο** της C. Αν μία καμπύλη δεν έχει ιδιάζοντα σημεία, θα λέγεται **ομαλή**, ενώ στην αντίθετη περίπτωση, η καμπύλη θα λέγεται **ιδιάζουσα**.

1.21 Ορισμός. Έστω ρητή συνάρτηση $\phi \in K(C)$. Θα λέμε ότι η $\phi \in K(C)$ είναι (καλά) ορισμένη σε ένα $P = (x,y) \in C(K)$ αν υπάρχουν $G(X,Y), H(X,Y) \in K[X,Y]$ τέτοια ώστε $\phi = \dfrac{G(X,Y)}{H(X,Y)}$ με $H(x,y) \neq 0$.

1.22 Ορισμός. Ο **τοπικός δακτύλιος της** C **στο** $P = (x,y) \in C(K)$ ορίζεται ως το σύνολο των ρητών συναρτήσεων επί της C που ορίζονται στο P, δηλαδή

$$\mathcal{O}_P \coloneqq \mathcal{O}_{C,P} = \{\phi \in K(C) : \eta\ \phi\ \text{ορίζεται στο}\ P\}$$

Προφανώς ισχύει ότι $K \subseteq K[C] \subseteq \mathcal{O}_P \subseteq K(C)$.

1.23 Ορισμός. Έστω C ομαλή καμπύλη και $f \in \mathcal{O}_{C,P}$ και t ένας uniformizer στο P. Έστω ότι $f = gt^n$ με $t \nmid g$. Τότε λέμε ότι η f έχει **πολλαπλότητα** n στο P. Συμβολίζουμε $v_P(f) = n$.

Μία συνάρτηση f έχει ρίζα στο P αν και μόνο αν $v_P(f) \geq 1$. Αν η f έχει πολλαπλότητα n στο P, τότε $f = ht^n$ για κάποιο $h \in \mathcal{O}_{C,P}$ με $h(P) \neq 0$ και t uniformizer στο P.

1.24 Ορισμός. Έστω $f = \dfrac{g}{h} \in K(C)^*$, με $g, h \in \mathcal{O}_{C,P}$. Η **πολλαπλότητα της** f **στο** P ορίζεται ως

$$v_P(f) \coloneqq v_P(g) - v_P(h)$$

Αν $v_P(f) > 0$ λέμε ότι η f έχει **ρίζα τάξης** $v_P(f)$ στο P και αν $v_p(f) < 0$ λέμε ότι η f έχει **πόλο τάξης** $-v_P(f)$ στο P.

1.25 Παρατήρηση. Ο ορισμός είναι ανεξάρτητος της αναπαράστασης της f. Πράγματι, αν $f = \frac{g}{h} = \frac{g'}{h'}$ με $h, h' \neq 0$ τότε $gh' = g'h$, οπότε

$$v_p(g) + v_P(h') = v_P(gh') = v_P(g'h) = v_P(g') + v_p(h),$$

άρα $v_p(g) - v_P(h) = v_P(g') - v_P(h')$, δηλαδή $v_p(\frac{g}{h}) = v_p(\frac{g'}{h'})$.

Μία ρητή συνάρτηση $\phi \in K(C)$ ορίζεται σχεδόν σε όλα (δηλαδή σε όλα εκτός από πεπερασμένου πλήθους) τα σημεία της καμπύλης. Η διαπίστωση αυτή είναι άμεση συνέπεια του ακόλουθου λήμματος:

1.26 Λήμμα. *Έστω $G(X,Y), H(X,Y) \in K[X,Y]$ πρώτα μεταξύ τους. Το σύνολο*

$$M(G,H) = \{(x,y) \in K \times K : G(x,y) = H(x,y) = 0\}$$

είναι πεπερασμένο και $M \subseteq \bar{K} \times \bar{K}$.

Απόδειξη. Αφού τα G και H είναι πρώτα μεταξύ τους στον δακτύλιο $K[X,Y]$, είναι πρώτα μεταξύ τους και στον δακτύλιο $K(X)[Y]$. Αυτό σημαίνει ότι υπάρχουν $a(X), b(X) \in K(X)$ τέτοια ώστε

$$a(X)G(X,Y) + b(X)H(X,Y) = 1.$$

Αν κάνουμε τα $a(X)$ και $b(X)$ ομώνυμα με κοινό παρονομαστή $Q(X) \in K[X]$, προφανώς μη μηδενικό, πολλαπλασιάζοντας την παραπάνω σχέση με $Q(X)$, παίρνουμε

$$A(X)G(X,Y) + B(X)H(X,Y) = Q(X)$$

όπου θέσαμε $A(X) = a(X)Q(X)$ και $B(X) = b(X)Q(X)$. Άρα για κάθε $(x,y) \in M(G,H)$ έχουμε $G(x,y) = H(x,y) = 0$, οπότε $Q(x) = 0$.

Εργαζόμενοι με ανάλογο τρόπο στον $K(Y)[X]$, βρίσκουμε ένα μη μηδενικό πολυώνυμο $R(Y) \in K[Y]$ τέτοιο ώστε για κάθε $(x,y) \in M(G,H)$ να έχουμε $R(y) = 0$.
Τα Q και R, ως πολυώνυμα, έχουν πεπερασμένο πλήθος ριζών, άρα το σύνολο

$$\{(x,y) \in K \times K : Q(x) = R(y) = 0\}$$

είναι πεπερασμένο. Συνεπώς και το $M(G,F)$ είναι πεπερασμένο.

Τέλος, αφού για κάθε $(x,y) \in M(G,H)$ είναι $Q(x) = R(y) = 0$, έπεται ότι $(x,y) \in \bar{K} \times \bar{K}$. Άρα $M(G,H) \subseteq \bar{K} \times \bar{K}$. ■

1.27 Πόρισμα. *Έστω $C : F(X,Y) = 0$ μία αφινική αλγεβρική καμπύλη. Αν $\phi \in K(C)$ τότε η ϕ δεν ορίζεται σε το πολύ πεπερασμένου πλήθους σημεία.*

Απόδειξη. Η ϕ έχει την μορφή $\phi(x,y) = \dfrac{G(\bar{x},\bar{y})}{H(\bar{x},\bar{y})}$ με $G(X,Y), H(X,Y) \in K[X,Y]$. Το H είναι πρώτο με το F (αν δεν ήταν, τότε επειδή το F είναι ανάγωγο, θα είχαμε $F \mid H$, οπότε για κάθε $(x,y) \in K[X]$ θα ήταν $H(x,y) = 0$, που σημαίνει ότι η ϕ δεν θα οριζόταν σε κανένα σημείο που είναι άτοπο). Καθώς τα πολυώνυμα H και F είναι πρώτα μεταξύ τους, από το Λήμμα 1.26 συμπεραίνουμε ότι το σύνολο $M(F,H)$ είναι πεπερασμένο. Η ϕ δεν ορίζεται σε ένα σημείο $(x,y) \in C(K)$ αν και μόνο αν $H(x,y) = 0$. Όμως η F μηδενίζεται για κάθε $(x,y) \in C(K)$, άρα το σύνολο των σημείων του $C(K)$ για τα οποία η ϕ δεν ορίζεται είναι υποσύνολο του $M(F,H)$ και κατά συνέπεια πεπερασμένο. ■

§3 Ρητές συναρτήσεις

1.28 Ορισμός. Έστω $C : f(X,Y) = 0$ και $D : g(X,Y) = 0$ δύο αφινικές καμπύλες ορισμένες σε ένα σώμα K. Μια **ρητή απεικόνιση** $h : C \to D$ είναι ένα ζεύγος $(\phi,\psi) \in K(C) \times K(C)$ τέτοιο ώστε $g(\phi,\psi) = 0$. Θα λέμε ότι η h **ορίζεται στο σημείο** P όταν οι ϕ και ψ ορίζονται στο P. Όταν αυτό συμβαίνει, θέτουμε $f(P) = (\phi(P),\psi(P)) \in D(K)$. Η h θα λέγεται **σταθερή** όταν οι ϕ και ψ είναι σταθερές.

1.29 Παρατήρηση. Αν $C_j : f_j(X,Y) = 0$, $j = 1,2,3$ τρεις αλγεβρικές καμπύλες ορισμένη σε ένα σώμα K και $f_1 : C_1 \to C_2$, $f_2 : C_2 \to C_3$ ρητές συναρτήσεις τότε υπάρχει ρητή συνάρτηση $f_2 \circ f_1 : C_1 \to C_3$ η οποία ορίζεται ως εξής: Αν $f_1 = (\phi_1,\psi_1)$, $f_2 = (\phi_2,\psi_2)$, $\phi_2,\psi_2 \in K(C_2)$ και γράφουμε $\phi_2 = \dfrac{G_1(\bar{x_2},\bar{y_2})}{H_1(\bar{x_2},\bar{y_2})}$ και $\psi_2 = \dfrac{G_2(\bar{x_2},\bar{y_2})}{H_2(\bar{x_2},\bar{y_2})}$ όπου $\bar{x_2} = X_2 + \langle F_2\rangle$ κλπ. τότε η σύνθεση είναι

$$f_2 \circ f_1 = \left(\frac{G_1(\phi_1,\psi_1)}{H_1(\phi_1,\psi_1)}, \frac{G_2(\phi_1,\psi_1)}{H_2(\phi_1,\psi_1)}\right).$$

Ισχύει ότι $(f_2 \circ f_1)(P) = f_2(f_1(P))$ για εκείνα τα P που και τα δύο μέλη ορίζονται.

1.30 Ορισμός. Δύο καμπύλες C και D θα λέγονται **αμφίρητα ισοδύναμες** όταν υπάρχουν απεικονίσεις $f : C \to D$ και $g : D \to C$ τέτοιες ώστε $f \circ g = \mathrm{id}|_D$ και $g \circ f = \mathrm{id}|_C$.

1.31 Θεώρημα. *Έστω C και D δύο αλγεβρικές καμπύλες ορισμένες σε ένα σώμα K. Υπάρχει αμφιμονοσήμαντη αντιστοιχία ανάμεσα στις μη σταθερές ρητές απεικονίσεις $C \to D$ και στους K-ομομορφισμούς αλγεβρών $K(D) \to K(C)$ και ορίζεται ως εξής:*

$$f = (\phi,\psi) \mapsto (\bar{x} \to \phi, \bar{y} \to \psi),$$
$$\phi \hookleftarrow (\phi(x),\psi(x)).$$

1.32 Πόρισμα. *Έστω C, D δύο αλγεβρικές καμπύλες ορισμένες σε ένα σώμα K. Οι C, D είναι αμφίρητα ισοδύναμες αν και μόνο αν τα αλγεβρικά σώματα συναρτήσεων $K(C)$ και $K(D)$ είναι ισόμορφα ως K-άλγεβρες.*

Επομένως, προκειμένου να μελετήσουμε κλάσεις ισοδυναμίας αμφίρητων απεικονίσεων μεταξύ αλγεβρικών καμπυλών, αρκεί να μελετήσουμε τα αντίστοιχα σώματα αλγεβρικών συναρτήσεων. Θα μελετήσουμε αυτά τα σώματα αλγεβρικά.

1.33 Ορισμός. Ένα αλγεβρικό σώμα συναρτήσεων μιας μεταβλητής ορισμένο σε ένα σώμα K είναι ένα σώμα $\mathcal{K}$, υπερβατική επέκταση του K και υπάρχει $X \in \mathcal{K}$ που είναι υπερβατικό υπέρ το K τέτοιο ώστε η επέκταση $\mathcal{K}/K(X)$ να είναι πεπερασμένη και διαχωρίσιμη.

1.34 Παρατήρηση. Αν παραλείψουμε στον ορισμό τη διαχωρισιμότητα τότε αλγεβρικό σώμα συναρτήσεων $\mathcal{K}/K$ είναι μια πεπερασμένα παραγόμενη επέκταση σωμάτων με βαθμό υπερβατικότητας 1.

1.35 Παρατήρηση. Αν το σώμα K είναι τέλειο, τότε ο παραπάνω ορισμός συμπίπτει με τον ορισμό 1.18.

1.36 Θεώρημα. *Έστω C αλγεβρική καμπύλη ορισμένη σε ένα σώμα K. Τότε το $K(C)$ είναι αλγεβρικό σώμα συναρτήσεων μιας μεταβλητής. Αντίστροφα, έστω $\mathcal{K}/K$ ένα αλγεβρικό σώμα συναρτήσεων υπέρ το K. Τότε υπάρχει αλγεβρική καμπύλη C ορισμένη στο K τέτοια ώστε $\mathcal{K} = K(C)$.*

1.37 Ορισμός. Μια αλγεβρική καμπύλη C θα λέγεται **ρητή** όταν το σώμα συναρτήσεων αυτής είναι ισόμορφο με το σώμα των ρητών συναρτήσεων μιας μεταβλητής $K(X)$ υπέρ το K.

1.38 Παράδειγμα. Έστω K ένα σώμα.

1) Η καμπύλη $C : Y = 0$ είναι μία ρητή καμπύλη. Είναι

$$K[C] = K[X, Y]/\langle Y \rangle \cong K[X]$$

και

$$K(C) = \mathrm{Quot}(K[C]) = \mathrm{Quot}(K[X]) = K(X).$$

2) Έστω $C : X^2 + Y^2 = 1$. Τότε

$$K[C] = K[X, Y]/\langle X^2 + Y^2 - 1 \rangle$$

και

$$K(C) = \mathrm{Quot}(K[C]) = K(T)$$

όπου το T ορίζεται μέσω των απεικονίσεων

$$(x, y) \mapsto \left(\frac{2T}{1+T^2}, \frac{1-T^2}{1+T^2} \right) \text{ και } T \mapsto \frac{1-y}{x}.$$

3) Έστω $C : Y^2 = X^3$. Η C είναι ιδιάζουσα (έχει κορυφή στο $(0, 0)$). Έχουμε $K(C) = K(X, Y) \cong K(T)$ όπου το T ορίζεται μέσω των απεικονίσεων

$$(x, y) \mapsto (T^2, T^3) \text{ και } T \mapsto \frac{y}{x}.$$

4) Η καμπύλη $C : Y^2 = X^2(X+1)$ έχει κόμβο. Είναι $K(C) = K(X,Y) \cong K(T)$ όπου το T ορίζεται μέσω των απεικονίσεων

$$(x,y) \mapsto (T^2-1, T(T^2-1)), T \text{ και } T \mapsto \frac{y}{x}.$$

5) Έστω $\mathrm{ch}(K) \neq 2,3$ και $a \in K^*$. Οι καμπύλες $C_1 : X^3+Y^3 = a$ και $C_2 : Y^2 = X^3 - 432a^2$ είναι αμφίρητα ισοδύναμες. Οι ρητές απεικονίσεις είναι οι

$$C_1 \to C_2, \ \ (x,y) \mapsto \left(\frac{12a}{x+y}, \frac{36a(x-y)}{x+y}\right)$$

και

$$C_2 \to C_1, \ \ (x,y) \mapsto \left(\frac{36a+y}{6x}, \frac{36a-y}{6x}\right).$$

□

§4 Σημεία και δακτύλιοι διακριτής εκτίμησης

Στόχος της παραγράφου είναι η διατύπωση της αντιστοιχίας ανάμεσα στα K-ρητά σημεία μιας ομαλής καμπύλης και στους δακτύλιους διακριτής εκτίμησης R τέτοιους ώστε $K[C] \leq R \leq K(C)$ και σώμα κλάσεων υπολοίπων το K. Αν το K είναι αλγεβρικά κλειστό, η δεύτερη συνθήκη δεν χρειάζεται. Επίσης έχουμε μία αμφιμονοσήμαντη αντιστοιχία ανάμεσα στους δακτύλιους διακριτής εκτίμησης, όπως παραπάνω, και τα maximal ιδεώδη $\mathfrak{m}$ του $K[C]$ τέτοια ώστε $K[C]/\mathfrak{m} = K$.

1.39 Πρόταση. *Έστω C καμπύλη ορισμένη σε ένα σώμα K και $P \in C(K)$. Τότε:*

1. *$\mathcal{O}_P/\mathfrak{m}_P = K$.*
2. *Το P είναι ομαλό σημείο της καμπύλης αν και μόνο αν $\dim_K(\mathfrak{m}_P/\mathfrak{m}_P^2) = 1$.*
3. *Η C είναι ομαλή στο P αν και μόνο αν ο τοπικός δακτύλιος $\mathcal{O}_P$ είναι DVR.*

Άμεση συνέπεια της Πρότασης 1.39 είναι ο τοπικός δακτύλιος $\mathcal{O}_p$ στο σημείο $P = (0,0)$ της καμπύλης $C : Y^2 = X^2(X+1)$, δεν είναι δακτύλιος διακριτής εκτίμησης.

1.40 Πρόταση. *Έστω C (ανάγωγη) καμπύλη ορισμένη σε ένα σώμα K. Τότε ισχύουν τα εξής:*

1. *Υπάρχει αμφιμονοσήμαντη απεικόνιση*

$$C(K) \leftrightarrow \{\mathfrak{m} : \mathfrak{m} \leq K[C] \ \text{ τέτοιο ώστε } \ K[C]/\mathfrak{m} = K\}.$$

   Η αντιστοιχία είναι η $P = (x,y) \mapsto (X-x, Y-y)$.

2. *Έστω $\mathfrak{m}$ ένα maximal ιδεώδες της ακέραιας περιοχής $K[C]$. Τότε ο δακτύλιος πηλίκο $K[C]/\mathfrak{m}$ είναι (προφανώς) σώμα και μάλιστα πεπερασμένη επέκταση του K.*

1.41 Πόρισμα. *Έστω C καμπύλη ορισμένη σε ένα αλγεβρικά κλειστό σώμα K. Τότε υπάρχει αμφιμονοσήμαντη αντιστοιχία*

$$C(K) \longleftrightarrow \{\mathfrak{m} : \mathfrak{m} \text{ } \textit{maximal ιδεώδες του } K[C]\}.$$

1.42 Θεώρημα. *Έστω C ομαλή καμπύλη ορισμένη σε ένα σώμα K. Τότε υπάρχει αμφιμονοσήμαντη αντιστοιχία*

$$C(K) \longleftrightarrow \{\mathrm{DVR}(R, \mathfrak{m}) : K[C] \leq R \leq K(C) \text{ τέτοια ώστε } R/\mathfrak{m} = K\}.$$

Η αντιστοιχία είναι η

$$P \mapsto (\mathcal{O}_P, \mathfrak{m}_P)$$
$$(R, \mathfrak{m}) \hookleftarrow (X + \mathfrak{m}, Y + \mathfrak{m}).$$

§5 Προβολικό επίπεδο

1.43 Ορισμός. Έστω K ένα σώμα. Θεωρούμε τη σχέση ισοδυναμίας στο σύνολο $K^3 \setminus \{(0,0,0)\}$ που ορίζεται από τη σχέση $(x,y,z) \sim (x',y',z')$ αν και μόνο αν υπάρχει $\lambda \in K^*$ τέτοιο ώστε $(x',y',z') = (\lambda x, \lambda y, \lambda z)$. Το σύνολο των κλάσεων ισοδυναμίας της παραπάνω σχέσης λέγεται **προβολικό επίπεδο** και συμβολίζεται $\mathbb{P}^2(K)$.

Τις κλάσεις ισοδυναμίας θα τις λέμε **σημεία** του $\mathbb{P}^2(K)$. Ένα τυχαίο σημείο του $\mathbb{P}^2(K)$ θα το συμβολίζουμε $[x,y,z]$.

1.44 Ορισμός. Ένα πολυώνυμο $F(X,Y,Z) \in K[X,Y,Z]$ λέγεται **ομογενές βαθμού** d αν κάθε μονώνυμό του έχει βαθμό d ως προς X,Y,Z, δηλαδή αν το F έχει τη μορφή

$$F(X,Y,Z) = \sum_{\substack{i_1,i_2,i_3 \in \mathbb{N}_0 \\ i_1+i_2+i_3=d}} a_{i_1,i_2,i_3} X^{i_1} Y^{i_2} Z^{i_3}$$

με $a_{i_1,i_2,i_3} \in K$.

1.45 Ορισμός. Μία **προβολική καμπύλη** είναι μία καμπύλη που ορίζεται από μία εξίσωση της μορφής $C : F(X,Y,Z) = 0$ όπου το πολυώνυμο $F(X,Y,Z) \in K[X,Y,Z]$ είναι ομογενές.

Για $Z = 1$ γράφουμε $f(X,Y) \coloneqq F(X,Y,1)$ και έτσι λαμβάνουμε μία αφινική καμπύλη.

Υπάρχει μια φυσιολογική αντιστοιχία μεταξύ των σημείων του $U_1 \coloneqq \{[x,y,z] \in \mathbb{P}^2(K) : z \neq 0\}$ και των σημείων του αφινικού επιπέδου $\mathbb{A}^2(K)$. Η αντιστοιχία είναι η εξής:

$$U_1 \to \mathbb{A}^2(K), \quad [x,y,z] \mapsto \left(\frac{x}{z}, \frac{y}{z}\right)$$

και αντίστροφα,

$$\mathbb{A}^2(K) \to U_1, \ \ (x,y) \mapsto [x,y,1].$$

Για λόγους απλότητας, θα γράφουμε μία προβολική καμπύλη στην αφινική της μορφή, όμως πάντα θα την θεωρούμε προβολικά. Αν C είναι μία προβολική καμπύλη, την αντίστοιχη αφινική για $Z=1$ θα την συμβολίζουμε C_{aff}.

Αν θέσουμε $U_2 \coloneqq \{[x,y,z] \in \mathbb{P}^2(K) : z=0\}$ τότε $U_1 \cup U_2 = \mathbb{P}^2(K) \setminus \{[0,1,0]\}$. Τα σημεία του U_2 λέγονται **επ΄άπειρον σημεία** του προβολικού επιπέδου.

Πολλές φορές είναι χρήσιμο να εργαζόμαστε με καμπύλες στο προβολικό επίπεδο. Αυτό γίνεται ως εξής: Έστω $C : f(X,Y) = 0$ με $f(X,Y) \in K[X,Y]$ μια αφινική αλγεβρική καμπύλη και d ο βαθμός του μεγιστοβάθμιου όρου του f. Τότε κάνουμε **ομογενοποίηση** του πολυωνύμου θέτοντας $F(X,Y,Z) \coloneqq Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$.
Έστω τώρα $C : F(X,Y,Z) = 0$ μια προβολική καμπύλη με $\deg(F) = d$. Αν

$$(x,y,z), (x',y',z') \in \mathbb{P}^2(K)$$

με $(x,y,z) \sim (x',y',z')$, οπότε $(x',y',z') = (\lambda x, \lambda y, \lambda z)$ για κάποιο $\lambda \in K^*$ και έχουμε:

$$\begin{aligned} F(x',y',z') = 0 &\Leftrightarrow F(\lambda x, \lambda y \lambda z) = 0 \\ &\Leftrightarrow \lambda^d F(x,y,z) = 0 \quad (F \text{ ομογενές βαθμού } d) \\ &\Leftrightarrow F(x,y,z) = 0 \quad (\lambda \neq 0) \end{aligned}$$

Αυτό σημαίνει ότι σημεία που ανήκουν στην ίδια κλάση δίνουν, ουσιαστικά την ίδια λύση της εξίσωσης, δηλαδή η καμπύλη ορίζεται ως το σύνολο των σημείων

$$\{[x,y,z] \in \mathbb{P}^2(K) : F(X,Y,Z) = 0\}.$$

Ο δακτύλιος συντεταγμένων της C είναι ο $K[C] = K[X,Y,Z]/\langle F(X,Y,Z)\rangle$. Το σύνολο των ρητών συναρτήσεων της C είναι το $K(C)$ το οποίο αποτελείται από στοιχεία της μορφής $\dfrac{H_1(X,Y,Z)}{H_2(X,Y,Z)}$ όπου $H_1, H_2 \in K[X,Y,Z]$ ομογενή πολυώνυμα ίσου βαθμού και $H_2 \neq 0$.

1.46 Ορισμός. Έστω $C : F(X,Y,Z) = 0$ με $F(X,Y,Z) \in K[X,Y,Z]$ μια προβολική καμπύλη. Το σημείο $P \in \mathbb{P}^2(\bar{K})$ θα λέγεται **ιδιάζον σημείο** της καμπύλης αν

$$F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0.$$

Αλλιώς, το P λέγεται **ομαλό** σημείο της C. Αν η C έχει ένα ιδιάζον σημείο, λέγεται **ιδιάζουσα**. Αν όλα τα σημεία της είναι ομαλά, λέγεται **ομαλή**.

§6 Διαιρέτες

Έστω $\mathcal{K}$ ένα αλγεβρικό σώμα συναρτήσεων ορισμένο πάνω από ένα σώμα K. Θεωρούμε το σύνολο

$$\mathrm{Pr}D(\mathcal{K}/K) \coloneqq \{\mathrm{DVR}(R,\mathfrak{m}) : K \leq R \leq \mathcal{K} \text{ και } \mathrm{Quot}(R) = K\}.$$

Το $\mathrm{Pr}D(\mathcal{K}/K)$ είναι το σύνολο των σημείων της αντίστοιχης ομαλής καμπύλης. Τα στοιχεία του λέγονται **πρώτοι διαιρέτες**. Το σύνολο

$$\mathrm{Pr}D(\mathcal{K}/K)(K) \coloneqq \{(R,\mathfrak{m}) \in \mathrm{Pr}D(\mathcal{K}/K) : R/\mathfrak{m} = K\}$$

είναι το σύνολο των K-ρητών σημείων της αντίστοιχης ομαλής καμπύλης. Αν P κάποιος πρώτος διαιρέτης τότε συμβολίζουμε τον αντίστοιχο δακτύλιο διακριτής εκτίμησης με $\mathcal{O}_p$, το (μοναδικό) maximal ιδεώδες με $\mathfrak{m}_P$, το αντίστοιχο σώμα κλάσεων υπολοίπων με K_P, έναν uniformizer με t_P κ.ο.κ.

1.47 Ορισμός. Ο **βαθμός ενός πρώτου διαιρέτη** ισούται με τον βαθμό της επέκτασης K_P ως K-διανυσματικό χώρο, δηλαδή

$$\deg(P) \coloneqq [K_P : K] = \dim_K(K_P)$$

Οι **ρητοί πρώτοι διαιρέτες** έχουν βαθμό 1. Έστω C αλγεβρική καμπύλη υπέρ το K. Τότε συμβολίζουμε

$$\mathrm{Pr}D(K(C)/K) \coloneqq \mathscr{C}.$$

Έτσι παίρνουμε μια εμφύτευση

$$\{P \in C(K) : C \text{ ομαλή στο } P\} \hookrightarrow \mathscr{C}(K).$$

Το πολύ πεπερασμένο πλήθος σημείων του $C(K)$ δεν ανήκουν στην εικόνα του $\{P \in C(K) : C \text{ ομαλή στο } P\}$

1.48 Ορισμός. Έστω $K(C)$ αλγεβρικό σώμα συναρτήσεων μιας μεταβλητής πάνω από ένα σώμα K, $f \in K(C)$ και $P \in \mathrm{Pr}D(\mathcal{K}/K)$. Θα λέμε ότι η f **ορίζεται στο** P όταν $f \in \mathcal{O}_P$.

Σε αυτήν την περίπτωση, το $f(P) \in K_p$ είναι η εικόνα της f ως προς τον κανονικό ομομορφισμό $\mathcal{O}_P \to \mathcal{O}_P/\mathfrak{m}_P \coloneqq K_P$.

1.49 Θεώρημα. *Έστω $K(C)$ ένα αλγεβρικό σώμα συναρτήσεων μιας μεταβλητής ορισμένο πάνω από ένα K και $f \in K(C)$. Τότε η f ορίζεται παντού αν και μόνο αν η f είναι σταθερή. Ισοδύναμα, αν και μόνο αν*

$$\bigcap_{P \in \mathrm{Pr}D(\mathcal{K}/K)} \mathcal{O}_P = \bar{K}.$$

Έστω K ένα τέλειο σώμα (τα σώματα χαρακτηριστικής 0 και τα πεπερασμένα σώματα είναι τέλεια). Αν $\bar{K}$ μία αλγεβρική θήκη του K, τότε αυτή είναι διαχωρίσιμη επέκταση του K. Η ομάδα των K-αυτομορφισμών του $\bar{K}$ είναι η **απόλυτη ομάδα Galois** του K και συμβολίζουμε $\mathrm{Gal}(\bar{K}/K)$. Ισχύει ότι

$$\{a \in \bar{K} : \sigma(a) = a \text{ για κάθε } \sigma \in \mathrm{Gal}(\bar{K}/K)\} = K$$

1.50 Σημείωση. Το Θεμελιώδες Θεώρημα της Θεωρίας Galois δεν ισχύει για άπειρες επεκτάσεις. Τον ενδιαφερόμενο αναγνώστη τον παραπέμπουμε στην μεταπτυχιακή εργασία της Ανθής Ζερβού [42]

Στη συνέχεια αυτής της παραγράφου, υποθέτουμε ότι το σώμα K είναι τέλειο. Θα θεωρούμε τους πρώτους διαιρέτες ως σημεία της καμπύλης.

1.51 Ορισμός. Έστω C μία ομαλή, προβολική και απολύτως ανάγωγη καμπύλη ορισμένη σε ένα σώμα K. Η ελεύθερη αβελιανή ομάδα με βάση το σύνολο $C(\bar{K})$ λέγεται **ομάδα διαιρετών** της C και συμβολίζεται $\mathrm{Div}(C)$. Τα στοιχεία της, τα οποία είναι γραμμικοί συνδυασμοί σημείων του $C(\bar{K})$, λέγονται **διαιρέτες** στην C. Γράφουμε

$$D = \sum_{P \in C(\bar{K})} n_p P$$

όπου $n_P \in \mathbb{Z}$ και $n_P = 0$ για όλα εκτός από πεπερασμένου πλήθους σημείων P. Συμβολίζουμε $n_P := v_P(D)$.

1.52 Ορισμός. Ο βαθμός ενός διαιρέτη $D = \sum_{P \in C(\bar{K})} n_p P$ είναι το άθροισμα

$$\deg(D) := \sum_{P \in C(\bar{K})} n_P$$

1.53 Παρατήρηση. Η απεικόνιση $\deg : \mathrm{Div}(C) \to \mathbb{Z}$, $D \mapsto \deg(D)$ είναι προσθετικός ομομορφισμός ομάδων.

1.54 Παρατήρηση. Το σύνολο $\{D \in \mathrm{Div}(C) : \deg(D) = 0\}$ αποτελεί υποομάδα της ομάδας $\mathrm{Div}(C)$ και συμβολίζεται $\mathrm{Div}^0(C)$. Προφανώς, $\mathrm{Div}^0(C) = \mathrm{Ker}(\deg)$.

1.55 Ορισμός. Ένας διαιρέτης D θα λέγεται **effective** αν $v_P(D) \geq 0$ για κάθε $P \in C(K)$. Για δύο διαιρέτες D_1 και D_2, θα γράφουμε $D_1 \geq D_2$ αν ο $D_1 - D_2$ είναι effective, δηλαδή αν $v_P(D_1) \geq v_P(D_2)$ για κάθε $P \in C(K)$.

1.56 Ορισμός. Ως **support** ενός διαιρέτη D, ορίζουμε το σύνολο

$$\{P \in C(\bar{K}) : v_P(D) \neq 0\},$$

δηλαδή ως το σύνολο των σημείων που εμφανίζονται στην ανάλυση του D με μη μηδενικό συντελεστή.

1.57 Ορισμός. Ένας διαιρέτης $D \in \mathrm{Div}(C)$ θα λέγεται **K-ρητός** αν μένει αναλλοίωτος από την δράση της απόλυτης ομάδας Galois του σώματος K, $\mathrm{Gal}(\bar{K}/K)$. Την υποομάδα των K-ρητών διαιρετών της C τη συμβολίζουμε $\mathrm{Div}(C(K))$.

1.58 Πρόταση. *Αν $f \in \bar{K}(C)^*$ τότε το πλήθος των σημείων για τα οποία $v_P(f) \neq 0$ είναι πεπερασμένο. Δηλαδή, η f έχει πεπερασμένο πλήθος ρίζες και πόλους.*

1.59 Ορισμός. Έστω $f \in \bar{K}(C)^*$ μία ρητή συνάρτηση. Ο διαιρέτης της f ορίζεται ως

$$\mathrm{div}(f) \coloneqq \sum_{P \in C(\bar{K})} v_p(f)P \in \mathrm{Div}(C).$$

1.60 Ορισμός. Ένας διαιρέτης $D \in \mathrm{Div}(C)$ λέγεται **κύριος διαιρέτης** αν υπάρχει ρητή συνάρτηση $f \in \bar{K}(C)^*$ τέτοια ώστε $D = \mathrm{div}(f)$.

Από τον ορισμό του κύριου διαιρέτη, άμεσα συνάγουμε την παρακάτω πρόταση:

1.61 Πρόταση. *Για κάθε $f, g \in \bar{K}(C)^*$, ισχύουν οι σχέσεις* $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$ *και* $\mathrm{div}(\frac{1}{f}) = -\mathrm{div}(f)$.

Συμπεραίνουμε λοιπόν ότι η απεικόνιση $\mathrm{div} : (\bar{K}(C)^*, \cdot) \to (\mathrm{Div}(C), +)$, $f \mapsto \mathrm{div}(f)$ είναι ομομορφισμός ομάδων. Επομένως, το σύνολο των κύριων διαιρετών μιας καμπύλης αποτελεί υποομάδα του $\mathrm{Div}(C)$. Η ομάδα των κύριων διαιρετών συμβολίζεται με $\mathrm{Princ}(C)$.

1.62 Πρόταση. *Κάθε κύριος διαιρέτης μιας καμπύλης έχει βαθμό 0.*

1.63 Πόρισμα. *Έστω $f \in \bar{K}(C)^*$. Τότε το πλήθος των ριζών της f είναι ίσο με το πλήθος των πόλων της, μετρώντας φυσικά και την πολλαπλότητά τους.*

Από το παραπάνω πόρισμα, αν $f \in \bar{K}(C)^*$, μπορούμε να γράψουμε

$$\mathrm{div}(f) = \mathrm{div}(f)_0 - \mathrm{div}(f)_\infty$$

όπου $\mathrm{div}(f)_0 = \sum_{P \ \text{ρίζα της} \ f} v_P(f)P$ και $\mathrm{div}(f)_\infty = \sum_{P \ \text{πόλος της} \ f} v_P(f)P$.

Μία σταθερά $c \in \bar{K}^*$ δεν έχει ούτε ρίζες ούτε πόλους. Άρα $\mathrm{div}(c) = 0$ για κάθε $c \in \bar{K}^*$.

Στην ομάδα $\mathrm{Div}(C)$, ορίζουμε την σχέση $\sim$ ως εξής: $D_1 \sim D_2$ αν και μόνο αν υπάρχει $f \in \bar{K}(C)^*$ τέτοια ώστε $D_2 = D_1 + \mathrm{div}(f)$. Προφανώς είναι σχέση ισοδυναμίας. Οι D_1 και D_2 λέγονται **γραμμικά ισοδύναμοι** και συμβολίζουμε $D_1 \equiv D_2$. Προφανώς αν $D_1 \equiv D_2$ τότε $\deg(D_1) = \deg(D_2)$. Το αντίστροφο δεν ισχύει. Η ομάδα πηλίκο $\mathrm{Div}(C)/\mathrm{Princ}(C)$ λέγεται **ομάδα του Picard** και συμβολίζουμε

$$\mathrm{Pic}(C) \coloneqq \mathrm{Div}(C)/\mathrm{Princ}(C).$$

Την κλάση ενός διαιρέτη D την συμβολίζουμε $[D]$.

1.64 Ορισμός. Έστω C ομαλή, προβολική και απολύτως ανάγωγη καμπύλη ορισμένη σε ένα αλγεβρικά κλειστό σώμα K και έστω $D \in \mathrm{Div}(C(K))$ ένας διαιρέτης. Ορίζουμε τον **χώρο Riemann-Roch** του D ως τον K-διανυσματικό χώρο

$$\mathscr{L}(D) = \{\phi \in K(C)^* : \mathrm{div}(\phi) + D \geq 0\} \cup \{0\}.$$

Αν $D = n_1P_1 + ... + n_mP_m$ και $\phi \in L(D)$ τότε από την συνθήκη $\mathrm{div}(\phi) + D \geq 0$, ισοδύναμα $\mathrm{div}(\phi) \geq -D$, παίρνουμε $v_{P_i}(\mathrm{div}(\phi)) \geq -n_{P_i}$ για κάθε $i = 1, ..., m$. Άρα:

Αν $n_{P_i} < 0$, η ϕ έχει πόλο τάξης το πολύ $-n_{P_i}$ στο P_i.

Αν $n_{P_i} > 0$, η ϕ έχει ρίζα στο P_i τάξης τουλάχιστον n_{P_i}.

Στην επόμενη πρόταση, συγκεντρώνουμε κάποιες βασικές ιδιότητες του χώρου Riemann-Roch.

1.65 Πρόταση. *Για τον χώρο Riemann-Roch $\mathscr{L}(D)$ ενός διαιρέτη $D \in \mathrm{Div}(C)$, ισχύουν τα εξής:*

1. *Αν $\deg(D) < 0$ τότε $\mathscr{L}(D) = \{0\}$, οπότε $\dim_K(\mathscr{L}(D)) = 0$.*
2. *Αν $D_1 \equiv D_2$ τότε $\mathscr{L}(D_1) \cong \mathscr{L}(D_2)$.*
3. *Αν $D \geq D'$ τότε $\mathscr{L}(D) \supseteq \mathscr{L}(D')$.*
4. *Αν $D = 0$ τότε $\mathscr{L}(D) = K$, οπότε $\dim_K(\mathscr{L}(0)) = 1$.*
5. *Αν D effective και $\deg(D) = 0$ τότε $\mathscr{L}(D) = K$, οπότε $\dim_K(\mathscr{L}(D)) = 1$*
6. *Αν $D \in \mathrm{Div}(C)$ τότε $\dim_K(\mathscr{L}(D)) \leq \deg(D) + 1$ Ειδικότερα, ο $\mathscr{L}(D)$ είναι K-διανυσματικός χώρος πεπερασμένης διάστασης.*

Απόδειξη.

1) Έστω $\phi \in \mathscr{L}(D) \setminus \{0\}$. Από τη συνθήκη $\mathrm{div}(\phi) \geq -D$ συμπεραίνουμε ότι

$$\deg(\mathrm{div}(\phi)) \geq -\deg(D) > 0$$

που είναι άτοπο διότι ο $\mathrm{div}(\phi)$ είναι κύριος διαιρέτης.

2) Έστω $D_1 - D_2 = \mathrm{div}(f)$, $f \in K(C)^*$. Αν $g \in \mathscr{L}(D_1)$, οπότε $\mathrm{div}(g) \geq -D_1$, τότε

$$\mathrm{div}(gf) = \mathrm{div}(g) + \mathrm{div}(f) = \mathrm{div}(g) + D_1 - D_2 \geq -D_1 + D_1 - D_2 = -D_2,$$

οπότε $gf \in \mathscr{L}(D_2)$. Έτσι, λαμβάνουμε έναν ισομορφισμό διανυσματικών χώρων

$$\phi : \mathscr{L}(D_1) \to \mathscr{L}(D_2), \ \ \phi(g) = gf :$$

Αν $g, h \in \mathscr{L}(D_1)$ τότε

$$\phi(g + h) = (g + h) \cdot f = gf + hf = \phi(g) + \phi(h),$$

άρα η ϕ είναι ομομορφισμός.
Αν $\phi(g) = \phi(h)$ τότε $gf = hf$ και αφού $f \in K(C)^*$, έπεται $g = h$. Άρα η ϕ είναι 1-1.

Τέλος, αν $h \in L(D_2)$ τότε

$$\phi(hf^{-1}) = hf^{-1}f = h,$$

άρα η f είναι επί.

3) Αν $\phi \in \mathscr{L}(D')$ τότε $\mathrm{div}(\phi) + D' \geq 0$ και αφού $D \geq D'$ έπεται ότι $\mathrm{div}(\phi) + D \geq 0$, που σημαίνει ότι $\phi \in \mathscr{L}(D)$. Άρα $\mathscr{L}(D) \supseteq \mathscr{L}(D')$.

4) Έστω $\phi \in \mathscr{L}(0)$. Τότε $\mathrm{div}(\phi) \geq 0$, δηλαδή $v_P(\mathrm{div}(\phi)) \geq 0$ για κάθε $P \in \mathrm{supp}(\mathrm{div}(\phi))$. Όμως $\deg(\mathrm{div}(\phi)) = 0$, δηλαδή

$$\sum_{P \in \mathrm{supp}(\mathrm{div}(\phi))} v_p(\phi) = 0,$$

άρα $v_P(\phi) = 0$ για κάθε $P \in \mathrm{supp}(\mathrm{div}(\phi))$. Αυτό συνεπάγεται ότι $\mathrm{div}(\phi) = 0$, δηλαδή η ϕ δεν έχει ούτε ρίζες ούτε πόλους. Άρα η ϕ είναι αναγκαστικά σταθερή, δηλαδή $\phi \in K$. Συνεπώς, $\mathscr{L}(0) \subseteq K$. Έστω τώρα $c \in K$. Τότε $\mathrm{div}(c) = 0$, άρα $\mathrm{div}(c) + 0 \geq 0$, δηλαδή $c \in \mathscr{L}(0)$.

5) Αν $D \geq 0$ και $\deg(D) = 0$ τότε $D = 0$ και το συμπέρασμα προκύπτει από το προηγούμενο.

6) Αν $\deg(d) < 0$, το αποτέλεσμα είναι άμεσο από το (1). Έστω λοιπόν $D \in \mathrm{Div}(C)$ με $\deg(D) \geq 0$ και έστω $\phi \in \mathscr{L}(D)$. Τότε $D + \mathrm{div}(\phi) \geq 0$, δηλαδή ο διαιρέτης $D' = D + \mathrm{div}(\phi)$ είναι effective. Από το (2), αφού $D' \equiv D$, $\dim_K(\mathscr{L}(D)) = \dim_K(\mathscr{L}(D'))$, οπότε μπορούμε να θεωρήσουμε ότι ο D είναι effective.

Παίρνουμε λοιπόν έναν effective διαιρέτη $D \in \mathrm{Div}(C)$ με $d := \deg(D) \geq 0$ και σημεία $P_1, ..., P_{d+1} \notin \mathrm{supp}(D)$. Θεωρούμε την απεικόνιση

$$j : \mathscr{L}(D) \to K^{d+1}, \;\; f \mapsto (f(P_1), ..., f(P_{d+1})).$$

Ο πυρήνας της απεικόνισης j είναι ο χώρος $\mathscr{L}(D - P_1 - ... - P_{d+1})$. Πράγματι,

$$\begin{aligned} f \in \mathscr{L}(D - P_1 - ... - P_{d+1}) &\Leftrightarrow \mathrm{div}(f) + D - P_1 - ... - P_{d+1} \geq 0 \\ &\Leftrightarrow \mathrm{div}(f) \geq P_1 + ... + P_{d+1} - D \end{aligned}$$

Το παραπάνω συμβαίνει αν και μόνο αν η f μηδενίζεται στα $P_1, ..., P_{d+1}$ (διότι

$$\{P_1, ..., P_{d+1}\} \cap \mathrm{supp}(D) = \emptyset,$$

οπότε τα $P_1, ..., P_{d+1}$ ανήκουν στο $\mathrm{supp}(D - P_1 - ... - P_{d+1})$), αν και μόνο αν

$$(f(P_1), ..., f(P_{d+1})) = (0, ..., 0),$$

αν και μόνο αν $f \in \mathrm{Ker}(j)$.

Όμως

$$\deg(D - P_1 - ... - P_{d+1}) = d - (d+1) = -1 < 0,$$

οπότε από το (1), $\dim_K(\mathscr{L}(D - P_1 - ... - P_{d+1})) = 0$, δηλαδή $\dim_K(\mathrm{Ker}(j)) = 0$. Άρα από την ανισότητα

$$\dim_K(\mathscr{L}(D)) \leq \dim_K(\mathrm{Ker}(j)) + d + 1$$

συμπεραίνουμε ότι $\dim_K(\mathscr{L}(D)) \geq d + 1$. ■

Ο πυρήνας του ομομορφισμού $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ είναι ο $\mathrm{Div}^0(C)$ και από την Πρόταση 1.62, $\mathrm{Princ}(C) \subseteq \mathrm{Div}^0(C)$. Άρα ο deg ανάγεται σε ομομορφισμό $\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Princ}(C) \to \mathbb{Z}$. Τον πυρήνα του τον συμβολίζουμε $\mathrm{Pic}^0(C)$.

Έστω C μία καμπύλη υπέρ το σώμα K. Υπάρχει πάντοτε μία αριθμητική αναλλοίωτη της καμπύλης $g = g(C) \in \mathbb{N}_0$ η οποία λέγεται **γένος της καμπύλης**. Η έννοια αυτή θα οριστεί παρακάτω, όταν διατυπωθεί το Θεώρημα Riemann-Roch.

1.66 Πρόταση. *Έστω C μια ομαλή, προβολική και απολύτως ανάγωγη καμπύλη γένους g ορισμένη σε ένα σώμα K. Τότε υπάρχει μια αβελιανή πολλαπλότητα J διάστασης g υπέρ το K τέτοια ώστε για κάθε σώμα L με $K \subseteq L \subseteq \bar{K}$ να έχουμε $J(L) = \mathrm{Pic}_L(C)^0$.*

1.67 Σημείωση. Η έννοια της αβελιανής πολλαπλότητας είναι αρκετά πολύπλοκη και δεν θα οριστεί στην παρούσα εργασία.

1.68 Ορισμός. Η αβελιανή πολλαπλότητα J που εμφανίζεται στην παραπάνω πρόταση λέγεται **Ιακωβιανή** της καμπύλης C υπέρ το K.

Αν $P_0 \in C(K)$, λαμβάνουμε μία φυσιολογική απεικόνιση $i : C \to J$ με $i(P) = [P - P_0]$. Η απεικόνιση αυτή είναι μορφισμός αλγεβρικών πολλαπλοτήτων και είναι 1-1 όταν $g > 0$. Αυτό αποδεικνύεται αργότερα, στην Πρόταση 1.81, μετά την διατύπωση του Θεωρήματος Riemann-Roch.

1.69 Θεώρημα. ***(Mordell-Weil.)*** *Έστω K ένα σώμα αριθμών (δηλαδή πεπερασμένη επέκταση του $\mathbb{Q}$) και έστω J η Ιακωβιανή μιας καμπύλης C υπέρ το K. Τότε η J είναι πεπερασμένα παραγόμενη αβελιανή ομάδα.*

§7 Παραγωγίσεις και διαφορικά

1.70 Ορισμός. Έστω V ένας $K(C)$-διανυσματικός χώρος. Μια K-γραμμική απεικόνιση $d : K(C) \to V$ θα λέγεται **παραγώγιση** όταν για κάθε $f, g \in K(C)$ ισχύει η σχέση

$$d(f \cdot g) = f d(g) + g d(f).$$

1.71 Ορισμός. Έστω C μια ομαλή και ανάγωγη καμπύλη ορισμένη σε ένα σώμα K. Ο **χώρος των διαφορικών** της C υπέρ το K είναι ένας μονοδιάστατος $K(C)$-διανυσματικός χώρος, τον οποίο συμβολίζουμε με $\Omega_C(K)$. Υπάρχει μια μη-τετριμμένη παραγώγιση $d : K(C) \to \Omega_C(K)$ (δηλαδή η d είναι παραγώγιση και υπάρχει $f \in K(C)$ τέτοια ώστε $df \neq 0$). Τα στοιχεία του $\Omega_C(K)$ λέγονται **διαφορικά** της C.

Αφού ο $\Omega_C(K)$ είναι $K(C)$-διανυσματικός χώρος διάστασης 1 τότε για κάποιο $g \in K(C)$ με $dg \neq 0$, κάθε $\omega \in \Omega_C(K)$ γράφεται στη μορφή $\omega = f dg$ με μοναδικό τρόπο.

1.72 Πρόταση. *Αν $\omega, \omega' \in \Omega_C(K)$ με $\omega' \neq 0$ τότε υπάρχει μοναδική ρητή συνάρτηση $f \in K(C)$ τέτοια ώστε $\omega = f\omega'$. Γράφουμε $\frac{\omega}{\omega'} = f$.*

Απόδειξη. Έστω $\omega, \omega' \in \Omega_C(K)$ με $\omega' \neq 0$ και έστω ότι το σύνολο $\{dt\}$ αποτελεί $K(C)$-βάση του $\Omega_C(K)$. Τότε υπάρχουν $h_1, h_2 \in K(C)$ με $h_2 \neq 0$ τέτοια ώστε $\omega = h_1 dg$ και $\omega' = h_2 dg$, δηλαδή

$$dg = \frac{\omega}{h_1} \text{ και } dg = \frac{\omega'}{h_2}.$$

Έτσι, λαμβάνουμε $\frac{\omega}{\omega'} = \frac{h_1}{h_2}$, οπότε $\omega = \frac{h_1}{h_2}\omega'$. Θέτοντας $f = \frac{h_1}{h_2}$ έχουμε το ζητούμενο. ■

1.73 Ορισμός. Έστω $\omega \in \Omega_C(K)$ με $\omega \neq 0$ και έστω $P \in C(K)$. Έστω επίσης $t \in K(C)$ ένας uniformizer στο P. Τότε η $v_P(\omega) \coloneqq v_P(\frac{\omega}{dt})$ είναι η εκτίμηση του ω στο P και δεν εξαρτάται από την επιλογή του t. Η εκτίμηση αυτή είναι μη-μηδενική για πεπερασμένου πλήθους σημεία $P \in C(\bar{K})$.

Όπως και με τις ρητές συναρτήσεις, έτσι και με ένα μη-μηδενικό διαφορικό, μπορούμε να συσχετίσουμε έναν διαιρέτη. Ο διαιρέτης

$$\operatorname{div}(\omega) = \sum_{P \in C(\bar{K})} v_P(\omega) P \in \operatorname{Div}(C)$$

λέγεται **διαιρέτης του** ω.

Αν $v_P(\omega) \geq 0$ (ή $\omega = 0$) τότε λέμε ότι το ω είναι **ολόμορφο** στο P. Όταν το ω είναι ολόμορφο για κάθε $P \in C(\bar{K})$, το ω λέγεται **ολόμορφο διαφορικό**. Τον K**-διανυσματικό χώρο των ολόμορφων διαφορικών της** C, το συμβολίζουμε $\Omega_C^{\text{reg}}(K)$.

1.74 Πρόταση. *Έστω C μια ομαλή και ανάγωγη καμπύλη γένους g ορισμένη σε ένα σώμα K. Το σύνολο $\Omega_C^{\text{reg}}(K)$ είναι K-διανυσματικός χώρος διάστασης g.*

Στο κεφάλαιο V, θα αποδείξουμε την παραπάνω πρόταση ειδικά για υπερελλειπτικές καμπύλες.

Έστω $W = \operatorname{div}(\omega)$, $\omega \in \Omega_C(K)$. Ο W λέγεται **κανονικός διαιρέτης**. Αν ω' είναι ένα άλλο μη μηδενικό διαφορικό τότε $\omega' = f\omega$ για κάποια ρητή συνάρτηση $f \in K(C)$, άρα $\operatorname{div}(\omega') = \operatorname{div}(f) + \operatorname{div}(\omega)$, δηλαδή $\operatorname{div}(\omega') \equiv W$. Αντίστροφα, έστω $W' \in \operatorname{Div}(C)$ ένας άλλος διαιρέτης με $W' \equiv W$. Τότε για κάποια ρητή συνάρτηση f, έχουμε

$$W' = \operatorname{div}(f) + W = \operatorname{div}(f) + \operatorname{div}(\omega) = \operatorname{div}(f\omega)$$

άρα και ο W' είναι κανονικός διαιρέτης. Δηλαδή, όλοι οι κανονικοί διαιρέτες είναι μεταξύ τους ισοδύναμα και κάθε διαιρέτης που είναι ισοδύναμος με έναν κανονικό διαιρέτη, είναι και αυτός κανονικός. Αυτό σημαίνει ότι το σύνολο των κανονικών διαιρετών σχηματίζει μια κλάση. Αυτή την λέμε **κανονική κλάση**. Ένα στοιχείο αυτής της κλάσης λέγεται **κανονικός διαιρέτης**.

§8 Το Θεώρημα των Riemann-Roch

1.75 Θεώρημα. *(**Riemann-Roch.**) Έστω C μια ομαλή, προβολική καμπύλη ορισμένη σε ένα σώμα K και W ένας κανονικός διαιρέτης. Τότε υπάρχει $g \in \mathbb{Z}$ τέτοιο ώστε για κάθε $D \in \mathrm{Div}(C)$ να ισχύει*

$$\dim_K(\mathscr{L}(D)) = \deg(D) + 1 - g + \dim_K(\mathscr{L}(W - D)).$$

1.76 Πόρισμα. *Ο αριθμός g ορίζεται μονοσήμαντα από την καμπύλη και ισχύει $g \geq 0$.*

Απόδειξη. Έστω διαιρέτης D με $\deg(D) > \deg(W)$. Από το (1) της Πρότασης 1.65, $\mathscr{L}(W - D) = \{0\}$, οπότε $\dim_K(\mathscr{L}(W - D)) = 0$. Από το Θεώρημα Riemann-Roch, $\dim_K(\mathscr{L}(D)) = \deg(D) + 1 - g$, οπότε ο αριθμός $g = \deg(D) + 1 - \dim_K(\mathscr{L}(D))$ ορίζεται μονοσήμαντα. ■

1.77 Ορισμός. Ο αριθμός $g \in \mathbb{N}_0$ παραπάνω λέγεται **γένος** της καμπύλης.

1.78 Πόρισμα. *Ισχύει $\dim_K(\mathscr{L}(W)) = g$ και $\deg(W) = 2g - 2$.*

Απόδειξη. Έστω $D = 0$. Από το (4) της Πρότασης 1.65, $\dim_K(\mathscr{L}(D)) = 0$. Από το Θεώρημα Riemann-Roch 1.75,

$$g = \dim_K(W) \geq 0.$$

Έστω $D = W$. Τότε $\dim_K(W) = \deg(W) + 1 - g + \dim_K(\mathscr{L}(0))$, δηλαδή $\deg(W) = \dim_K(\mathscr{L}(W)) - 1 + g - \dim_K(\mathscr{L}(0))$. Αντικαθιστώντας $\dim_K(W) = g$ και $\dim_K(\mathscr{L}(0)) = 1$, παίρνουμε $\deg(W) = 2g - 2$ ■

1.79 Πρόταση. *Έστω C μια ομαλή, προβολική καμπύλη ορισμένη σε ένα σώμα K γένους g και $D \in \mathrm{Div}(C)$ με $\deg(D) > 2g - 2$. Τότε, $\dim_K(\mathscr{L}(D)) = \deg(D) - g + 1$.*

Απόδειξη. Είναι

$$\deg(W - D) = \deg(W) - \deg(D) = 2g - 2 - \deg(D) < 0,$$

άρα από το (1) της πρότασης 1.65, $\dim_K(W - D) = 0$ και συνεπώς από το Θεώρημα Riemann-Roch, $\dim_K(\mathscr{L}(D)) = \deg(D) - g + 1$. ■

1.80 Πρόταση. *Αν $\deg(D) \geq 2g$ τότε $\dim_K(\mathscr{L}(D - P)) = \dim_K(\mathscr{L}(D)) - 1$ για κάθε σημείο $P \in C(K)$.*

Απόδειξη. Αφού $\deg(D) \geq 2g > 2g-2$, από την προηγούμενη πρόταση,

$$\dim_K(\mathscr{L}(D)) = \deg(D) + 1 - g.$$

Επίσης, $\deg(D-P) = \deg(D) - 1 \geq 2g - 1 > 2g - 2$ άρα πάλι από την προηγούμενη πρόταση,

$$\begin{aligned}\dim_K(\mathscr{L}(D-P)) &= \deg(D-P) + 1 - g \\ &= (\deg(D) + 1 - g) - \deg(P) \\ &= \dim_K(\mathscr{L}(D)) - 1\end{aligned}$$

1.81 Πρόταση. *Έστω C μία ομαλή, προβολική και απολύτως ανάγωγη καμπύλη γένους $g > 0$ ορισμένη σε ένα σώμα K. Έστω επίσης $P_0 \in C(K)$. Τότε η απεικόνιση $i : C \to J$ με $i(P) = [P - P_0]$ είναι 1-1.*

Απόδειξη. Ας υποθέσουμε ότι $g > 0$ και ότι η απεικόνιση i δεν είναι 1-1. Τότε υπάρχουν δύο σημεία $P_1, P_2 \in C(\bar{K})$ με $P_1 \neq P_2$ τέτοια ώστε $i(P_1) = i(P_2)$, δηλαδή $[P_1 - P_0] = [P_2 - P_0]$. Αυτό σημαίνει ότι $[P_1 - P_2] = 0$, οπότε υπάρχει ρητή συνάρτηση $\phi \in \bar{K}(C)^*$ τέτοια ώστε

$$\operatorname{div}(\phi) = P_1 - P_2 \ \ (1).$$

Η ϕ έχει ρίζα στο P_1 και πόλο στο P_2, επομένως δεν είναι σταθερή. Από την (1),

$$\operatorname{div}(\phi) + P_2 = P_1 \geq 0,$$

που σημαίνει ότι $\phi \in L(P_2)$. Η ϕ^n έχει πόλο τάξης n στο P_2, επομένως

$$\langle 1, \phi, \phi^2, ..., \phi^n \rangle \subseteq L(nP_2)$$

και ιδιαίτερα,

$$\dim_K(L(nP_2)) \geq n + 1.$$

Όμως για $n > 2g - 2$, από την Πρόταση 1.79 έχουμε ότι

$$\dim_K(L(nP_2)) = n + 1 - g.$$

Συνδυάζοντας τις δύο τελευταίες σχέσεις, παίρνουμε $g = 0$ που είναι άτοπο. ■

1.82 Πρόταση. *Έστω C μια ομαλή, προβολική καμπύλη ορισμένη σε ένα σώμα K γένους g και έστω $P \in C(K)$. Τότε για κάθε $n \geq 2g$, υπάρχει $f \in K(C)$ τέτοια ώστε* $\operatorname{div}(f)_\infty = nP$.

Απόδειξη. Έστω $D = (n-1)P$. Έχουμε

$$\deg((n-1)P) = n - 1 \geq 2g - 1 > 2g - 2,$$

άρα από την Πρόταση 1.79,

$$\dim_K(\mathscr{L}(D)) = \deg(D) + 1 - g = n - 1 + 1 - g = n - g. \quad (1)$$

Όμοια, αν $D' = nP$ τότε $\deg(D') = n > 2g-2$, άρα πάλι από την Πρόταση 1.79 έχουμε

$$\dim_K(\mathscr{L}(D')) = \deg(D') + 1 - g = n + 1 - g. \quad (2).$$

Από τις (1) και (2), $\dim_K(\mathscr{L}(D')) \geq \dim_K(\mathscr{L}(D))$ που σημαίνει ότι $\mathscr{L}(D) \subsetneq \mathscr{L}(D')$, δηλαδή

$$\mathscr{L}((n-1)P) \subsetneq \mathscr{L}(nP).$$

Επομένως, υπάρχει ρητή συνάρτηση $f \in \mathscr{L}(nP) \setminus \mathscr{L}((n-1)P)$.

Το $f \in \mathscr{L}(nP)$ σημαίνει ότι $\mathrm{div}(f) \geq -nP$ και αφού $-n < 0$, η f έχει πόλο στο P τάξης το πολύ n.

Από την άλλη, το $f \notin \mathscr{L}((n-1)P)$, σημαίνει ότι $\mathrm{div}(f) < -(n-1)P$, ισοδύναμα $-\mathrm{div}(f) > (n-1)P$, ισοδύναμα $\mathrm{div}\left(\frac{1}{f}\right) > (n-1)P$, άρα η $\frac{1}{f}$ έχει ρίζα στο P τάξης μεγαλύτερης του $n-1$, άρα η f έχει πόλο στο P τάξης μεγαλύτερης του $n-1$.

Συμπεραίνουμε λοιπόν ότι η f έχει πόλο μόνο στο P, τάξης ακριβώς n, δηλαδή $\mathrm{div}(f)_\infty = nP$. ■

1.83 Ορισμός. Έστω $P \in C(K)$. Ο φυσικός αριθμός $n \geq 0$ θα λέγεται **αριθμός πόλου** όταν υπάρχει $f \in K(C)$ τέτοια ώστε $\mathrm{div}(f)_\infty = nP$. Αν δεν υπάρχει τέτοιος αριθμός, λέγεται **τρυπάριθμος** (gap number).

Από την Πρόταση 1.82, προκύπτει ότι κάθε φυσικός αριθμός $n \geq 2g(C)$ είναι αριθμός πόλου. Όμως τι συμβαίνει αν $n < 2g(C)$; Ισχύει το ακόλουθο θεώρημα:

1.84 Θεώρημα. *Έστω C αφινική αλγεβρική καμπύλη γένους g ορισμένη σε ένα σώμα K και $P \in C(K)$. Τότε υπάρχουν ακριβώς g τρυπάριθμοι $i_1 = 1, ..., i_g \leq 2g-1$ του σημείου P. Αν το σώμα K είναι αλγεβρικά κλειστό τότε για σχεδόν όλα τα σημεία $P \in C(K)$ έχουμε την ίδια ακριβώς ακολουθία τρυπαρίθμων.*

Αυτά τα σημεία λέγονται **κανονικά** (ordinary). Κάθε μη κανονικό σημείο $P \in C(K)$ λέγεται **σημείο Weierstrass** της C. Αποδεικνύεται ότι αν μία καμπύλη έχει γένος $g \geq 2$ τότε υπάρχει τουλάχιστον ένα σημείο του Weierstrass στην καμπύλη.

§9 Καμπύλες γένους 0

1.85 Πρόταση. *Έστω $C : F(X,Y) = 0$ μια ομαλή και προβολική καμπύλη ορισμένη σε ένα σώμα, όπου $\deg(F) = n$. Τότε για το γένος g της καμπύλης ισχύει ο τύπος*

$$g = \frac{(n-1)(n-2)}{2}.$$

1.86 Ορισμός. Έστω K ένα σώμα. Ένας K-διανυσματικός χώρος A θα λέγεται **K-άλγεβρα** όταν είναι ορισμένη και η πράξη του πολλαπλασιασμού στον A τέτοια ώστε ο A να είναι και δακτύλιος ως προς τις πράξεις της πρόσθεσης και του πολλαπλασιασμού και να ισχύει

$$(la)b = a(lb) = l(ab)$$

για κάθε $l \in K$ και $a, b \in A$.

Έστω K ένα αλγεβρικά κλειστό σώμα και $C : f(X, Y) = 0$, όπου $f(X, Y) \in K[X, Y]$ με $\deg(f) = n$, μία ανάγωγη προβολική καμπύλη γένους g ορισμένη σε ένα αλγεβρικά κλειστό σώμα K. Από τον τύπο του γένους της Πρότασης 1.85, προκύπτει ότι αν $g = 0$ τότε $n = 1$ ή $n = 2$ και ότι αν $\deg(f) = 1$ ή 2 τότε $g = 0$. Δηλαδή, $g = 0$ αν και μόνο αν $\deg(f) = 1$ ή 2.

1.87 Θεώρημα. *Έστω C μια προβολική ομαλή καμπύλη ορισμένη σε ένα αλγεβρικά κλειστό σώμα K. Τα επόμενα είναι ισοδύναμα:*

1. *Η C είναι γένους 0.*
2. *$K(C) \cong K(\mathbb{P}^1(K))$ (ως K-άλγεβρες).*
3. *$K(C) \cong K(X)$ (σώμα ρητών συναρτήσεων μιας μεταβλητής με συντελεστές από το K).*

Απόδειξη. Αφού η $\mathbb{P}^1(K)$ είναι ευθεία, είναι $\deg(F) = 1$, οπότε το γένος της καμπύλης $\mathbb{P}^1(K)$ είναι 0. Επομένως αρκεί να δείξουμε την ισοδυναμία (1) $\Leftrightarrow$ (3).

Υποθέτουμε ότι $K(C) \cong K(X)$ και θα δείξουμε ότι $g = 0$. Θεωρούμε τον διαιρέτη $P_\infty = \mathrm{div}(X)_\infty$. Έστω $r \geq 0$. Θεωρούμε τον χώρο $\mathscr{L}(rP_\infty)$. Σε αυτόν τον χώρο, οι συναρτήσεις $1, X, ..., X^r$ είναι K-γραμμικά ανεξάρτητες άρα $r + 1 \leq \dim_K(\mathscr{L}(rP_\infty))$. Αν επιλέξουμε το r έτσι ώστε $\deg(D) = r \geq 2g - 2$ τότε

$$r + 1 \leq \dim_K(\mathscr{L}(rP_\infty)) = \deg(rP_\infty) + 1 - g,$$

άρα $g \leq 0$. Όμως $g \geq 0$ οπότε τελικά $g = 0$.

Υποθέτουμε ότι $g = 0$. Έστω $P \in C$ και $D = P$, οπότε $\deg(D) = 1$. Επειδή $\deg(D) = 1 \geq 2 \cdot 0 - 2 \geq -2$ έπεται $\dim_K(\mathscr{L}(D)) = \deg(D) + 1 - g = 2$. Συνεπώς $\mathscr{L}(D) \neq \{0\}$ και έχει διάσταση 2, άρα $D \equiv D'$ για κάποιον effective διαιρέτη $D' \geq 0$ (διότι αν $\phi \in \mathscr{L}(D)$ τότε $D + \mathrm{div}(\phi) \geq 0$ και παίρνουμε $D' = D + \mathrm{div}(\phi)$). Επομένως, $D' \geq 0$ και αφού $D' \equiv D$, έπεται $\mathscr{L}(D') \cong \mathscr{L}(D)$, οπότε $\dim_K(\mathscr{L}(D')) = 2$, άρα υπάρχει $f \in \mathscr{L}(D') \setminus K$ με $\mathrm{div}(f) \neq 0$ και $\mathrm{div}(f) + D' \geq 0$. Επομένως έχουμε $D' \geq 0$, $\mathrm{div}(f) + D' \geq 0$ και $\deg(D') = \dim_K(\mathscr{L}(D')) + g - 1 = 1$. Αυτό όμως είναι δυνατόν μόνο όταν $D' = \mathrm{div}(f)_\infty$, οπότε

$$[K(C) : K(f)] = \deg(\mathrm{div}(f)_\infty) = \deg(D') = 1,$$

και τελικά, $K(X) = K(f)$.

■

1.88 Σημείωση. Αν το σώμα δεν είναι αλγεβρικά κλειστό τότε ισχύει ότι $K(C) \cong K(X)$ αν και μόνο αν $g = 0$ και υπάρχει $D \in \mathrm{Div}(C)$ τέτοιο ώστε $\deg(D) = 1$. Το τελευταίο μεταφράζεται ως ύπαρξη ρητού σημείου. Αν το K δεν είναι αλγεβρικά κλειστό τότε ένα «σημείο» μπορεί να έχει βαθμό μεγαλύτερο του 1.

§10 Καμπύλες γένους 1

1.89 Ορισμός. Έστω $C : F(X, Y) = 0$ μια ανάγωγη, ομαλή προβολική καμπύλη ορισμένη σε ένα σώμα K. Η C θα λέγεται **ελλειπτική καμπύλη** αν έχει γένος $g = 1$ και υπάρχει $P \in C$ τέτοιο ώστε $\deg(P) = 1$.

1.90 Σημείωση. Θα υποθέτουμε ότι το K είναι αλγεβρικά κλειστό, οπότε κάθε σημείο P θα έχει βαθμό 1.

1.91 Θεώρημα. *Η καμπύλη C είναι ελλειπτική αν και μόνο αν υπάρχουν $X, Y \in K(C)$ τέτοια ώστε:*

1. $K(C) = K(X, Y)$.
2. $[K(C) : K(X)] = 2$.
3. $Y^2 = f(X)$ *όπου* $f(X) \in K[X]$ *με* $\deg(f(X)) = 3$ *και το* $f(X)$ *έχει μόνο απλές ρίζες.*

Απόδειξη. Έστω $P \in C$ και $D = P$. Είναι $\deg(D) = \deg(P) = 1$ και

$$\deg(D) = 1 > 2g - 2.$$

Άρα $\dim_K(\mathscr{L}(P)) = 1 - g + \deg(P) = 1$, άρα $\mathscr{L}(P) = K$. Επίσης, $\dim_K(\mathscr{L}(P)) = \deg(2P) + 1 - g = 2$. Άρα μια βάση του $\mathscr{L}(2P)$ είναι το σύνολο $\{1, X\}$ όπου $X \in \mathscr{L}(2P) \setminus \mathscr{L}(P)$ (δηλαδή $2P = \mathrm{div}(X)_\infty$). Συνεχίζουμε όμοια. Ο $\mathscr{L}(3P)$ έχει διάσταση 3, άρα $\mathscr{L}(3P) \supsetneq \mathscr{L}(2P)$ και έχει K-βάση το σύνολο $\{1, X, Y\}$ όπου $Y \in \mathscr{L}(3P) \setminus \mathscr{L}(2P)$ και $\mathrm{div}(Y)_\infty = 3P$.

Είναι $\dim \mathscr{L}(4P) = 4$, άρα $\mathscr{L}(4P) \supsetneq \mathscr{L}(3P)$ και ο $\mathscr{L}(4P)$ έχει βάση $\{1, X, Y, X^2\}$ με $X^2 \in \mathscr{L}(4P)$ (το X έχει πόλο τάξης 2 στο P άρα το X^2 έχει πόλο τάξης 4 στο $4P$).

Είναι $\dim \mathscr{L}(5P) = 5$ και ο $\mathscr{L}(5P) = 5$ έχει βάση το $\{1, X, Y, X^2, XY\}$ με $XY \in \mathscr{L}(5P)$ ($XY \in \mathscr{L}(5P)$ διότι το X έχει πόλο τάξης 2 στο P και το Y έχει πόλο τάξης 3 στο P, άρα η συνάρτηση XY έχει πόλο τάξης 5 στο P).

Όμοια, $\dim_K(\mathscr{L}(6P)) = 6$ και $X^3, Y^2 \in \mathscr{L}(6P)$, άρα ο $\mathscr{L}(6P)$ έχει βάση το

$$\{1, X, Y, X^2, XY, X^3\}$$

ή το $\{1, X, Y, X^2, XY, Y^2\}$. Επομένως, το σύνολο $\{1, X, Y, X^2, XY, X^3, Y^2\}$ είναι K-γραμμικώς εξαρτημένο.

Άρα έχουμε $a_{-1}Y^2+a_1XY+a_3Y = a_0X^3+a_2X^2+a_4X+a_6$ με $a_i \in K$ και $a_{-1}a_0 \neq 0$ (αν ήταν $a_{-1}a_0 = 0$ τότε θα είχαμε $a_{-1} = a_0 = 0$ και το σύνολο $\{1, X, Y, X^2, XY\}$ θα ήταν γραμμικώς εξαρτημένο που είναι άτοπο). Πολλαπλασιάζοντας και τα δύο μέλη με $a_{-1}^3a_0^2$ παίρνουμε

$$(a_{-1}^2a_0Y)^2+a_1a_{-1}^3a_0^2XY+a_3a_{-1}a_0^2Y = (a_{-1}a_0X)^3+a_2a_{-1}^3a_0^2X^2+a_4a_{-1}^3a_0^2X^2+a_6a_{-1}^3a_0^2.$$

Κάνοντας την αντικατάσταση $X \leftarrow a_{-1}a_0X$ και $Y \leftarrow a_{-1}^2a_0Y$ παίρνουμε μια εξίσωση της μορφής

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

με $a_i \in K$. Αν $\mathrm{ch}K \neq 2$ τότε μέσω της αντικατάστασης $Y \leftarrow Y - \frac{1}{2}(a_1X + a_3)$ παίρνουμε μια εξίσωση της μορφής

$$Y^2 = X^3 + b_2X^2 + b_4X + b_6$$

με $b_i \in K$. Τέλος, αν $\mathrm{ch}K \neq 3$ τότε με την αντικατάσταση $X \leftarrow X - \frac{1}{3}b_2$ παίρνουμε

$$Y^2 = X^3 + g_2X + g_3$$

για κάποια $g_2, g_3 \in K$.

Επιπλέον,

$$[K(X,Y) : K(X)] = \deg(\mathrm{div}(X)_\infty) = \deg(2P) = 2.$$

Αν το $f(X) = X^3 + g_2X + g_3$ είχε πολλαπλή ρίζα, έστω α τότε θα είχαμε

$$f(X) = (X - \alpha)^2(X - \beta)$$

για κάποιο $\beta \in K$. Η αντικατάσταση $Y \leftarrow Y(X - \alpha)$ θα έδινε $Y^2(X - \alpha)^2 = (X - \alpha^2)(X - \beta)$, δηλαδή $Y^2 = X - \beta$ που θα σήμαινε ότι $K(X,Y) = K(X)$, οπότε $g = 0$, άτοπο. Άρα το $f(X)$ έχει μόνο απλές ρίζες.

Το αντίστροφο όταν το K είναι αλγεβρικά κλειστό είναι προφανές. Αφού το $f(X)$ έχει μόνο απλές ρίζες (που σημαίνει ότι η καμπύλη είναι ομαλή), από την Πρόταση 1.85,

$$g = \frac{(3-1)(3-2)}{2} = 1$$

■

1.92 Ορισμός. Έστω C μια κυβική καμπύλη. Αν η C έχει εξίσωση της μορφής

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

λέμε ότι η C έχει τη **μορφή του Weierstrass**. Η προβολική εξίσωση είναι η

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

Για $Z = 0$ παίρνουμε $X^3 = 0$, οπότε αν $\mathrm{ch}(K) = 0$, $X = 0$. Άρα το επ΄άπειρον σημείο της καμπύλης σε αυτήν την περίπτωση είναι το $[0, 1, 0]$.

Κεφάλαιο II

p-αδικοί αριθμοί και το τοπικό-γενικό αξίωμα

Ως γνωστό, το σώμα των πραγματικών αριθμών $\mathbb{R}$ είναι η πλήρωση του σώματος των ρητών αριθμών $\mathbb{Q}$ ως προς την μετρική που ορίζει η απόλυτη τιμή. Στις αρχές του $20^{ου}$ αιώνα, ο Kurt Hensel, αναρωτήθηκε για την ύπαρξη και άλλων πληρώσεων του $\mathbb{Q}$ ως προς κάποια άλλη μετρική και απέδειξε ότι για κάθε πρώτο αριθμό p, υπάρχει μία μετρική, και οι μετρικές αυτές για $p, q \in \mathbb{P}$ με $p \neq q$ δεν είναι ισοδύναμες. Η πλήρωση του $\mathbb{Q}$ ως προς μία p-αδική μετρική λέγεται σώμα των p-αδικών αριθμών. Πρόκειται για μία εξόχως εξαιρετική ιδέα με σημαντικότατες εφαρμογές στη Θεωρία Αριθμών.

Για μία εκτενέστερη μελέτη της θεωρίας των p-αδικών αριθμών, παραπέμπουμε τον ενδιαφερόμενο αναγνώστη σε κάποιο από τα βιβλία [1], [12], [17], [18], [24], [25] ή [28].

§1 Βασικά στοιχεία των p-αδικών αριθμών

2.1 Ορισμός. Έστω K σώμα. Μία **απόλυτη τιμή** στο K είναι μια απεικόνιση

$$\begin{aligned} K &\to [0, +\infty) \\ x &\mapsto |x|, \end{aligned}$$

η οποία για όλα τα $a, b \in K$ ικανοποιεί τις ακόλουθες ιδιότητες:

1. $|a| = 0 \Leftrightarrow a = 0$.
2. $|a \cdot b| = |a| \cdot |b|$.
3. $|a + b| \leq |a| + |b|$.

Μία απόλυτη τιμή με τις παραπάνω ιδιότητες λέγεται **αρχιμήδεια απόλυτη τιμή**. Αν αντικαταστήσουμε την συνθήκη (3) με την ισχυρότερη $|a+b| \leq \max\{|a|, |b|\}$ τότε η απόλυτη τιμή που προκύπτει λέγεται **μη-αρχιμήδεια απόλυτη τιμή**.

Δύο απόλυτες τιμές $|\cdot|_1$ και $|\cdot|_2$ ενός σώματος K λέγονται **ισοδύναμες** αν υπάρχει $\alpha \in (0, +\infty)$ τέτοιο ώστε $|a|_1 = |a|_2^{\alpha}$ για κάθε $a \in K$.

2.2 Παράδειγμα. Η συνηθισμένη απόλυτη τιμή είναι αρχιμήδεια απόλυτη τιμή στα σώματα $\mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$.

2.3 Παράδειγμα. Αν $v : K \to \mathbb{Z} \cup \{\infty\}$ είναι μια διακριτή εκτίμηση τότε λαμβάνουμε μία μη-αρχιμήδεια απόλυτη τιμή $|\cdot|_v$ θέτοντας

$$|a|_v = \begin{cases} 0, & \text{αν } a = 0 \\ c^{v(a)} & \text{αν } a \neq 0 \end{cases}$$

για κάποιο $c \in (0,1)$.

Οι κλάσεις ισοδυναμίας της $|\cdot|_v$ δεν εξαρτώνται από την επιλογή του c.

Έστω $v_p : \mathbb{Q} \to \mathbb{Z}$ με $p \in \mathbb{P}$ η **p-αδική εκτίμηση** (βλ. και Παράδειγμα 1.12), δηλαδή όπου αν $a \in \mathbb{Q}$ τότε ορίζουμε $v_p(a) = \infty$ αν $a = 0$ και αν $a \neq 0$ και $a = \dfrac{a}{b}p^n$ με $b \neq 0$ και $p \nmid a, b$ τότε $v_p(a) = n$.

Για $v = v_p$ και $c = p^{-1}$, λαμβάνουμε μία μη-αρχιμήδεια απόλυτη τιμή, την p-αδική απόλυτη τιμή:

2.4 Ορισμός. Έστω $p \in \mathbb{P}$ και v_p η p-αδική εκτίμηση στο $\mathbb{Q}$. Η **p-αδική απόλυτη τιμή** στο $\mathbb{Q}$ ορίζεται ως

$$|a|_p = \begin{cases} 0, & \text{αν } a = 0 \\ p^{-v_p(a)} & \text{αν } a \neq 0 \end{cases}$$

Τη συνηθισμένη απόλυτη τιμή την συμβολίζουμε συνήθως με $|\cdot|_\infty$.

2.5 Λήμμα. ***(product formula.)*** *Έστω $a \in \mathbb{Q}^*$. Τότε*

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |a|_p = 1.$$

Απόδειξη. Έστω $a \in \mathbb{Z}_+$ και $a = p_1^{b_1} \cdots p_s^{b_s}$, $p_i \in \mathbb{P}, b_i \in \mathbb{N}$ η ανάλυσή του σε γινόμενο πρώτων παραγόντων. Για κάθε $q \in \mathbb{P} \setminus \{p_1, ..., p_s\}$ ισχύει ότι $|a|_q = 1$. Για τα $p_1, ..., p_s$ ισχύει ότι $|a|_{p_i} = p^{-b_i}$ για $i = 1, ..., s$ και επιπλέον, $|a|_\infty = p_1^{b_1} \cdots p_s^{b_s}$. Άρα καταλήξαμε στο συμπέρασμα για $a \in \mathbb{Z}_+$.

Έστω τώρα $a \in \mathbb{Q}$ με $a = \varepsilon \dfrac{a_1}{a_2}$, $a_1, a_2 \in \mathbb{Z}_+$, $a_2 \neq 0$, $\varepsilon = \pm 1$. Τότε,

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |a|_p = \prod_{p \in \mathbb{P} \cup \{\infty\}} \left| \varepsilon \frac{a_1}{a_2} \right|_p = \prod_{p \in \mathbb{P} \cup \{\infty\}} \frac{|a_1|_p}{|a_2|_p} = \frac{\displaystyle\prod_{p \in \mathbb{P} \cup \{\infty\}} |a_1|_p}{\displaystyle\prod_{p \in \mathbb{P} \cup \{\infty\}} |a_2|_p} = 1.$$

■

Ένας τρόπος να κατασκευάσουμε το $\mathbb{R}$ από το $\mathbb{Q}$ είναι ο εξής: Θεωρούμε το σύνολο ακολουθιών

$$\Omega = \{\{a_n\}_{n\in\mathbb{N}} : \{a_n\}_{n\in\mathbb{N}} \text{ ακολουθία Cauchy ρητών αριθμών}\}$$

και ορίζουμε τις πράξεις $\oplus$ και $\odot$ με

$$\{a_n\} \oplus \{b_n\} = \{a_n + b_n\}$$

και

$$\{a_n\} \odot \{b_n\} = \{a_n b_n\}.$$

Η τριάδα $(\Omega, \oplus, \odot)$ αποτελεί αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο. Επιπλέον, θεωρούμε το σύνολο

$$M = \{\{a_n\}_{n\in\mathbb{N}} : \{a_n\}_{n\in\mathbb{N}} \text{ μηδενική ακολουθία Cauchy ρητών αριθμών}\}.$$

Το $(M, \oplus, \odot)$ είναι maximal ιδεώδες του $(\Omega, \oplus, \odot)$. Έπεται ότι ο δακτύλιος πηλίκο Ω/M είναι σώμα. Το ονομάζουμε σώμα των πραγματικών αριθμών και το συμβολίζουμε $\mathbb{R}$.

Η παραπάνω κατασκευή μπορεί να γίνει χρησιμοποιώντας οποιαδήποτε απόλυτη τιμή σε ένα σώμα K, και παράγει την **πλήρωση** του K ως προς την απόλυτη τιμή και περιέχει το K ως πυκνό υποσύνολό του. Εφαρμόζουμε αυτήν την διαδικασία στο $\mathbb{Q}$ ως προς την p-αδική απόλυτη τιμή.

2.6 Ορισμός. Η πλήρωση του $\mathbb{Q}$ ως προς την p-αδική απόλυτη τιμή είναι το **σώμα $\mathbb{Q}_p$ των p-αδικών αριθμών**. Η κλειστότητα του $\mathbb{Z}$ στο $\mathbb{Q}_p$ είναι ο **δακτύλιος $\mathbb{Z}_p$ των p-αδικών ακεραίων**. Την πλήρωση του $\mathbb{Q}$ ως προς την συνηθισμένη απόλυτη τιμή τη συμβολίζουμε $\mathbb{Q}_\infty := \mathbb{R}$.

Η p-αδική εκτίμηση v_p και η p-αδική απόλυτη τιμή $|\cdot|_p$ επεκτείνονται στο $\mathbb{Q}_p$. Η απόλυτη τιμή ορίζει μια μετρική και συνεπώς μια τοπολογία στο $\mathbb{Q}_p$. Η κλειστή μοναδιαία μπάλα είναι το

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : v_p(a) \geq 0\} = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}.$$

Ο δακτύλιος $\mathbb{Z}_p$ είναι δακτύλιος διακριτής εκτίμησης με διακριτή εκτίμηση την v_p. Το σύνολο των μονάδων είναι το $\{a \in \mathbb{Z}_p : v_p(a) = 0\}$ ενώ το maximal ιδεώδες είναι το $p\mathbb{Z}_p = \{a \in \mathbb{Z}_p : v_p(a) \geq 1\}$. Το **σώμα υπολοίπων (residue field)** είναι το $\mathbb{Z}_p/p\mathbb{Z}_p$ και ισχύει

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

Τον ομομορφισμό αναγωγής $\mathbb{Z}_p \to \mathbb{F}_p$ τον γράφουμε $a \mapsto \bar{a}$. Κάθε $a \in \mathbb{Z}_p$ γράφεται στη μορφή

$$a = \sum_{i=k}^{\infty} a_i p^i$$

όπου $a_i \in \mathbb{F}_p$ και $k \in \mathbb{N}_0$, ενώ κάθε $a \in \mathbb{Q}_p$ γράφεται στη μορφή

$$a = \sum_{i=k}^{\infty} a_i p^i$$

όπου $a_i \in \mathbb{F}_p$ και $k \in \mathbb{Z}$. Γενικότερα, κάθε δυναμοσειρά με συντελεστές στο $\mathbb{Z}_p$ συγκλίνει σε κάποιο στοιχείο του $p\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p < 1\}$. Αυτό είναι συνέπεια του ακόλουθου λήμματος.

2.7 Λήμμα. *Έστω $\{a_n\}_{n\in\mathbb{N}}$ μία ακολουθία στοιχείων του $\mathbb{Q}_p$. Τότε η σειρά $\sum_{n=0}^{\infty} a_n$ συγκλίνει στο $\mathbb{Q}_p$ αν και μόνο αν $a_n \to 0$ καθώς $n \to \infty$.*

Απόδειξη. Έστω ότι η σειρά συγκλίνει, $S_n = \sum_{m=0}^{n} a_m$ η σειρά των μερικών αθροισμάτων και ότι η σειρά συγκλίνει στο l. Τότε $a_n = S_n - S_{n-1}$, οπότε $a_n \to l - l = 0$. Το ενδιαφέρον επικεντρώνεται στην αντίστροφη κατεύθυνση.

Έστω ότι $a_n \to 0$ καθώς $n \to \infty$. Αυτό σημαίνει ότι για κάθε $\varepsilon > 0$, υπάρχει $N \geq 0$ τέτοιο ώστε $|a_n|_p < \varepsilon$ για κάθε $n \geq N$. Αφού η p-αδική απόλυτη τιμή είναι μη αρχιμήδεια, έχουμε

$$|S_{n+m} - S_n|_p = \left| \sum_{k=n+1}^{n+m} a_k \right|_p \leq \max\{|a_k|_p : n+1 \leq k \leq n+m\} \leq \varepsilon.$$

Συνεπώς, η ακολουθία των μερικών αθροισμάτων $\{S_n\}_{n\in\mathbb{N}}$ είναι Cauchy και συνεπώς συγκλίνει στο $\mathbb{Z}_p$ (διότι ο $\mathbb{Q}_p$ είναι πλήρης). ■

Αν λοιπόν θεωρήσουμε μια δυναμοσειρά $\sum_{n=0}^{\infty} a_n x^n$ με $a_n \in \mathbb{Z}_p$ (που σημαίνει ότι $|a_n| \leq 1$ για κάθε $\in \mathbb{N}$), τότε αν $|x|_p < 1$ έχουμε

$$|a_n x^n|_p = |a_n|_p \cdot |x|_p^n \leq |x|_p^n \to 0,$$

δηλαδή $|a_n x^n| \to 0$. Συνεπώς από το προηγούμενο Λήμμα 2.7, η δυναμοσειρά $\sum_{n=0}^{\infty} a_n x^n$ συγκλίνει στο $\mathbb{Q}_p$. Ιδιαίτερα, η δυναμοσειρά $\sum_{n=0}^{\infty} a_n p^n$ συγκλίνει στο $\mathbb{Q}_p$: Αν θέσουμε $x = p$ τότε $|p|_p = \dfrac{1}{p} < 1$, οπότε η δυναμοσειρά συγκλίνει. Επίσης, παρατηρούμε ότι

$$\left| \sum_{n=0}^{\infty} a_n p^n \right| \leq \max\{|a_n p^n| : n \in \mathbb{N}\} < 1,$$

διότι $|a_n p^n| < 1$ για κάθε $n \in \mathbb{N}_0$, που σημαίνει ότι η σειρά συγκλίνει στο $p\mathbb{Z}_p$.

§2 Το Λήμμα του Hensel

Σε αυτήν την παράγραφο, θα διατυπώσουμε και θα αποδείξουμε τρεις μορφές του Λήμματος του Hensel. Οι δύο πρώτες δίνουν τις απαραίτητες συνθήκες ώστε μία

ρίζα ενός πολυωνύμου στο $\mathbb{F}_p$ να ανάγεται σε ρίζα στο $\mathbb{Z}_p$, ενώ η τελευταία αφορά το πότε μπορούμε να αναγάγουμε την παραγοντοποίηση ενός πολυωνύμου στο $\mathbb{F}_p$ σε παραγοντοποίηση στο $\mathbb{Z}_p$. Ξεκινάμε με την απόδειξη ενός απλού τεχνικού λήμματος.

2.8 Λήμμα. *Έστω $f(X) \in \mathbb{Z}_p[X]$. Τότε $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$ για κάποιο $g(X,Y) \in \mathbb{Z}_p[X]$.*

Απόδειξη. Γράφουμε $f(X) = \sum_{i=0}^{n} a_i X^i$, οπότε

$$f(X+Y) = \sum_{i=0}^{n} a_i (X+Y)^i = a_0 + \sum_{i=1}^{n} a_i (X+Y)^i.$$

Από το διωνυμικό θεώρημα,

$$\begin{aligned}(X+Y)^i &= \sum_{j=0}^{i} \binom{i}{j} Y^j X^{i-j} \\ &= X^i + iYX^{i-1} + \sum_{j=2}^{i} Y^j X^{i-j} \\ &= X^i + iYX^{i-1} + Y^2 \sum_{j=2}^{i} \binom{i}{j} Y^{j-2} X^{i-j}.\end{aligned}$$

Θέτουμε $g_i(X,Y) = \sum_{j=2}^{i} \binom{i}{j} Y^{j-2} X^{i-j}$. Έτσι,

$$\begin{aligned}f(X+Y) &= a_0 + \sum_{i=1}^{n} a_i (X^i + iYX^{i-1} + Y^2 g_i(X,Y)) \\ &= \sum_{i=0}^{n} a_i X^i + Y \sum_{i=1}^{n} iX^{i-1} + Y^2 \sum_{i=1}^{n} g_i(X,Y) \\ &= f(X) + Yf'(X) + g(X,Y)Y^2\end{aligned}$$

όπου θέσαμε $g(X,Y) = \sum_{i=1}^{n} g_i(X,Y)$.

■

2.9 Θεώρημα. ***(Λήμμα του Hensel.)*** *Έστω $f(X) \in \mathbb{Z}_p[X]$ και $a \in \mathbb{Z}_p$ για τα οποία*

$$f(a) \equiv 0 \mod p \text{ και } f'(a) \not\equiv 0 \mod p.$$

Τότε υπάρχει μοναδικό $\alpha \in \mathbb{Z}_p$ τέτοιο ώστε $f(\alpha) = 0$ και $\alpha \equiv a \mod p$.

Απόδειξη. Θα δείξουμε με επαγωγή ότι για κάθε $n \geq 1$, υπάρχει $a_n \in \mathbb{Z}_p$ τέτοιο ώστε $f(a_n) \equiv 0 \mod p^n$ και $a_n \equiv a \mod p$. Η περίπτωση $n = 1$ είναι τετριμμένη: αρκεί να πάρουμε $a_1 = a$. Υποθέτουμε ότι η επαγωγική υπόθεση ισχύει για n και θα δείξουμε ότι ισχύει και για $n+1$, δηλαδή θα βρούμε $a_{n+1} \in \mathbb{Z}_p$ τέτοιο ώστε $f(a_{n+1}) \equiv 0 \mod p^{n+1}$ και $a_{n+1} \equiv a \mod p$.

Αν $f(a_{n+1}) \equiv 0 \mod p^{n+1}$ τότε $f(a_{n+1}) \equiv 0 \mod p^n$, που σημαίνει ότι κάθε ρίζα του $f(X) \mod p^{n+1}$ ανάγεται σε ρίζα του $f(X) \mod p^n$. Από την επαγωγική υπόθεση, υπάρχει a_n τέτοιο ώστε $f(a_n) \equiv 0 \mod p^n$. Από την $a_{n+1} \equiv a_n \mod p^n$, παίρνουμε ότι $a_{n+1} = a_n + p^n t_n$ για κάποιο $t_n \in \mathbb{Z}_p$. Ψάχνουμε τώρα το t_n έτσι ώστε $f(a_{n+1}) \equiv 0 \mod p^{n+1}$, δηλαδή $f(a_n + p^n t_n) \equiv 0 \mod p^{n+1}$. Από το Λήμμα 2.8,για κάποιο $z \in \mathbb{Z}_p$ είναι

$$f(a_n + p^n t_n) = f(a_n) + f'(a_n)p^n t_n + z p^{2n} t_n^2 \equiv f(a_n) + f'(a_n)p^n t_n \mod p^{n+1}$$

και $a_n \equiv a \mod p$, συνεπώς

$$f'(a_n)p^n t_n \equiv f'(a)p^n t_n \mod p^{n+1}.$$

Επομένως,

$$\begin{aligned} f(a_n + p^n t_n) \equiv 0 \mod p^{n+1} &\Leftrightarrow f(a_n) + f'(a_n)p^n t_n \equiv 0 \mod p^{n+1} \\ &\Leftrightarrow t_n \equiv -\frac{f(a_n)}{f'(a)p^n} \end{aligned}$$

όπου στην δεύτερη συνεπαγωγή, χρησιμοποιήσαμε το γεγονός $p^n \not\equiv 0 \mod p^{n+1}$ $f'(a) \not\equiv 0 \mod p$. Επιπλέον, $\dfrac{f(a_n)}{p^n} \in \mathbb{Z}_p$ καθώς $f(a_n) \equiv 0 \mod p^n$, δηλαδή $p^n \mid f(a_n)$).

Για την παραπάνω επιλογή του t_n, έχουμε ότι $f(a_{n+1}) \equiv 0 \mod p^{n+1}$ και ότι $a_{n+1} \equiv a_n + p^n t_n \equiv a_n \mod p^n$. Αυτό ολοκληρώνει την επαγωγή.

Ξεκινώντας με το $a_1 = a$, κατασκευάζουμε μια ακολουθία $a_1, a_2, \ldots$ στο $\mathbb{Z}_p$ τέτοια ώστε $f(a_n) \equiv 0 \mod p^n$ και $a_{n+1} \equiv a_n \mod p^n$ για όλα τα n. Θα αποδείξουμε ότι η ακολουθία αυτή είναι Cauchy στο $\mathbb{Z}_p$. Αφού η a_n είναι ακολουθία p-αδικών αριθμών, αρκεί να δείξουμε ότι για κάθε $\varepsilon > 0$, υπάρχει $n_0 \in \mathbb{N}$ τέτοιο ώστε για κάθε $n \geq n_0$ να ισχύει $|a_{n+1} - a_n|_p < \varepsilon$ (βλ. [12, σελ. 48]). Πράγματι, αφού $a_{n+1} \equiv a_n \mod p^n$ για κάθε $n \in \mathbb{N}$, έχουμε ότι για κάθε $n \in \mathbb{N}$, $a_{n+1} - a_n = p^n c$ για κάποιο $c \in \mathbb{Z}_p$. Το c, ως στοιχείο του $\mathbb{Z}_p$ έχει απόλυτη τιμή μικρότερη του 1, άρα αν επιλέξουμε $n_0 = [-\log_p \varepsilon] + 1$, έχουμε

$$|a_{n+1} - a_n|_p = |p^n c|_p = |p^n|_p |c|_p = \frac{1}{p^n}|c|_p < \frac{1}{p^n} < \frac{1}{p^{n_0}} = \frac{1}{p^{[-\log_p \varepsilon]+1}} < \frac{1}{p^{-\log_p \varepsilon}} = \varepsilon.$$

Συνεπώς, η ακολουθία $a_1, a_2, \ldots$ είναι Cauchy και αφού ο $\mathbb{Z}_p$ είναι πλήρης, το όριο της ακολουθίας ανήκει στο $\mathbb{Z}_p$, Έστω α αυτό το όριο.

Θέλουμε να δείξουμε ότι $f(\alpha) = 0$ και $\alpha \equiv a \mod p$. Από την $a_{n+1} \equiv a_n \mod p^n$ για κάθε $n \in \mathbb{N}$, παίρνουμε ότι $a_m \equiv a_n \mod p^n$ για κάθε $m > n$, άρα $\alpha \equiv a_n \mod p^n$ καθώς $m \to \infty$. Για $n = 1$ παίρνουμε $\alpha \equiv a \mod p$.

Για τυχαίο n, έχουμε $\alpha \equiv a_n \mod p^n$, οπότε $f(\alpha) \equiv f(a_n) \equiv 0 \mod p^n$, άρα $|f(\alpha)|_p \leq \dfrac{1}{p^n}$ για κάθε $n \in \mathbb{N}$. Επομένως, $f(\alpha) = 0$.

Μένει να δείξουμε ότι το α είναι η μοναδική ρίζα του $f(X)$ στο $\mathbb{Z}_p$ για την οποία ισχύει η ισοτιμία $\alpha \equiv a \mod p$. Έστω β μία άλλη ρίζα του $f(X)$ στο $\mathbb{Z}_p$ με $\beta \equiv a \mod p$. Για να δείξουμε ότι $\beta = \alpha$, αρκεί να δείξουμε ότι $|\beta - \alpha|_p \leq \dfrac{1}{p^n}$ για κάθε n, ή, ισοδύναμα, $\beta \equiv \alpha \mod p^n$ για κάθε $n \in \mathbb{N}$. Προχωράμε με επαγωγή. Για $n = 1$ είναι προφανές. Αν $n \geq 1$ και θεωρήσουμε γνωστή την ισοτιμία $\beta \equiv \alpha \mod p^n$ τότε αν γράψουμε $\beta = \alpha + p^n\gamma_n$ για κάποιο $\gamma_n \in \mathbb{Z}_p$, υπολογίζουμε όπως πριν

$$f(\beta) = f(\alpha + p^n\gamma_n) \equiv f(\alpha) + f'(\alpha)p^n\gamma^n \mod p^{n+1}.$$

Όμως είναι $f(\beta) = f(\alpha) = 0$, άρα $f'(\alpha)p^n\gamma_n \equiv 0 \mod p^{n+1}$. Αφού $f'(a) \equiv f'(\alpha) \not\equiv 0 \mod p$, έπεται ότι $\gamma_n \equiv 0 \mod p$. τελικά $\beta \equiv \alpha \mod p^{n+1}$, οπότε $\beta \equiv \alpha \mod p^n$ για κάθε $n \in \mathbb{N}$. ■

2.10 Θεώρημα. ***(ισχυρή μορφή του Λήμματος του Hensel).*** *Έστω $f(X) \in \mathbb{Z}_p[X]$ και $a \in \mathbb{Z}_p$ τέτοιο ώστε $|f(a)|_p < |f'(a)|_p^2$. Τότε υπάρχει μοναδικό $\alpha \in \mathbb{Z}_p$ τέτοιο ώστε $f(\alpha) = 0$ και $|\alpha - a|_p < |f'(a)|_p$.*

Απόδειξη. Θέτουμε $b = \dfrac{f(a)}{f'(a)^2}$, οπότε $f(a) = f'(a)^2 b$ και $|b|_p < 1$. Αν $|\alpha - a|_p < |f'(a)|_p$ τότε $v_p(\alpha - a) > v_p(f'(a))$, δηλαδή $\alpha - a = p^{k_1}u_1$ και $f'(a) = p^{k_2}u_2$ με $k_1 > k_2$ και $u_1, u_2 \in \mathbb{Z}_p^*$, άρα $\alpha - a = f'(a)u_1u_2p^{k_1-k_2}$, δηλαδή $\alpha = a + f'(a)p^{k_1-k_2}u_1u_2$. Θέτουμε $s = p^{k_1-k_2}u_1u_2$. Αφού $k_1 - k_2 > 0$ και $u_1, u_2 \in \mathbb{Z}_p^*$, είναι $|s|_p < 1$.

Αυτό μας οδηγεί στο να αναζητήσουμε λύση της μορφής $\alpha = a + f'(a)s$ για μοναδικό $s \in \mathbb{Z}_p$ με $|s|_p < 1$. Από το Λήμμα 2.8, για κάθε $s \in \mathbb{Z}_p$, υπάρχει $g(X, Y) \in \mathbb{Z}_p[X, Y]$ τέτοιο ώστε

$$\begin{aligned} f(a + f'(a)s) &= f(a) + f'(a)(f'(a)s) + g(a, f'(a)s)(f'(a)s)^2 \\ &= f'(a)b + f'(a)^2 s + g(a, f'(a)s)f'(a)^2 s^2 \\ &= f'(a)^2(b + s + g(a, f'(a)s)s^2) \end{aligned}$$

Θέτουμε $h(X) = b + X + g(a, f'(a)X)X^2 \in \mathbb{Z}_p[X]$. Το $h(X)$ έχει σταθερό όρο b, άρα $|h(0)|_p = |b|_p < 1$ και $|h'(0)|_p = |1|_p \not\equiv 0 \mod p$. Από το Λήμμα του Hensel, υπάρχει $\beta \in \mathbb{Z}_p$ τέτοιο ώστε $h(\beta) = 0$ και $|\beta|_p < 1$, οπότε το $\alpha := a + f'(a)\beta$ είναι η μοναδική ρίζα του $f(X)$ στο $\mathbb{Z}_p$ τέτοιο ώστε $|\alpha - a|_p < |f'(a)|_p$. ■

2.11 Θεώρημα. ***(Δεύτερη μορφή του Λήμματος του Hensel)*** *Έστω $f(X) \in \mathbb{Z}_p[X]$ και $f(X) \equiv \bar{g}(X)\bar{h}(X) \mod p\mathbb{Z}_p$ όπου $\mu\kappa\delta(\bar{g}, \bar{h}) = 1$ με $\bar{g}, \bar{h} \in \mathbb{F}_p[X]$ και $\bar{g}(X)$ μονικό. Τότε $f(X) = g(X)h(X)$ για κάποια $g, h \in \mathbb{Z}_p[X]$ τέτοια ώστε $\deg(g) = \deg(\bar{g})$, $g(X) \equiv \bar{g}(X) \mod p\mathbb{Z}_p$, $h(X) \equiv \bar{h}(X) \mod p\mathbb{Z}_p$ και $g(X)$ μονικό.*

Απόδειξη. Έστω $d = \deg(f)$ και $m = \deg(\bar{g})$, οπότε $\deg(\bar{h}) \leq d - m$. Έστω $g_0, h_0 \in \mathbb{Z}_p[X]$ τέτοια ώστε $g_0 = \bar{g}$, $h_0 = \bar{h}$ και $\deg(g_0) = m$, $\deg(h_0) \leq d - m$. Αφού μκδ$(\bar{g}, \bar{h}) = 1$, υπάρχουν πολυώνυμα $a, b \in \mathbb{Z}_p[X]$ τέτοια ώστε $ag_0 + bh_0 \equiv 1 \mod p\mathbb{Z}_p$.

Μπορούμε να γράψουμε

$$g = g_0 + r_1 p + r_2 p^2 + \ldots \text{ και } h = h_0 + q_1 p + q_2 p^2 + \ldots$$

όπου $r_i, q_i \in \mathbb{Z}_p[X]$ πολυώνυμα βαθμού $\deg(r_i) < m$ και $\deg(q_i) \leq d - m$ και $p \nmid g_0$, $p \nmid h_0$. Στη συνέχεια, θα καθορίσουμε τα πολυώνυμα

$$g_{n-1} = g_0 + r_1 p + \ldots + r_{n-1} p^{n-1} \text{ και } h_{n-1} = h_0 + q_1 p + \ldots + q_{n-1} p^{n-1} \quad (1)$$

έτσι ώστε $f \equiv g_{n-1} h_{n-1} \mod p^n$. Περνώντας στο όριο καθώς $n \to \infty$, θα πάρουμε $f = gh$.

Για τον καθορισμό των g_{n-1} και h_{n-1}, αρκεί να καθορίσουμε τα r_n και q_n. Κάνουμε επαγωγή στο n. Για $n = 1$ είναι τετριμμένο. Έστω ότι υπάρχουν τα g_{n-1} και h_{n-1}. Μέσω αυτών, θα βρούμε τα g_n και h_n.
Από τις (1), λαμβάνουμε τις σχέσεις $g_n = g_{n-1} + r_n p^n$, $h_n = h_{n-1} + q_n p^n$, $g_{n-1} \equiv g_0 \mod p$ και $h_{n-1} \equiv h_0 \mod p$. Η σχέση $f \equiv g_n h_n \mod p^{n+1}$ γίνεται

$$\begin{aligned} f &\equiv (g_{n-1} r_n p^n)(h_{n-1} + q_n p^n) \mod p^{n+1} \\ &\equiv g_{n-1} h_{n-1} + (g_{n-1} q_n + h_{n-1} r^n) p^n + r_n q_n p^{2n} \mod p^{n+1} \\ &\equiv g_{n-1} h_{n-1} + (g_{n-1} q_n + h_{n-1} r_n) p^n \mod p^{n+1} \text{ (διότι } 2n \geq n+1) \end{aligned}$$

Άρα $f - g_{n-1} h_{n-1} \equiv (g_{n-1} q_n + h_{n-1} r_n) p^n \mod p^{n+1}$. Διαιρώντας και τα δύο μέλη με p^n, παίρνουμε

$$\begin{aligned} p^{-n}(f - g_{n-1} h_{n-1} &\equiv g_{n-1} q_n + h_{n-1} r_n \mod p \\ &\equiv g_0 q_n + h_0 r_n \mod p. \end{aligned}$$

Θέτουμε $f_n = p^{-n}(f - g_{n-1} h_{n-1}) \in \mathbb{Z}_p[X]$ (διότι $f - g_{n-1} h_{n-1} \equiv 0 \mod p^n$, οπότε $p^n \mid (f - g_{n-1} h_{n-1})$). Αφού $g_0 a + h_0 b \equiv 1 \mod p$, έχουμε $(g_0 a + h_0 b) f_n \equiv f_n \mod p$, δηλαδή $g_0 a f_n + h_0 b f_n \equiv f_n \mod p$.

Εκτελώντας την διαίρεση του $b f_n$ με το g_0, παίρνουμε ότι $b f_n = q g_0 + r_n$ όπου $\deg(r_n) < \deg(g_0) = m$. Αφού $g_0 = \bar{g}$ και $\deg(g_0) = \deg(g)$, ο μεγιστοβάθμιος συντελεστής του g_0 δεν διαιρείται από το p, άρα είναι μονάδα. Άρα $q(X) \in \mathbb{Z}_p[X]$ και από τις $b f_n = q g_0 + p_n$, λαμβάνουμε την ισοτιμία $g_0 a f_n + h_0 (q g_0 + r_n) \equiv f_n \mod p$, δηλαδή $g_0 (a f_n + h_0 q) + h_0 r_n \equiv f_n \mod p$. Διαγράφοντας από το $a f_n + h_0 q$ τους όρους με συντελεστή που διαιρείται από το p, παίρνουμε ένα πολυώνυμο q_n τέτοιο ώστε $g_0 q_n + h_0 r_n \equiv f_n \mod p$, οπότε $g_0 q_n + h_0 r_n = pk + f_n$ για κάποιο $k \in \mathbb{Z}_p[X]$ με $\deg(k) < \deg(f_n) < d$. Από τις $\deg(f_n) \leq d$, $\deg(g_0) = m$, $\deg(h_0 r_n) < d - m + m = d$ και $\deg(k) < d$, παίρνουμε $\deg(q_n) \leq d + d - d - m = d - m$.

■

§3 Τετράγωνα στο $\mathbb{Q}_p$

Στην παρούσα παράγραφο, εξετάζουμε πότε ένα στοιχείο του $\mathbb{Q}_p$, $p \in \mathbb{P}$ είναι τέλειο τετράγωνο στο $\mathbb{Q}_p$. Διακρίνουμε δύο περιπτώσεις: $p \neq 2$ και $p = 2$.

2.12 Λήμμα. *Έστω $p \in \mathbb{P} \setminus \{2\}$.*

1. *Το b είναι τετράγωνο του $\mathbb{Z}_p^*$ αν και μόνο αν υπάρχει $a \in \mathbb{Z}_p^*$ τέτοιο ώστε $a^2 \equiv b \mod p\mathbb{Z}_p$.*

2. *Ένα στοιχείο του $\mathbb{Q}_p$ είναι τετράγωνο αν και μόνο αν μπορεί να γραφτεί στη μορφή $p^{2n}u^2$ όπου $n \in \mathbb{Z}$ και $u \in \mathbb{Z}_p^*$.*

3. *Η ομάδα $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ είναι ισόμορφη προς την ομάδα $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ και ένα πλήρες σύστημα αντιπροσώπων των συμπλόκων της είναι το $\{1, p, u, pu\}$ όπου u μονάδα του $\mathbb{Z}_p$ που δεν είναι τετράγωνο.*

Απόδειξη.

1) Έστω $b \in \mathbb{Z}_p^*$ τέλειο τετράγωνο. Αυτό σημαίνει ότι υπάρχει $a \in \mathbb{Z}_p^*$ τέτοιο ώστε $b = a^2$. Συνεπώς, $a^2 \equiv b \mod p\mathbb{Z}_p$.

Αντίστροφα, υποθέτουμε ότι υπάρχει $a \in \mathbb{Z}_p^*$ τέτοιο ώστε $a^2 \equiv b \mod p\mathbb{Z}_p$. Θέτουμε $f(X) = X^2 - b \in \mathbb{Z}_p[X]$. Έχουμε $f(a) \equiv 0 \mod p$ και $f'(a) \equiv 2a \not\equiv 0 \mod p$, διότι $a \in \mathbb{Z}_p^*$ και $p \neq 2$. Άρα από το Λήμμα του Hensel 2.9, η λύση $X = a$ ανάγεται σε λύση στο $\mathbb{Z}_p^*$.

2) Υποθέτουμε ότι το $x \in \mathbb{Q}_p$ είναι τέλειο τετράγωνο, δηλαδή υπάρχει $y \in \mathbb{Q}_p$ τέτοιο ώστε $x = y^2$. Αφού $y \in \mathbb{Q}_p$, μπορούμε να γράψουμε $y = p^n u$ για κάποια $n \in \mathbb{Z}$ και $u \in \mathbb{Z}_p^*$. Άρα $x = p^{2n}u^2$.

Η αντίστροφη κατεύθυνση είναι προφανής.

3) Θεωρούμε την απεικόνιση $\phi : \mathbb{Q}_p^* \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ με τύπο

$$\phi(x) = \phi(p^n u) = \begin{cases} ([n]_2, 0), & \text{αν το } u \text{ είναι τετράγωνο στο } \mathbb{Z}_p^* \\ ([n]_2, 1), & \text{αλλιώς} \end{cases}$$

όπου γράφουμε $x = p^n u$ με $n \in \mathbb{Z}$ και $u \in \mathbb{Z}_p^*$.

Η απεικόνιση ϕ είναι ομομορφισμός και είναι επί αφού αν επιλέξουμε ένα $u \in \mathbb{Z}_p^*$ τέτοιο ώστε η εικόνα του μέσω του ομομορφισμού αναγωγής $\mathbb{Z}_p \to \mathbb{F}_p$ να μην είναι τετραγωνικό υπόλοιπο, έχουμε

$$\phi(1) = \phi(p^0 u^0) = (0, 0),$$
$$\phi(p) = \phi(p^1 u^0) = (1, 0),$$

$$\phi(u) = \phi(p^0 u^1) = (0,1),$$
$$\phi(pu) = \phi(p^1 u^1) = (1,1).$$

Επίσης είναι $x = p^n u \in \mathrm{Ker}(\phi)$ αν και μόνο αν $([n]_2, 0) = (0,0)$ και το u είναι τέλειο τετράγωνο, δηλαδή αν και μόνο αν ο n είναι άρτιος και το u είναι τέλειο τετράγωνο στο $\mathbb{Z}_p^*$. Άρα από το (2) έχουμε $x \in \mathrm{Ker}(\phi)$ αν και μόνο αν το x είναι τέλειο τετράγωνο στο $\mathbb{Q}_p^*$, οπότε $\mathrm{Ker}(\phi) = (\mathbb{Q}_p^*)^2$.

Συνεπώς, από το Πρώτο Θέωρημα Ισομορφισμών Ομάδων,

$$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Άρα $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 4$. Από την απόδειξη προκύπτει ότι ένα πλήρες σύστημα αντιπροσώπων των συμπλόκων της ομάδας $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ είναι το $\{1, p, u, pu\}$.

■

2.13 Λήμμα.

1. *Το b είναι τετράγωνο του $\mathbb{Z}_2^*$ αν και μόνο αν $b \equiv 1 \mod 8\mathbb{Z}_2$.*
2. *Ένα στοιχείο $x = 2^n u$ του $\mathbb{Q}_2$ είναι τετράγωνο αν και μόνο αν ο n είναι άρτιος και $u \equiv 1 \mod 8\mathbb{Z}_2$.*
3. *Η ομάδα $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ είναι ισόμορφη με την $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ και ένα πλήρες σύστημα αντιπροσώπων των κλάσεων είναι το $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.*

Απόδειξη.

1) Υποθέτουμε ότι $b \in \mathbb{Z}_2^*$. Τότε η εικόνα του μέσω του ομομορφισμού αναγωγής modulo 8 θα είναι τετραγωνικό υπόλοιπο του $\mathbb{Z}/8\mathbb{Z}$, δηλαδή είναι $0, 1$ ή 4. Όμως επειδή το b είναι αντιστρέψιμο στο $\mathbb{Z}_2^*$, η εικόνα του θα είναι αντιστρέψιμη στο $\mathbb{Z}/8\mathbb{Z}$, επομένως είναι 1 στο $\mathbb{Z}/8\mathbb{Z}$. Άρα $b \equiv 1 \mod 8\mathbb{Z}_2$.

Αντίστροφα, υποθέτουμε ότι $b \equiv 1 \mod 8\mathbb{Z}_2$. Θέτουμε $f(X) = X^2 - b \in \mathbb{Z}_2[X]$. Είναι $f(1) \equiv 0 \mod 8\mathbb{Z}_2$, άρα και $v_2(f(1)) \geq 3$, δηλαδή $|f(1)|_2 \leq \frac{1}{8}$. Επίσης, $f'(1) = 2$ που σημαίνει ότι $|f'(1)|_2 = \frac{1}{2}$. Έχουμε λοιπόν ότι $f(1) \equiv 0 \mod 2\mathbb{Z}_2$ και $|f(1)|_2 < |f'(1)|_2^2$, άρα από την ισχυρή μορφή του Λήμματος του Hensel, το 1 ανάγεται σε ρίζα του f στο $\mathbb{Z}_2$, δηλαδή το b είναι τέλειο τετράγωνο στο $\mathbb{Z}_2^*$.

2) Παρόμοια με το 2 του προηγούμενου λήμματος.

3) Θεωρούμε την απεικόνιση $\phi : \mathbb{Q}_2^* \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ με τύπο

$$\phi(2^n u) = \begin{cases} ([n]_2, 0, 0), & u \equiv +1 \mod 8\mathbb{Z}_2 \\ ([n]_2, 1, 0), & u \equiv -1 \mod 8\mathbb{Z}_2 \\ ([n]_2, 0, 1), & u \equiv +5 \mod 8\mathbb{Z}_2 \\ ([n]_2, 1, 1), & u \equiv -5 \mod 8\mathbb{Z}_2. \end{cases}$$

Εύκολα βλέπουμε ότι η ϕ είναι ομομορφισμός ομάδων. Επίσης είναι επί διότι

$$\begin{aligned}
\phi(1) = \phi(2^0 \cdot 1) = (0,0,0), \;\; \phi(-1) = \phi(2^0 \cdot (-1)) = (0,1,0),\\
\phi(2) = \phi(2^1 \cdot 1) = (1,0,0), \;\; \phi(-2) = \phi(2^1 \cdot (-1)) = (1,1,0),\\
\phi(5) = \phi(2^0 \cdot 5) = (0,0,1), \;\; \phi(-5) = \phi(2^0 \cdot (-5)) = (0,1,1),\\
\phi(10) = \phi(2^1 \cdot 5^1) = (1,0,1), \;\; \phi(-10) = \phi(2 \cdot (-5)) = (1,1,1).
\end{aligned}$$

Επιπλέον, $x = 2^n u \in \mathrm{Ker}(\phi)$ αν και μόνο αν $\phi(2^n u) = 0$, δηλαδή αν και μόνο αν $([n]_2, 0, 0) = (0,0,0)$, δηλαδή αν και μόνο αν ο n είναι άρτιος και $u \equiv 1 \mod 8\mathbb{Z}_2$. Άρα από το (2) έχουμε $x \in \mathrm{Ker}(\phi)$ αν και μόνο αν το x είναι τετράγωνο στο $\mathbb{Q}_2$, επομένως $\mathrm{Ker}(\phi) = (\mathbb{Q}_2^*)^2$.

Από το Πρώτο Θεώρημα Ισομορφισμών Ομάδων συμπεραίνουμε ότι

$$\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Άρα $[\mathbb{Q}_2^* : (\mathbb{Q}_2^*)^2] = 8$ και από την απόδειξη προκύπτει ότι ένα πλήρες σύστημα αντιπροσώπων των συμπλόκων της ομάδα $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ είναι το $\{\pm 1, \pm 2, \pm 3, \pm 10\}$. ■

§4 Το τοπικό-γενίκο αξίωμα (local-global principle)

Θεωρούμε μια προβολική καμπύλη C (ή γενικότερα μία πολλαπλότητα), υπέρ το $\mathbb{Q}$. Ενδιαφερόμαστε για την εύρεση όλων των ρητών σημείων της. Θεωρούμε τα σώματα $\mathbb{Q}_p$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$. Από τον εγκλεισμό $\mathbb{Q} \subseteq \mathbb{Q}_p$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$, έπεται ότι $C(\mathbb{Q}) \subseteq C(\mathbb{Q}_p)$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$. Επομένως, αν για κάποιο p ισχύει $C(\mathbb{Q}_p) = \emptyset$ τότε προκύπτει ότι $C(\mathbb{Q}) = \emptyset$.

2.14 Παράδειγμα. Θεωρούμε την προβολική καμπύλη $C : X^2 + Y^2 + Z^2 = 0$. Είναι φανερό ότι $C(\mathbb{R}) = \emptyset$ (υπενθυμίζουμε ότι το σημείο $[0,0,0]$ δεν ανήκει στο προβολικό επίπεδο), άρα και $C(\mathbb{Q}) = \emptyset$. □

2.15 Ορισμός. Έστω C προβολική καμπύλη υπέρ το $\mathbb{Q}$. Θα λέμε ότι η C έχει **τοπικά παντού ρητά σημεία** όταν $C(\mathbb{Q}_p) \neq \emptyset$ για όλα τα $p \in \mathbb{P} \cup \{\infty\}$.

Είναι προφανές ότι αν $C(\mathbb{Q}) \neq \emptyset$ τότε η καμπύλη C έχει τοπικά παντού ρητά σημεία. Είναι λογικό να αναρωτηθεί κανείς αν είναι αληθές το αντίστροφο. Ισχύει το ακόλουθο θεώρημα.

2.16 Θεώρημα. ***(Hasse-Minkowski.)*** *Έστω $V \subseteq \mathbb{P}^n(\mathbb{Q})$ μια προβολική πολλαπλότητα υπέρ το $\mathbb{Q}$ από μία ομογενή τετραγωνική εξίσωση. Οι ακόλουθες προτάσεις είναι ισοδύναμες:*

1. *Η V έχει τοπικά παντού ρητά σημεία.*

2. Η V έχει ένα τουλάχιστον ρητό σημείο, δηλαδή $V(\mathbb{Q}) \neq \emptyset$.

2.17 Παρατήρηση. Υπάρχει αλγόριθμος ο οποίος αποφασίζει αν δοθείσα πολλαπλότητα V υπέρ το $\mathbb{Q}$ (ή σε ένα αλγεβρικό σώμα αριθμών) έχει τοπικά παντού ρητά σημεία.

Στη συνέχεια, περιοριζόμαστε σε καμπύλες. Κατηγοριοποιούμε τις καμπύλες ανάλογα με το γένος τους και διακρίνουμε τις περιπτώσεις $g = 0$, $g = 1$ και $g \geq 2$.

Καμπύλες γένους 0

Το ακόλουθο θεώρημα είναι συνέπεια του Θεωρήματος Riemann-Roch.

2.18 Θεώρημα. *Έστω C μία καμπύλη γένους 0 ορισμένη ορισμένη σε ένα σώμα K. Τότε η C είναι ισόμορφη με μία ομαλή επίπεδη καμπύλη βαθμού 2 (δηλαδή με μία κωνική τομή). Επιπλέον, αν $C(K) \neq \emptyset$ τότε η C είναι ισόμορφη με την προβολική ευθεία $\mathbb{P}^1$.*

Μία κωνική τομή ορίζεται από μία εξίσωση δευτέρου βαθμού στο $\mathbb{P}^2$. Επομένως μπορούμε να εφαρμόσουμε το Θεώρημα Hasse-Minkowski σε καμπύλες γένους 0 και παίρνουμε το ακόλουθο Θεώρημα.

2.19 Θεώρημα. ***(Η Αρχή του Hasse).*** *Έστω C μία καμπύλη γένους 0 υπέρ το $\mathbb{Q}$. Τα ακόλουθα είναι ισοδύναμα:*

1. *$C(\mathbb{Q}) \neq \emptyset$.*
2. *$C(\mathbb{Q}_p) \neq \emptyset$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$.*

Ακριβέστερα, ισχύει το εξής:

2.20 Θεώρημα. ***(Legendre-Hasse)*** *Έστω*

$$C : aX^2 + bY^2 + cZ^2 = 0 \quad (1)$$

μία προβολική καμπύλη δευτέρου βαθμού υπέρ το $\mathbb{Q}$ όπου a, b, c είναι μη μηδενικοί ακέραιοι, ελεύθεροι τετραγώνων. Αυτή είναι ομαλή καμπύλη γένους 0. Τα ακόλουθα είναι ισοδύναμα:

1. *$C(\mathbb{Q}) \neq \emptyset$.*
2. *$C(\mathbb{Q}_p) \neq \emptyset$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$.*
3. *$C(\mathbb{Q}_p) \neq \emptyset$ για κάθε $p \mid 2abc$.*

2.21 Παρατήρηση. Κάθε κωνική στο προβολικό επίπεδο $\mathbb{P}^2(\mathbb{Q})$ μπορεί να γραφτεί στην μορφή (1) συμπληρώνοντας τα τετράγωνα και κάνοντας κατάλληλη αλλαγή μεταβλητών. Για να ελέγξουμε την ύπαρξη σημείων τοπικά παντού (συνθήκη 2), αρκεί να ελέγξουμε την ύπαρξη τοπικών σημείων για πεπερασμένο πλήθος πρώτων αριθμών (συνθήκη 3).

Καμπύλες γένους 1

2.22 Θεώρημα. *Αν C είναι μία καμπύλη γένους 1 ορισμένη σε ένα σώμα K και $P_0 \in C(K)$ τότε η C είναι ισόμορφη με μία ελλειπτική καμπύλη στον $\mathbb{P}^2(K)$ στη* ***μορφή του Weierstrass***

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

όπου ο ισομορφισμός απεικονίζει το P_0 στο επ΄άπειρον σημείο της καμπύλης, $[0, 1, 0]$.

2.23 Θεώρημα. ***(Mordell)*** *Αν C είναι μία καμπύλη γένους 1 ορισμένη σε ένα σώμα K και $P_0 \in C(K)$ όπου $K = \mathbb{Q}$ ή ένα αλγεβρικό σώμα αριθμών, τότε το $C(K)$ είναι πεπερασμένα παραγόμενη αβελιανή ομάδα με ταυτοτικό στοιχείο το P_0.*

Μέχρι σήμερα, για καμπύλες C γένους 1 ορισμένες στο $\mathbb{Q}$:

(i) δεν υπάρχει γνωστός αλγόριθμος που αποφασίζει αν $C(\mathbb{Q}) \neq \emptyset$ και
(ii) δεν υπάρχει γνωστός αλγόριθμος για τον υπολογισμό μια Mordell-Weil βάσης του $C(\mathbb{Q})$ αν είναι μη κενό.

Επίσης, όπως φαίνεται από το επόμενο παράδειγμα, που οφείλεται στον Selmer, δεν ισχύει ούτε η αρχή του Hasse

2.24 Παράδειγμα. Έστω C η προβολική καμπύλη γένους 1 υπέρ το $\mathbb{Q}$ που ορίζεται από την εξίσωση $3X^3 + 4Y^3 + 5Z^3 = 0$. Τότε $C(\mathbb{Q}_p) \neq \emptyset$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$ αλλά $C(\mathbb{Q}) = \emptyset$.

Καμπύλες γένους ≥ 2

Ένα πολύ σημαντικό θεώρημα για την μελέτη των ρητών σημείων μια καμπύλης γένους μεγαλύτερου ή ίσου του 2 είναι το εξής:

2.25 Θεώρημα. ***(Faltings).*** *Έστω C μία καμπύλη γένους $g \geq 2$ υπέρ το $\mathbb{Q}$. Τότε το σύνολο $C(\mathbb{Q})$ είναι πεπερασμένο.*

Ενώ η διατύπωση του Θεωρήματος του Faltings είναι απλή και κομψή, οι γνωστές αποδείξεις είναι πολύ δύσκολες και δεν υποδεικνύουν κάποιον αλγόριθμο εύρεσης των ρητών σημείων. Έως σήμερα, για καμπύλες γένους $g \geq 2$,

(i) δεν υπάρχει γνωστός αλγόριθμος υπολογισμού του $C(\mathbb{Q})$ και
(ii) δεν υπάρχει γνωστός αλγόριθμος που αποφασίζει αν $C(\mathbb{Q}) \neq \emptyset$.

Υπάρχουν όμως κάποιες τεχνικές που σε ορισμένες περιπτώσεις μας βοηθούν να αποφασίσουμε αν το $C(\mathbb{Q})$ είναι κενό, ή αν δεν είναι κενό, να καθορίσουμε τα στοιχεία του. Παρά το ότι δεν πρόκειται να ασχοληθούμε με όλες τις δυνατές περιπτώσεις, πληροφοριακά αναφέρουμε ονομαστικά κάποιες από αυτές:

1. Τοπικές Μέθοδοι (Local Methods)
2. Πηλίκα (Quotients)
3. Κάθοδος (Descent)
4. Μέθοδος του Chabauty
5. Το Κόσκινο (Sieve) των Mordell-Weil

Επιστρέφουμε στην γενική περίπτωση. Εξαιρετικά σημαντικό για τα επόμενα είναι και το παρακάτω Θεώρημα.

2.26 Θεώρημα. ***(Hasse-Weil).*** *Έστω $\bar{C}$ μια ομαλή, απολύτως ανάγωγη προβολική καμπύλη γένους g ορισμένη στο πεπερασμένο σώμα με q στοιχεία $\mathbb{F}_q$, χαρακτηριστικής $p \in \mathbb{P}$. Τότε*

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

2.27 Σημείωση. Το Θεώρημα των Hasse-Weil είναι ισοδύναμο με την Εικασία του Riemann για την περίπτωση χαρακτηριστικής p.

Κεφάλαιο III

Υπερελλειπτικές καμπύλες

§1 Βασικοί ορισμοί και ιδιότητες

3.1 Ορισμός. Έστω $a_1, a_2, a_3 \in \mathbb{N}_0$ και K ένα σώμα. Θεωρούμε τη σχέση ισοδυναμίας στο σύνολο $K^3 \setminus \{(0,0,0)\}$ που ορίζεται από τη σχέση $(x,y,z) \sim (x',y',z')$ αν και μόνο αν υπάρχει $\lambda \in K^*$ τέτοιο ώστε $(x',y',z') = (\lambda^{a_1}x, \lambda^{a_2}y, \lambda^{a_3}z)$. Το σύνολο των κλάσεων ισοδυναμίας της παραπάνω σχέσης λέγεται **προβολικό επίπεδο με βάρη** a_1, a_2, a_3 και συμβολίζεται $\mathbb{P}^2_{(a_1,a_2,a_3)}(K)$.

Τις κλάσεις ισοδυναμίας θα τις λέμε **σημεία** του $\mathbb{P}^2_{(a_1,a_2,a_3)}(K)$. Ένα τυχαίο σημείο του $\mathbb{P}^2_{(a_1,a_2,a_3)}(K)$ θα το συμβολίζουμε $[x,y,z]$.

Στη συνέχεια, θα περιοριστούμε στην περίπτωση $(a_1,a_2,a_3) = (1,g+1,1)$ με $g \in \mathbb{N}_0$, δηλαδή στο προβολικό επίπεδο με βάρη $\mathbb{P}^2_g(K) \coloneqq \mathbb{P}^2_{(1,g+1,1)}(K)$.
Ο δακτύλιος συντεταγμένων του $\mathbb{P}^2_g(K)$ είναι ο $K[X,Y,Z]$ που αναθέτει βάρη $1, g+1, 1$ στα X,Y,Z αντιστοίχως. Ένα πολυώνυμο $f(X,Y,Z) \in K[X,Y,Z]$ λέγεται **ομογενές πολυώνυμο βαθμού** d **στο** $\mathbb{P}^2_g(K)$ αν όλοι οι όροι του έχουν βαθμό d, δηλαδή αν το f έχει τη μορφή

$$f(X,Y,Z) = \sum_{\substack{i_1,i_2,i_3 \in \mathbb{N}_0 \\ i_1+(g+1)i_2+i_3=d}} a_{i_1,i_2,i_3} X^{i_1} Y^{i_2} Z^{i_3}$$

με $a_{i_1,i_2,i_3} \in K$.

3.2 Σημείωση. Για $g = 0$ λαμβάνουμε το συνηθισμένο προβολικό επίπεδο και τη συνηθισμένη έννοια του ομογενούς πολυωνύμου.

Όπως και στο συνηθισμένο προβολικό επίπεδο, υπάρχει μια φυσιολογική αμφιμονοσήμαντη αντιστοιχία μεταξύ των σημείων του $U_1 \coloneqq \{[x,y,z] \in \mathbb{P}^2_g(K) : z \neq 0\}$ και των σημείων του αφινικού επιπέδου $\mathbb{A}^2(K)$. Η αντιστοιχία είναι η εξής:

$$U_1 \to \mathbb{A}^2(K), \;\; [x,y,z] \mapsto (\frac{x}{z}, \frac{y}{z^{g+1}})$$

και αντίστροφα,

$$\mathbb{A}^2(K) \to U_1, \;\; (x,y) \mapsto [x,y,1].$$

Όμοια, λαμβάνουμε μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των σημείων του $U_2 := \{[x, y, z] \in \mathbb{P}^2_g(K) : x \neq 0\}$ και του $\mathbb{A}^2(K)$. Παρατηρούμε ότι $U_1 \cup U_2 = \mathbb{P}^2_g(K) \setminus \{[0, 1, 0]\}$.

3.3 Ορισμός. Έστω $g \in \mathbb{N}$, $g \geq 2$. Μια **υπερελλειπτική καμπύλη** γένους g πάνω από ένα σώμα K με $\mathrm{ch}K \neq 2$ είναι μια υποπολλαπλότητα του $\mathbb{P}^2_g(K)$ που ορίζεται από μία εξίσωση της μορφής $Y^2 = F(X, Z)$ όπου $F \in K[X, Z]$ ένα ομογενές (κατά τη συνηθισμένη έννοια) πολυώνυμο βαθμού $2g + 2$ και είναι ελεύθερο τετραγώνου (στην περίπτωσή μας, να μην διαιρείται από ομογενές πολυώνυμο βαθμού μεγαλύτερο ή ίσο του 2).

Αν η C είναι καμπύλη ορισμένη σε ένα σώμα K, τότε τα K-ρητά σημεία της είναι το σύνολο

$$C(K) = \{[x, y, z] \in \mathbb{P}^2_g(K) : y^2 = F(x, z)\}.$$

Αν $K = \mathbb{Q}$ τότε αντί για $\mathbb{Q}$-ρητά σημεία, λέμε απλώς ρητά σημεία.

3.4 Παρατήρηση. Η συνθήκη ότι το $F(X, Z)$ στον παραπάνω ορισμό είναι ελεύθερο τετραγώνου εξασφαλίζει ότι μία υπερελλειπτική καμπύλη είναι πάντοτε ομαλή.

3.5 Παρατήρηση. Το πολυώνυμο $Y^2 - F(X, Z)$ που εμφανίζεται στον ορισμό είναι ανάγωγο. Πράγματι, το $Y^2 - F(X, Z)$ ως πολυώνυμο του Y είναι μονικό και βαθμού 2, άρα η μοναδική παραγοντοποίηση που μπορεί να επιδέχεται είναι η

$$Y^2 - F(X, Z) = (Y - H_1(X, Z))(Y - H_2(X, Z))$$

με $H_1(X, Z), H_2(X, Z) \in K[X, Z]$. Η παραπάνω σχέση γράφεται και

$$Y^2 - F(X, Z) = Y^2 - Y(H_1(X, Z) + H_2(X, Z)) + H_1(X, Z)H_2(X, Z).$$

Συγκρίνοντας συντελεστές στα δύο μέλη παίρνουμε ότι

$$F(X, Z) = -H_1(X, Z)H_2(X, Z)$$

και

$$H_1(X, Z) + H_2(X, Z) = 0.$$

Συνδυάζοντας αυτές τις δύο σχέσεις, καταλήγουμε στο ότι $F(X, Z) = H_1^2(X, Z)$ που είναι άτοπο διότι το $F(X, Z)$ είναι ελεύθερο τετραγώνου, εξ υποθέσεως.

3.6 Παρατήρηση. Προηγουμένως είδαμε ότι $U_1 \cup U_2 = \mathbb{P}^2_g(K) \setminus \{[0, 1, 0]\}$. Η εξαίρεση του σημείου $[0, 1, 0]$ δεν θα επηρεάσει την μελέτη των υπερελλειπτικών καμπυλών καθώς το εν λόγω σημείο δεν αποτελεί σημείο υπερελλειπτικής καμπύλης (αρκεί μόνο μια απλή αντικατάσταση στην εξίσωση της καμπύλης για να το διαπιστώσουμε).

Ο προβολικός ορισμός των K-ρητών σημείων της καμπύλης έχει νόημα, αφού αν $(x, y, z), (x', y', z') \in \mathbb{P}^2_g(K)$ με $(x, y, z) \sim (x', y', z')$, τότε $(x', y', z') = (\lambda x, \lambda^{g+1} y, \lambda z)$ για κάποιο $\lambda \in K^*$ και έχουμε:

$$\begin{aligned} y'^2 = F(x',z') &\Leftrightarrow \lambda^{2g+2}y^2 = F(\lambda x, \lambda z) \\ &\Leftrightarrow \lambda^{2g+2}y^2 = \lambda^{2g+2}F(x,z) \quad (F \text{ ομογενές βαθμού } 2g+2) \\ &\Leftrightarrow y^2 = F(x,z) \quad (\lambda \neq 0), \end{aligned}$$

Ο υποδακτύλιος του $K(C)$ που αποτελείται από τις συναρτήσεις που ορίζονται παντού (δηλαδή σε όλα τα σημεία του $C(\bar{K})$ όπου $\bar{K}$ μία αλγεβρική θήκη του K) εκτός ίσως από τα επ΄άπειρον σημεία, είναι ισόμορφος με τον δακτύλιο $K[C_{\text{aff}}] \coloneqq K[X,Y]\langle Y^2 - f(X)\rangle$. Έπεται ότι $\text{Quot}(K(C)) \cong \text{Quot}(K[C_{\text{aff}}])$. Αυτό μας επιτρέπει να γράφουμε τις εξισώσεις σε αφινική μορφή. Απλά παραδείγματα συναρτήσεων στην C είναι οι $1, X, X^2, ..., Y, XY, ...$: αυτές είναι ομαλές σε όλα εκτός τα επ΄άπειρον σημεία. Παρατηρούμε επίσης ότι αν $\phi \in K(C)$ τότε λόγω της εξίσωσης της καμπύλης $Y^2 = f(X)$, μπορούμε να αντικαταστήσουμε του Y^2 με το $f(X)$, οπότε η ϕ γράφεται στη μορφή $\phi(X,Y) = h_1(X) + h_2(X)Y$ με $h_1(X), h_2(X) \in K[X]$.

Για λόγους απλότητας, θα γράφουμε την καμπύλη στην αφινική μορφή $C : Y^2 = f(X)$ αλλά θα θεωρούμε πάντοτε την καμπύλη ως προβολική καμπύλη.

3.7 Σημείωση. Για να μπορούμε να κατασκευάσουμε το $F(X,Z)$ από το $f(X)$ μέσω ομογενοποίησης, πρέπει $\deg(f) = 2g+1$ ή $2g+2$. Αν ήταν $\deg(f) < 2g+1$ τότε το $F(X,Z)$ θα είχε ως παράγοντα το Z^2, που θα σήμαινε ότι το $F(X,Z)$ δεν θα ήταν ελεύθερο τετραγώνου, το οποίο είναι άτοπο.

Έστω $F(X,Z) = a_{2g+2}X^{2g+2} + a_{2g+1}X^{2g+1}Z + ... + a_1XZ^{2g+1} + a_0Z^{2g+2}$, $a_i \in K$ ένα ομογενές πολυώνυμο βαθμού $2g+2$ στον $K[X,Z]$. Θεωρούμε την υπερελλειπτική καμπύλη $Y^2 = F(X,Z)$. Τα σημεία $[x,y,z] \in C(K)$ με $z \neq 0$ έχουν τη μορφή $[x,y,z]$ όπου $y^2 = f(x)$, η με άλλα λόγια, είναι τα K-ρητά σημεία του U_1. Συχνά, ένα τέτοιο σημείο θα το συμβολίζουμε (x,y). Τα υπόλοιπα σημεία λέγονται **επ΄άπειρον σημεία**. Τα βρίσκουμε αν στην εξίσωση αντικαταστήσουμε $Z = 0$. Έτσι, η εξίσωση γίνεται $Y^2 = a_{2g+2}X^{2g+2}$. Αν $X = 0$ τότε $[X,Y,Z] = [0,0,0] \notin \mathbb{P}^2_g(K)$, δηλαδή για $X = 0$ δεν έχουμε λύση. Αν $X \neq 0$ τότε χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε $X = 1$. Η εξίσωση γίνεται $Y^2 = a_{2g+2}$.

Αν $a_{2g+2} = 0$ τότε η μοναδική λύση είναι η $[1,0,0]$, που σημαίνει ότι η καμπύλη έχει μοναδικό επ΄άπειρον σημείο. Θα χρησιμοποιούμε τον συμβολισμό $\infty \coloneqq [1,0,0]$.

Αν το a_{2g+2} είναι μη μηδενικό τέλειο τετράγωνο στο K, έστω $a_{2g+2} = s^2$, $s \in K^*$ τότε έχουμε δύο επ΄άπειρον σημεία, τα $[1,s,0]$ και $[1,-s,0]$ (τα συμβολίζουμε ∞_s και ∞_{-s} αντίστοιχα). Σε διαφορετική περίπτωση, η καμπύλη δεν έχει επ΄άπειρον σημεία (αλλά έχουμε επ΄άπειρον σημεία στην επέκταση $K(\sqrt{a_{2g+2}})$).

Συμπέρασμα: Μια υπερελλειπτική καμπύλη ορισμένη σε ένα σώμα K έχει 0,1 ή 2 επ΄άπειρον σημεία και όταν έχει, είναι K- ρητά σημεία της.

3.8 Παράδειγμα. Έστω $K = \mathbb{Q}$ και $C : Y^2 = X^5 + 1$. Επειδή ο βαθμός του $X^5 + 1$ είναι 5, έπεται ότι το γένος της καμπύλης C είναι 2 και η προβολική εξίσωση της καμπύλης είναι $Y^2 = X^5Z + Z^6$. Για $Z = 0$, η εξίσωση γίνεται $Y^2 = 0$, οπότε $Y = 0$ και $X \in \mathbb{Q}^*$, άρα ένα ρητό σημείο της είναι το επ΄άπειρον σημείο $\infty = [1, 0, 0]$. Κάποια άλλα ρητά σημεία της καμπύλης είναι τα $(0, 1), (0, -1)$ και $(-1, 0)$. Στο κεφάλαιο V θα αποδείξουμε ότι τα παραπάνω σημεία αποτελούν ακριβώς το σύνολο των ρητών σημείων της C, δηλαδή $C(\mathbb{Q}) = \{\infty, (0, 1), (0, -1), (-1, 0)\}$. □

Κάθε υπερελλειπτική καμπύλη C έχει έναν μη-τετριμμένο αυτομορφισμό , που ονομάζεται **υπερελλειπτική involution** και συμβολίζεται $\iota = \iota_C$. Αν η C δίνεται από την εξίσωση $Y^2 = F(X, Z)$ τότε ο ι απεικονίζει το σημείο $[x, y, z]$ στο $[x, -y, z]$. Τα σταθερά σημεία του ι είναι τα $2g + 2$ σημεία $[x, 0, z]$, όπου $[x, z] \in \mathbb{P}^1$ είναι ρίζα του ομογενούς πολυωνύμου F. Επιπλέον, έχουμε την **υπερελλειπτική απεικόνιση πηλίκο** $\pi = \pi_C$,

$$\pi : C \to \mathbb{P}^1, \ \ [x, y, z] \mapsto [x, z].$$

Αφού το $[0, 1, 0]$ δεν είναι σημείο της καμπύλης, η π είναι καλά ορισμένη. Τότε ο ι είναι ο μη τετριμμένος αυτομορφισμός του διπλού καλύμματος π και τα σταθερά σημεία του ι είναι τα σημείο διακλάδωσης του π. Στις υπερελλειπτικές καμπύλες, τα σημεία του Weierstrass συμπίπτουν με τα σημεία διακλάδωσης (βλ. [37, σελ. 7])

Έστω $C : Y^2 = F(X, Z)$ μια υπερελλειπτική καμπύλη γένους g ορισμένη σε ένα σώμα K. Ο δακτύλιος συντεταγμένων της C υπέρ το K είναι ο $K[C] \coloneqq K[X, Y, Z]/\langle Y^2 - F(X, Z)\rangle$. Το πολυώνυμο $Y^2 - F(X, Z)$ είναι ανάγωγο και ομογενές στον $\mathbb{P}^2_g$, άρα το ο δακτύλιος συντεταγμένων $K[C]$ είναι ακέραια περιοχή με βάρη $(1, g + 1, 1)$ στα (X, Y, Z) αντίστοιχα.

Το ακόλουθο λήμμα ισχύει γενικά για κάθε καμπύλη. Αν το $P \in C(K)$ είναι ομαλό σημείο της καμπύλης τότε ο τοπικός δακτύλιος $\mathcal{O}_{C,P}$ είναι δακτύλιος διακριτής εκτίμησης.

3.9 Λήμμα. *Έστω $C : Y^2 = F(X, Z)$ μια υπερελλειπτική καμπύλη ορισμένη σε ένα σώμα K και έστω $P = [x, y, z] \in C(K)$. Τότε ο τοπικός δακτύλιος $\mathcal{O}_P$ είναι δακτύλιος διακριτής εκτίμησης με σώμα πηλίκων $K(C)$.*

Απόδειξη. Υποθέτουμε ότι $z = 1$ έτσι ώστε $(x, y) \in C_{\text{aff}}$ (η περίπτωση $x = 1$ αποδεικνύεται αναλόγως).

Αρχικά, υποθέτουμε ότι $x \neq 0$. Θα δείξουμε ότι υπάρχει K-γραμμικός ομομορφισμός δακτυλίων $K[C_{\text{aff}}] \to K[\![t]\!]$ που στέλνει το X στο $x + t$ και το Y σε μια δυναμοσειρά με σταθερό όρο y. Προς αυτό, αρκεί να ελέγξουμε ότι το $f(x + t) \in K[\![t]\!]$ έχει τετραγωνική ρίζα στο $K[\![t]\!]$ της μορφής $\tilde{y} = y + a_1t + a_2t^2 + ...$ Αυτό προκύπτει αν αναπτύξουμε το $f(x + t)$ σε δυνάμεις του t, χρησιμοποιώντας το ανάπτυγμα Taylor. Λαμβάνουμε

$$f(x + t) = y^2 + b_1t + b_2t^2 + ...$$

και αντικαθιστώντας στην αφινική εξίσωση, παίρνουμε μια εξίσωση της μορφής

$$(y + a_1t + a_2t^2 + ...)^2 = y^2 + b_1t + b_2t^2 + ...$$

Αναπτύσσοντας το αριστερό μέλος, παίρνουμε ένα σύστημα της μορφής $2ya_n = ..$ και έτσι μπορούμε να βρούμε τους συντελεστές του $\tilde{y}$.

Ο ομομορφισμός $K[X,Y] \to K[\![t]\!]$, $X \mapsto x+t$, $Y \mapsto \tilde{y}$ έχει πυρήνα που περιέχει το $Y^2 - f(X)$ (αφού η εικόνα του $Y^2 - f(X) \in K[X,Y]$ μέσω του ομομορφισμού είναι $\tilde{y}^2 - f(x+t) = 0$), άρα επάγει έναν K-γραμμικό ομομορφισμό $\alpha : K[X,Y]/\langle Y^2 - f(X)\rangle := K[C_{\text{aff}}] \to K[\![t]\!]$ με $\alpha(\phi(X,Y)) = \phi(x+t, y+a_1t+a_2t^2+...)$.

Επιπλέον, ο ομομορφισμός α είναι 1-1: μία βάση του $K[C_{\text{aff}}]$ είναι το σύνολο

$$\{1, X, X^2, ..., X^n, ..., Y, XY, X^2Y, ...\}$$

αφού λόγω της εξίσωσης $Y^2 = f(X)$, κάθε δύναμη του Y μεγαλύτερη του 1 μπορεί να εκφρασθεί ως προς X. Αν λοιπόν $h(x) \in K[C_{\text{aff}}]$ τότε $h(X) = h_1(X) + h_2(X)Y$ για κάποια $h_1(X,Y), h_2(X,Y) \in K[X]$. Άρα

$$\alpha(h(X)) = \alpha(h_1(X)+h_2(X)Y) = \alpha(h_1(X))+\alpha(h_2(X))\alpha(Y) = h_1(x+t)+h_2(x+t)\tilde{y}.$$

Αν $h_1(X) = 0$ τότε $h_1(x+t) = 0$ και $h_2(x+t) = 0$ (διότι $\tilde{y} \neq 0$). Αν $h_2(X) = 0$ τότε $h_2(x+t) = 0$ και $h_1(x+t) = 0$. Δηλαδή, αν $h_1(X) = 0$ ή $h_2(X) = 0$ τότε $h_1(x+t) = 0$ και $h_2(x+t) = 0$. Αν λοιπόν είχαμε $\alpha(h(X)) = 0$ αλλά $h_1(x+t) \neq 0$ ή $h_2(x+t) = 0$ τότε θα είχαμε $h_1(X) \neq 0$ και $h_2(X) \neq 0$, οπότε $h_1(X) + h_2(X)Y \neq 0$. τότε πολλαπλασιάζοντας την σχέση $h_1(x+t) + h_2(x+t)\tilde{y} = 0$ με την $h_1(x+t) + h_2(x+t)\tilde{y} = 0$, παίρνουμε $h_1(x+t)^2 = h_2(x+t)^2 f(x+t)^2$ (διότι $\tilde{y^2} = f(x+t)$). Άρα το $f(x+t)$ είναι τέλειο τετράγωνο που είναι άτοπο. Συνεπώς $h_1 = h_2 = 0$ και $h(X) = 0$ και συμπεραίνουμε ότι ο γραμμικός ομομορφισμός α είναι 1-1.

Ο σταθερός όρος του $\alpha(\phi)$ είναι το $\phi(x,y) = \phi(P)$ (από Taylor). Τα αντιστρέψιμα στοιχεία του $K[\![t]\!]$ είναι οι δυναμοσειρές του t με μη μηδενικό σταθερό όρο. Άρα ο α επεκτείνεται σε $K-$γραμμικό ομομορφισμό $\alpha : \mathcal{O}_{C,P} \to K[\![t]\!]$. Η εκτίμηση του $\mathcal{O}_{C,P}$ θα είναι η $v_P = v \circ \alpha$ όπου v η εκτίμηση του $K[\![t]\!]$. Αποδεικνύεται ότι η σύνθεση μιας εκτίμησης με έναν 1-1 ομομορφισμό δακτυλίων είναι εκτίμηση και περιέχει στοιχείο με εκτίμηση 1 (δηλαδή uniformizer) (βλ.[37, σελ. 9]). Εδώ, επιλέγουμε το $\alpha(X-x) = t$.

Θα δείξουμε ότι με αυτή την εκτίμηση, ο $\mathcal{O}_{C,P}$ είναι δακτύλιος διακριτής εκτίμησης. Αν $\phi \in \mathcal{O}_{C,P}$ με $v_P(\phi) = 0$ τότε $v(\alpha(\phi)) = 0$. Αυτό σημαίνει ότι η δυναμοσειρά ϕ έχει σταθερό όρο, επομένως $\phi \in \mathcal{O}^*_{C.P}$. Μένει να δείξουμε ότι το ιδεώδες $\mathfrak{m}_P = \{\phi \in \mathcal{O}_{C,P} : v_P(\phi) > 0\}$ είναι κύριο. Θα δείξουμε ότι $\mathfrak{m}_P = \langle X - x\rangle$. Η $Y^2 = f(X)$ γράφεται $Y^2 - y^2 = f(X) - y^2$ ή, ισοδύναμα, $(Y-y)(Y+y) = f(X) - y^2$. Όμως το x είναι ρίζα του πολυωνύμου $f(X) - y^2$ άρα $f(X) - y^2 = (X-x)f_1(X)$ για κάποιο $f_1 \in K[C_{\text{aff}}]$. Επίσης, $(Y+y)(P) = 2y \neq 0$ (γιατί εξ υποθέσεως $y \neq 0$ και $\text{ch}K \neq 0$). Άρα

$$Y - y = \frac{f_1(X)}{Y+y}(X-x)$$

και συνεπώς, $Y - y \in (X-x)\mathcal{O}_{C,P}$. Μπορούμε να γενικεύσουμε αυτό το αποτέλεσμα: έστω $h \in K[X,Y]$ με $h(P) = 0$. Τότε $h(X,Y) \in \mathcal{O}_{C,P}(X-x)$. Άρα κάθε $\phi \in K[C_{\text{aff}}]$

έχει αντιπρόσωπο $\dfrac{h_1(X,Y)}{h_2(X,Y)}$ με $h_1(P) \neq 0$ ή $h_2(P) \neq 0$. Αν $\phi \in \mathfrak{m}_P$ πρέπει $h_1(P) = 0$ (διότι αν $\phi \in \mathfrak{m}_p$, η ϕ δεν έχει σταθερό όρο) και $h_2(P) \neq 0$. Άρα $\phi \in \mathcal{O}_{C,P}(X - x)$, επομένως $\mathfrak{m}_P = \langle X - x \rangle$. Αποδείξαμε λοιπόν ότι στην περίπτωση $y \neq 0$, ο δακτύλιος $\mathcal{O}_{C,P}$ είναι δακτύλιος διακριτής εκτίμησης.
Αν $y = 0$ τότε $f(x) = 0$ οπότε από τον τύπο του Taylor, λαμβάνουμε $f(x + a) = f'(x)a + ...$ με $f'(x) \neq 0$ (διότι το $f(X) \coloneqq F(X, 1)$ δεν έχει πολλαπλές ρίζες). Όπως πριν, λύνουμε την εξίσωση $t^2 = f(x + a_2t^2 + a_4t^4) + ...$ και βρίσκουμε μια δυναμοσειρά $\tilde{x} = x + a_2t^2 + a_4t^4 + ... \in K[\![t]\!]$ τέτοια ώστε $t^2 = f(\tilde{x})$. Έτσι παίρνουμε έναν $K-$ομομορφισμό δακτυλίων $\alpha : \mathcal{O}_{C,P} \to K[\![t]\!]$ με $\alpha(\phi(X, Y)) = \phi(\tilde{x}, t)$. Βρίσκουμε ότι το maximal ιδεώδες $\mathfrak{m}_P$ του $\mathcal{O}_{C,P}$ είναι κύριο και παράγεται από το t.

Προφανώς $\mathrm{Quot}(\mathcal{O}_{C,P}) \subseteq K(C)$. Για τον αντίστροφο εγκλεισμό, αρκεί να παρατηρήσουμε ότι οι συναρτήσεις X και Y είναι ομαλές στο P, δηλαδή $X, Y \in \mathcal{O}_{C,P}$, οπότε $K(C) \subseteq \mathrm{Quot}(\mathcal{O}_{C,P})$. Τελικά, $\mathrm{Quot}(\mathcal{O}_{C,P}) = K(C)$. ■

3.10 Παρατήρηση. Στην παραπάνω απόδειξη, κατασκευάσαμε τους uniformizers για τα σημεία $P = (x, y)$ μιας υπερελλειπτικής καμπύλης. Αν $y \neq 0$ παίρνουμε τον $t = X - x$ ενώ αν $y = 0$ παίρνουμε τον $t = y$. Συναρτήσει των X και Y, ένας uniformizer στο επ'άπειρον σημείο $[1, s, 0]$ είναι ο $t = \dfrac{1}{X}$ αν $s \neq 0$ και ο $t = \dfrac{Y}{X^{g+1}}$ αν $s = 0$.

§2 Αναγωγή υπερελλειπτικών καμπυλών

Θεωρούμε μια υπερελλειπτική καμπύλη $C : Y^2 = F(X, Z)$ ορισμένη στο $\mathbb{Q}_p$ έτσι ώστε οι συντελεστές του F να ανήκουν στο $\mathbb{Z}_p$. Τότε μπορούμε να αναγάγουμε τους συντελεστές $\mod p$ και να πάρουμε ένα ομογενές πολυώνυμο $\bar{F} \in \mathbb{F}_p[X, Z]$ βαθμού $2g+2$. Αν το $\bar{F}$ είναι ελεύθερο τετραγώνων και $p \neq 2$, λέμε ότι η C έχει **καλή αναγωγή**. Αν η C είναι υπέρ το $\mathbb{Q}$ με $F \in \mathbb{Z}[X, Z]$ τότε λέμε ότι η C έχει **καλή αναγωγή στο** p αν η C έχει καλή αναγωγή ως καμπύλη ορισμένη στο $\mathbb{Q}_p$. Διαφορετικά, λέμε ότι η C έχει **κακή αναγωγή** στο p.

3.11 Παρατήρηση. Αφού έχουμε καλή (μη ιδιάζουσα) καμπύλη, δεν θα θεωρήσουμε minimal models.

Και στις δύο περιπτώσεις, το να έχει η καμπύλη καλή αναγωγή στο p είναι ισοδύναμο με το $p \nmid D(F)$ και $p \neq 2$ (διότι σε χαρακτηριστική 2, μία εξίσωση της μορφής $Y^2 = f(X)$ είναι πάντοτε ιδιάζουσα), όπου με $D(F)$ συμβολίζουμε την διακρίνουσα του πολυωνύμου F. Αν η C είναι καμπύλη υπέρ το $\mathbb{Q}$ με $F \in \mathbb{Z}[X, Z]$ τότε $D(F) \in \mathbb{Z} \setminus \{0\}$ (σύμφωνα με τον ορισμό της υπερελλειπτικής καμπύλης). Αυτό σημαίνει ότι μια τέτοια καμπύλη μπορεί να έχει κακή αναγωγή το πολύ σε πεπερασμένου πλήθους πρώτους (καθώς η διακρίνουσα ως ακέραιος αριθμός διαιρείται από το πολύ πεπερασμένου πλήθους πρώτους).

Ακόμη και αν η C έχει κακή αναγωγή, μπορούμε να γράψουμε $\bar{C}$ για την καμπύλη ορισμένη στο $\mathbb{F}_p$, οριζόμενη από την εξίσωση $Y^2 = \bar{F}(X, Z)$ (η οποία είναι υπερελλειπτική καμπύλη γένους g όταν η C έχει καλή αναγωγή). Δεδομένου ενός σημείου $P = [x, y, z] \in C(\mathbb{Q}_p)$, μπορούμε να πολλαπλασιάσουμε και τις τρεις συντεταγμένες με κατάλληλη δύναμη του p έτσι ώστε $x, z \in \mathbb{Z}_p$ και τα x, z να μην διαιρούνται και τα δύο με το p. Τότε έχουμε και $y \in \mathbb{Z}_p$ αφού $y^2 = F(x, z) \in \mathbb{Z}_p$. Άρα το $\bar{P} = [\bar{x}, \bar{y}, \bar{z}]$ είναι σημείο στον $\mathbb{P}^2_g(\mathbb{F}_p)$ που ανήκει στην $\bar{C}$ (αφού τα x, z δεν διαιρούνται ταυτοχρόνως από το p, τουλάχιστον ένα από τα $\bar{x}, \bar{z}$ είναι μη μηδενικό). Επομένως λαμβάνουμε μια **απεικόνιση αναγωγής**

$$\rho_p : C(\mathbb{Q}_p) \to \bar{C}(\mathbb{F}_p), \;\; P \mapsto \bar{P}.$$

Με χρήση του λήμματος του Hensel συνάγουμε το παρακάτω χρήσιμο αποτέλεσμα.

3.12 Πόρισμα. *Έστω $C : Y^2 = F(X, Z)$ μια υπερελλειπτική καμπύλη ορισμένη στο $\mathbb{Q}_p$ τέτοια ώστε $F \in \mathbb{Z}_p[X, Z]$. Θεωρούμε την υπερελλειπτική καμπύλη $\bar{C} : Y^2 = \bar{F}(X, Z)$ ορισμένη στο $\mathbb{F}_p$. Αν $Q \in \bar{C}(\mathbb{F}_p)$ είναι ομαλό σημείο της καμπύλης τότε υπάρχει σημείο $P \in C(\mathbb{Q}_p)$ τέτοιο ώστε $\bar{P} = Q$.*

Απόδειξη. Θα το αποδείξουμε γενικά για αφινικές καμπύλες στο επίπεδο ορισμένες στο $\mathbb{Q}_p$. Έστω $C : F(X, Y) = 0$ μία αφινική καμπύλη ορισμένη στο $\mathbb{Q}_p$. Υποθέτουμε ότι το Q βρίσκεται στο U_1. Με μετατόπιση του άξονα των συντεταγμένων μπορούμε να θεωρήσουμε ότι $Q = (0, 0) \in \mathbb{F}_p^2$. Με κατάλληλη αλλαγή συντεταγμένων, μπορούμε επίσης να θεωρήσουμε ότι η εξίσωση της καμπύλης έχει τη μορφή $f(X, Y) = 0$ με $f(X, Y) \in \mathbb{Z}_p[X, Y]$ και $p \nmid f_Y(0, 0)$. Αφού το $Q = (0, 0)$ είναι ομαλό σημείο της $\bar{C}(\mathbb{F}_p)$, έχουμε $p \nmid f_Y(0, 0)$. Επίσης, μπορούμε να υποθέσουμε ότι $f_Y(0, 0) = 1$ (αν δεν είναι 1, πολλαπλασιάζουμε την εξίσωση της καμπύλης με $f_Y(0, 0)^{-1}$). Από τον τύπο του Taylor,

$$f(0, Y) = f(0, 0) + f_Y(0, 0)y + \frac{1}{2} f_{YY}(0, 0)Y^2 + ... + \frac{1}{n!} f_{Y^n}(0, 0)Y^n$$

όπου n ο φυσικός αριθμός μετά τον οποίο οι μερικές παράγωγοι ως προς Y είναι ταυτοτικά ίσες με μηδέν. Αφού το $Y = 0$ είναι ρίζα του $f(0, Y)$, μπορούμε να γράψουμε $f(0, 0) = pa_0$ για κάποιο $a_0 \in \mathbb{Z}_p$. Άρα

$$f(0, Y) = pa_0 + Y + a_2 Y^2 + ... + a_n Y^n$$

με $a_0, a_2, ..., a_n \in \mathbb{Z}_p$.
Το $f(0, Y)$ είναι πολυώνυμο ως προς Y του οποίου η αναγωγή $\bmod p$,

$$\bar{f}(0, Y) = Y + a_2 Y^2 + ... + a_n Y^n,$$

έχει ρίζα την $Y = 0$. Από το Λήμμα του Hensel 2.9, η ρίζα $Y = 0 \in \mathbb{F}_p$ ανάγεται σε ρίζα, έστω y στο $p\mathbb{Z}_p$ (είναι στο $p\mathbb{Z}_p$ γιατί αν ήταν στο $\mathbb{Z}_p \setminus p\mathbb{Z}_p$, η αναγωγή $\bmod p$ θα ήταν μη μηδενική). Τελικά το σημείο $P = (0, y) \in \bar{C}(\mathbb{F}_p)$ ανάγεται στο Q, δηλαδή $\bar{P} = Q$. ■

3.13 Πόρισμα. *Έστω $C : Y^2 = F(X, Z)$ μία υπερελλειπτική καμπύλη γένους g τέτοια ώστε $F \in \mathbb{Z}[X, Z]$ και έστω $p \in \mathbb{P}$ τέτοιος ώστε $p > 4g^2 - 2$ και η C να έχει καλή αναγωγή στον p. Τότε $C(\mathbb{Q}_p) \neq \emptyset$, δηλαδή η καμπύλη C έχει $\mathbb{Q}_p$-ρητά σημεία.*

Απόδειξη. Έστω $\bar{C}$ η αναγωγή της $C \mod p$. Αφού εξ υποθέσεως η C έχει καλή αναγωγή $\mod p$, η $\bar{C}$ είναι υπερελλειπτική καμπύλη γένους g και συγκεκριμένα είναι ομαλή, προβολική και απολύτως ανάγωγη υπέρ το $\mathbb{F}_p$. Καθώς $|\mathbb{F}_p| = p$, από το Θεώρημα των Hasse-Weil 2.26 έχουμε ότι $\bar{C}(\mathbb{F}_p) \geq p + 1 - 2g\sqrt{p} > 0$ διότι

$$(p + 1)^2 = p^2 + 2p + 1 > p^2 + 2p > (4g^2 - 2)p + 2p = 4g^2 p,$$

από το οποίο προκύπτει ότι $p + 1 > 2g\sqrt{p}$. Άρα $\bar{C}(\mathbb{F}_p) \neq \emptyset$. Η $\bar{C}$ είναι ομαλή, άρα από το Πόρισμα 3.12 για κάθε σημείο $Q \in \bar{C}(\mathbb{F}_p)$, υπάρχουν σημεία $P \in C(\mathbb{Q}_p)$ τέτοια ώστε $\bar{P} = Q$. Επομένως, $C(\mathbb{Q}_p) \neq \emptyset$. ■

3.14 Παρατήρηση. Η υπόθεση ότι η C έχει καλή αναγωγή είναι απαραίτητη: Έστω $f(X) = X^{2g+2} + a_{2g+1}X^{2g+1} + ... + a_1X + a_0 \in \mathbb{Z}[X]$ ένα μονικό πολυώνυμο βαθμού $2g+2$ του οποίου η αναγωγή $\mod p$ είναι ανάγωγο πολυώνυμο. Θεωρούμε την αφινική καμπύλη $C : Y^2 = pf(X)$, καθώς και την προβολική της μορφή, $Y^2 = pF(X, 1) = p \cdot (X^{2g+2} + a_{2g+1}X^{2g+1}Z + ... + a_1XZ^{2g+1} + a_0Z^{2g+2})$. Προφανώς η C έχει κακή αναγωγή στο p.
Αν $x \in \mathbb{Z}_p$ έχουμε $p \nmid f(x)$ (διότι η αναγωγή του $f \mod p$ είναι ανάγωγο πολυώνυμο), οπότε $v_p(f(x)) = 1$. Από το Λήμμα 2.12, συμπεραίνουμε ότι το $pf(x)$ δεν είναι τετράγωνο στο $\mathbb{Q}_p$.

Αν $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p$, ισοδύναμα $v_p(x) < 0$ τότε η $v_p(f(x))$ ισούται με την ελάχιστη εκτίμηση των προσθεταίων του $f(x)$, δηλαδή $v_p(f(x)) = v_p(x^{2g+2}) = (2g + 2)v_p(x)$, οπότε $v(pf(x)) = (2g + 2)v_p(x) + 1$, δηλαδή η εκτίμηση του $pf(x)$ είναι περιττή. Πάλι από το Λήμμα 2.12, το $pf(x)$ δεν είναι τετράγωνο στο $\mathbb{Q}_p$.

Μένει να εξατάσουμε τι συμβαίνει στα επ΄άπειρον σημεία. Αφού το $f(X)$ έχει άρτιο βαθμό και είναι μονικό, τα επ΄άπειρον σημεία της καμπύλης είναι τα $[1, 1, 0]$ και $[1, -1, 0]$. Έχουμε $pF(1, 0) = p$ που έχει εκτίμηση 1, άρα δεν είναι τέλειο τετράγωνο.

Αφού σε κάθε περίπτωση το $pf(x)$ δεν είναι τετράγωνο στο $\mathbb{Q}_p$, η εξίσωση $Y^2 = pF(X)$ δεν έχει λύσεις στο $\mathbb{Q}_p$, επομένως $C(\mathbb{Q}_p) = \emptyset$.

Υπενθυμίζουμε ότι μια καμπύλη C υπέρ το $\mathbb{Q}$ έχει σημεία τοπικά παντού αν $C(\mathbb{Q}_p) \neq \emptyset$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$. Με το επόμενο θεώρημα, μπορούμε να αποφανθούμε αν μία υπερελλειπτική καμπύλη υπέρ το $\mathbb{Q}$ έχει ή δεν έχει σημεία τοπικά παντού.

3.15 Θεώρημα. *Έστω C μια υπερελλειπτική καμπύλη γένους g υπέρ το $\mathbb{Q}$ με εξίσωση $Y^2 = F(X, Z)$ όπου $F \in \mathbb{Z}[X, Z]$. Τότε μέσω μια πεπερασμένης διαδικασίας, μπορούμε να ελέγξουμε αν η C έχει σημεία τοπικά παντού ή αν δεν έχει.*

Απόδειξη. Στην περίπτωση του $\mathbb{R}$, αρκεί να ελέγξουμε ότι το F δεν έχει ρίζα στο $\mathbb{P}^1(\mathbb{R})$ και έχει αρνητικό μεγιστοβάθμιο συντελεστή.

Για όλους τους πρώτους $p \in \mathbb{P}$ με $p > 4g^2-2$ για τους οποίους η C έχει καλή αναγωγή στον p, $C(\mathbb{Q}_p) \neq \emptyset$ σύμφωνα με το Πόρισμα 3.13. Οι πρώτοι με κακή αναγωγή $\mod p$ έχουν, όπως είδαμε, πεπερασμένο πλήθος, άρα μπορούμε να ελέγξουμε την ύπαρξη $\mathbb{Q}_p$-ρητών σημείων με πεπερασμένη διαδικασία.

Για τους πρώτους $p \in \mathbb{P}$ με $p \leq 4g^2 - 2$, για τους οποίους η C έχει καλή αναγωγή $\mod p$ (το πλήθος των οποίων είναι προφανώς πεπερασμένο), ακολουθούμε την εξής διαδικασία:

Αν $\bar{C}(\mathbb{F}_p) = \emptyset$ τότε $C(\mathbb{Q}_p) = \emptyset$ (διότι αν το $C(\mathbb{Q}_p)$ περιείχε κάποιο σημείο τότε σύμφωνα με το Πόρισμα 3.12 το σημείο αυτό θα αναγόταν σε σημείο του $C(\mathbb{F}_p)$). Αν το $\bar{C}(\mathbb{F}_p)$ περιέχει ομαλά σημεία τότε από το Πόρισμα 3.12, $C(\mathbb{Q}_p) \neq \emptyset$.

Έστω τώρα ότι το $\bar{C}(\mathbb{F}_p)$ είναι μη κενό και περιέχει μόνο μη ομαλά σημεία. Εξετάζουμε κάθε $Q \in \bar{C}(\mathbb{F}_p)$ ξεχωριστά. Έπειτα από μια αλλαγή συντεταγμένων, μπορούμε να υποθέσουμε ότι $Q = (0, \bar{y}) \in U_1$. Για λόγους απλότητας , θα υποθέσουμε ότι $p \neq 2$. Αν η καμπύλη C έχει εξίσωση $Y^2 = F(X)$ τότε το $\bar{f}$ έχει πολλαπλή ρίζα στο 0 (διότι το Q δεν είναι ομαλό). Άρα από την εξίσωση παίρνουμε ότι $\bar{x} = 0$. Αφού το $\bar{f}$ έχει πολλαπλή ρίζα το 0, μπορούμε να γράψουμε

$$f(X) = pa_0 + pa_1X + a_2X^2 + a_3X^3 + ... + a_{2g+2}X^{2g+2}$$

με $a_j \in \mathbb{Z}_p$. Αν $p \nmid a_0$, τότε $v_p(f(x))$ για κάθε $x \in p\mathbb{Z}_p$, οπότε το Q δεν ανάγεται σε σημείο στο $C(\mathbb{Q}_p)$. Αλλιώς, θεωρούμε τον μετασχηματισμό $X \leftarrow pX$, $Y \leftarrow pY$ και την μετασχηματισμένη εξίσωση $(pY)^2 = f(pX)$, ισοδύναμα,

$$Y^2 = p^{-2}f(pX) = p^{-1}a_0 + a_1X + a_2X^2 + pa_3X^3 + ... + p^{2g}a_{2g+2}X^{2g+2} := f_1(X).$$

Έστω C_1 η καμπύλη που ορίζει η μετασχηματισμένη εξίσωση. Οι C και C_1 είναι ισόμορφες. Αναζητούμε σημεία $(x, y) \in C_1(\mathbb{Q}_p)$ με $x \in \mathbb{Z}_p$ και $y^2 = f_1(x)$. Επαναλαμβάνουμε αναδρομικά την παραπάνω διαδικασία. Η αναδρομή κάποια στιγμή σταματάει (αλλιώς η f θα είχε πολλαπλή ρίζα, βλ. [37, σελ. 16]) και έτσι δείχνουμε ότι είτε το Q ανάγεται σε σημείο στο $C(\mathbb{F}_p)$, οπότε $C(\mathbb{Q}_p) \neq \emptyset$ είτε όχι, οπότε $C(\mathbb{Q}_p) = \emptyset$. ■

3.16 Παράδειγμα. Η καμπύλη $C : Y^2 = f(X)$ με $f(X) = 2X^6 - 4 \in \mathbb{Q}[X]$ δεν έχει ρητά σημεία. Θα αποδείξουμε ότι δεν έχει $\mathbb{Q}_2$-σημεία.

Αν $x \in 2\mathbb{Z}_2$ τότε

$$f(x) \equiv 2x^6 - 4 \equiv -4 \equiv 124 \equiv 4 \cdot 31 \mod 2^7,$$

οπότε $f(x) = 4u$ με $u \equiv -1 \mod 8$. Επομένως σύμφωνα με το Λήμμα 2.13, το $f(x)$ δεν είναι τετράγωνο στο $\mathbb{Q}_2$.

Αν $x \in \mathbb{Z}_2^*$ τότε $v_2(f(x)) = 1$, οπότε σύμφωνα με το Λήμμα 2.13, το $f(x)$ δεν είναι τετράγωνο.

Αν $x \in \mathbb{Q}_2 \setminus \mathbb{Z}_2$ τότε $x = \dfrac{u}{2^n}$ με $u \in \mathbb{Z}_p^*$, οπότε $v_2(x) = -n$. Έτσι,

$$f(x) = 2\left(\frac{u}{2^n}\right)^6 - 4 = 2u^6 2^{-6n} - 4 = u^6 2^{1-6n} - 2^2 = 2^{1-6n}(u^6 - 2^{1+6n}),$$

άρα $v_2(f(x)) = 1-6n$ που είναι περιττός, επομένως το $f(x)$ δεν είναι τέλειο τετράγωνο.

Συμπεραίνουμε λοιπόν ότι σε καμία περίπτωση το $f(x)$ δεν είναι τετράγωνο. Επίσης, το 2 δεν είναι τετράγωνο στο $\mathbb{Q}_2$, άρα η καμπύλη δεν έχει ούτε τα επ΄άπειρον σημεία στο $\mathbb{Q}_2$. Τελικά, $C(\mathbb{Q}_2) = \emptyset$.

Όμως, $C(\mathbb{R}) \neq \emptyset$ και για κάθε $p \in \mathbb{P}$ με $p \neq 2$ έχουμε $C(\mathbb{Q}_p) \neq \emptyset$: Η διακρίνουσα του $f(X)$ είναι $2^{21} \cdot 3^6$ άρα η C έχει κακή αναγωγή μόνο για $p = 2, 3$. Για $p > 4g^2 - 2 = 13$, $C(\mathbb{Q}_p) \neq \emptyset$ σύμφωνα με το Πόρισμα 3.13 αφού η C έχει καλή αναγωγή. Για $p = 3, 5, 7, 11, 13$ η C έχει τα $\mathbb{F}_p$-σημεία $(1, 1), (0, 1), \infty, (1, 8)$ και $(0, 10)$ αντίστοιχα, άρα ανάγονται σε $\mathbb{Q}_p$-σημεία. □

§3 Διαιρέτες και η ομάδα του Picard

Σε αυτήν την παράγραφο, αναφέρουμε κάποια χρήσιμα παραδείγματα που αφορούν διαιρέτες υπερελλειπτικών καμπυλών και αποδεικνύουμε ότι ένας κύριος διαιρέτης πάνω από υπερελλειπτική καμπύλη έχει βαθμό 0. Με K θα συμβολίζουμε ένα τέλειο σώμα χαρακτηριστικής 0.

3.17 Παράδειγμα. Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη γένους g ορισμένη σε ένα σώμα K. Θα υπολογίσουμε τον διαιρέτη $\operatorname{div}(X - x)$ για $x \in K$. Η εξίσωση $X - x = 0$ έχει λύση x, η οποία μέσω της εξίσωσης της καμπύλης, αντιστοιχείται στα $\pm\sqrt{f(x)}$. Άρα, αν $\deg(f) = 2g + 2$ τότε

$$\operatorname{div}(X - x) = (x, \sqrt{f(x)}) + (x, -\sqrt{f(x)}) - \infty_s - \infty_{-s},$$

όπου s είναι μία τετραγωνική ρίζα του μεγιστοβάθμιου συντελεστή του $f(X)$, ενώ αν $\deg(f) = 2g + 1$ τότε

$$\operatorname{div}(X - x) = (x, \sqrt{f(x)}) + (x, -\sqrt{f(x)}) - 2 \cdot \infty.$$

Τα επ΄άπειρον σημεία εμφανίζονται διότι η συνάρτηση $X - x$ έχει πόλο σε αυτά. Για κάθε $x \in K$, ο διαιρέτης $D_x := (x, y) + (x, -y)$ όπου $y = \sqrt{f(x)} \in \bar{K}$ είναι K-ρητός: Αν $y \in K$ τότε και τα δύο σημεία $(x, y), (x, -y)$ μένουν αναλλοίωτα από την δράση της $\operatorname{Gal}(\bar{K}/K)$. Αν $y \notin K$ τότε η επέκταση $K(y)/K$ έχει βαθμό 2 και $\operatorname{Gal}(K(y)/K) = \{\mathrm{id}, \sigma\}$ όπου $\sigma((x, y)) = (x, -y)$ για κάθε $x \in K$ και $y \in K(y)$. Συνεπώς, η δράση της $\operatorname{Gal}(K(y)/K)$ είτε αφήνει τα $(x, y), (x, -y)$ σταθερά, οπότε ο D_x παραμένει αναλλοίωτος είτε εναλλάσσει τη σειρά των (x, y) και $(x, -y)$, οπότε και πάλι ο διαιρέτης D_x μένει αναλλοίωτος.

Και στις δύο περιπτώσεις, ο D_x μένει αναλλοίωτος από την δράση της ομάδας Galois, που σημαίνει ότι ο διαιρέτης D_x είναι K-ρητός.

Όμοια, ο διαιρέτης

$$D_\infty := \begin{cases} \infty_s + \infty_{-s}, & \text{αν } \deg(f) = 2g+2 \\ 2\infty, & \text{αν } \deg(f) = 2g+1 \end{cases}$$

όπου s είναι μία τετραγωνική ρίζα του μεγιστοβάθμιου συντελεστή του $f(X)$, είναι K-ρητός.

□

3.18 Παράδειγμα. Οι διαιρέτες D_x του παραπάνω παραδείγματος είναι ανά δύο γραμμικά ισοδύναμοι, αφού

$$\operatorname{div}\left(\frac{X-x_1}{X-x_2}\right) = \operatorname{div}(X-x_1) - \operatorname{div}(X-x_2) = D_{x_1} - D_\infty - (D_{x_2} - D_\infty) = D_{x_1} - D_{x_2}.$$

□

Η απόλυτη ομάδα Galois $\mathrm{Gal}(\bar{K}/K)$ δρα στο σύνολο $\bar{K}(C)$ (μέσω της δράσης της στους συντελεστές του αριθμητή και του παρονομαστή ενός στοιχείου του $\bar{K}(C)$). Η απεικόνιση div είναι συμβατή με την δράση της $\mathrm{Gal}(\bar{K}/K)$ από τις δύο πλευρές, δηλαδή $\sigma(\operatorname{div}(\phi)) = \operatorname{div}(\sigma(\phi))$ για κάθε $\sigma \in \mathrm{Gal}(\bar{K}/K)$ και για κάθε $\phi \in \bar{K}(C)$. Έτσι, αν $\phi \in K(C)^*$ τότε $\sigma(\phi) = \phi$, οπότε $\sigma(\operatorname{div}(\phi)) = \operatorname{div}(\sigma(\phi)) = \operatorname{div}(\phi)$, δηλαδή ο διαιρέτης $\operatorname{div}(\phi)$ είναι K-ρητός ή, με άλλα λόγια, $\operatorname{div}(\phi) \in \mathrm{Div}(C(K))$. Επίσης, λαμβάνουμε μία δράση της $\mathrm{Gal}(\bar{K}/K)$ στην ομάδα του Picard, $\mathrm{Pic}(C)$. Γράφουμε $\mathrm{Pic}(C(K))$ για την υποομάδα των στοιχείων που μένουν αναλλοίωτα από τη δράση και λέμε ότι αυτά τα στοιχεία είναι K-ρητά.

3.19 Παράδειγμα. Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη ορισμένη σε ένα σώμα K. Σύμφωνα με το Παράδειγμα 3.17, αν $\deg(f) = 2g+2$ τότε

$$\operatorname{div}(X) = (0, \sqrt{f(0)}) + (0, -\sqrt{f(0)}) - \infty_s - \infty_{-s} = D_0 - D_\infty$$

όπου s η τετραγωνική ρίζα του μεγιστοβάθμιου συντελεστή του f, ενώ αν $\deg(f) = 2g+1$ τότε

$$\operatorname{div}(X) = (0, \sqrt{f(0)}) + (0, -\sqrt{f(0)}) - 2 \cdot \infty.$$

Τώρα θα υπολογίσουμε τον διαιρέτη $\operatorname{div}(Y)$. Αν $\deg(f) = 2g+2$, τότε

$$\operatorname{div}(Y) = \sum_{a : f(a)=0} (a,0) - (g+1)D_\infty,$$

ενώ αν $\deg(f) = 2g+1$ τότε

$$\operatorname{div}(Y) = \sum_{a : f(a)=0} (a,0) - (2g+1)\infty.$$

Σημειώνουμε ότι αφού κάθε πολυώνυμο με μεταβλητές X και Y είναι ομαλό στον C_{aff}, στον διαιρέτη ενός τέτοιου πολυωνύμου, αρνητικός συντελεστής μπορεί να εμφανισθεί μόνο σε επ΄άπειρον σημεία . □

Στην παράγραφο 6 του πρώτου κεφαλαίου είχαμε αναφέρει πως ο βαθμός ενός κύριου διαιρέτη είναι 0 (Πρόταση 1.62). Στην περίπτωση των υπερελλειπτικών καμπυλών, αυτό επιβεβαιώνεται και από τα παραπάνω παραδείγματα. Στην επόμενη πρόταση, το αποδεικνύουμε για υπερελλειπτικές καμπύλες.

3.20 Πρόταση. *Έστω C μια υπερελλειπτική καμπύλη ορισμένη σε ένα σώμα K και $\phi \in \bar{K}(C)^*$. Τότε* $\deg(\mathrm{div}(\phi)) = 0$.

Απόδειξη. Η υπερελλειπτική involution ι δρα στο $\bar{K}(C)^*$ και στο $\mathrm{Div}(C)$ στέλνοντας το (x, y) στο $(x, -y)$. Είναι $\deg(\iota(\phi)) = \deg(\mathrm{div}(\phi))$, οπότε

$$\deg(\mathrm{div}(\phi \cdot \iota(\phi))) = \deg(\mathrm{div}(\phi)) + \mathrm{div}(\iota(\phi)) = 2\deg(\mathrm{div}(\phi)). \tag{3.1}$$

Η ϕ αναπαρίσταται μέσω μιας συνάρτησης στο $\mathbb{P}^2_g(K)$ της μορφής $h_1(X) + h_2(X)Y$ με $h_1(X)$, $h_2(X) \in \bar{K}(X)$. Είναι $\iota(\phi) = h_1(X) - h_2(X)Y$, άρα το

$$\phi \cdot \iota(\phi) = h_1(X)^2 - h_2(X)^2Y^2 = h_2(X)^2 - h_2(X)^2 f(X) \in \bar{K}(X)$$

είναι συνάρτηση μόνο του X. Γράφοντας προβολικά την $\phi \cdot \iota(\phi)$ ως πηλίκο δύο ομογενών πολυωνύμων του $\bar{K}[X, Z]$, βλέπουμε ότι έχει το ίδιο πλήθος ριζών και πόλων, άρα $\deg(\mathrm{div}(\phi \cdot \iota(\phi))) = 0$. Από την (3.1) προκύπτει ότι $\deg(\mathrm{div}(\phi)) = 0$. ■

3.21 Παράδειγμα. Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη περιττού βαθμού γένους g. Θα βρούμε μία βάση για τον χώρο Riemann-Roch $\mathscr{L}(n \cdot \infty)$, $n \in \mathbb{N}$.
Το σύνολο των ρητών συναρτήσεων της C που είναι ομαλές εκτός του ∞ είναι ο δακτύλιος συντεταγμένων $K[X, Y]$ της C_{aff}. Μία K-βάση του $K[X, Y]$ είναι το σύνολο

$$\{1, X, X^2, ..., Y, XY, X^2Y, ...\}.$$

Από το Παράδειγμα 3.19 έχουμε ότι $v_\infty(X) = -2$ και $v_\infty(Y) = -(2g + 1)$. Άρα για κάθε $n \in \mathbb{N}$,

$$v_\infty(X^n) = nv_\infty(X) = -2n$$

και

$$v_\infty(X^nY) = v_\infty(X^n) + v_\infty(Y) = -(2n + 2g + 1).$$

Βλέπουμε ότι τα στοιχεία της βάσης έχουν όλα μεταξύ τους διαφορετική εκτίμηση στο ∞. Έτσι, η εκτίμηση ενός γραμμικού συνδυασμού στοιχείων της βάσης, είναι ίση με την μικρότερη εκτίμηση από τα στοιχεία της βάσης που προκύπτουν στον γραμμικό συνδυασμό με μη μηδενικό συντελεστή.

Από την Πρόταση 1.65, γνωρίζουμε ότι $\mathscr{L}(0) = K = \langle 1 \rangle$. Επίσης, $\phi \in \mathscr{L}(\infty)$ αν και μόνο αν $\mathrm{div}(\phi) \geq -\infty$, δηλαδή αν και μόνο αν η ϕ παρουσιάζει πόλο στο ϕ το πολύ τάξης 1. Συνεπώς η ϕ πρέπει να έχει εκτίμηση 0 στο ∞, καθώς κανένα στοιχείο της βάσης δεν έχει εκτίμηση 1. Άρα $\mathscr{L}(\infty) = \langle 1 \rangle$. Όμοια, $\phi \in \mathscr{L}(2 \cdot \infty)$ αν και μόνο αν $\mathrm{div}(\phi) \geq 2 \cdot \infty$, δηλαδή αν και μόνο αν η ϕ παρουσιάζει πόλο στο ϕ το πολύ τάξης 2. Άρα $\mathscr{L}(2 \cdot \infty) = \langle 1, X \rangle$.

Συνεχίζοντας με τον ίδιο τρόπο, βρίσκουμε βάση για τον χώρο $\mathscr{L}(n\cdot\infty)$ για κάθε $n\in\mathbb{N}_0$ (βλ. επόμενη σελίδα).

$$\begin{aligned}
\mathscr{L}(0) &= \langle 1\rangle\\
\mathscr{L}(\infty) &= \langle 1\rangle\\
\mathscr{L}(2\cdot\infty) &= \langle 1, X\rangle\\
\mathscr{L}(3\cdot\infty) &= \langle 1, X\rangle\\
&\vdots\\
\mathscr{L}(2n\cdot\infty) &= \langle 1, X, X^2, ..., X^n\rangle \text{ αν } n\le g\\
\mathscr{L}((2n+1)\cdot\infty) &= \langle 1, X, X^2, ..., X^n\rangle \text{ αν } n< g\\
&\vdots\\
\mathscr{L}(2g\cdot\infty) &= \langle 1, X, X^2, ..., X^g\rangle\\
\mathscr{L}((2g+1)\cdot\infty) &= \langle 1, X, X^2, ..., X^g, Y\rangle\\
\mathscr{L}((2g+2)\cdot\infty) &= \langle 1, X, X^2, ..., X^g, Y, X^{g+1}\rangle\\
&\vdots\\
\mathscr{L}(2n\cdot\infty) &= \langle 1, X, X^2, ..., X^g, Y, X^{g+1}, XY, ..., X^{n-g-1}Y, X^n\rangle \text{ αν } n\ge g+1\\
\mathscr{L}((2n+1)\cdot\infty) &= \langle 1, X, X^2, ..., X^g, Y, X^{g+1}, XY, ..., X^n, X^{n-g}Y\rangle \text{ αν } n\ge g\\
&\vdots
\end{aligned}$$

Για τις διαστάσεις των παραπάνω χώρων, έχουμε

$$\dim_K(\mathscr{L}(n\cdot\infty)) = \begin{cases} 0, & \text{αν } n<0\\ [\frac{n}{2}]+1, & \text{αν } 0\le n\le 2g\\ n-g+1, & \text{αν } 2g+1\le n\end{cases}$$

□

§4 Ιακωβιανή και αναπαράσταση σημείων

Έστω C μία ομαλή, προβολική και απολύτως ανάγωγη καμπύλη γένους g ορισμένη σε ένα σώμα K. Όπως έχουμε ήδη αναφέρει, μπορούμε να ταυτίσουμε την Ιακωβιανή $J(K)$ μια καμπύλης με την ομάδα $\mathrm{Pic}^0(C)$. Το πλεονέκτημα αυτής της προσέγγισης είναι ότι μπορούμε να αναπαραστήσουμε σημεία της Ιακωβιανής με διαιρέτες πάνω στην καμπύλη. Επίσης, μπορούμε να χρησιμοποιήσουμε αυτήν την αναπαράσταση για να κάνουμε υπολογισμούς στην ομάδα $J(K)$.

Αν $P_0\in C(K)$ τότε λαμβάνουμε μία φυσιολογική απεικόνιση $i: C\to J$, $i(P)=[P-P_0]$. Η απεικόνιση αυτή είναι μορφισμός αλγεβρικών πολλαπλοτήτων, που είναι 1-1 αν $g>0$, οπότε ταυτίζουμε τα στοιχεία του $C(K)$ με αυτά του $J(K)\cap C(K)$. Έτσι, το πρόβλημα της εύρεσης του συνόλου $C(K)$, μπορεί να ταυτισθεί με την εύρεση του

συνόλου $J(K) \cap i(C(K))$, δηλαδή ελέγχουμε ποια σημεία της $J(K)$ προέρχονται από σημεία του $C(K)$. Για παράδειγμα, αν $J(K) = \{0\}$ τότε $i(P) = 0$, δηλαδή $[P - P_0] = 0$, οπότε $P = P_0$, και συνεπώς $C(K) = \{P_0\}$.

3.22 Πρόταση. *Έστω C μια ομαλή, προβολική, απολύτως ανάγωγη καμπύλη γένους g ορισμένη σε ένα σώμα K. Σταθεροποιούμε ένα σημείο $P_0 \in C(K)$. Τότε για κάθε $Q \in J(K)$, υπάρχει μοναδικός effective διαιρέτης $D_Q \in \mathrm{Div}(C(K))$ ελάχιστου βαθμού τέτοιος ώστε $Q = [D_Q - \deg(D_Q) \cdot P_0]$.*

Απόδειξη. Έστω $D \in \mathrm{Div}^0(C)$ ένας διαιρέτης τέτοιος ώστε $Q = [D]$. Αρχικά, εργαζόμαστε στο $\bar{K}$ (διότι αν το K δεν είναι αλγεβρικά κλειστό, δεν είναι απαραίτητο ότι μία K-ρητή γραμμική κλάση ισοδυναμίας περιέχει K-ρητούς διαιρέτες). Θεωρούμε τους χώρους $\mathscr{L}_n = \mathscr{L}(D + n \cdot P_0)$ για $n \geq -1$. Είναι $\mathscr{L}_n \subseteq \mathscr{L}_{n+1}$ διότι αν $\phi \in \mathscr{L}_n$ τότε $\mathrm{div}(\phi) + D + nP_0 \geq 0$ άρα και $\mathrm{div}(\phi) + D + (n+1) \geq 0$ που σημαίνει ότι $\phi \in \mathscr{L}_{n+1}$. Άρα έχουμε την ακολουθία

$$\{0\} = \mathscr{L}_{-1} \subseteq \mathscr{L}_0 \subseteq \mathscr{L}_1 \subseteq \ldots$$

Ισχυριζόμαστε ότι $\dim_K(\mathscr{L}_{n+1}) - \dim_K(\mathscr{L}_n) \in \{0, 1\}$. Πράγματι, από το Θεώρημα Riemann-Roch 1.75,

$$\begin{aligned} \dim_K(\mathscr{L}_n) &= \deg(D + nP_0) - g + 1 + \dim_K(\mathscr{L}(W - D - nP_0)) \\ &= \deg(D) + n - g + \dim_K(\mathscr{L}(W - D - nP_0)) \end{aligned}$$

Ο βαθμός του διαιρέτη $D + nP_0$ αυξάνεται καθώς το n μεγαλώνει, άρα για κάποιο $n_0 \in \mathbb{N}$ θα έχουμε $\deg(D + n_0 P_0) \geq \deg(W)$, άρα έχουμε

$$\begin{aligned} \dim_K(\mathscr{L}_{n_0+1}) &= \dim_K(\mathscr{L}(D + (n_0+1)P_0)) \\ &= (\deg(D) + n_0 + 1 - g) + 1 \ \text{(Πόρισμα 1.79)} \\ &= \dim_K(\mathscr{L}_{n_0}) + 1 \end{aligned}$$

Αυτό συνεπάγεται ότι υπάρχει μοναδικός ελάχιστος $n \in \mathbb{N}_0$ τέτοιος ώστε $\dim_K(\mathscr{L}_n) = 1$. Έστω ϕ ένα μη τετριμμένο στοιχείο του $\mathscr{L}_n$, οπότε $\mathrm{div}(\phi) + D + nP \geq 0$. Θέτουμε $D_Q = \mathrm{div}(\phi) + D + nP$. Προφανώς ο D_Q είναι effective, δεν εξαρτάται από την επιλογή της ϕ και

$$Q = [D] = [D + \mathrm{div}(\phi)] = [D_Q - nP_0].$$

Επίσης είναι εμφανές ότι ο D_Q είναι ο μοναδικός διαιρέτης με αυτές τις ιδιότητες και δεν υπάρχει διαιρέτης μικρότερου βαθμού με τις ίδιες ιδιότητες (λόγω της μοναδικότητας του n). Επιπλέον, ο D_Q είναι K-ρητός, διότι για κάθε $\sigma \in \mathrm{Gal}(\bar{K}/K)$ έχουμε

$$\begin{aligned} [\sigma(D_Q) - nP_0] &= [\sigma(D_Q - nP_0)] \ \text{(διότι } P_0 \in C(K)) \\ &= \sigma([D_Q - nP_0]) \ \text{(λόγω της συμβατότητας της δράσης)} \\ &= \sigma(Q) \\ &= Q \ \text{(διότι } Q \in J(K)) \\ &= [D_Q - nP_0], \end{aligned}$$

δηλαδή $[\sigma(D_Q) - nP_0] = Q = [D_Q - nP_0]$. Όμως ο D_Q είναι ο μοναδικός effective διαιρέτης βαθμού n που ικανοποιεί την $Q = [D_Q - nP_0]$, οπότε $\sigma(D_Q) = D_Q$, που σημαίνει ότι ο D_Q είναι K-ρητός.

Τέλος,

$$\dim_K(\mathscr{L}_g)) = g - g + 1 + \dim_K(\mathscr{L}(W - D - gP_0)) = 1 + \dim_K(\mathscr{L}(W - D - gP_0)) \geq 1,$$

οπότε $n \leq g$ (διότι n ο ελάχιστος για τον οποίο $\dim_K(\mathscr{L}_n) = 1$). ■

3.23 Ορισμός. Έστω $C : Y^2 = f(X)$ υπερελλειπτική καμπύλη περιττού βαθμού γένους g ορισμένη σε ένα σώμα K. Θα λέμε ότι ένας διαιρέτης $D \in \mathrm{Div}(C)$ βρίσκεται σε **γενική θέση** αν είναι effective, $\infty \notin \mathrm{supp}(D)$ και δεν υπάρχει σημείο $P \in C$ τέτοιο ώστε $D \geq P + \iota(P)$.

3.24 Σημείωση. Η συνθήκη ότι δεν υπάρχει σημείο $P \in C$ τέτοιο ώστε $D \geq P + \iota(P)$ για κάθε $P \in C$ σημαίνει ότι για οποιοδήποτε σημείο P, τα P και $\iota(P)$ δεν ανήκουν και τα δύο στο $\mathrm{supp}(D)$. Αν ήταν $P, \iota(P) \in \mathrm{supp}(D)$ τότε αφού ο D είναι effective, θα είχαμε $v_P(D) \geq 1$ και $v_{\iota(P)}(D) \geq 1$, το οποίο σημαίνει ότι $D \geq P + \iota(P)$, που είναι άτοπο.

3.25 Λήμμα. *Έστω $C : Y^2 = f(X)$ υπερελλειπτική καμπύλη ορισμένη σε ένα σώμα K και $P = (x, y)$ ένα σημείο της C που δεν είναι σημείο του Weierstrass. Αν $\phi(X, Y) \in \bar{K}(C)$ μία ρητή συνάρτηση η οποία δεν έχει πόλο στο P, τότε για κάθε $k \geq 0$, υπάρχουν μοναδικές σταθερές $c_0, ..., c_k \in \bar{K}$ και $\phi_k(X, Y) \in \bar{K}(C)$ η οποία δεν έχει πόλο στο P, τέτοιες ώστε*

$$\phi(X, Y) = \sum_{i=0}^{k} c_i (X - x)^i + (X - x)^{k+1} \phi_k(X, Y).$$

Απόδειξη. Θέτουμε $c_0 = \phi(x, y)$ και θεωρούμε την ρητή συνάρτηση

$$\phi_1(X, Y) = \frac{\phi(X, Y) - \phi(x, y)}{X - x}.$$

Η $X - x$ έχει ρίζα στο P τάξης 1 και η $\phi(X, Y) - \phi(x, y)$ έχει ρίζα στο P τάξης τουλάχιστον 1, επομένως $v_P(\phi_1(X, Y)) \geq 0$, δηλαδή η $\phi_1(X, Y)$ δεν έχει πόλο στο P. Συνεπώς, μπορούμε να γράψουμε

$$\phi(X, Y) = c_0 + (X - x)\phi_1(X, Y)$$

όπου η ϕ_1 δεν έχει πόλο στο P. Συνεχίζοντας επαγωγικά, λαμβάνουμε τον ζητούμενο τύπο για την $\phi(X, Y)$. ■

Το επόμενο Λήμμα οφείλεται στον Mumford (βλ. [21]).

3.26 Λήμμα. *Έστω $C : Y^2 = f(X)$ υπερελλειπτική καμπύλη περιττού βαθμού γένους g ορισμένη σε ένα σώμα K και $D \in \mathrm{Div}(C(K))$ ένας διαιρέτης σε γενική θέση στην C. Τότε υπάρχουν μοναδικά πολυώνυμα $a(X), b(X) \in K[X]$ τέτοια ώστε:*

1. *Το* $a(X)$ *είναι μονικά βαθμού* $d \coloneqq \deg(D)$.
2. $\deg(b(X)) < d$.
3. *Ισχύει η ισοτιμία* $f(X) \equiv b^2(X) \mod a(X)$.
4. *Αν* $(x, y) \in C_{\text{aff}}$ *τότε* $(x, y) \in \text{supp}(D)$ *αν και μόνο αν* $a(x) = 0$ *και* $b(x) = y$.

Αντίστροφα, κάθε ζεύγος πολυωνύμων (a, b) *που ικανοποιεί τις πρώτες τρεις ιδιότητες, προσδιορίζει έναν διαιρέτη* D *σε γενική θέση.*

Απόδειξη. Έστω $D = \sum_P v_P(D)P$. Το πολυώνυμο

$$a(X) \coloneqq \prod_{P=(x,y)\in \text{supp}(D)} (X - x)$$

ικανοποιεί την (1) και το πρώτο μέρος της (4) και είναι μονοσήμαντα ορισμένο.

Για τον προσδιορισμό του b, ουσιαστικά παρεμβάλουμε τα σημεία του support του D. Πιο συγκεκριμένα, έστω $P_i = (x_i, y_i) \in \text{supp}(D)$, $i = 1, ..., r = |\text{supp}(D)|$. Αφού ο D είναι K-ρητός και σε γενική θέση, ισχύει ότι $(x_i, y_i) \in C(K)$ για κάθε $i = 1, ..., r$. Με αυτόν τον συμβολισμό,

$$a(X) = \prod_{i=1}^{r} (X - x_i)^{v_{P_i}(D)}.$$

Από το Λήμμα 3.25, μπορούμε για κάθε $(x_i, y_i) \in \text{supp}(D)$ να γράψουμε

$$Y = \sum_{j=1}^{n_i-1} c_j (X - x_i)^j + (X - x_i)^{n_i} \phi_{n_i}$$

για κάποιες σταθερές $c_j \in K$ και ρητές συναρτήσεις $\phi_{n_i} \in K(C)$, όπου $n_i = v_{P_i}(D)$ και $c_0 = y_i$. Θέτουμε

$$b_{x_i} = \sum_{j=1}^{n_i-1} c_j (X - x)^j.$$

Έτσι για κάθε x_i, έχουμε την ισοτιμία

$$Y \equiv b_{x_i} \mod (X - x_i)^{n_i},$$

και συνεπώς

$$f(X) \equiv b_{x_i}^2 \mod (X - x_i)^{n_i}$$

για κάθε x_i. Τελικά, λαμβάνουμε ένα σύστημα ισοτιμιών $f(X) \equiv b_{x_i} \mod (X - x_i)^{n_i}$ για $i = 1, ..., r$ όπου τα πολυώνυμα $(X - x_i)^{n_i}$ είναι πρώτα μεταξύ τους (διότι τα x_i είναι διαφορετικά ανά δύο). Από το Κινέζικο Θεώρημα Υπολοίπων, το σύστημα έχει

λύση, έστω b, η οποία είναι μοναδική $\mod \prod_{i=1}^{r}(X-x_i)^{n_i} = a(X)$ αν απαιτήσουμε $\deg(b) < \deg(a)$.

Για το αντίστροφο, έστω $a(X) = \prod_{i=1}^{d}(X-x_i)$. Τότε ο διαιρέτης

$$D = \sum_{x:a(x)=0} v_{(X-x)}(a)(x, b(x))$$

είναι effective και έχει βαθμό $d = \deg(a)$. Επίσης, αν το $P = (x, 0)$ είναι σημείο Weierstrass τότε $v_P(D) = 0$ ή 1: Αν ήταν $v_P(D) \geq 2$ τότε θα είχαμε $(X-x)^2 \mid a(X)$ και $(X-x)^2 \mid b^2(X)$, αφού $b(x) = 0$. Όμως από την ισοτιμία $f(X) \equiv b^2(X) \mod a(X)$ θα είχαμε ότι $(X-x)^2 \mid f(X)$, δηλαδή το f θα είχε πολλαπλή ρίζα, που είναι άτοπο. Επιπλέον, ο D δεν περιέχει ταυτοχρόνως ένα σημείο (x, y) μαζί με το $(x, -y)$ (διότι αν αυτό συνέβαινε θα είχαμε $b(x) = y = -y$, δηλαδή $y = 0$, δηλαδή το σημείο Weierstrass $(x, 0)$ θα βρισκόταν στην ανάλυση του D με συντελεστή 2, άτοπο). Τέλος, ισχύει ότι $\infty \notin \mathrm{supp}(D)$. Συνεπώς ο D βρίσκεται σε γενική θέση. ■

3.27 Ορισμός. Η αναπαράσταση ενός διαιρέτη D ως ζεύγος πολυωνύμων όπως παραπάνω, λέγεται **αναπαράσταση Mumford** του D.

3.28 Λήμμα. *Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη περιττού βαθμού γένους g ορισμένη σε ένα σώμα K. Τότε για κάθε $P \in J(K)$, υπάρχει μοναδικός διαιρέτης $D \in \mathrm{Div}(C(K))$ σε γενική θέση βαθμού $d = \deg(D) \leq g$ τέτοιος ώστε $P = [D - d \cdot \infty]$.*

Απόδειξη. Από την Πρόταση 3.22, υπάρχει μοναδικός effective διαιρέτης $D \in \mathrm{Div}(C(K))$ ελάχιστου βαθμού d τέτοιος ώστε $P = [D - d \cdot \infty]$. Πρέπει να δείξουμε ότι ο D είναι σε γενική θέση και ότι για κάθε διαιρέτη D' σε γενική θέση βαθμού $d' \leq g$ τέτοιο ώστε $P = [D' - d' \cdot \infty]$ έχουμε $D' = D$.

Αν ο D δεν ήταν σε γενική θέση τότε θα είχαμε $D \geq D_x$ για κάποιο $x \in K$ ή $D \geq \infty$. Στην πρώτη περίπτωση ($D \geq D_x$), από το Παράδειγμα 3.17, ο D_x είναι γραμμικά ισοδύναμος με τον διαιρέτη $2 \cdot \infty$, άρα

$$P = [D - d \cdot \infty] = [(D - D_x) - (d-2) \cdot \infty],$$

που αντίκειται στον ορισμό του d.

Στη δεύτερη περίπτωση ($D \geq \infty$), έχουμε

$$P = [D - d \cdot \infty] = [(D - \infty) - (d-1) \cdot \infty],$$

το οποίο πάλι αντίκειται στον ορισμό του d.

Αν ο D' είναι σε γενική θέση, έχει βαθμό $\deg(D') = d' \leq g$ και $[D' - d' \cdot \infty] = [D - d \cdot \infty]$, τότε $[D' - D] = [d' - d \cdot \infty]$. Όμως γνωρίζουμε ότι $[D + \iota(D)] = [2d \cdot \infty]$,

επομένως παίρνουμε $[D' + \iota(D)] = [(d' + d) \cdot \infty]$. Συνεπώς, υπάρχει $\phi \in \mathscr{L}((d' + d)\infty)$ τέτοια ώστε $\mathrm{div}(\phi)_0 = D' + \iota(D)$. Όμως, $d' + d \leq g$, επομένως από το Παράδειγμα 3.21 έχουμε $\mathscr{L}((d' + d)\infty) \subseteq \langle 1, X, X^2, ..., X^g \rangle$, που σημαίνει ότι $\phi \in K[X]$. Όμως τότε ο διαιρέτης $\mathrm{div}(\phi)$ είναι άθροισμα διαιρετών της μορφής D_x, το οποίο είναι δυνατόν μόνο όταν $D' = \iota(\iota(D))$, αφού οι διαιρέτες D' και $\iota(D)$ βρίσκονται σε γενική θέση. ■

3.29 Θεώρημα. *Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη περιττού βαθμού γένους g ορισμένη σε ένα σώμα K. Έστω $P_1, P_2 \in J(K)$ με αναπαραστάσεις Mumford (a_1, b_1) και (a_2, b_2) αντίστοιχα. Τότε μπορούμε να υπολογίσουμε την αναπαράσταση Mumford του $P_1 + P_2$ ως εξής:*

Σύνθεση: *προσθέτουμε τους διαιρέτες και αφαιρούμε διαιρέτες της μορφής $D_x = (x, y) + (x, -y)$:*

1. *Θέτουμε $d(X) = \mu\kappa\delta(a_1(X), a_2(X), b_1(X) + b_2(X))$.*
2. *Θέτουμε $a(X) = \dfrac{a_1(X)a_2(X)}{d^2(X)}$.*
3. *Έστω $b(X)$ το μοναδικό πολυώνυμο με βαθμό μικρότερο του $\deg(a(X))$ που ικανοποιεί τις ισοτιμίες*

$$b(X) \equiv b_1(X) \mod \frac{a_1(X)}{d(X)}, \quad b(X) \equiv b_2(X) \mod \frac{a_2(X)}{d(X)}$$

και

$$f(X) \equiv b(X)^2 \mod a(X).$$

Τότε το (a, b) αναπαριστά έναν διαιρέτη D τέτοιο ώστε $P_1 + P_2 = [D - \deg(D) \cdot \infty]$.

Αναγωγή: *Όσο $\deg(a) > g$, επαναλαμβάνουμε την ακόλουθη διαδικασία:*

1. *Γράφουμε $f(X) - b^2(X) = \lambda a(X)c(X)$ για κάποια $\lambda \in K^*$ και $c(X) \in K[X]$ μονικό.*
2. *Αντικαθιστούμε το $a(X)$ με το $c(X)$. Σημειώνουμε ότι $\deg(c) < \deg(a)$.*
3. *Αντικαθιστούμε το $b(X)$ με το υπόλοιπό του $-b(X) \mod c(X)$.*

Τώρα το (a, b) αναπαριστά έναν διαιρέτη D τέτοιο ώστε $P_1 + P_2 = [D - \deg(D) \cdot \infty]$ και $\deg(D) \leq g$.

Απόδειξη.

Σύνθεση: Έστω $P_i = [D_i - \deg(D_i) \cdot \infty]$, $i = 1, 2$. Από τον ορισμό της αναπαράστασης Mumford,

$$a_i(X) = \prod_{(x,y) \in \mathrm{supp}(D_i)} (X - x),$$

$\deg(b_i) < \deg(a_i), b_i(x) = y$ για κάθε $(x, y) \in \mathrm{supp}(D_i)$ και $f(X) \equiv b_i^2(X) \mod a_i(X)$. Ξεκινάμε με την ύπαρξη του b. Από την $f \equiv b_1^2 \mod a_1$ παίρνουμε

$$f \equiv b_1^2 \mod \mu\kappa\delta(a_1, a_2).$$

Όμοια, λαμβάνουμε

$$f \equiv b_2^2 \mod \mu\kappa\delta(a_1, a_2).$$

Από τις δύο τελευταίες προκύπτει ότι $b_1^2 \equiv b_2^2 \mod \mu\kappa\delta(a_1, a_2)$, δηλαδή

$$(b_1 - b_2)(b_1 + b_2) \equiv \mod \mu\kappa\delta(a_1, a_2),$$

ή, ισοδύναμα,

$$(b_1 - b_2)\frac{b_1 + b_2}{d} \equiv 0 \mod \mu\kappa\delta\left(\frac{a_1}{d}, \frac{a_2}{d}\right). (1)$$

Όμως είναι $d = \mu\kappa\delta(a_1, a_2, b_1 + b_2)$, ισοδύναμα

$$d = \mu\kappa\delta(\mu\kappa\delta(a_1, a_2), b_1 + b_2),$$

ισοδύναμα

$$\mu\kappa\delta\left(\mu\kappa\delta\left(\frac{a_1}{d}, \frac{a_2}{d}\right), \frac{b_1 + b_2}{d}\right) = 1.$$

Λοιπόν από την (1),

$$\mu\kappa\delta\left(\frac{a_1}{d}, \frac{a_2}{d}\right) | (b_1 - b_2).$$

Από το Κινεζικό Θεώρημα Υπολοίπων προκύπτει ότι υπάρχει $b' \in K[X]$ τέτοιο ώστε

$$b' \equiv b_1 \mod \frac{a_1}{d} \text{ και } b' \equiv b_2 \mod \frac{a_2}{d}.$$

Από αυτές, παίρνουμε $f \equiv b'^2 \mod a'$ όπου $a' = \dfrac{a_1 a_2}{d\mu\kappa\delta(a_1, a_2)}$.

Τώρα θα δείξουμε ότι υπάρχει b τέτοιο ώστε $b \equiv b' \mod a'$ και $f \equiv b^2 \mod a$. Παρατηρούμε ότι

$$a = a'\mu\kappa\delta(\frac{a_1}{d}, \frac{a_2}{d}),$$

αφού

$$a'\mu\kappa\delta(\frac{a_1}{d}, \frac{a_2}{d}) = \frac{\frac{a_1 a_2}{d}}{\mu\kappa\delta(\frac{a_1}{d}, \frac{a_2}{d})} \cdot \mu\kappa\delta(\frac{a_1}{d}, \frac{a_2}{d}) = \frac{a_1 a_2}{d} = a.$$

Επίσης, παρατηρούμε ότι $a \mid a'^2$: Είναι

$$a'^2 = \frac{a^2}{\mu\kappa\delta(\frac{a_1}{d}, \frac{a_2}{d})^2} = \frac{a}{\mu\kappa\delta(\frac{a_1}{d}, \frac{a_2}{d})^2} \cdot a$$

και επειδή $\mu\kappa\delta(\dfrac{a_1}{d}, \dfrac{a_2}{d}) \mid a = \dfrac{a_1 a_2}{d^2}$, έπεται ότι $a \mid a'^2$.

Λόγω της $f \equiv b'^2 \mod a'$, γράφουμε $f = b'^2 + a'c'$, $c \in K[X]$. Ψάχνουμε το b έτσι ώστε $b \equiv b' \mod a'$ ή, ισοδύναμα, ψάχνουμε ένα $h \in K[X]$ τέτοιο ώστε $b = b' + a'h'$. Λύνουμε την ισοτιμία $f \equiv b^2 \mod a$. Έχουμε

$$\begin{aligned} f \equiv b^2 \mod a &\Rightarrow b'^2 + a'c' \equiv (b' + a'h')^2 \mod a \\ &\Rightarrow a'c' \equiv 2b'a'h' + a'^2h'^2 \mod a \\ &\Rightarrow a'c' \equiv 2b'a'h' \mod a \ (\text{διότι } a \mid a'^2) \\ &\Rightarrow 2b'h' \equiv c' \mod \text{μκδ}(\frac{a_1}{d}, \frac{a_2}{d}) \ (\text{διαιρέσαμε με } a') \end{aligned}$$

Ισχυριζόμαστε ότι $\text{μκδ}(\frac{a_1}{d}, \frac{a_2}{d}, b') = 1$. Έτσι θα έχουμε την λύση $h' = \frac{c'}{2b'}$.

Θέτουμε $s = \text{μκδ}(\frac{a_1}{d}, \frac{a_2}{d}, b')$. Για να είναι $s = 1$, αρκεί να δείξουμε ότι δεν έχει ρίζες. Είναι $s \mid \text{μκδ}(a_1, a_2, b_1, b_2) \mid f$. Αν το ξ είναι μία ρίζα του s τότε το ξ είναι και ρίζα των f, a_1, a_2, b_1 και b_2, οπότε και του d. Από την $f \equiv b_i^2 \mod a_i$ για $i = 1, 2$ συμπεραίνουμε ότι το ξ είναι απλή ρίζα των a_1 και a_2 (αφού το f έχει μόνο απλές ρίζες). Άρα το ξ δεν μπορεί να είναι ρίζα των $\frac{a_1}{d}, \frac{a_2}{d}$, επομένως δεν μπορεί να είναι ρίζα του s. Συνεπώς το s δεν έχει ρίζες που σημαίνει ότι $s = 1$.

Θεωρούμε τον διαιρέτη D' που είναι το άθροισμα των διαιρετών της μορφής $D_x = (x, y) + (x, -y)$ που περιέχονται στον διαιρέτη $D_1 + D_2$. Ο διαιρέτης $D \coloneqq D_1 + D_2 - D'$ βρίσκεται σε γενική θέση διότι $D_1 + D_2 \geq D'$, $\infty \notin \text{supp}D$ (αφού $\infty \notin \text{supp}(D_1) \cup \text{supp}(D_2)$) και δεν περιέχει διαιρέτες της μορφής D_x λόγω της κατασκευής του. Θα δείξουμε ότι ο D έχει αναπαράσταση Mumford (a, b).

Προφανώς το $a(X)$ είναι μονικό. Θα δείξουμε ότι $\deg(a) = \deg(D)$.
Έστω $D' = (x_1, y_1) + (x_1, -y_1) ... + (x_n, y_n) + (x_n, -y_n)$. Είναι $\deg(D')' = 2n$. Θα αποδείξουμε ότι $d = \prod_{i=1}^{n}(X - x_i)$. Αφού οι D_1, D_2 είναι σε γενική θέση, είναι $(x_i, y_i) \in \text{supp}(D_1)$ και $(x_i, -y_i) \in \text{supp}(D_2)$ ή αντίστροφα. Αυτό σημαίνει ότι μπορούμε να γράψουμε

$$a_1 = g_1(X) \prod_{i=1}^{n}(X - x_i) \ \text{ και } \ a_2 = g_2(X) \prod_{i=1}^{n}(X - x_i)$$

όπου

$$g_i(X) = \prod_{(x_i, y_i) \in \text{supp}(D_i) \setminus \text{sup}(D')} (X - x_i), \ \ i = 1, 2.$$

Επιπλέον, για κάθε $(x, y) \in \text{supp}(D')$, είναι $b_1(x) = -b_2(x)$, δηλαδή $b_1(x) + b_2(x) = 0$, δηλαδή $X - x \mid (b_1(X) + b_2(X))$. Άρα μπορούμε να γράψουμε

$$(b_1 + b_2)(X) = g_3(X) \prod_{i=1}^{n}(X - x_i).$$

Συνεπώς το $d(X)$ είναι κοινός διαιρέτης των $a_1(X), a_2(X)$ και $(b_1+b_2)(X)$. Αν ο $d(X)$ είχε και άλλον παράγοντα της μορφής $X-x_k$ τότε θα είχαμε $(x_k,y_k),(x_k,-y_k) \in \mathrm{supp}(D')$ για κάποιο $y_k \in K$, άτοπο. Άρα $d(X)=\prod_{i=1}^{n}(X-x_i)$. Συνεπώς έχουμε

$$\deg(D)=\deg(D_1)+\deg(D_2)-\deg(D')=\deg(a_1)+\deg(a_2)-2n=\deg(\frac{a_1a_2}{d^2}).$$

Στη συνέχεια θα δείξουμε ότι $b(x_i)=y_i$ για κάθε $(x_i,y_i)\in \mathrm{supp}(D)$. Αν $(x_i,y_i)\in \mathrm{supp}(D_1)$ τότε $a_1(x_i)=0$ οπότε από την $b(X)\equiv b_1(X) \mod \frac{a_1(X)}{d(X)}$ παίρνουμε $b(x_i)=b_1(x_i)=y_i$. Όμοια αν $(x_i,y_i)\in \mathrm{supp}(D_2)$. Συνεπώς το ζεύγος (a,b) είναι αναπαράσταση Mumford του D.

Απομένει να δείξουμε ότι

$$[D-\deg(D)\cdot\infty]=P_1+P_2.$$

Προς αυτό, θεωρούμε τον διαιρέτη $\mathrm{div}((X-x_1)\cdots(X-x_n))$. Οι ρίζες του πολυώνυμου $(X-x_1)\cdots(X-x_n)$ είναι οι $x_1,...,x_n$. Από την εξίσωση της καμπύλης, η ρίζα x_i αντιστοιχεί στις $\pm y_i$. Άρα

$$\mathrm{div}((X-x_1)\cdots(X-x_n))=D'-2n\cdot\infty$$

που σημαίνει ότι $[D']=[2n\cdot\infty]$. Έτσι,

$$\begin{aligned}
&[D-\deg(D)\cdot\infty]=[D_1+D_2-\deg(D_1)\cdot\infty-\deg(D_2)\cdot\infty]\\
\Leftrightarrow\ &[D_1+D_2-D']=[(\deg(D_1)+\deg(D_2)-\deg(D))\cdot\infty]\\
\Leftrightarrow\ &[D']=[(\deg(a_1)+\deg(a_2)-\deg(a)\infty]\\
\Leftrightarrow\ &[D']=[(\deg(a_1)+\deg(a_2)-\deg(a_1)-\deg(a_2)+\deg(d^2))\cdot\infty]\\
\Leftrightarrow\ &[D']=[2\deg(d)\cdot\infty]\\
\Leftrightarrow\ &[D']=[2n\cdot\infty]
\end{aligned}$$

Συνεπώς $[D-\deg(D)\cdot\infty]=[D_1+D_2-\deg(D_1)\cdot\infty-\deg(D_2)\cdot\infty]$.

Αναγωγή: Έχουμε

$$\begin{aligned}
Y-b(X)=0 &\Leftrightarrow Y=b(X)\\
&\Leftrightarrow b^2(X)=f(X)\\
&\Leftrightarrow f(X)-\lambda a(X)c(X)=f(X)\\
&\Leftrightarrow a(X)c(X)=0
\end{aligned}$$

Έστω $\mathrm{div}(c(X))=\iota(D')-\deg(c)\cdot\infty$. Τότε $\mathrm{div}(ac)=D-\deg(a)\cdot\infty+\iota(D')-\deg(c)\cdot\infty$. Αυτό σημαίνει ότι $D+\iota(D')\sim\deg(a)\cdot\infty+\deg(c)\cdot\infty$. Όμως $D'+\iota(D')\sim 2\deg(c)\cdot\infty$, επομένως $D-\deg(a)\infty\sim D'-\deg(c)\cdot\infty$.

Γράφουμε $-b(X) = c(X)q(X) + b'(X)$ για κάποιο $q(X) \in K[X]$. Θα δείξουμε ότι το ζεύγος (c, b') είναι αναπαράσταση Mumford του D' με $\deg(c) < \deg(a)$.

Αρχικά, από τον ορισμό του D' είναι $c(x_i) = 0$ αν και μόνο αν $(x_i, y_i) \in \mathrm{supp}(D')$. Επίσης, από την $f - b^2 \equiv \lambda ac$ έπεται ότι $f \equiv (-b')^2 \mod c$.

Θα δείξουμε ότι $\deg(c) < \deg(a)$. Ισχύει ότι $\deg(b) \leq \deg(a) - 1$, οπότε $\deg(f - b^2) \leq \max\{2g + 1, 2\deg(a) - 2\}$. Αν $\deg(a) \geq g + 1$ η προηγούμενη ανισότητα γίνεται $\deg(f - b^2) \leq \max\{2\deg(a) - 1, 2\deg(a) - 2\}$, επομένως $\deg(f - b^2) < 2\deg(a)$. Αφού $\deg(c) = \deg(f - b^2) - \deg(a)$ συμπεραίνουμε ότι $\deg(c) < \deg(a)$.

Τέλος, θα δείξουμε ότι $b'(x_i) = y_i$ για κάθε $(x_i, y_i) \in \mathrm{supp}(D')$. Από την ισότητα $-b(X) = c(X)q(X) + b'(X)$, αν $(x_i, y_i) \in \mathrm{supp}(D')$, έχουμε $b'(x_i) = -b(x_i)$.
Συνεχίζοντας την διαδικασία της αναγωγής, τελικά λαμβάνουμε έναν διαιρέτη D τέτοιο ώστε $P_1 + P_2 = [D - \deg(D) \cdot \infty]$ με $\deg(D) \leq g$. ■

3.30 Παράδειγμα. Θεωρούμε την υπερελλειπτική καμπύλη γένους 2, $C : Y^2 = X^5 + 1$ υπέρ το $\mathbb{Q}$. Θα υπολογίσουμε την τάξη του στοιχείου $P = [(0, 1) - \infty] \in J(\mathbb{Q})$. Το P έχει αναπαράσταση

$$\boxed{P = (a_1, b_1) = (X, 1)}.$$

Θα προσθέτουμε το P με τον εαυτό του έως ότου πάρουμε το ταυτοτικό στοιχείο $(1, 0)$.

Υπολογισμός του $2P$:
1) Θέτουμε $d = \mu\kappa\delta(X, X, 2) = 1$.

2) Θέτουμε

$$a_2(X) = \frac{a_1 a_1}{1^2} = X.$$

3) Βρίσκουμε το μοναδικό $b_2(X) \in K[X]$ με $\deg(b_2) < \deg(a_2)$ τέτοιο ώστε

$$b_2 \equiv b_1 \mod a_1 \text{ και } f \equiv b_2^2 \mod a_2.$$

Οι παραπάνω ισοτιμίες γίνονται

$$b_2 \equiv 1 \mod X \text{ και } X^5 + 1 \equiv b_2^2 \mod X^2,$$

δηλαδή

$$b_2 \equiv 1 \mod X \text{ και } b_2^2 \equiv 1 \mod X^2.$$

Οι σχέσεις $b_2 \equiv 1 \mod X$ και $\deg(b_2) < 2$ δίνουν ότι $b_2 \equiv 1 + \beta X$ για κάποιο $\beta \in K[X]$. Άρα

$$\begin{aligned}(1 + \beta X)^2 \equiv 1 \mod X^2 &\Rightarrow \beta^2 X^2 + 2\beta \\ &\Rightarrow X + 1 \equiv 1 \mod X^2 \\ &\Rightarrow 2\beta X \equiv 0 \mod X^2 \\ &\Rightarrow \beta = 0.\end{aligned}$$

Συνεπώς, $b_2 = 1$ και

$$\boxed{2P = (a_2, b_2) = (X^2, 1)}.$$

Υπολογισμός του $3P$: $3P = P + 2P$.

1) Θέτουμε $d = \text{μκδ}(a_1, a_2, b_1 + b_2) = \text{μκδ}(X, X^2, 2) = 1$.

2) Θέτουμε

$$a_3(X) = \frac{a_1 a_2}{d^2} = \frac{X \cdot X^2}{1^2} = X^3.$$

3) Βρίσκουμε το μοναδικό $b_3(X) \in K[X]$ με $\deg(b_3) < \deg(a_3) = 3$ τέτοιο ώστε

$$b_3 \equiv b_1 \mod \frac{a_1}{d}, b_3 \equiv b_2 \mod \frac{a_2}{d} \text{ και } f \equiv b_3^2 \mod a_3,$$

δηλαδή

$$b_3 \equiv 1 \mod X, b_3 \equiv 1 \mod X^2 \text{ και } b_3^2 \equiv 1 \mod X^3.$$

Βλέπουμε ότι $b_3 = 1$, οπότε $3P = (a_3, b_3) = (X^3, 1)$. Όμως $\deg(a_3) = 3 > g = 2$, οπότε κάνουμε ένα βήμα αναγωγής:

1) Γράφουμε $f - b_3^2 = X^5 + 1 - 1 = X^5 = X^3 \cdot X^2 = a_3 X^2$.

2) Αντικαθιστούμε το a_3 με το c.

3) Αντικαθιστούμε το b_3 με το $-b_3 \mod c$, δηλαδή με το -1.

Άρα

$$\boxed{3P = (a_3, b_3) = (X^2, -1)}.$$

Υπολογισμός του $4P$: $4P = P + 3P$.

1) Θέτουμε $d = \text{μκδ}(a_1, a_3, b_1 + b_3) = \text{μκδ}(X, X^2, 0) = X$.

2) Θέτουμε

$$a_4 = \frac{a_1 a_3}{d^2} = \frac{X \cdot X^2}{X^2} = X.$$

3) Βρίσκουμε το μοναδικό $b_4 \in K[X]$ με $\deg(b) < 1$ τέτοιο ώστε

$$b_4 \equiv b_1 \mod \frac{a_1}{d}, b_4 \equiv b_3 \mod \frac{a_3}{d} \text{ και } f \equiv b_4^2 \mod a_4,$$

δηλαδή

$$b_4 \equiv 1 \mod 1, b_4 \equiv -1 \mod X \text{ και } b_4^2 \equiv 1 \mod X.$$

Προφανώς $b_4 = -1$, οπότε

$$\boxed{4P = (a_4, b_3) = (X, -1)}.$$

Υπολογισμός του $5P$: $5P = P + 4P$.

1) Θέτουμε $d = \text{μκδ}a_1, a_4, b_1 + b_4 = \text{μκδ}(X, X, 0) = X$.

2) Θέτουμε

$$a_5 = \frac{a_1 a_4}{d^2} = \frac{X \cdot X}{X^2} = 1.$$

3) Τώρα είναι $\deg(b_5) < \deg(a_5) = 0$, οπότε $b_5 = 0$.

Συνεπώς

$$\boxed{5P = (a_5, b_5) = (1, 0)}.$$

Τελικά, το σημείο $P = [(0, 1) - \infty]$ έχει τάξη 5.

Παρόμοια, μπορούμε να δείξουμε ότι το σημείο $[(-1, 0) - \infty]$ έχει τάξη 2. □

§5 Υπολογισμός της $J(\mathbb{Q})_{\text{tors}}$

Από το Θεώρημα των Morderll-Weil 1.69, η $J(\mathbb{Q})$ είναι πεπερασμένα παραγόμενη αβελιανή ομάδα, άρα μπορούμε να γράψουμε $J(\mathbb{Q}) = J(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$ για όπου r ο βαθμός (rank) της Ιακωβιανής. Συνεπώς για τον προσδιορισμό της $J(\mathbb{Q})$, αρκεί να βρούμε την $J(\mathbb{Q})_{\text{tors}}$, τον βαθμό της, καθώς και γεννήτορες του ελεύθερου μέρους της.

3.31 Λήμμα. *Έστω C μία υπερελλειπτική καμπύλη υπέρ το $\mathbb{Q}$ με Ιακωβιανή J, και έστω $p \in \mathbb{P}$ στον οποίο η C έχει καλή αναγωγή. Συμβολίζουμε την Ιακωβιανή της $\bar{C}$ με $\bar{J}$. Τότε υπάρχει μια απεικόνιση αναγωγής $J(\mathbb{Q}) \to \bar{J}(\mathbb{F}_p)$ που είναι ομομορφισμός ομάδων.*

Αν σταθεροποιήσουμε ένα σημείο $P_0 \in C(\mathbb{Q})$ και συμβολίσουμε την επαγόμενη εμφύτευση της C στην J με $i : P \mapsto [P - P_0]$, τότε υπάρχει επίσης και η εμφύτευση $\bar{i} : \bar{C} \to \bar{J}$, $P \mapsto [P - \bar{P}_0]$, και το ακόλουθο διάγραμμα αντιμετατίθεται:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\ i\ } & J(\mathbb{Q}) \\ \Big\downarrow{\scriptstyle \rho_{p,C}} & & \Big\downarrow{\scriptstyle \rho_{p,J}} \\ \bar{C}(\mathbb{F}_p) & \xrightarrow{\ \bar{i}\ } & \bar{J}(\mathbb{F}_p) \end{array}$$

Απόδειξη. Βλ. [37, σελ. 27]. ■

3.32 Παρατήρηση. Το παραπάνω λήμμα ισχύει και αν αντικαταστήσουμε το $\mathbb{Q}$ με το $\mathbb{Q}_p$.

3.33 Θεώρημα. *Έστω C μία υπερελλειπτική καμπύλη υπέρ το $\mathbb{Q}$ γένους $g \geq 1$ με Ιακωβιανή J, και έστω $p \in \mathbb{P}$ στον οποίο η C έχει καλή αναγωγή. Τότε η απεικόνιση αναγωγής $J(\mathbb{Q}) \to \bar{J}(\mathbb{F}_p)$ περιορίζεται σε έναν 1-1 ομομορφισμό ομάδων στην $J(\mathbb{Q})_{\text{tors}}$.*

Απόδειξη. Αποδεικνύεται ότι η απεικόνιση αναγωγής $J(\mathbb{Q}_p) \to \bar{J}(\mathbb{F}_p)$ έχει πυρήνα, έστω $J(\mathbb{Q}_p)_1$, ισόμορφο με $\mathbb{Z}_p^g$, ο οποίος δεν έχει torsion μέρος. Αν τώρα $P \in \text{Ker}(J(\mathbb{Q})_{\text{tors}} \to \bar{J}(\mathbb{F}_p)$, το P ανήκει και στον $J(\mathbb{Q}_p)_1$, επομένως το P είναι αναγκαστικά το μηδενικό στοιχείο της $J(\mathbb{Q})_{\text{tors}}$. ■

Για τον υπολογισμό της τάξης της $J(\mathbb{F}_p)$, είναι πολύ βολικός ο παρακάτω τύπος.

3.34 Λήμμα. *Έστω C μία υπερελλειπτική καμπύλη $Y^2 = f(X)$ με $\deg(f) = 5$ και Ιακωβιανή J ορισμένη στο πεπερασμένο σώμα με q στοιχεία $\mathbb{F}_q$. Τότε*

$$|J(\mathbb{F}_q)| = \frac{|C(\mathbb{F}_{q^2})| + |C(\mathbb{F}_q)|^2}{2} - q.$$

Απόδειξη. Από το Λήμμα 3.22, αρκεί να μετρήσουμε το πλήθος των $\mathbb{F}_q$-ρητών διαιρετών της καμπύλης που βρίσκονται σε γενική θέση και έχουν βαθμό μικρότερο ή ίσο του 2. Τέτοιος διαιρέτης βαθμού 0 είναι μόνο ο μηδενικός διαιρέτης, ο οποίος αντιπροσωπεύει το ταυτοτικό στοιχείο της ομάδας $J(\mathbb{F}_q)$.

Βαθμού 1 είναι όλα τα ρητά σημεία εκτός του ∞, που είναι συνολικά $|C(\mathbb{F}_q)| - 1$.

Μένει να μετρήσουμε τους διαιρέτες βαθμού 2 με τις ζητούμενες ιδιότητες. Η επέκταση $\mathbb{F}_q^2/\mathbb{F}_q$ είναι Galois βαθμού 2 και $\text{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q) = \{id, \sigma\}$ όπου αν $1, a$ είναι μία βάση της επέκτασης, τότε $\sigma(a) = a^q$. Η $\text{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ δρα στα σημεία της καμπύλης με τον εξής τρόπο: $\tau((x, y)) = (\tau(x), \tau(y))$ για κάθε $\tau \in \text{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$.

Διακρίνουμε δύο είδη διαιρετών D που βρίσκονται σε γενική θέση και έχουν βαθμό ίσο με 2: αυτούς που είναι άθροισμα δύο ρητών σημείων της καμπύλης (δηλαδή $D = (x_1, y_1) + (x_2, y_2)$ με $(x_1, y_1), (x_2, y_2) \in C(\mathbb{F}_q) \setminus \{\infty\}$) και αυτούς που είναι άθροισμα ενός $\mathbb{F}_{q^2}$-ρητού σημείου της καμπύλης που δεν είναι $\mathbb{F}_q$-ρητό συν το συζυγές μέσω της $\sigma \in \text{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ (δηλαδή $D = (x, y) + \sigma((x, y))$ για $(x, y) \in C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)$). Για την επιλογή των σημείων της πρώτης μορφής υπάρχουν

$$\frac{|C(\mathbb{F}_q)|(|C(\mathbb{F}_q)| - 1)}{2}$$

τρόποι: Αν $(x_1, y_1) \neq (x_2, y_2)$ τότε έχουμε $\binom{|C(\mathbb{F}_q)| - 1}{2}$ διαιρέτες και αν $(x_1, y_1) = (x_2, y_2)$ έχουμε $|C(\mathbb{F}_q)| - 1$ διαιρέτες (εξαιρούμε το ∞). Άρα, συνολικά έχουμε

$$\begin{aligned}\binom{|C(\mathbb{F}_q)| - 1}{2} + |C(\mathbb{F}_q)| - 1 &= \frac{|C(\mathbb{F}_q)| - 2)(|C(\mathbb{F}_q)| - 1)}{2} + |C(\mathbb{F}_q)| - 1 \\ &= \frac{|C(\mathbb{F}_q)|(|C(\mathbb{F}_q)| - 1)}{2}\end{aligned}$$

διαιρέτες.

Για την επιλογή των σημείων των διαιρετών της δεύτερης μορφής, αφού ο διαιρέτης καθορίζεται από ένα σημείο, υπάρχουν

$$\frac{|C(\mathbb{F}_{q^2})| - |C(\mathbb{F}_q)|}{2}$$

τρόποι.

Έχουμε εξαιρέσει τους διαιρέτες των οποίων το support περιέχει το ∞, όμως κάποιοι από τους παραπάνω διαιρέτες έχουν τη μορφή $P + \iota(P)$ όπου ι η υπερελλειπτική involution, και πρέπει να τους αφαιρέσουμε από την καταμέτρηση. Αφού κάθε στοιχείο του $\mathbb{F}_q$ είναι τετράγωνο στο $\mathbb{F}_{q^2}$, η εξίσωση $Y^2 = f(X)$ έχει δύο λύσεις $\pm y$ στο $\mathbb{F}_{q^2}$ για κάθε $x \in \mathbb{F}_q$, . Αυτό σημαίνει πως έχουμε μετρήσει τους διαιρέτες της μορφής $(x, y) + (x, -y) = (x, y) + \iota((x, y))$ με $x \in \mathbb{F}_q$, οι οποίοι έχουν πλήθος q.

Τελικά, οι διαιρέτες της καμπύλης με τις ζητούμενες ιδιότητες έχουν πλήθος

$$\begin{aligned} |J(\mathbb{F}_q)| &= 1 + |C(\mathbb{F}_q)| - 1 + \frac{|C(\mathbb{F}_q|)(|C(\mathbb{F}_q)| - 1)}{2} + \frac{|C(\mathbb{F}_{q^2})| - |C(\mathbb{F}_q)|}{2} - q \\ &= \frac{|\bar{C}(\mathbb{F}_{q^2})| + |\bar{C}(\mathbb{F}_q)|^2}{2} - q. \end{aligned}$$

■

3.35 Παράδειγμα. Θεωρούμε πάλι την καμπύλη $C : Y^2 = X^5 + 1$ υπέρ το $\mathbb{Q}$. Στο παράδειγμα 3.30, είδαμε ότι το σημείο $P_1 = [(0, 1) - \infty]$ έχει τάξη 5 στην $J(\mathbb{Q})$ και εύκολα βλέπουμε ότι το σημείο $P_2 = [(-1, 0) - \infty]$ έχει τάξη 2. Άρα το σημείο $P_1 + P_2$ έχει τάξη 10, επομένως $|J(\mathbb{Q})_{\text{tors}}| \geq 10$. Από την άλλη, η C έχει καλή αναγωγή στον πρώτο $p = 3$ (η διακρίνουσα του πολυωνύμου $X^5 + 1$ είναι 5^5) και $|\bar{J}(\mathbb{F}_3)| = 10$ (ο υπολογισμός γίνεται στο τέλος). Από το Θεώρημα 3.33, $|J(\mathbb{Q})_{\text{tors}}| \leq 10$. Συνεπώς $|J(\mathbb{Q})_{\text{tors}}| = 10$. Αφού η $J(\mathbb{Q})_{\text{tors}}$ είναι αβελιανή, συμπεραίνουμε ότι $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/10\mathbb{Z}$ (υπάρχουν δύο ομάδες τάξης 10: η (κυκλική) $\mathbb{Z}/10\mathbb{Z}$ και η (μη αβελιανή) διεδρική D_{10}). Είναι $J(\mathbb{Q})_{\text{tors}} = \langle P_1 + P_2 \rangle$. Θα βρούμε την αναπαράσταση Mumford του $P_1 + P_2$, έστω (a, b). Οι αναπαραστάσεις Mumford των σημείων P_1 και P_2 είναι $(a_1, b_1) = (X, 1)$ και $(a_2, b_2) = (X + 1, 0)$ αντίστοιχα. Θέτουμε $d = \text{μκδ}(a_1, a_2, b_1 + b_2) = 1$, οπότε $a = \dfrac{a_1 a_2}{d^2} = X(X + 1)$. Το b ικανοποιεί τις $b(-1) = 0$ και $b(0) = 1$, οπότε $b = X + 1$, δηλαδή $(a, b) = (X(X + 1), X + 1)$.

Υπολογισμός του $|\bar{J}(\mathbb{F}_3)|$: Από το Λήμμα 3.34, έχουμε

$$|\bar{J}(\mathbb{F}_3)| = \frac{|\bar{C}(\mathbb{F}_9)| + |\bar{C}(\mathbb{F}_3)|^2}{3} - p.$$

Εύκολα βρίσκουμε ότι

$$\bar{C}(\mathbb{F}_3) = \{(0, 1), (0, 2), (2, 0), \infty\},$$

οπότε $|\bar{C}(\mathbb{F}_3)| = 4$.

Στη συνέχεια, θεωρούμε το πολυώνυμο $X^2+1 \in \mathbb{F}_3[X]$, το οποίο είναι ανάγωγο υπέρ το $\mathbb{F}_3$. Έστω a μια ρίζα του, δηλαδή $a^2 = -1$. Τότε το σύνολο $\{1, a\}$ αποτελεί βάση του $\mathbb{F}_9$ και

$$\mathbb{F}_9 = \{0, 1, 2, a, 2a, a+1, 2a+1, a+2, 2a+2\}.$$

Τα τετράγωνα των στοιχείων του $\mathbb{F}_9$ είναι τα

$$\begin{aligned} 0^2 &= 0 \\ 1^2 &= 1 \\ 2^2 &= 2 \\ a^2 &= 2 \\ (2a)^2 &= 2 \\ (a+1)^2 &= 2a \\ (2a+1)^2 &= a \\ (a+2)^2 &= a \\ (2a+2)^2 &= 2a. \end{aligned}$$

Για κάθε $x \in \mathbb{F}_9$, ελέγχουμε αν το x^5+1 είναι τέλειο τετράγωνο στο $\mathbb{F}_9$, και έτσι βρίσκουμε το σύνολο $\bar{C}(\mathbb{F}_9)$. Εν τέλει, καταλήγουμε στο ότι

$$\begin{aligned} \bar{C}(\mathbb{F}_9) = \{&(0,1), (0,2), (2,0), (a+1, a+1), (a+1, 2a+2), \\ &(2a+1, 2a+1), (2a+1, a+2), (1,a), (1,2a), \infty\} \end{aligned}$$

δηλαδή $|\bar{C}(\mathbb{F}_9)| = 10$, επομένως,

$$|\bar{J}(\mathbb{F}_3)| = \frac{4^2+10}{2} - 3 = 10.$$

Συγκεκριμένα,

$$\begin{aligned} \bar{J}(\mathbb{F}_3) = \{&[0 - 0\cdot\infty], [(2,0) - \infty], [(0,1) - \infty], [(0,2) - \infty], [2\cdot(0,1) - 2\cdot\infty], \\ &[2\cdot(0,2) - 2\cdot\infty], [(0,1) + (2,0) - 2\cdot\infty], [(0,2) + (2,0) - 2\cdot\infty], \\ &[(a+1, a+1) + (2a+1, 2a+1) - 2\cdot\infty], \\ &[(2a+1, a+2) + (a+1, 2a+2) - 2\cdot\infty]\} \end{aligned}$$

□

3.36 Παράδειγμα. Θεωρούμε την υπερελλειπτική καμπύλη $C : Y^2 = X^5 - X + 1$. Η διακρίνουσα του $X^5 - X + 1$ είναι $19 \cdot 151$, άρα η καμπύλη έχει καλή αναγωγή στους πρώτους 3 και 5 και ισχύει ότι $|\bar{J}(\mathbb{F}_3)| = 29$ και $|\bar{J}(\mathbb{F}_5)| = 71$. Από το Θεώρημα 3.33, η $J(\mathbb{Q})_{\text{tors}}$ εμφυτεύεται στις ομάδες $\bar{J}(\mathbb{F}_3)$ και $\bar{J}(\mathbb{F}_5)$, δηλαδή εμφυτεύεται σε δύο ομάδες με τάξεις 29 και 71. Άρα το $|J(\mathbb{Q})_{\text{tors}}|$ διαιρεί τον μκδ$(29, 71) = 1$, επομένως $|J(\mathbb{Q})_{\text{tors}}| = 1$ που σημαίνει ότι $J(\mathbb{Q})_{\text{tors}} = \{[(1,0) - \infty]\}$. □

Τα προηγούμενα παραδείγματα υποδηλώνουν το πως μπορούμε να εφαρμόσουμε το Θεώρημα 3.33 για να υπολογίσουμε την $J(\mathbb{Q})_{\text{tors}}$. Επιλέγουμε κάποιους πρώτους στους οποίους η καμπύλη μας έχει καλή αναγωγή και υπολογίζουμε το $\bar{J}(\mathbb{F}_p)$. Τότε από το Θεώρημα 3.33, η τάξη της ομάδας $J(\mathbb{Q})_{\text{tors}}$ διαιρεί τον μέγιστο κοινό διαιρέτη των $\bar{J}(\mathbb{F}_p)$. Αν ο μέγιστος κοινός διαιρέτης είναι 1 τότε βρίσκουμε $|J(\mathbb{Q})_{\text{tors}}| = 1$. Ακόμη και αν δεν είναι 1, έχουμε υπολογίσει ένα άνω φράγμα για το $|J(\mathbb{Q})_{\text{tors}}|$.

Για την εύρεση ενός κάτω φράγματος, μπορούμε να πάρουμε κατάλληλα σημεία της $J(\mathbb{Q})$ και να υπολογίσουμε την τάξη τους (όπως στο Παράδειγμα 3.35).

Σε κάποιες περιπτώσεις, μπορούμε να βρούμε ένα καλύτερο άνω φράγμα μελετώντας την δομή των ομάδων $\bar{J}(\mathbb{F}_p)$. Για παράδειγμα, αν βρούμε ότι $\bar{J}(\mathbb{F}_3) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) := G_3$ και $\bar{J}(\mathbb{F}_5) \cong \mathbb{Z}/20\mathbb{Z} := G_5$, συμπεραίνουμε ότι $|J(\mathbb{Q})_{\text{tors}}| \leq 2$, διότι η μόνη μη τετριμμένη ομάδα που είναι εμφυτεύσιμη και στην G_3 και στην G_5 είναι η $\mathbb{Z}/2\mathbb{Z}$, ενώ μκδ$(|G_3|, |G_5|) = 4$.

3.37 Παράδειγμα. Συνεχίζουμε να εργαζόμαστε με την υπερελλειπτική καμπύλη $C : Y^2 = X^5 - X + 1$. Είδαμε ότι $J(\mathbb{Q})_{\text{tors}} = \{[(1,0) - \infty]\}$, άρα κάθε σημείο διαφορετικό από το ταυτοτικό $[(1,0) - \infty]$ έχει άπειρη τάξη.

Θα δείξουμε ότι το σημείο $P = [(0,1) - \infty] \in J(\mathbb{Q})$ έχει άπειρη τάξη, χωρίς να χρησιμοποιήσουμε το γεγονός $J(\mathbb{Q})_{\text{tors}} = \{0\}$. Βρίσκουμε ότι η τάξη του $\bar{P}$ στις $\bar{J}(\mathbb{F}_3)$ και $\bar{J}(\mathbb{F}_5)$ είναι 29 και 71 αντίστοιχα. Όμως, αν το P ήταν σημείο στρέψης, από το Θεώρημα 3.33 θα είχαμε ότι το $\bar{P}$ έχει την ίδια τάξη για κάθε πρώτο $p > 2$ στον οποίο η C έχει καλή αναγωγή, που είναι άτοπο. Άρα το P έχει άπειρη τάξη. □

Κεφάλαιο IV

Η 2-ομάδα του Selmer

§1 Η απεικόνιση δ

Στο τέλος του προηγούμενου κεφαλαίου, είδαμε τρόπους εύρεσης της $J(\mathbb{Q})_{\text{tors}}$. Σε αυτό το κεφάλαιο, θα δούμε πως μπορούμε να βρούμε τον βαθμό (rank) της $J(\mathbb{Q})$.

Για να βρούμε ένα κάτω φράγμα για το r, επιλέγουμε σημεία της $J(\mathbb{Q})$ και ελέγχουμε αν είναι γραμμικώς ανεξάρτητα. Το δύσκολο μέρος είναι ο υπολογισμός ενός άνω φράγματος. Σε αυτό, βοηθάει η γνώση της 2-ομάδας του Selmer.

Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη γένους g υπέρ το $\mathbb{Q}$. Χάριν απλότητας, θα υποθέσουμε ότι $\deg(f) = 2g + 1$ και ότι το f είναι μονικό. Θεωρούμε τον δακτύλιο πηλίκο $A = \mathbb{Q}[X]/\langle f(X)\rangle$. Γράφουμε θ για την εικόνα του X στο A, δηλαδή $A = \mathbb{Q}[\theta]$ και το θ είναι ρίζα του f. Αν το f είναι ανάγωγο υπέρ το $\mathbb{Q}$ τότε το A είναι αλγεβρικό σώμα αριθμών. Αν $f(X) = f_1(X)\cdots f_k(X)$ η ανάλυση του $f(X)$ σε γινόμενο ανάγωγων μονικών παραγόντων τότε

$$A = \mathbb{Q}[X]/\langle f(X)\rangle \cong (\mathbb{Q}[X]/\langle f_1(X)\rangle) \times \cdots \times (\mathbb{Q}[X]/\langle f_k(X)\rangle).$$

Αν το $f(X)$ αναλύεται σε γινόμενο γραμμικών παραγόντων του $\mathbb{Q}[X]$,

$$f(X) = \prod_{i=1}^{2g+1} (X - a_i),$$

τότε

$$A = \bar{\mathbb{Q}}[X]/\langle f(X)\rangle \cong \bar{\mathbb{Q}}[X]/\langle X - a_1\rangle \times \cdots \times \bar{\mathbb{Q}}[X]/\langle X - a_{2g+1}\rangle \cong \bar{\mathbb{Q}}_1 \times \cdots \times \mathbb{Q}^{2g+1}$$

μέσω των απεικονίσεων

$$X \mapsto (X + \langle f_1(X)\rangle, ..., X + \langle f_{2g+1}(X)\rangle) \mapsto (a_1, ..., a_{2g+1}).$$

Θεωρούμε έναν διαιρέτη D σε γενική θέση με αναπαράσταση Mumford (a, b). Υποθέτουμε ότι μκδ$(a, f) = 1$. Ορίζουμε $\delta(D) = (-1)^{\deg(a)}a(\theta) \in A^*$ (το $\delta(D)$ ανήκει στο

A^* διότι από την μκδ$(a,f)=1$, το θ δεν είναι ρίζα του a, που σημαίνει ότι $a(\theta)\neq 0$). Για έναν διαιρέτη $D_x=(x,y)+(x,-y)$ με $f(x)\neq 0$, ορίζουμε $\delta(D_x)=(\theta-x)^2$.

Θέτουμε $\bar{A}=\bar{\mathbb{Q}}[X]/\langle f(X)\rangle=\bar{\mathbb{Q}}[\theta]$ και $D=\sum_P n_P P$. Τότε

$$a(X)=\prod_{P=(x,y)\in\mathrm{supp}(D)}(X-x)^{n_P},$$

οπότε

$$\delta(D)=\prod_{P=(x,y)\in\mathrm{supp}(D)}(X(P)-\theta)^{n_P}.$$

Ορίζουμε το σύνολο $\mathrm{Div}^{\perp}(C(Q))$ ως το σύνολο των ρητών διαιρετών της C που έχουν βαθμό 0 και το support τους δεν περιέχει σημεία Weierstrass.

Θεωρούμε έναν διαιρέτη $D\in\mathrm{Div}^{\perp}(C(Q))$. Ο διαιρέτης $D-\deg(D)\cdot\infty$ έχει βαθμό 0, οπότε υπάρχει $\phi(X,Y)\in\mathbb{Q}[X,Y]$ τέτοιο ώστε $\mathrm{div}(\phi)=D-\deg(D)\cdot\infty$ (παίρνουμε πολυώνυμο διότι ένας διαιρέτης του $\mathrm{Div}^{\perp}(C(Q))$ δεν περιέχει το ∞ στην ανάλυσή του, οπότε η ϕ δεν πρέπει να έχει πόλους). Το ϕ γράφεται στη μορφή $\phi(X,Y)=h_1(X)+h_2(X)Y$ με $h_1(X),h_2(X)\in\mathbb{Q}[X]$. Αφού

$$\phi(X,Y)(h_1(X)-h_2(X)Y)=h_1^2(X)-h_2^2(X)f(X)\in\mathbb{Q}[X],$$

ο διαιρέτης D έχει αναπαράσταση Mumford (a,b) όπου $a(X)=\lambda(h^2(X)-h_2^2(X)f(X))$ για κάποιο $\lambda\in\mathbb{Q}$ τέτοιο ώστε το πολυώνυμο να είναι μονικό. Έτσι,

$$\delta(D)=(-1)^{\deg(a)}a(\theta)=(-1)^{\deg(a)}\lambda(h_2^2(\theta)-h_2^2(\theta)f(\theta))=(-1)^{\deg(a)}\lambda h_2^2(\theta),$$

διότι $f(\theta)=0$.

Στη συνέχεια, θα δείξουμε ότι $\delta(D)\in(A^*)^2$. Το f έχει περιττό βαθμό, άρα ο μεγιστοβάθμιος όρος του $h_1^2-h_2^2f(X)$ προέρχεται είτε από το h_1^2 είτε από το h_2^2f. Και στις δύο περιπτώσεις, αφού το f είναι μονικό, ο μεγιστοβάθμιος συντελεστής του $h_1^2-h_2^2f$ είναι τέλειο τετράγωνο του $\mathbb{Q}$. Έστω μ^2 ο μεγιστοβάθμιος συντελεστής του $h_1^2-h_2^2f$.

Αν $\deg(h_1^2)>\deg(h_2^2f)$ τότε $\deg(a)$ άρτιος και ο μεγιστοβάθμιος συντελεστής προκύπτει από το h_1^2, οπότε έχουμε $1=\lambda\mu^2$, δηλαδή $\lambda\in(A^*)^2$.

Αν $\deg(h_1^2)<\deg(h_2^2f)$ τότε $\deg(a)$ περιττός και ο μεγιστοβάθμιος συντελεστής προκύπτει από το h_2^2f, οπότε έχουμε $1=-\lambda\mu^2$, δηλαδή $-\lambda\in(A^*)^2$.

Συνεπώς,

$$\delta(D)=\begin{cases}\lambda h_1(\theta)^2, & \deg(h_1^2)<\deg(h_2^2f)\\ -\lambda h_1(\theta)^2, & \deg(h_1^2)>\deg(h_2^2f)\end{cases}$$

οπότε και στις δύο περιπτώσεις, $\delta(D) \in (A^*)^2$. Συνεπώς, ο ομομορφισμός δ ανάγεται σε ομομορφισμό

$$\delta : \frac{\mathrm{Div}^{\perp}(C(\mathbb{Q}))}{\mathrm{Div}^{\perp}(C(\mathbb{Q})) \cap \mathrm{Princ}(C(\mathbb{Q}))} \to \frac{A^*}{(A^*)^2}.$$

Για να δείξουμε ότι ο δ ανάγεται σε ομομορφισμό $\delta : J(\mathbb{Q}) \to A^*/(A^*)^2$, αρκεί να δείξουμε ότι κάθε διαιρέτης της Ιακωβιανής $J(\mathbb{Q})$ αναπαρίσταται από κάποιον διαιρέτη του $\mathrm{Div}^{\perp}(C(\mathbb{Q}))$. Αυτό το αποδεικνύουμε χρησιμοποιώντας το ακόλουθο λήμμα.

4.1 Λήμμα. *(βλ. [19, σελ.17]). Έστω K σώμα. Κάθε K-ρητός διαιρέτης βαθμού 0 γράφεται στη μορφή αθροισμάτων και διαφορών διαιρετών της μορφής* $\sum_{i=1}^{r} \sigma_i(Q) - r \cdot \infty$ *όπου το σύνολο $\{\sigma_i(Q) : 1 \le i \le r\}$ είναι πλήρες σύνολο των $\mathrm{Gal}(\bar{K}/K)$-συζυγών του Q.*

Απόδειξη. Έστω D ένας K-ρητός διαιρέτης βαθμού 0. Τότε για κάποιο $n \in \mathbb{N}_0$ μπορούμε να γράψουμε $D = \sum_{i=1}^{n} P_i - \sum_{i=1}^{n} Q_i$ με $P_i, Q_i \in C(\bar{K})$ για $i = 1, ..., n$. Καθώς

$$D = \sum_{i=1}^{n} P_i - \sum_{i=1}^{n} Q_i = \left(\sum_{i=1}^{n} P_i - n \cdot \infty\right) - \left(\sum_{i=1}^{n} Q_i - n \cdot \infty\right),$$

αρκεί να αποδείξουμε την πρόταση για διαιρέτες της μορφής $\sum_{i=1}^{n} P_i - n \cdot \infty$. Έστω λοιπόν $D = \sum_{i=1}^{n} P_i - n \cdot \infty$.

Θα προχωρήσουμε με επαγωγή στο n. Για $n = 1$, έχουμε $D = P_1 - \infty$. Για να είναι ο D K-ρητός, πρέπει αναγκαστικά $P_1 \in C(K)$, που σημαίνει ότι σταθεροποιείται από όλα τα στοιχεία της $\mathrm{Gal}(\bar{K}/K)$. Συνεπώς, το αποτέλεσμα ισχύει για $n = 1$. Υποθέτουμε ότι κάθε διαιρέτης της μορφής $\sum_{i=1}^{k} P_i - k \cdot \infty$ γράφεται στη ζητούμενη μορφή.

Θεωρούμε την $\mathrm{Gal}(\bar{K}/K)$-τροχιά του P_1 που είναι η $A \coloneqq \{\sigma(P_1) : \sigma \in \mathrm{Gal}(\bar{K}/K)\}$. Τα στοιχεία του A είναι συζυγή ανά δύο και αφού ο D είναι K-ρητός, έπεται ότι $\sigma(P_1) \in \mathrm{supp}(D)$ για κάθε $\sigma \in \mathrm{Gal}(\bar{K}/K)$, δηλαδή $A \subseteq \mathrm{supp}(D)$. Δίχως βλάβη της γενικότητας, γράφουμε $A = \{P_i : 1 \le i \le r\}$ για κάποιο $r \le n$.

Αν $r = n$ έχουμε τελειώσει.

Αν $r < n$ τότε γράφουμε

$$\begin{aligned}
\sum_{i=1}^{n} P_i - n \cdot \infty &= \sum_{i=1}^{r} P_i + \sum_{i=r+1}^{n} -(n - r + r)\infty \\
&= \left(\sum_{i=1}^{r} \sigma_i(P_1) - r \cdot \infty\right) + \left(\sum_{i=r+1}^{n} P_i - (n - r) \cdot \infty\right) \\
&= \left(\sum_{i=1}^{r} \sigma_i(P_1) - r \cdot \infty\right) + \left(\sum_{j=1}^{n-r} P_j - (n - r) \cdot \infty\right)
\end{aligned}$$

όπου $\sigma_i(P_1) = P_i$ για κάθε $\sigma_i \in \mathrm{Gal}(\bar{K}/K)$. Αφού $n - r < n$, από την επαγωγική υπόθεση, ο διαιρέτης $\sum_{j=1}^{n-r} P_j - (n-r)\cdot\infty$, και κατά συνέπεια και ο D, γράφεται στη ζητούμενη μορφή.

■

4.2 Πρόταση. *(βλ. [19, σελ.18]). Έστω K σώμα και $C : Y^2 = f(X)$ υπερελλειπτική καμπύλη γένους g, βαθμού $2g+1$. Κάθε στοιχείο της $J(K)$ αναπαρίσταται από κάποιον K-ρητό διαιρέτη βαθμού 0 του οποίου το support δεν περιέχει σημεία Weierstrass (δηλαδή σημεία της μορφής $(x, 0)$).*

Απόδειξη. Από το προηγούμενο Λήμμα 4.1, αρκεί να δείξουμε ότι κάθε διαιρέτης της μορφής $D = \sum_{i=1}^{r} \sigma_i(Q_1) - r\cdot\infty$ όπου το σύνολο $\{\sigma_i(Q_1) : 1 \le i \le r\}$ είναι πλήρες σύνολο των $\mathrm{Gal}(\bar{K}/K)$-συζυγών του K, είναι γραμμικά ισοδύναμος με κάποιον διαιρέτη του οποίου το support δεν περιέχει σημεία Weierstrass.

Αρχικά, υποθέτουμε ότι το Q_1 δεν είναι σημείο Weierstrass οπότε $Q_1 = (x_1, y_1)$ με $y_1 \neq 0$. Θέτουμε $R_1 = (x_1, -y_1)$. Έστω $x_1, ..., x_{2g+1}$ οι ρίζες της εξίσωσης $f(X) = y_1^2$ και $Q_j = (x_j, y_j)$. Θα υπολογίσουμε τον διαιρέτη

$$D' \coloneqq \mathrm{div}\left(\prod_{i=1}^{r} \frac{(X - \sigma_i(x_1))^g}{Y - \sigma_i(y_1)}\right).$$

Είναι

$$D' = \sum_{i=1}^{r} g\cdot\mathrm{div}(X - \sigma_i(x_1)) - \sum_{r=1}^{r} \mathrm{div}(Y - \sigma_i(y_1)).$$

Από το Παράδειγμα 3.21 έχουμε

$$\begin{aligned}\mathrm{div}(X - \sigma_i(x_1)) &= (\sigma_i(x_1), \sigma_i(y_1)) + (\sigma_i(x_1), -\sigma_i(y_1)) - 2\cdot\infty \\ &= \sigma_i((x_1, y_1)) + \sigma_i((x_1, -y_1)) - 2\cdot\infty \\ &= \sigma_i(Q_1) + \sigma_i(R_1)\end{aligned}$$

και

$$\mathrm{div}(Y - \sigma_i(y_1)) = \sum_{j=1}^{2g+1} \sigma_i(Q_j) - (2g+1)\cdot\infty.$$

Άρα

$$\begin{aligned}D' &= \sum_{i=1}^{n} g(\sigma_i(Q_1) + \sigma_i(R_1)) - 2\cdot\infty - \sum_{i=1}^{r}\sum_{j=1}^{2g+1}(\sigma_i(Q_j)) - r(2g+1)\cdot\infty \\ &= r\cdot\infty + g\sum_{i=1}^{r}\sigma_i(Q_1) + g\sum_{i=1}^{r}\sigma_i(R_1) - \sum_{j=1}^{2g+1}\sum_{i=1}^{r}\sigma_i(Q_j)\end{aligned}$$

Συνεπώς,

$$D' + D = g\sum_{i=1}^{r}\sigma_i(Q_1) + g\sum_{i=1}^{r}\sigma_i(R_1) - \sum_{j=2}^{2g+1}\sum_{i=1}^{r}\sigma_i(Q_j),$$

που σημαίνει (αφού ο D' είναι κύριος), ότι ο D είναι γραμμικά ισοδύναμος με διαιρέτη του οποίου το support δεν περιέχει σημεία Weierstrass.

Έστω τώρα ότι το Q_1 είναι σημείο Weierstrass και έστω $Q_1 = (a_1, 0)$. Προφανώς τα συζυγή σημεία του Q_1 είναι και αυτά σημεία Weierstrass. Αν όλα τα άλλα $2g$ σημεία Weierstrass είναι συζυγή του Q_1 τότε αν θέσουμε $s_i(Q) = (a_i, 0) = Q_i$ για $\sigma_i \in \mathrm{Gal}(\bar{K}/K)$ τότε

$$D = \sum_{i=1}^{2g+1} Q_i - (2g+1)\cdot\infty = \sum_{i=1}^{2g+1}\sigma_i(Q_i) - d\cdot\infty = \mathrm{div}(Y).$$

Αυτό σημαίνει ότι ο D είναι κύριος, άρα είναι γραμμικά ισοδύναμος με τον διαιρέτη κάθε K-ρητής συνάρτησης. Ειδικά, $D \sim 0$ που δεν περιέχει σημεία Weierstrass.
Υποθέτουμε λοιπόν ότι τα συζυγή του Q_1 είναι τα $Q_1, Q_2, ..., Q_r$ όπου $Q_i = (a_i, 0)$ και $r < 2g+1$.
Επιπλέον, μπορούμε να υποθέσουμε ότι $r \leq g$ ως εξής: Θέτουμε

$$g(X, Y) = \frac{1}{Y}\prod_{i=r+1}^{2g+1}(X - a_i,)$$

οπότε

$$\begin{aligned}\mathrm{div}(g) &= \sum_{i=r+1}^{2g+1}\mathrm{div}(X - a_i) - \mathrm{div}(Y)\\ &= \sum_{i=r+1}^{2g+1}(2Q_i - 2\cdot\infty) - \sum_{i=1}^{2g+1}(Q_i - (2g+1)\cdot\infty)\\ &= -\sum_{i=1}^{r}Q_i + \sum_{i=r+1}^{2g+1}Q_i - (2g+1-2r)\cdot\infty.\end{aligned}$$

Άρα

$$\begin{aligned}\mathrm{div}(g) + D &= -\sum_{i=1}^{r}Q_i + \sum_{i=r+1}^{2g+1}Q_i - (2g+1-2r)\cdot\infty + \sum_{i=1}^{r}Q_i - r\cdot\infty\\ &= \sum_{i=r+1}^{2g+1}Q_i - (2g+1-r)\cdot\infty \coloneqq D'.\end{aligned}$$

Δηλαδή, $D \sim D'$.

Έστω τώρα $g(X,Y) = Y - \prod_{i=1}^{r}(X-a_i)$. Έστω $(x,y) \in C(\bar{K})$ τέτοιο ώστε $g(x,y)=0$, δηλαδή $y = \prod_{i=1}^{r}(x-a_i)$. Από την εξίσωση της καμπύλης έχουμε επιπλέον ότι $y^2 = f(x) = \prod_{i=1}^{2g+1}(x-a_i)$, άρα

$$\prod_{i=1}^{2g+1}(x-a_i) = y^2 = \prod_{i=1}^{r}(x-a_i)^2.$$

Άρα

$$0 = \prod_{i=1}^{2g+1}(x-a_i) - \prod_{i=1}^{r}(x-a_i)^2 = \prod_{i=1}^{r}(x-a_i)\left(\prod_{i=r+1}^{2g+1}(x-a_i) - \prod_{i=1}^{r}(x-a_i)\right).$$

Έστω $i \in \{r+1,...,d\}$ και $P_i = (x_i, y_i)$ σημεία της C όπου τα x_j είναι ρίζες του πολυωνύμου

$$\prod_{i=r+1}^{2g+1}(X-a_i) - \prod_{i=1}^{r}(X-a_i)$$

και $y_j = \prod_{i=1}^{r}(x-a_i) \neq 0$. Τότε

$$\operatorname{div}(g) = \sum_{i=1}^{r} Q_i + \sum_{i=r+1}^{2g+1} P_i - (2g+1)\cdot\infty.$$

Θέτουμε $h(X) = \prod_{i=r+1}^{2g+1}(X-x_i)$. Τότε αν $R_i = (x_i, y_i)$ έχουμε

$$\operatorname{div}(h) = \sum_{i=r+1}^{2g+1} P_i + \sum_{i=r+1}^{2g+1} R_i - 2(2g+1-r)\cdot\infty.$$

Άρα

$$D + \operatorname{div}\left(\frac{h}{f}\right) = D + \operatorname{div}(h) - \operatorname{div}(f) = \sum_{i=r+1}^{2g+1} R_i - (2g+1-r)\cdot\infty.$$

Αφού για $i \in \{r+1,...,2g+1\}$ υποθέσαμε ότι $y_i \neq 0$, τα R_i δεν είναι σημεία Weierstrass για κάθε $i \in \{r+1,...,2g+1\}$. Συνεπώς, σύμφωνα την προηγούμενη περίπτωση,

συμπεραίνουμε ότι ο D είναι γραμμικά ισοδύναμος με κάποιον διαιρέτη του οποίου το support δεν περιέχει σημεία Weierstrass. ■

Δείξαμε λοιπόν ότι ο ομομορφισμός δ ανάγεται σε ομομορφισμό $\delta : J(\mathbb{Q}) \to A^*/(A^*)^2$. Μπορούμε να γράψουμε έναν διαιρέτη σε γενική θέση ως άθροισμα διαιρετών D_j με αναπαράσταση Mumford (a_j, b_j) έτσι ώστε το a_j να είναι ανάγωγο. Αν $a_j \nmid f$ τότε υπολογίζουμε το $\delta([D_j - \deg(D_j)\cdot\infty])$ όπως πριν, ως το σύμπλοκο του $(-1)^{\deg(a_j)}a_j(\theta)$ mod $(A^*)^2$. Αν $a_j \mid f$ τότε γράφουμε $f = a_j a_j'$ και αποδεικνύεται ότι

$$\delta([D_j - \deg(D_j)\cdot\infty]) = (-1)^{\deg(a_j)}a_j(\theta) + (-1)^{\deg(a_j')}a_j'(\theta),$$

(βλ.[37, σελ. 30]) οπότε μπορούμε να υπολογίσουμε εύκολα το δ σε κάθε σημείο της $J(\mathbb{Q})$, δεδομένης της αναπαράστασης Mumford του σημείου.

4.3 Λήμμα. *Ο ομομορφισμός $\delta : J(\mathbb{Q}) \to A^*/(A^*)^2$ έχει πυρήνα $2J(\mathbb{Q})$.*

Απόδειξη. Αρχικά παρατηρούμε ότι $2J(\mathbb{Q}) \subseteq \mathrm{Ker}(\delta)$ διότι αν $P \in J(\mathbb{Q})$ τότε

$$\delta(2P) = \delta(P+P) = \delta(P)^2 \equiv 0 \mod (A^*)^2.$$

Μένει να δείξουμε ότι $\mathrm{Ker}(\delta) \subseteq 2J(\mathbb{Q})$.
Έστω $P \in \mathrm{Ker}(\delta)$ και έστω (a,b) η αναπαράσταση Mumford του P με $\deg(a) \le g$. Για απλότητα, υποθέτουμε ότι μκδ$(a,f) = 1$ (η γενική περίπτωση είναι όμοια αλλά πιο πολύπλοκη). Σε αυτήν την περίπτωση, το $(-1)^{\deg(a)}a(\theta)$ είναι τέλειο τετράγωνο. Θέτουμε $s^2(\theta) := (-1)^{\deg(a)}a(\theta)$ με $s(X) \in \mathbb{Q}[X]$ και $\deg(s) \le 2g$.

Ισχυριζόμαστε ότι υπάρχουν πολυώνυμα $q, u, v \in \mathbb{Q}[X]$ τέτοια ώστε το σύστημα ισοτιμιών

$$v \equiv qs \mod f, \;\; v \equiv ub \mod a$$

να έχει μη τετριμμένη λύση (q,u,v) τέτοια ώστε $\deg(q) \le g$, $\deg(u) \le \frac{\deg(a)}{2} - 1$, $\deg(v) \le g + \frac{\deg(a)}{2}$ και q μονικό. Μετατρέπουμε το σύστημα των ισοτιμιών πολυωνύμων σε σύστημα των συντελεστών. Έστω ότι οι συντελεστές (άγνωστοι) των q, u, v είναι οι

$$q_0, ..., q_g, u_0, ..., u_{\lceil \frac{\deg(a)}{2} \rceil - 1}, v_0, ..., v_{g + \lfloor \frac{\deg(a)}{2} \rfloor}.$$

Το πλήθος των αγνώστων είναι

$$g + 1 + \lceil \frac{\deg(a)}{2} - 1 \rceil + g + \lfloor \frac{\deg(a)}{2} \rfloor + 1 = 2g + \deg(a) + 2$$

ενώ το πλήθος των εξισώσεων είναι $\deg(g) + \deg(a) = 2g + 1 + \deg(a)$. Άρα έχουμε περισσότερους αγνώστους από εξισώσεις που σημαίνει ότι το σύστημα έχει μη τετριμμένη λύση (q,u,v).

Αν $q = 0$ τότε $v \equiv 0 \mod f$, δηλαδή $f \mid v$. Όμως

$$\deg(v) \le g + \frac{\deg(a)}{2} \le g + \frac{g}{2} = \frac{2g+g}{2} = \frac{2g}{2} < \frac{2g+2}{2} = 2g+1 = \deg(f).$$

Συνεπώς, $v = 0$. Από τις σχέσεις $ub \equiv 0 \mod a$ και μκδ$(a, b) = 1$ συμπεραίνουμε ότι $a \mid u$. Όμως,

$$\deg(u) < \frac{\deg(a)}{2} < \deg(a),$$

οπότε $u = 0$. Δηλαδή, $(q, v, u) = 0$, που είναι άτοπο. Άρα $q \neq 0$. Πολλαπλασιάζοντας τα q, v, u με τον αντίστροφο του μεγιστοβάθμιου συντελεστή του q, μπορούμε να υποθέσουμε ότι το q είναι μονικό.

Έχουμε

$$\begin{aligned} v \equiv ub \mod a &\Rightarrow v^2 \equiv u^2 b^2 \mod a \\ &\Rightarrow v^2 \equiv u^2 f \mod a \quad (f^2 \equiv b^2 \mod a) \\ &\Rightarrow 0 \equiv v^2 - u^2 f \mod a \quad (1) \end{aligned}$$

Επίσης, $v^2 \equiv q^2 s^2 \mod f$. Όμως

$$(-1)^{\deg(a)} a(\theta) = s(\theta)^2 \Rightarrow (-1)^{\deg(a)} a(X) \equiv s^2(X) \mod f(X).$$

Άρα $v^2(X) \equiv (-1)^{\deg(a)} a(X) q^2(X) \mod f(X)$ (2).
Από τις (1), (2) και το γεγονός ότι μκδ$(a, f) = 1$ παίρνουμε

$$v^2 - u^2 f \equiv (-1)^{\deg(a)} a q^2 \mod af \Rightarrow u^2 f \equiv v^2 - (-1)^{\deg(a)} a q^2 \mod af.$$

Θα δείξουμε ότι $u^2 f = v^2 - (-1)^{\deg(a)} a q^2$. Προς αυτό, λογω της προηγούμενης ισοτιμίας, αρκεί να δείξουμε ότι $\deg(v^2 - (-1)^{\deg(a)} a q^2) < \deg(af)$.
Έχουμε

$$\deg(af) = \deg(a) + \deg(f) = 2g + 1 + \deg(a)$$

$$\deg(v^2) \leq 2\deg(v) \leq 2g + \deg(a)$$

$$\deg(aq^2) = \deg(a) + \deg(q^2) = \deg(a) + 2\deg(q) \leq \deg(a) + 2g.$$

Συνεπώς,

$$\deg(v^2 - (-1)^{\deg(a)} a q^2) \leq 2g + \deg(a) < 2g + 1 + \deg(a) = \deg(af).$$

Άρα $u^2 f = v^2 - (-1)^{\deg(a)} a q^2$.

Μπορούμε να υποθέσουμε ότι μκδ$(q, u) = 1$ (διαφορετικά θα διαιρούσαμε και τα δύο μέλη της ισότητας με τον μκδ(q, u), (ο οποίος διαιρεί και το v)). Διακρίνουμε δύο περιπτώσεις:

Αν $u = 0$ τότε $v^2 = (-1)^{\deg(a)} a q^2$. Όμως αφού μκδ$(q, u) = 1$, συμπεραίνουμε ότι $q = 1$, οπότε $v^2 = (-1)^{\deg(a)} a^2$, συνεπώς ο a είναι τέλειο τετράγωνο και $a = v^2$. Έτσι, το P έχει αναπαράσταση Mumford (v^2, b) που σημαίνει ότι $P = 2Q$ με $Q \in J(Q)$ όπου το Q έχει αναπαράσταση Mumford (v, b). Άρα $P \in 2J(\mathbb{Q})$.

Αν $u \neq 0$, θεωρούμε ένα $r(X) \in \mathbb{Q}[X]$ τέτοιο ώστε $ru \equiv v \mod q$. Θα δείξουμε ότι αν ένα $Q \in J(\mathbb{Q})$ έχει αναπαράσταση Mumford (q, r) τότε το P έχει αναπαράσταση Mumford (q^2, r), οπότε θα έχουμε $P = 2Q \in 2J(\mathbb{Q})$.

Από την $u^2 f = v^2 - (-1)^{\deg(a)} a q^2$ παίρνουμε $u^2 f \equiv r^2 u^2 \equiv v^2 \mod q$, συνεπώς $u^2 f \equiv r^2 u^2 \mod q$. Αφού μκδ$(u, q) = 1$, έπεται ότι $f \equiv r^2 \mod q$. Επομένως, το ζεύγος (q, r) αναπαριστά ένα σημείο $Q \in J(\mathbb{Q})$.

Θεωρούμε τη ρητή συνάρτηση $\phi(X, Y) = u(X)Y - v(X) \in \mathbb{Q}(C)^*$. Είναι

$$(uY - v)(uY + v) = u^2 Y^2 - v^2 = u^2 f - v^2 = -(-1)^{\deg(a)} a q^2.$$

οπότε

$$\mathrm{div}((uY - v)(uY + v)) = \mathrm{div}(aq^2) = \mathrm{div}(a) + 2\mathrm{div}(q),$$

επομένως, $[\mathrm{div}(a)] = [-2\mathrm{div}(q)]$, δηλαδή $[P - \deg(a)] = -2[Q - \deg(q)]$, συνεπώς $P = 2 \cdot (-Q)$, δηλαδή $P \in 2J(\mathbb{Q})$. ■

′

4.4 Παρατήρηση. Από το Πρώτο Θεώρημα Ισομορφισμού Ομάδων, παίρνουμε τον ισομορφισμό

$$\delta(J(\mathbb{Q})) \cong J(\mathbb{Q})/2J(\mathbb{Q}) \cong J(\mathbb{Q})_{\mathrm{tors}}/2J(\mathbb{Q})_{\mathrm{tors}} \times (\mathbb{Z}/2\mathbb{Z})^r,$$

όπου το r είναι ο βαθμός της $J(\mathbb{Q})$. Γράφοντας την πεπερασμένη αβελιανή ομάδα $J(\mathbb{Q})_{\mathrm{tors}}$ ως γινόμενο κυκλικών ομάδων τάξης πρώτων αριθμών, βλέπουμε ότι

$$J(\mathbb{Q})_{\mathrm{tors}}/2J(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^m$$

όπου m ο αριθμός των κυκλικών παραγόντων τάξης 2. Το m είναι η διάσταση της $J(\mathbb{Q})[2]$ ως $\mathbb{F}_2$-διανυσματικό χώρο, όπου $J(\mathbb{Q})[2] \coloneqq \{P \in J(\mathbb{Q}) : 2P = 0\}$. Συνεπώς,

$$\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta)) = \dim_{\mathbb{F}_2}(J(\mathbb{Q})[2]) + r.$$

4.5 Παρατήρηση. Αν βρούμε ένα άνω φράγμα για το $\dim_{\mathbb{F}_2}(\delta(J(\mathbb{Q})))$, έστω s, τότε θα έχουμε $r \leq s - m$, δηλαδή ένα άνω φράγμα για το r. Το m μπορούμε να το υπολογίζουμε χρησιμοποιώντας το επόμενο λήμμα.

4.6 Λήμμα. *Έστω $C : Y^2 = f(X)$ μια υπερελλειπτική καμπύλη περιττού βαθμού ορισμένη σε ένα σώμα K. Έστω $f = cf_1 f_2 \cdots f_n$ η ανάλυση του f σε ανάγωγους παράγοντες στο $K[X]$ όπου f_j μονικά και $c \in K^*$. Τότε τα σημεία P_j με αναπαράσταση Mumford $(f_j, 0)$ παράγουν την ομάδα $J(K)[2]$, με μοναδική σχέση μεταξύ των γεννητόρων την $P_1 + ... + P_n = 0$. Συγκεκριμένα,* $\dim_{\mathbb{F}_2}(J(K)[2]) = n - 1$.

Απόδειξη. Είναι $J(K)[2] = \{P \in J(K) : 2P = 0\}$ που σημαίνει ότι $P \in J(K)[2]$ αν και μόνο αν $P = -P$. Αν το P έχει αναπαράσταση Mumford (a, b) τότε το $-P$ έχει αναπαράσταση Mumford $(a, -b)$. Η αναπαράσταση ενός σημείου είναι μοναδική, άρα

αν $P = -P$ τότε $(a, b) = (a, -b)$, οπότε $b = 0$.

Αφού $b = 0$, από την σχέση $f \equiv b^2 \mod a$, παίρνουμε $f \equiv 0 \mod a$, δηλαδή $a \mid f$. Επειδή $a(X) \in K[X]$, το $a(X)$ είναι γινόμενο κάποιων f_j βαθμού $\leq g$ (αν ήταν $a = f_1 f_2$ με $\deg(f_1), \deg(f_2) > g \geq g + 1$ τότε $\deg(a) \geq 2g + 2 > \deg(f)$, άτοπο). Έστω $a(X) = f_{j_1} \cdots f_{j_r}$ όπου $\{j_1, ..., j_r\} \subseteq \{1, ..., n\}$. Έτσι, $P = P_{j_1} + ... + P_{j_r}$ όπου το P_{j_i} έχει αναπαράσταση Mumford $(f_{j_i}, 0)$, $i \in \{1, ..., r\}$. Άρα το σύνολο $\{P_1, ..., P_n\}$ όπου το P_i έχει αναπαράσταση $(f_i, 0)$ παράγει την ομάδα $J(K)[2]$.

Με τα $P_1, ..., P_n$ μπορούμε να φτιάξουμε 2^n στοιχεία, αθροίζοντας κάποια από αυτά και συμπεριλαμβάνοντας και το μηδενικό στοιχείο, όμως λόγω της $P = -P$ για κάθε $P \in J(K)[2]$, μόνο τα μισά από αυτά τα στοιχεία είναι διαφορετικά μεταξύ τους. Συνεπώς η $J(K)[2]$ έχει 2^{n-1} στοιχεία, ή, ισοδύναμα, $\dim_{\mathbb{F}_2}(J(K)[2]) = n - 1$. Αφού έχουμε n γεννήτορες, αυτοί πρέπει να είναι γραμμικώς εξαρτημένοι μέσω μιας σχέσης. Παρατηρούμε ότι

$$\mathrm{div}(Y) = \sum_{i=1}^{n} (f_i, 0) = \sum_{i=1}^{n} P_i,$$

άρα $\sum_{i=1}^{n} P_i = 0$, η οποία είναι η μοναδική σχέση μεταξύ των γεννητόρων. ■

Το m που ορίσαμε στην Παρατήρηση 4.4 είναι ίσο με το $n - 1$ του Λήμματος 4.6. Με πιο απλά λόγια, το m ισούται με το πλήθος των ανάγωγων παραγόντων του $f(X)$ υπέρ το $\mathbb{Q}$ μείον 1.

4.7 Ορισμός. Έστω K σώμα και A μία αντιμεταθετική K- άλγεβρα πεπερασμένης διάστασης. Τότε για κάθε $a \in A$, η απεικόνιση $m_a : A \to A$, $m_a(x) = ax$ είναι K-γραμμική. Θέτουμε $N_{A/K}(a) = \det(m_a)$ και ονομάζουμε αυτήν την ποσότητα **norm** του a.

Η ορίζουσα είναι πολλαπλασιαστική απεικόνιση, οπότε η απεικόνιση $N_{A/K} : A \to K$ ικανοποιεί την $N_{A/K}(aa') = N_{A/K}(a) N_{A/K}(a')$. Ειδικότερα, λαμβάνουμε έναν ομομορφισμό ομάδων $N_{A/K} : A^* \to K^*$.

4.8 Παράδειγμα. Έστω K ένα σώμα. Θεωρούμε μία τετραγωνική K-άλγεβρα A τέτοια ώστε $A = K[Y]/\langle Y^2 - a \rangle$ (αν $\mathrm{ch}(K) = 2$, αυτή δεν είναι η πιο γενική τετραγωνική άλγεβρα). Έστω $\alpha \in A$ η εικόνα του Y στην A, έτσι ώστε $\alpha^2 = a$. Τότε το $(1, \alpha)$ είναι διατεταγμένη K-βάση του A. Έστω $z = z_1 + z_2\alpha \in A$ με $z_1, z_2 \in K$. Θεωρούμε την απεικόνιση $m_z : A \to A$ με τύπο $m_z(x) = zx$. Είναι

$$m_z(1) = 1 \cdot z = z_1 + z_2\alpha = 1 \cdot (z_2) + \alpha \cdot (z_2)$$

και

$$m_z(\alpha) = \alpha \cdot z = \alpha z_1 + \alpha^2 z_2 = \alpha z_1 + a z_2 = 1 \cdot (a z_2) + \alpha \cdot (z_1).$$

Άρα ο πίνακας της απεικόνισης m_z είναι ο

$$M = \begin{bmatrix} z_1 & a z_2 \\ z_2 & z_1 \end{bmatrix}.$$

Συνεπώς, $N_{A/K}(z) = \det(M) = z_1^2 - az_2^2$.

Μια ενδιαφέρουσα περίπτωση είναι η εξής: Αν θεωρήσουμε το $K(C)$ ως τετραγωνική άλγεβρα υπέρ το $K(X)$, όταν $C : Y^2 = f(X)$ μια υπερελλειπτική καμπύλη, για μία ρητή συνάρτηση $\phi = h_1(X) + h_2(X)Y \in K(C)$, έχουμε $N_{K(C)/K(X)}(\phi) = h_1(X)^2 - h_2(X)^2 f(X)$. □

4.9 Παράδειγμα. Έστω K σώμα και $f \in K[X]$ μονικό πολυώνυμο βαθμού n. Θεωρούμε την K-άλγεβρα $A = K[X]/\langle f(X)\rangle$ και έστω θ η εικόνα του X στο A. Τότε το $(1, \theta, ..., \theta^{n-1})$ είναι μία διατεταγμένη K-βάση του A. Θα δείξουμε ότι $N_{A/K}(a-\theta) = f(a)$ για κάθε $a \in A$. Για την απεικόνιση $m_{a-\theta} : A \to A$ με τύπο $m_{a-\theta}(X) = (a-\theta)X$ έχουμε

$$\begin{aligned}
m_{a-\theta}(1) &= a - \theta = a \cdot 1 + (-1) \cdot \theta + 0 \cdot \theta^2 + ... \\
m_{a-\theta}(\theta) &= a\theta - \theta^2 = 0 \cdot 1 + a \cdot \theta + (-1)\theta^2 + 0 \cdot \theta^3 + ... \\
&\vdots \\
m_{a-\theta}(\theta^{n-1}) &= a\theta^{n-1} - \theta^n \\
m_{a-\theta}(\theta^n) &= b_0 \cdot 1 + b_1 \cdot \theta + ... + b_{n-2}\theta^{n-2} + (b_{n-1} + a)\theta^{n-1}
\end{aligned}$$

όπου για το τελευταίο γράψαμε

$$f(X) = X^n + b_{n-1}X^{n-1} + ... + b_0, b_i \in K,$$

οπότε $\theta^n = -b_{n-1}\theta^{n-1} - ... - b_0$.

Συνεπώς ο πίνακας της απεικόνισης $m_{a-\theta}$ είναι ο

$$M = \begin{bmatrix} a & 0 & 0 & \cdots & 0 & b_0 \\ -1 & a & 0 & \cdots & 0 & b_1 \\ 0 & -1 & a & \cdots & 0 & b_2 \\ \vdots & \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & -1 & a + b_{n-1} \end{bmatrix} = aI - A$$

όπου I ο ταυτοτικός $n \times n$ πίνακας και

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & 0 & \cdots & 0 & -b_2 \\ \vdots & \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -b_{n-1} \end{bmatrix}$$

ο συνοδός πίνακας του f. Άρα $\det(M) = \det(aI - A) = f(a)$.

Έστω τώρα $s(\theta) \in A$ όπου $s(X) \in K[X]$. Εργαζόμενοι στο $\bar{K}$ γράφουμε

$$s(X) = c\prod_{j=1}^{m}(X-\sigma_j) \text{ και } f(X) = \prod_{i=1}^{n}(X-\theta_i).$$

Τότε,

$$\begin{aligned} N_{A/K}(s(\theta)) &= N_{A/K}(c\prod_{j=1}^{m}(\theta-\sigma_j)) = c^n\prod_{j=1}^{m}N_{\bar{A}/\bar{K}}(\theta-\sigma_j) = c^n\prod_{j=1}^{m}(-1)^n N_{\bar{A}/\bar{K}}(\sigma_j-\theta) = \\ &= (-1)^{mn}c^n\prod_{j=1}^{m}f(\sigma_j) = (-1)^{mn}c^n\prod_{j=1}^{m}\prod_{i=1}^{n}(\sigma_j-\theta_i) = c^n\prod_{j=1}^{m}\prod_{i=1}^{n}(\theta_i-\sigma_i) \\ &= c^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\theta_i-\sigma_j) = \prod_{i=1}^{n}c\prod_{j=1}^{m}(\theta_i-\sigma_i) = \prod_{i=1}^{n}s(\theta_i) = \mathrm{Res}(s,f) \end{aligned}$$

όπου $\mathrm{Res}(s,f)$ η απαλείφουσα των πολυωνύμων s και f. □

4.10 Λήμμα. *Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη περιττού βαθμού ορισμένη σε ένα σώμα K με Ιακωβιανή J. Ορίζουμε $A = K[X]/\langle f(X)\rangle$ και θεωρούμε τον ομομορφισμό $\delta : J(K) \to A^*/(A^*)^2$ όπως πριν. Τότε το σύνολο $\delta(J(K))$ περιέχεται στον πυρήνα του ομομορφισμού $N_{A/K} : A^*/(A^*)^2 \to K^*/(K^*)^2$.*

Απόδειξη. Έστω $P \in J(K)$. Από το Λήμμα 3.28 και την Πρόταση 4.2, μπορούμε να αναπαραστήσουμε το $P \in J(K)$ στη μορφή $[D - \deg(D)\cdot\infty]$, όπου D ένας διαιρέτης σε γενική θέση του οποίου η ανάλυση δεν περιέχει σημεία του Weierstrass (δεν υποθέτουμε αναγκαστικά ότι $\deg(D) \le g$). Έστω (a,b) η αναπαράσταση Mumford του D με $a = \prod_{j=1}^{d}(X-x_i)$. Χρησιμοποιώντας το αποτέλεσμα του Παραδείγματος 4.8,

$$N_{A/K}(\delta(D)) = N_{A/K}((-1)^d a(\theta)) = \prod_{j=1}^{d}f(x_i) = \prod_{j=1}^{d}b(x_i)^2 = \mathrm{Res}(b,a)^2 \in (K^*)^2,$$

δηλαδή $N_{A/K}(\delta(D)) \equiv 1 \mod (K^*)^2$ για κάθε $P \in J(K)$. Συνεπώς έχουμε το ζητούμενο αποτέλεσμα. ■

Θεωρούμε μία υπερελλειπτική καμπύλη $C : Y^2 = f(X)$ περιττού βαθμού υπέρ το $\mathbb{Q}$. Τον πυρήνα του ομομορφισμού $N_{A/\mathbb{Q}} : A^*/(A^*)^2 \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ τον συμβολίζουμε H. Για κάθε $p \in \mathbb{P}\cup\{\infty\}$, θέτουμε $A_p = \mathbb{Q}_p[X]/\langle f(X)\rangle$ γράφουμε H_p για τον αντίστοιχο πυρήνα του ομομορφισμού

$$N_{A_p/\mathbb{Q}_p} : A_p^*/(A_p^*)^2 \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2.$$

Από την εμφύτευση $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, επάγεται ένας ομομορφισμός $\rho_p : H \to H_p$. Γράφουμε δ_p για την απεικόνιση $J(\mathbb{Q}_p) \to H_p$ (που είναι η απεικόνιση δ όταν θεωρούμε την C ως καμπύλη ορισμένη στο $\mathbb{Q}_p$).

§2 Ο υπολογισμός της 2-ομάδας του Selmer

Τώρα μπορούμε να ορίσουμε την 2-ομάδα του Selmer. Μέσω της 2-ομάδας του Selmer, μπορούμε να βρούμε ένα άνω φράγμα για τον βαθμό (rank) της Ιακωβιανής μιας υπερελλειπτικής καμπύλης περιττού βαθμού.

4.11 Ορισμός. Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη περιττού βαθμού υπέρ το $\mathbb{Q}$ με Ιακωβιανή J. Ορίζουμε την **2-ομάδα του Selmer** της J ως

$$\mathrm{Sel}^2(J(\mathbb{Q})) \coloneqq \{\alpha \in H : \rho_p(\alpha) \in \mathrm{Im}(\delta_p) \text{ για κάθε } p \in \mathbb{P} \cup \{\infty\}\}$$

4.12 Θεώρημα. *Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη περιττού βαθμού υπέρ το $\mathbb{Q}$ με Ιακωβιανή J. Τότε $\delta(J(\mathbb{Q})) \subseteq \mathrm{Sel}^2(J(\mathbb{Q}))$, και η $\mathrm{Sel}^2(J(\mathbb{Q}))$ είναι πεπερασμένη και υπολογίσιμη.*

Απόδειξη. Για κάθε $p \in \mathbb{P} \cup \{\infty\}$, έχουμε το ακόλουθο αντιμεταθετικό διάγραμμα:

$$\begin{array}{ccc} J(\mathbb{Q}) & \xrightarrow{\delta} & H \\ \downarrow & & \downarrow \rho_p \\ J(\mathbb{Q}_p) & \xrightarrow{\delta_p} & H_p \end{array}$$

Άρα για κάθε $P \in J(\mathbb{Q})$ και κάθε $p \in \mathbb{P} \cup \{\infty\}$ έχουμε $\rho_p(\delta(P)) = \delta_p(P)$, οπότε $\delta(P) \in \mathrm{Sel}^2(J(\mathbb{Q}))$, επομένως $\delta(J(\mathbb{Q})) \subseteq \mathrm{Sel}^2(J(\mathbb{Q}))$.

Θα δείξουμε ότι η $\mathrm{Sel}^2(J(\mathbb{Q}))$ είναι πεπερασμένη, για την ειδική περίπτωση όπου το f αναλύεται σε γραμμικούς παράγοντες του $\mathbb{Q}[X]$. Με κατάλληλο πολλαπλασιασμό, μπορούμε να υποθέσουμε ότι το f είναι μονικό και ότι όλες του οι ρίζες είναι ακέραιοι αριθμοί. Έστω $t_1, ..., t_{2g+1}$ οι ρίζες του. Τότε $A \cong \mathbb{Q}^{2g+1}$ (αφού οι παράγοντες του f είναι γραμμικοί), η απεικόνιση $\mathbb{Q}[X] \to A$ είναι η $s \mapsto (s(t_1), ..., s(t_{2g+1}))$ και η norm είναι $(\alpha_1, ..., \alpha_{2g+1}) \mapsto \alpha_1 \cdots \alpha_{2g+1}$, οπότε

$$H = \{(\alpha_1, ..., \alpha_{2g+1}) : \alpha_1, ..., \alpha_{2g+1} \in \mathbb{Q}^*/(\mathbb{Q}^*)^2, \alpha_1 \cdots \alpha_{2g+1} = 1\}.$$

Κάθε στοιχείο του $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ έχει μοναδικό αντιπρόσωπο έναν ακέραιο αριθμό ελεύθερο τετραγώνου. Έστω H' η υποομάδα του H έτσι ώστε οι ελεύθεροι τετραγώνου ακέραιοι που αντιπροσωπεύουν τις συντεταγμένες των στοιχείων της να διαιρούνται μόνο από τους πρώτους αριθμούς που διαιρούν τις διαφορές $t_j - t_i$ για κάποια i, j με $1 \leq i < j \leq 2g + 1$ (αυτοί είναι ακριβώς οι πρώτοι που διαιρούν τη διακρίνουσα του f και ο 2 είναι ένας από αυτούς, διότι τουλάχιστον δύο από τα t_i είναι και οι δύο άρτιοι ή περιττοί). Αν $p_1, ..., p_k$ αυτοί οι πρώτοι τότε

$$H' = \langle -1, p_1, ..., p_k \rangle^{2g}.$$

Η H' είναι προφανώς πεπερασμένη. Για να δείξουμε ότι η $\mathrm{Sel}^2(J(\mathbb{Q}))$ είναι πεπερασμένη, αρκεί να δείξουμε ότι $\mathrm{Sel}^2(J(\mathbb{Q})) \subseteq H'$. Αυτό έπεται από την ακόλουθη πρόταση: Αν

το p δεν διαιρεί καμία από τις διαφορές $t_i - t_j$, τότε η εικόνα του δ_p περιέχεται σε μια υποομάδα του H_p της οποίας τα στοιχεία μπορούν να αναπαρασταθούν από $(2g+1)$-άδες p-αδικών μονάδων (το $\rho_p(\alpha)$ ανήκει σε αυτήν την υποομάδα αν και μόνο αν το α μπορεί να αναπαρασταθεί χρησιμοποιώντας ακέραιους ελεύθερους τετραγώνου που δεν διαιρούνται από το p).

Έστω λοιπόν $P \in J(\mathbb{Q}_p)$ με αναπαράσταση $[D - \deg(D)\cdot\infty]$ και αναπαράσταση Mumford (a,b). Τότε $\delta_p(D) = \pm(a(t_1), ..., a(t_{2g+1}))$ (το πρόσημο είναι $+$ αν $\deg(a)$ άρτιος και $-$ αν $\deg(a)$ περιττός). Μπορούμε να υποθέσουμε ότι το a είναι ανάγωγο (αλλιώς παραγοντοποιούμε το a και γράφουμε το D ως άθροισμα διαιρετών με αναπαράσταση (a_j, b)). Το a έχει συντελεστές στο $\mathbb{Z}_p$ και το $\bar{a} \in \mathbb{F}_p[X]$ έχει το πολύ μία ρίζα στο $\mathbb{F}_p$, ή αλλιώς ο σταθερός όρος του a έχει την μικρότερη αρνητική εκτίμηση από όλους τους συντελεστές και είναι ο μοναδικός τέτοιος συντελεστής.

Στην πρώτη περίπτωση, το $a(t_j)$ μπορεί να διαιρείται από το p για το πολύ ένα j. Οπότε, για όλα εκτός από το πολύ ένα j, είναι $v_p(a(t_j)) = 0$, και επειδή το άθροισμα των εκτιμήσεων πρέπει να είναι άρτιος αριθμός (διότι από το Λήμμα 4.10, $\delta_p(D) \in \mathrm{Ker}(N)$), όλες οι εκτιμήσεις είναι άρτιοι αριθμοί, που σημαίνει ότι τα $a(t_j)$ είναι μονάδες modulo $(\mathbb{Q}^*)^2$.

Στην δεύτερη περίπτωση, όλα τα $a(t_j)$ έχουν την ίδια αρνητική εκτίμηση με τον σταθερό όρο του a. Αφού το f έχει περιττό αριθμό ριζών και το άθροισμα των εκτιμήσεων πρέπει να είναι άρτιος, κάθε εκτίμηση είναι άρτια, οπότε πάλι τα $a(t_j)$ είναι μονάδες modulo $(\mathbb{Q}_p^*)^2$

Για την υπολογισιμότητα της $\mathrm{Sel}^2(J(\mathbb{Q}))$, παραπέμπουμε στο [37, σελ.34]. ■

4.13 Παρατήρηση. Από την παραπάνω πρόταση, λαμβάνουμε την ανισότητα

$$\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta)) \leq \dim_{\mathbb{F}_2}(\mathrm{Sel}^2(J(\mathbb{Q}))).$$

Η πιο ευνοϊκή περίπτωση είναι να ισχύει ότι $\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta)) = \dim_{\mathbb{F}_2}(\mathrm{Sel}^2(J(\mathbb{Q})))$, οπότε και έχουμε

$$r = \dim_{\mathbb{F}_2}(\mathrm{Sel}^2(J(\mathbb{Q}))) - \dim_{\mathbb{F}_2}(J(\mathbb{Q})[2])$$

(βλ. Παρατήρηση 4.4).

Αν είναι $\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta)) < \dim_{\mathbb{F}_2}(\mathrm{Sel}^2(J(\mathbb{Q})))$ τότε δεν μπορούμε να προσδιορίσουμε τον βαθμό r της Ιακωβιανής.

(βλ. [19, σελ. 27] και [23, σελ. 13]).

Συνοψίζοντας, για μία υπερελλειπτική καμπύλη $Y^2 = f(X)$ υπέρ το $\mathbb{Q}$, όπου $f(X)$ μονικό περιττού βαθμού που αναλύεται πλήρως υπέρ το $\mathbb{Q}$, για τον υπολογισμό της ομάδας του Selmer ακολουθούμε τα εξής βήματα:

1. Βρίσκουμε το σύνολο $S = \{\infty, 2\} \cup \{p \in \mathbb{P} : p \mid D(f)\}$.

2. Βρίσκουμε γεννήτορες για την ομάδα H'
3. Για κάθε $p \in S$, υπολογίζουμε την εικόνα $\mathrm{Im}(\delta_p) \subseteq H_p$.
4. Για κάθε $p \in S$, υπολογίζουμε τον πυρήνα του ομομορφισμού $\rho_p : H' \to H_p$.
5. Υπολογίζουμε την 2-ομάδα του Selmer

$$\mathrm{Sel}^2(J(\mathbb{Q})) = \bigcap_{p \in S} \rho_p^{-1}(\mathrm{Im}(\delta_p)).$$

Στο τρίτο βήμα, ο παρακάτω τύπος είναι εξαιρετικά χρήσιμος (βλ. [37, σελ. 35]):

$$\dim_{\mathbb{F}_2}(\delta_p(J(\mathbb{Q}_p))) = \dim_{\mathbb{F}_2}(J(\mathbb{Q}_p)[2]) + \begin{cases} 0, & \text{αν } p \neq 2, \infty \\ g, & \text{αν } p = 2 \\ -g, & \text{αν } p = \infty. \end{cases}$$

Γνωρίζοντας λοιπόν από πριν την διάσταση του $\delta_p(J(\mathbb{Q}_p))$ υπέρ το $\mathbb{F}_2$, επιλέγουμε σημεία $P \in J(\mathbb{Q}_p)$ μέχρι οι εικόνες τους $\delta_p(P)$ να παράγουν έναν $\mathbb{F}_2$-διανυσματικό χώρο με τη ζητούμενη διάσταση. Αν ονομάσουμε G αυτό το σύνολο σημείων τότε

$$\rho_p^{-1}(\mathrm{Im}(\delta_p)) = \langle \mathrm{Ker}(\rho_p), \delta(P) : P \in G \rangle.$$

4.14 Παράδειγμα. Θεωρούμε την υπερελλειπτική καμπύλη $C : Y^2 = f(X)$ με

$$f(X) = X(X-1)(X-2)(X-5)(X-6).$$

Το $f(X)$ έχει βαθμό 5 και η C έχει γένος 2. Οι πρώτοι αριθμοί που διαιρούν τις διαφορές των ριζών του f είναι οι $2, 3, 5$, οπότε $S = \{\infty, 2, 3, 5\}$. Έχουμε

$$H = \{(\alpha_1, ..., \alpha_5) : \alpha_1, ..., \alpha_5 \in \mathbb{Q}^*/(\mathbb{Q}^*)^2, \alpha_1 \cdots \alpha_5 \equiv 1 \mod (\mathbb{Q}^*)^2\}.$$

Έστω H' η υποομάδα της H της οποίας οι ελεύθεροι τετραγώνου ακέραιοι που αντιπροσωπεύουν τις συνιστώσες των στοιχείων της διαιρούνται μόνο από τις διαφορές των ριζών, δηλαδή

$$H' = \langle -1, 2, 3, 5 \rangle^4 = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}^4.$$

Για ευκολία, στον Πίνακα 4.1 παραθέτουμε τους αντιπροσώπους των στοιχείων της H' στις ομάδες $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ για $p \in S$. Τους βρίσκουμε χρησιμοποιώντας τη συνάρτηση **Q_p_mod_squares** του Παραρτήματος.

Από το Λήμμα 4.6 έχουμε $\dim_{\mathbb{F}_2}(J(\mathbb{Q})[2]) = 5 - 1 = 4$ και

$$J(\mathbb{Q})[2] = \langle [(0,0) - \infty], [(1,0) - \infty], [(2,0) - \infty], [(5,0) - \infty] \rangle.$$

Οι γεννήτορες έχουν αναπαραστάσεις Mumford

$$(X, 0), (X-1, 0), (X-2, 0), (X-5, 0)$$

	1	-1	2	-2	3	-3	5	-5	6	-6	10	-10	15	-15	30	-30
∞	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1
2	1	-1	2	-2	3	-3	-3	3	6	-6	-6	6	-1	1	-2	2
3	1	-1	-1	1	3	-3	-1	1	-3	3	1	-1	-3	3	3	-3
5	1	1	2	2	2	2	5	5	1	1	10	10	10	10	5	5

Πίνακας 4.1: Αντιπρόσωποι των στοιχείων της H' στις ομάδες $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ για $p = \infty, 2, 3, 5$

αντίστοιχα. Θέτουμε $a_1(X) = X, a_2(X) = X-1, a_3(X) = X-2, a_4(X) = X-5$ και $a_5(X) = X-6$. Βρίσκουμε τις εικόνες των γεννητόρων μέσω της δ.

Για το $\delta([(0,0)-\infty])$: Είναι $a_1(1) = 1, a_1(2) = 2, a_1(5) = 5, a_1(6) = 6$ ενώ για την πρώτη συντεταγμένη l_1 ισχύει ότι $l_1 \cdot 1 \cdot 2 \cdot 5 \cdot 6 \equiv 1 \mod (\mathbb{Q}^*)^2$, οπότε $l_1 = 15$. Έτσι,

$$\delta([(0,0)-\infty]) = (15, -1, -2, -5, -6).$$

Όμοια βρίσκουμε

$$\delta([(1,0)-\infty]) = (1, -5, -1, -1, -5)$$
$$\delta([(2,0)-\infty]) = (2, 1, 6, -3, -1)$$

και

$$\delta([(5,0)-\infty]) = (5, 1, 3, -15, -1).$$

Σε κάθε περίπτωση, μπορούμε να παραλείπουμε την πέμπτη συντεταγμένη, αφού αυτή εξαρτάται από τις άλλες τέσσερις μέσω της συνθήκης που ορίζει την H. Άρα

$$\delta(J(\mathbb{Q})[2]) = \langle (15, -1, -2, -5), (1, -5, -1, -1), (2, 1, 6, -3), (5, 1, 3, -15) \rangle.$$

Αφού το $f(X)$ αναλύεται σε γραμμικούς παράγοντες του $\mathbb{Q}[X]$, η ανάλυσή του παραμένει ίδια και στο $\mathbb{Q}_p[X]$ για κάθε $p \in S$, επομένως για κάθε $p \in S$ έχουμε

$$\dim_{\mathbb{F}_2}(J(\mathbb{Q}_p)[2]) = \dim_{\mathbb{F}_2}(J(\mathbb{Q})[2])$$

Έχουμε ότι $\dim_{\mathbb{F}_2}(\delta_\infty(J(\mathbb{Q}_\infty)) = \dim_{\mathbb{F}_2}(\delta_\infty(J(\mathbb{R})) = 4-2 = 2$ και ένα πλήρες σύστημα αντιπροσώπων της ομάδας $\mathbb{R}^*/(\mathbb{R}^*)^2$ είναι το $\{-1, 1\}$. Επίσης,

$$\delta_\infty([(0,0)-\infty]) = (1, -1, -1, -1), \delta_\infty([(1,0)-\infty]) = (1, -1, -1, -1),$$

$$\delta_\infty([(2,0)-\infty]) = (1, 1, 1, -1), \delta_\infty([(5,0)-\infty]) = (1, 1, 1, -1),$$

οπότε

$$\delta_\infty(J(\mathbb{Q}_\infty)) = \langle (1, -1, -1, -1), (1, 1, 1, -1) \rangle.$$

Επιπλέον,

$$\begin{aligned} \mathrm{Ker}(\rho_\infty) = \langle &(2,1,1,1), (1,2,1,1), (1,1,2,1), (1,1,1,2), \\ &(3,1,1,1), (1,3,1,1), (1,1,3,1), (1,1,1,3), \\ &(5,1,1,1), (1,5,1,1), (1,1,5,1), (1,1,1,5) \rangle, \end{aligned}$$

(όλα τα στοιχεία αυτά απεικονίζονται στο $(1,1,1,1)$ μέσω της ρ_p, (βλ. Πίνακα 4.1), άρα

$$\begin{aligned}\rho_\infty^{-1}(\mathrm{Im}(\delta_\infty)) = \langle &(2,1,1,1),(1,2,1,1),(1,1,2,1),(1,1,1,2),\\ &(3,1,1,1),(1,3,1,1),(1,1,3,1),(1,1,1,3),\\ &(5,1,1,1),(1,5,1,1),(1,1,5,1),(1,1,1,5),\\ &(15,-1,-2,-5),(2,1,6,-3)\rangle\end{aligned}$$

Έχουμε ότι $\dim_{\mathbb{F}_2}(\delta_2(\mathbb{Q}_2)) = 4+2 = 6$ και ένα πλήρες σύστημα αντιπροσώπων της ομάδας $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ είναι το $\{\pm1,\pm2,\pm3,\pm6\}$. Βρίσκουμε

$$\delta_2([0,0)-\infty]) = (-1,-1,-2,3),\ \ \delta_2([(1,0)-\infty]) = (1,3,-1,-1),$$

$$\delta_2([(2,0)-\infty]) = (2,1,6,3),\ \ \delta_2([(5,0)-\infty]) = (-3,1,3,1).$$

Τα παραπάνω σημεία παράγουν έναν υπόχωρο διάστασης 4, άρα χρειαζόμαστε άλλους δύο γεννήτορες. Με τη συνάρτηση **find_possibilities** του Παραρτήματος, βλέπουμε ότι η καμπύλη έχει δύο σημεία της μορφής $(7,\alpha),(10,\beta)\in C(\mathbb{Q}_2)$. Εύκολα βλέπουμε ότι $(10,120)\in C(\mathbb{Q})$. Για το πρώτο, θέτουμε $g(Y) = Y^2 - f(7) = Y^2 - 420$. Έχουμε $g(2) = -416$, $|g(2)|_2 = \dfrac{1}{2^5}$, $g'(Y) = 2Y$ και $|g'(2)|_2^2 = \frac{1}{2^4}$, οπότε $|g(2)|_2 \le |g'(2)|_2^2$. Επομένως, από το Λήμμα του Hensel 2.10, υπάρχει $\alpha\in C(\mathbb{Q}_2)$ τέτοιο ώστε $g_2(\alpha)=0$ και έτσι παίρνουμε το σημείο $(7,\alpha)\in C(\mathbb{Q}_2)$. Υπολογίζουμε

$$\delta([(7,\alpha)-\infty]) = (7,6,5,2),\ \ \delta([(10,\beta)-\infty]) = (10,9,8,5),$$

συνεπώς

$$\delta_2([(7,\alpha)-\infty]) = (-1,6,-3,2),\ \ \delta_2([(10,\beta)-\infty]) = (-6,1,2,-3).$$

Με τη συνάρτηση **cp_span** του SAGE, ελέγχουμε ότι τα παραπάνω έξι στοιχεία παράγουν υπόχωρο διάστασης 6, οπότε

$$\begin{aligned}\delta_2(J(\mathbb{Q}_2)) = \langle &(-1,-1,-2,3),(1,3,-1,-1),(2,1,6,-3),(-3,1,3,-1)\\ &(-1,6,-3,2),(-6,1,2,-3)\rangle\end{aligned}$$

Επιπλέον,

$$\mathrm{Ker}(\rho_2) = \langle(-15,1,1,1),(1,-15,1,1),(1,1,-15,1),(1,1,1,-15)\rangle$$

οπότε

$$\begin{aligned}\rho_2^{-1}(\mathrm{Im}(\delta_2)) = \langle &(-15,1,1,1),(1,-15,1,1),(1,1,-15,1),(1,1,1,-15)\\ &(15,-1,-2,-5),(1,-5,-1,-1),(2,1,6,-3),(5,1,3,-15),\\ &(-7,-6,-5,-2),(-10,-9,-8,-5)\rangle,\end{aligned}$$

Έχουμε ότι $\dim_{\mathbb{F}_2}(\delta_3(\mathbb{Q}_3)) = 4 + 0 = 4$ και ένα πλήρες σύστημα αντιπροσώπων της ομάδας $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2$ είναι το $\{\pm 1, \pm 3\}$. Βρίσκουμε

$$\delta_3([(0,0) - \infty]) = (-3,-1,1,1), \delta_3([(1,0) - \infty]) = (1,1,-1,-1),$$

$$\delta_3([(2,0) - \infty]) = (-1,1,-3,-3), \delta_3([(5,0) - \infty]) = (-1,1,3,3).$$

Όμως τα παραπάνω στοιχεία παράγουν έναν υπόχωρο διάστασης 3, οπότε πρέπει να βρούμε έναν άλλον γεννήτορα. Παρατηρούμε ότι $(3,6) \in C(\mathbb{Q})$ και βρίσκουμε ότι $\delta([(3,6) - \infty]) = (3,2,1,-2)$ και $\delta_3([(3,6) - \infty]) = (3,-1,1,1)$, το οποίο μαζί με τα προηγούμενα, παράγουν έναν χώρο διάστασης 4, οπότε

$$\begin{aligned}\delta_3(J(\mathbb{Q}_3)) = \langle &(-3,-1,1,1), (1,1,-1,-1), (-1,1,-3,-3), (-1,1,3,3),\\ &(3,-1,1,1)\rangle.\end{aligned}$$

Επιπλέον,

$$\begin{aligned}\mathrm{Ker}(\rho_3) = \langle &(-2,1,1,1), (1,-2,1,1), (1,1,-2,1), (1,1,1,-2)\\ &(-5,1,1,1), (1,-5,1,1), (1,1,-5,1), (1,1,1,-5)\rangle\end{aligned}$$

άρα

$$\begin{aligned}\rho_3^{-1}(\mathrm{Im}(\delta_3)) = \langle &(-2,1,1,1), (1,-2,1,1), (1,1,-2,1), (1,1,1,-2)\\ &(-5,1,1,1), (1,-5,1,1), (1,1,-5,1), (1,1,1,-5),\\ &(15,-1,-2,-5), (1,-5,-1,-1), (2,1,6,-3), (5,1,3,-15),\\ &(3,2,1,-2)\rangle\end{aligned}$$

Έχουμε ότι $\dim_{\mathbb{F}_2}(\delta_5(\mathbb{Q}_5)) = 4$ και ένα πλήρες σύστημα αντιπροσώπων της ομάδας $\mathbb{Q}_5/(\mathbb{Q}_5^*)^2$ είναι το $\{1,2,5,10\}$. Βρίσκουμε

$$\begin{aligned}\delta_5([(0,0) - \infty]) = (10,1,2,5), \delta_5([(1,0) - \infty]) = (1,5,1,1),\\ \delta_5([(2,0) - \infty]) = (2,1,1,2), \delta_5([(5,0) - \infty]) = (5,1,2,10),\\ \delta_5([(3,6) - \infty]) = (2,2,1,2)\end{aligned}$$

τα οποία παράγουν έναν υπόχωρο διάστασης 4, δηλαδή

$$\delta_5(J(\mathbb{Q}_5)) = \langle (10,1,2,5), (1,5,1,1), (2,1,1,2), (5,1,2,10), (2,2,1,2)\rangle.$$

Επιπλέον,

$$\mathrm{Ker}(\rho_5) = \langle (6,1,1,1), (1,6,1,1), (1,1,6,1), (1,1,1,6)\rangle,$$

άρα

$$\begin{aligned}\rho_5^{-1}(\mathrm{Im}(\delta_5)) = \langle &(-1,1,1,1), (1,-1,1,1), (1,1,-1,1), (1,1,1,-1),\\ &(6,1,1,1), (1,6,1,1), (1,1,6,1), (1,1,1,6),\\ &(15,-1,-2,-5), (1,-5,-1,-1), (2,1,6,-3), (5,1,3,-15)\\ &(3,2,1,-2)\rangle\end{aligned}$$

Σε αυτό το σημείο, κάνουμε την εξής παρατήρηση: Οι εικόνες των σημείων

$$[(0,0)-\infty],[(1,0)-\infty],[(2,0)-\infty],[(5,0)-\infty],[(3,6)-\infty]$$

μέσω της δ, παράγουν έναν υπόχωρο διάστασης 5 (το ελέγχουμε με την **cp_span**), επομένως

$$\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta)) \geq 5.$$

Χρησιμοποιώντας τις συναρτήσεις του Παραρτήματος **cp_span** (για να γράψουμε τα $\rho_p^{-1}(\mathrm{Im}(\delta_p))$, $p \in S$ σε μορφή συνόλου), **multi_intersect** (για να βρούμε την τομή τους) και **same_set** (για να ελέγξουμε την δεύτερη ισότητα παρακάτω), συμπεραίνουμε ότι

$$\begin{aligned}\mathrm{Sel}^2(J(\mathbb{Q})) &= \bigcap_{p\in\{2,3,5,\infty\}} \rho_p^{-1}(\mathrm{Im}(\delta_p)) \\ &= \langle (15,-1,-2,-5),(1,-5,-1,-1),(2,1,6,-3),(5,1,3,-15),(3,2,1,-2)\rangle\end{aligned}$$

οπότε $\dim_{\mathbb{F}_2}(\mathrm{Sel}^2(J(\mathbb{Q}))) = 5$, επομένως από την

$$5 \leq \dim_{\mathbb{F}_2}(\mathrm{Im}(\delta)) \leq \dim_{\mathbb{F}_2}(\mathrm{Sel}^2(J(\mathbb{Q}))) = 5$$

παίρνουμε ότι $\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta)) = 5$, οπότε

$$r = 5 - 4 = 1.$$

Αφού $|J(\mathbb{Q})[2]| = 16$ και $J(\mathbb{Q})[2] \leq J(\mathbb{Q})_{\mathrm{tors}}$, έχουμε ότι $16 \mid |J(\mathbb{Q})_{\mathrm{tors}}|$. Από την άλλη μεριά, η καμπύλη έχει καλή αναγωγή στους πρώτους 7 και 11 (διότι $D(f) = 2^{12}\cdot 3^4\cdot 5^4$) με τη συνάρτηση **J(L,F)** του Παραρτήματος, βρίσκουμε ότι ότι $|\bar{J}(\mathbb{F}_7)| = 3\cdot 16$ και $\bar{J}(\mathbb{F}_{11}) = 11\cdot 16$. Από το Θεώρημα 3.33, η $J(\mathbb{Q})_{\mathrm{tors}}$ εμφυτεύεται στις $J(\mathbb{F}_7)$ και $J(\mathbb{F}_{11})$. Επομένως, η $J(\mathbb{Q})_{\mathrm{tors}}$ εμφυτεύεται σε μία ομάδα τάξης $\mu\kappa\delta(3\cdot 16, 11\cdot 16) = 16$, δηλαδή $|J(\mathbb{Q})_{\mathrm{tors}}| \mid 16$. Τελικά, $|J(\mathbb{Q})_{\mathrm{tors}}| = 16$, δηλαδή $J(\mathbb{Q})_{\mathrm{tors}} = J(\mathbb{Q})[2]$. Αυτό σημαίνει ότι

$$J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}$$

και το $P = [(3,6)-\infty]$ είναι σημείο της Ιακωβιανής με άπειρη τάξη.

□

Όταν το πολυώνυμο $f(X)$ δεν αναλύεται πλήρως υπέρ το $\mathbb{Q}$ τότε είναι απαραίτητη η χρήση Αλγεβρική Θεωρίας Αριθμών. Θα περιγράψουμε κάποιες βασικές έννοιες και προτάσεις αλγεβρική θεωρίας αριθμών προκειμένου να τις εφαρμόσουμε στο δεύτερο παράδειγμα.

Στοιχεία αλγεβρικής θεωρία αριθμών

4.15 Ορισμός. Αλγεβρικό σώμα αριθμών λέγεται κάθε υπόσωμα του $\mathbb{C}$ το οποίο είναι πεπερασμένη επέκταση του $\mathbb{Q}$. Έστω K ένα αλγεβρικό σώμα αριθμών. Ο $\alpha \in K$ θα λέγεται **ακέραιος αλγεβρικός αριθμός** όταν το ανάγωγό του πολυώνυμο, $\mathrm{Irr}(\alpha,\mathbb{Q})$ ανήκει στον $\mathbb{Z}[X]$.

Το σύνολο των ακέραιων αλγεβρικών αριθμών αποτελεί δακτύλιο, ο οποίος λέγεται **δακτύλιος των ακεραίων αλγεβρικών** του K και τον συμβολίζουμε R_K. Για $K = \mathbb{Q}$, ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του σώματος $\mathbb{Q}$ είναι το $\mathbb{Z}$.

Ως γνωστό, ο δακτύλιος $\mathbb{Z}$ είναι ευκλείδεια περιοχή και συνεπώς περιοχή κυρίων ιδεωδών, οπότε και περιοχή μονοσήμαντης ανάλυσης. Ο δακτύλιος των ακεραίων αλγεβρικών αριθμών δεν είναι εν γένει περιοχή μονοσήμαντης ανάλυσης, όμως είναι πάντοτε **δακτύλιος του Dedekind**, δηλαδή κάθε ιδεώδες αυτού αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών. Επομένως, αν $p \in \mathbb{P}$, το κύριο ιδεώδες $\langle p \rangle$ γράφεται στη μορφή

$$\langle p \rangle = pR_K = P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k}$$

με P_i, $i = 1, ..., k$ πρώτα ιδεώδη του R_K, $e_i \in \mathbb{N}$.

4.16 Ορισμός. Το e_i λέγεται **δείκτης διακλάδωσης** του πρώτου ιδεώδους P_i του R_K υπέρ το $\mathbb{Q}$ και συμβολίζεται $e_i = e_{K/\mathbb{Q}}(P_i)$. Το ιδεώδες P_i θα λέγεται **διακλαδιζόμενο** στην επέκταση $K/\mathbb{Q}$ όταν $e_{K/\mathbb{Q}}(P_i) > 1$.

4.17 Ορισμός. Ο πρώτος αριθμός $p \in \mathbb{P}$ **διακλαδίζεται** στην επέκταση $K/\mathbb{Q}$ όταν υπάρχει $i \in \{1, ..., k\}$ τέτοιο ώστε $e_i = e_{K/\mathbb{Q}}(P_i) > 1$.

Έστω $D_K \in \mathbb{Z}$ η διακρίνουσα του K. Ισχύει το παρακάτω.

4.18 Θεώρημα. ***(Θεώρημα της διακρίνουσας).*** *Ο πρώτος αριθμός p διακλαδίζεται στην επέκταση $K/\mathbb{Q}$ ακριβώς τότε όταν $p \mid D_K$.*

Σε κάθε ιδεώδες του R_K, αντιστοιχούμε έναν φυσικό αριθμό, ο οποίος λέγεται norm του ιδεώδους. Για τα πρώτα ιδεώδη P του R_K ισχύει ότι $\mathrm{norm}(P) = p^f$, $f \in \mathbb{N}$ και $p \in \mathbb{P}$ ο μοναδικός πρώτος αριθμός που ανήκει στο ιδεώδες P.

4.19 Ορισμός. Ο φυσικός αυτός αριθμός f λέγεται **βαθμός αδρανείας** του P και συμβολίζεται $f_{K/\mathbb{Q}}(P)$.

4.20 Θεώρημα. ***(Νόμος Ανάλυσης).*** *Έστω μία επέκταση K του $\mathbb{Q}$ βαθμού $n < \infty$. Αν*

$$\langle p \rangle = p \cdot R_K = P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k}$$

και $\mathrm{norm}(P_i) = p_i^{f_i}$ *τότε ισχύει*

$$e_1 f_1 + e_2 f_2 + ... + e_k f_k = n.$$

Όπως από τους ακέραιους αριθμούς κατασκευάζουμε τους ρητούς, έτσι και από τα ιδεώδη του R_K (τα οποία θα τα λέμε **ακέραια ιδεώδη**), κατασκευάζουμε τα **κλασματικά ιδεώδη** του σώματος K (το μηδενικό ιδεώδες δεν θεωρείται ιδεώδες στην Θεωρία Αριθμών). Στο σύνολο των ιδεωδών του K ορίζουμε μια σχέση ισοδυναμίας. Αν A, B ιδεώδη του K, τότε $A \sim B$ αν και μόνο αν το AB^{-1} είναι κύριο ιδεώδες του K.

4.21 Θεώρημα. *Το πλήθος των κλάσεων ιδεωδών είναι πεπερασμένο για κάθε αλγεβρικό σώμα αριθμών.*

4.22 Ορισμός. Το πλήθος των κλάσεων λέγεται **αριθμός κλάσεων ιδεωδών** του K και συμβολίζεται h_K.

Ισχύει το εξής:

4.23 Θεώρημα. *Είναι $h_K = 1$ αν και μόνο αν ο δακτύλιος των ακέραιων αλγεβρικών αριθμών R_K είναι περιοχή μονοσήμαντης ανάλυσης.*

Ως γνωστό, η επέκταση $K/\mathbb{Q}$ είναι **απλή**, δηλαδή υπάρχει $\theta \in K$ τέτοιο ώστε $K = \mathbb{Q}(\theta)$. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $\theta \in R_K$.

4.24 Θεώρημα. ***(Νόμος ανάλυσης στο K).*** *Έστω ότι $K = \mathbb{Q}(\theta)$ με $\theta \in R_K$ και υποθέτουμε ότι ισχύει $R_K = \mathbb{Z}[\theta]$. Αν $p \in \mathbb{P}$, $f(X) = \mathrm{Irr}(\theta, \mathbb{Q})$ και $f(X) = f_1(X)^{e_1} \cdots f_k(X)^{e_k} \mod p$ η ανάλυση του $f(X)$ σε γινόμενο αναγώγων πολυνύμων του $R_K[X]$ τότε $pR_K = P_1^{e_1} \cdots P_k^{e_k}$ και $f_i \coloneqq \deg(f_i(X))$.*

4.25 Ορισμός. Αν $K = \mathbb{Q}(\theta)$ αλγεβρικό σώμα αριθμών με $\theta \in R_K$ και

$$f(X) = \mathrm{Irr}(\theta, \mathbb{Q}) = (X - \theta_1)(X - \theta_2) \cdots (X - \theta_n)$$

με $\theta_1 = \theta$, τότε αν r_1 το πλήθος των πραγματικών ριζών του $f(X)$ και $2r_2$ το πλήθος των μιγαδικών, τότε η **ταυτότητα** του σώματος K είναι το ζεύγος (r_1, r_2). Προφανώς $[K : \mathbb{Q}] = r_1 + 2r_2$.

Το επόμενο θεώρημα αφορά στην δομή της ομάδας των μονάδων του σώματος K.

4.26 Θεώρημα. ***(Θεώρημα μονάδων του Dirichlet).*** *Η ομάδα των μονάδων του R_K, R_K^* είναι πεπερασμένα παραγόμενη αβελιανή ομάδα με βαθμό (rank) $r = r_1 + r_2 - 1$. Επομένως, υπάρχουν μονάδες $\varepsilon_1, ..., \varepsilon_r \in R^*$ τέτοιες ώστε κάθε $\varepsilon \in R^*$ να γράφεται μονοσήμαντα στη μορφή*

$$\varepsilon = \zeta^s \cdot \varepsilon_1^{s_1} \cdots \varepsilon_r^{s_r}$$

με $s, s_i \in \mathbb{N}$ για κάθε $i \in \{1, ..., r\}$ και ζ μία ρίζα της μονάδας που ανήκει στο K.

Στην ειδική περίπτωση που η επέκταση $K/\mathbb{Q}$ είναι Galois, ο νόμος ανάλυσης γράφεται ως εξής: Αν $p \in \mathbb{P}$ τότε $pR_K = (P_1 P_2 \cdots P_n)^e$ και $\mathrm{norm}(P_i) = f$ για κάθε $i = 1, 2, ..., r$. Επομένως,

$$n = [K : \mathbb{Q}] = r \cdot e \cdot f.$$

Στην περίπτωση της κυκλοτομικής επέκτασης $K = \mathbb{Q}(\zeta_p)$ όπου $p \in \mathbb{P}$ και ζ_p μία πρωταρχική p-ρίζα της μονάδας, η διακρίνουσα του K είναι

$$D_K = (-1)^{p(p-1)} p^{p-2},$$

συνεπώς ο μόνος διακλαδιζόμενος πρώτος είναι ο p, ο οποίος μάλιστα διακλαδίζεται πλήρως και $pR_K = P^{p-1}$ με $P = \langle 1 - \zeta_p \rangle$.

Τοπικά σώματα αριθμών

Κατ΄ αναλογία προς τα αλγεβρικά σώματα αριθμών, τα τοπικά σώματα μπορούν να ορισθούν ως πεπερασμένες επεκτάσεις κάποιου p-αδικού σώματος $\mathbb{Q}_p$. Στην Θεωρία Αριθμών, αν K είναι ένα αλγεβρικό σώμα αριθμών και P ένα πρώτο ιδεώδες του δακτυλίου των ακεραίων αλγεβρικών αριθμών R_K, τότε, κατ΄ αναλογία προς τους πρώτους αριθμούς, θεωρούμε την πλήρωση του K ως προς την απόλυτη τιμή που προκύπτει από την διακριτή εκτίμηση v_P που ορίζει το ιδεώδες P. Το σώμα αυτό συμβολίζεται με K_P και λέγεται **P-αδικό σώμα**. Η εκτίμηση v_P επεκτείνεται κατά μοναδικό τρόπο σε μία διακριτή εκτίμηση του K_P. Αν R_P ο δακτύλιος εκτίμησης και $P \cdot R_P$ το αντίστοιχο maximal ιδεώδες του K_P, τότε το σώμα κλάσεων πηλίκων (residue class field) R_P/P_P είναι πεπερασμένο.

4.27 Θεώρημα. *Έστω K σώμα εφοδιασμένο με εκτίμηση $v(x)$. Οι παρακάτω προτάσεις είναι ισοδύναμες:*

(α) Το K είναι P-αδικό σώμα με την P-αδική εκτίμηση.

(β) Για το K ισχύουν τα εξής:

1. *έχει χαρακτηριστική 0.*
2. *είναι πλήρες ως προς την εκτίμηση $v(x)$.*
3. *Το σώμα κλάσεων υπολοίπων R/P (όπου R ο δακτύλιος εκτίμησης του P και P το πρώτο ιδεώδες εκτίμησης του K) είναι πεπερασμένο*

(γ) Το K είναι πεπερασμένη επέκταση κάποιου $\mathbb{Q}_p$, $p \in \mathbb{P}$.

Το $\langle p \rangle = p\mathbb{Z}_p$ επεκτείνεται στο K_P και έχει τη μορφή $pR_P = (PR_P)^e$.

4.28 Ορισμός. Ο φυσικός αριθμός e λέγεται **δείκτης διακλάδωσης** της επέκτασης $K_P/\mathbb{Q}_P$ και ο βαθμός της επέκτασης $f := [R_P : \mathbb{Z}_p]$ βαθμός αδρανείας της επέκτασης αυτής.

4.29 Θεώρημα. *Ισχύει η ισότητα*

$$n = [K_P : \mathbb{Q}_p] = ef.$$

4.30 Ορισμός. Η επέκταση $K_P/\mathbb{Q}_p$ θα λέγεται **μη διακλαδιζόμενη** όταν $e = 1$ (και $f = n$). Θα λέγεται **πλήρως διακλαδιζόμενη** όταν $e = n$ (και $f = 1$).

Κυκλοτομικές επεκτάσεις των p-αδικών σωμάτων.

Θα αναφερθούμε στην ειδική μορφή που χρειαζόμαστε.

4.31 Θεώρημα. *Έστω $p \in \mathbb{P}$ και ζ_q μία πρωταρχική q-ρίζα της μονάδας, $q \in \mathbb{P}$. Υποθέτουμε ότι $q \neq p$. Η επέκταση $\mathbb{Q}_p(\zeta_q)/\mathbb{Q}_p$ είναι μη-διακλαδιζόμενη με βαθμό f όπου f είναι ο ελάχιστος φυσικός αριθμός τέτοιος ώστε $p^f \equiv 1 \mod q$.*

4.32 Θεώρημα. *Έστω $p \in \mathbb{P}$ και ζ_p μία πρωταρχική p-ρίζα της μονάδας. Η επέκταση $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ είναι πλήρως διακλαδιζόμενη βαθμού $e = \phi(p) = p - 1$. Ο δακτύλιος εκτίμησης του $\mathbb{Q}_p(\zeta_p)$ είναι ο $\mathbb{Z}_p[\zeta_p]$ και το $1 - \zeta_p$ είναι ένας normalizer του $\mathbb{Z}_p[\zeta_p]$ με norm p.*

Συνεχίζουμε με το παράδειγμα.

4.33 Παράδειγμα. Θεωρούμε την υπερελλειπτική καμπύλη γένους 2 υπέρ το $\mathbb{Q}$, $C : Y^2 = X^5 + 1$. Θέτουμε $f(X) = X^5 + 1$. Η ανάλυση του $f(X)$ σε ανάγωγα πολυώνυμα του $\mathbb{Q}[X]$ είναι

$$f(X) = (X + 1)(X^4 - X^3 + X^2 - X + 1).$$

Μία ρίζα του $X^4 - X^3 + X^2 - X + 1$ είναι η $-\zeta_5$ όπου ζ_5 είναι μία πρωταρχική 5- ρίζα της μονάδας. Αφού $\mathbb{Q}(-\zeta_5) = \mathbb{Q}(\zeta_5)$, έχουμε

$$A_C \cong \mathbb{Q} \times \mathbb{Q}(\zeta_5).$$

Ο δακτύλιος των ακεραίων αλγεβρικών αριθμών R του σώματος $K = \mathbb{Q}(\zeta_5)$ είναι ο $R = \mathbb{Z}[\zeta_5]$ και είναι περιοχή κυρίων ιδεωδών. Επομένως οι «κακοί» πρώτοι είναι οι 2 και 5.

Από τον νόμο ανάλυσης στα κυκλοτομικά σώματα έχουμε ότι το 2 αδρανεί στο $K = \mathbb{Q}(\zeta_5)$, ενώ το 5 διακλαδίζεται πλήρως στο K, δηλαδή $2R = P_1$ ενώ $5R = P_2^4$ και μάλιστα $P_2 = \langle \pi \rangle$ όπου $\pi = 1 - \zeta_5$. Η επέκταση $K/\mathbb{Q}$ είναι πλήρως μιγαδική, δηλαδή $[K : \mathbb{Q}] = 4$ με $r_1 = 0$ και $r_2 = 2$. Επομένως, σύμφωνα με το θεώρημα μονάδων του Dirichlet, η ομάδα των μονάδων του K, $E(R_K)$ είναι μία πεπερασμένα παραγόμενη αβελιανή ομάδα με rank $r_1 + r_2 - 1 = 1$. Αυτό σημαίνει ότι $E(R_K) \cong \langle -1 \rangle \times \langle \varepsilon_0 \rangle$ και μάλιστα γνωρίζουμε ότι $\varepsilon_0 = 1 + \zeta_5$. Από τα παραπάνω συνάγεται ότι η ομάδα H' όπως ορίσθηκε πιο πριν, μπορεί να θεωρηθεί ως η ομάδα

$$H' = \langle -1, 2, 1 + \zeta_5, 1 - \zeta_5 \rangle.$$

Το πολυώνυμο $f(X)$ παραμένει ανάγωγο και στα p-αδικά σώματα $\mathbb{Q}_2$ και $\mathbb{Q}_5$ (αυτό προκύπτει άμεσα από τα παραπάνω, αφού, αν το $f(X) \in \mathbb{Q}[X]$ είναι ανάγωγο υπέρ το $\mathbb{Q}$, τότε είναι ανάγωγο υπέρ το $\mathbb{Q}_p$ για κάποιον πρώτο $p \in \mathbb{P}$ αν και μόνο αν έχει μοναδικό πρώτο διαιρέτη στο $K = \mathbb{Q}(\alpha)$ όπου α μία ρίζα του $f(X)$. Συνεπώς, αν περάσουμε στα p-αδικά σώματα $\mathbb{Q}_2$ και $\mathbb{Q}_5$, έχουμε

$$H_2 = \mathbb{Q}_2(\zeta_5)^*/(\mathbb{Q}_2(\zeta_5)^*)^2 \text{ και } H_5 = \mathbb{Q}_5(\zeta_5)^*/(\mathbb{Q}_5(\zeta_5)^*)^2,$$

$\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta_2)) = 3$ και $\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta_5)) = 1$. Στη συνέχεια, βρίσκουμε βάση για τις H_2 και H_5 (βλ. [41, σελ. 39]). Έστω K μία πεπερασμένη επέκταση του $\mathbb{Q}_p$. Έστω $p \in \mathbb{P} \setminus \{2\}$ Σταθεροποιούμε έναν uniformizer $\pi \in K$. Τότε $K^*/(K^*)^2 = \langle \pi, u \rangle$ όπου u είναι μονάδα του K η οποία δεν είναι τέλειο τετράγωνο. Αφού όλες οι μονάδες του K που δεν είναι τέλειο τετράγωνο είναι ισοδύναμες modulo τετράγωνα, η βάση είναι καλώς ορισμένη. Από την άλλη μεριά, κάθε επιλογή uniformizer $\bmod \pi^2$ δίνει

διαφορετική βάση.

Η περίπτωση $p = 2$ είναι δυσκολότερη. Έστω k το σώμα υπολοίπων του K, e ο βαθμός διακλάδωσης και f ο βαθμός αδρανείας του K υπέρ το $\mathbb{Q}_2$. Έτσι, $[K : \mathbb{Q}_2] = ef$ και $[k : \mathbb{F}_2] = f$. Σταθεροποιούμε έναν uniformizer $\pi \in K^*$ και έστω $b_1, ..., b_f$ ένα σύνολο στοιχείων του K των οποίων τα υπόλοιπα αποτελούν βάση του k ως $\mathbb{F}_2$-διανυσματικό χώρο. Αν $\dim(K^*/(K^*)^2) = ef + 2$ τότε τα $ef + 1$ στοιχεία

$$\pi, 1 + b_1\pi, ..., 1 + b_f\pi, 1 + b_1\pi^2 + ... + 1 + b_f\pi^3, ..., 1 + b_1\pi^{2e-1}, ..., 1 + b_f\pi^{2e-1}$$

είναι ανεξάρτητα modulo τετράγωνα. Συμπληρώνουμε την βάση με ένα στοιχείο μ που δεν είναι τέλειο τετράγωνο στο $1 + \langle\pi\rangle^{2e} = 1 + \langle 4\rangle$. Αν τα μ, μ' είναι δύο στοιχεία που δεν είναι τέλεια τετράγωνα και είναι $1 \mod 4$ τότε τα μ και μ' είναι ισοδύναμα modulo τετράγωνα.
Στη συνέχεια, υπολογίζουμε τις εικόνες των δ_∞, δ_5 και δ_2 για τους γεννήτορες της H'.

Υπολογισμός του δ_∞: Προφανώς, επειδή το K είναι πλήρως μιγαδική επέκταση του $\mathbb{Q}$, το σώμα K εμφυτεύεται στο $\mathbb{C}^4$, οπότε, αφού το $\mathbb{C}$ είναι αλγεβρικά κλειστό, έπεται ότι η δ_∞ είναι τετριμμένη.

Υπολογισμός του δ_5: Γνωρίζουμε ότι $\dim_{\mathbb{F}_2}(\mathrm{Im}(\delta_5)) = \dim(\mathrm{Im}(\delta)) + 0 = 1$. Στο Παράδειγμα 3.30, δείξαμε ότι η ομάδα $J(\mathbb{Q})[2]$ της υπερελλειπτικής καμπύλης C έχει τάξη 2 και παράγεται από το $[(-1, 0) - \infty]$. Συνεπώς η $\mathrm{Im}(\delta_5)$ παράγεται από το

$$\delta_5([(-1, 0) - \infty]) = (1 - \zeta_5)\square.$$

Τώρα, η H_5 έχει διάσταση 2 και παράγεται από τα 2 και $1 - \zeta_5$ (αυτό ισχύει για κάθε πρώτο $p \neq 2$). Το $\pi = 1 - \zeta_5$ είναι ένας uniformizer και το 2 μία μονάδα του $\mathbb{Q}_5(\zeta_5)$ η οποία δεν είναι τέλειο τετράγωνο στο $\mathbb{Q}_5(\zeta_5)$. Επομένως, $H_5 = \langle 2, 1 - \zeta_5\rangle$.

Οι εικόνες των γεννητόρων της H' στην H_5 είναι οι

-1	1
2	2
$1 + \zeta_5$	2
$1 - \zeta_5$	$1 - \zeta_5$

.

Το -1 είναι τέλειο τετράγωνο στο $\mathbb{Q}_5$, συνεπώς και στο $\mathbb{Q}_5(\zeta_5)$. Το 2 είναι μονάδα στο $\mathbb{Q}_5(\zeta_5)$, η οποία δεν είναι τέλειο τετράγωνο σε αυτό. Παρατηρούμε ότι όλες οι μονάδες στο $\mathbb{Q}_5(\zeta_5)$ οι οποίες δεν είναι τέλεια τετράγωνα στο $\mathbb{Q}_5(\zeta_5)$ ανήκουν στην ίδια κλάση modulo τετράγωνα. Επομένως, η εικόνα του $1 + \zeta_5$ είναι το 2, αφού $1 + \zeta_5$ επίσης μονάδα του $\mathbb{Q}_5(\zeta_5)$. Αυτό μπορούμε να το δούμε εφαρμόζοντας το θεώρημα του Dirichlet. Τέλος, η κλάση του π^n modulo τετράγωνα καθορίζεται πλήρως από το $n \mod 2$. Συνεπώς, $\delta_5(1 - \zeta_5) = 1 - \zeta_5$.

Σημείωση: Όλες οι ομάδες είναι στοιχειώδεις 2-ομάδες. Η H' έχει τάξη $2^4 = 16$ και η H_5 έχει τάξη $2^2 = 4$. Η απεικόνιση $\rho_5 : H' \to H_5$, σύμφωνα με τα παραπάνω, είναι

επιμορφισμός ομάδων. Επομένως, η $\mathrm{Ker}(\rho_5)$ έχει τάξη 4, δηλαδή είναι ισόμορφη με την ομάδα του Klein. Άρα παράγεται από δύο οποιαδήποτε στοιχεία τάξης 2. Το ένα από αυτά τα στοιχεία είναι το -1. Για το δεύτερο, παρατηρούμε ότι

$$\rho_5(2(1+\zeta_5)) = \rho_5(2)\rho_5(1+\zeta_5) = 2\cdot 2 = 5 = 1 \mod (\mathbb{Q}_5(\zeta_5)^*)^2.$$

Συνεπώς, $2(1+\zeta_5) \in \mathrm{Ker}(\rho_5)$ και $2(1+\zeta_5) \neq -1$. Άρα $\mathrm{Ker}(\rho_5) = \langle -1, 2(1+\zeta_5)\rangle$.

Επομένως, $\rho_5^{-1}(\mathrm{Im}(\delta_5)) = \langle -1, 2(1+\zeta_5), 1-\zeta_5\rangle$.

Ανάλογα, αλλά αρκετά πιο δύσκολα, υπολογίζουμε τις εικόνες των γεννητόρων της H' μέσω της δ_2. Συγκεκριμένα, σύμφωνα με τα παραπάνω, βρίσκουμε

$$H_2 = \langle -1, 2, 1-2\zeta_5, 1-2\zeta_5^2, 1-2\zeta_5^3, 1+4\zeta_5\rangle$$

Επίσης, (βλ. [37, σελ. 37]),

$$\rho_2(-1) = -1\Box, \rho_2(2) = 2\Box, \rho_2(1+\zeta_5) = (-1)(1-2\zeta_5^2)(1-2\zeta_5^3)\Box$$

και

$$\rho_2(1-\zeta_5) = (1-2\zeta_5)(1-2\zeta_5^2)(1+4\zeta_5)\Box.$$

Ειδικότερα, η ρ_2 είναι 1-1 στην H'. Οι τελευταίες ισότητες μπορούν να επιβεβαιωθούν εκτελώντας τις παρακάτω εντολές στην MAGMA.

```
K<z> := NumberField(Polynomial([1,1,1,1,1]));
pr2 := Decomposition(Integers(K), 2)[1,1];
K2, toK2 := Completion(K, pr2);
IsSquare(toK2(-(1+z)*(1-2*z^2)*(1-2*z^3)));
IsSquare(toK2((1-z)*(1-2*z)*(1-2*z^2)*(1+4*z)));
```

Από το Λήμμα του Hensel, υπάρχουν σημεία $P_1, P_2 \in C(\mathbb{Q}_2)$ με $X(P_1) = 2$ και $X(P_2) = 4$. Πράγματι, αν θέσουμε $g_1(Y) = Y^2 - f(2) = Y^2 - 33$ τότε $g_1'(Y) = 2Y$ και έχουμε

$$|g_1(1)|_2 = |-32|_2 = \frac{1}{2^5}$$

και

$$|g_1'(1)|_2^2 = |2|_2^2 = \frac{1}{2^2},$$

οπότε $|g_1(1)|_2 < |g_1'(1)|^2$. Συνεπώς, από το Λήμμα του Hensel 2.10, υπάρχει $\alpha \in C(\mathbb{Q}_2)$ τέτοιο ώστε $g_1(\alpha) = 0$ και έτσι παίρνουμε το σημείο $(2, \alpha) \in C(\mathbb{Q}_2)$.

Επίσης, αν θέσουμε $g_2(Y) = Y^2 - f(4) = Y^2 - 2^{10} - 1$ τότε $g_2'(Y) = 2Y$ και έχουμε

$$|g_1(1)|_2 = |-2^{10}|_2 = \frac{1}{2^{10}}$$

και

$$|g_1'(1)|_2^2 = |2|_2^2 = \frac{1}{2^2},$$

οπότε $|g_1(1)|_2 < |g_1'(1)|_2^2$. Συνεπώς, από το Λήμμα του Hensel 2.10, υπάρχει $\beta \in C(\mathbb{Q}_2)$ τέτοιο ώστε $g_2(\beta) = 0$ και έτσι παίρνουμε το σημείο $(4, \beta) \in C(\mathbb{Q}_2)$.
Βρίσκουμε ότι (βλ. [37, σελ. 37])

$$\delta_2([P_1 - \infty]) = (2 + \zeta_5)\square = (-1)(1 - 2\zeta_5)(1 - 2\zeta_5^2)(1 - 2\zeta_5^2)(1 + 4\zeta_5)\square,$$

$$\delta_2([P_2 - \infty]) = (4 + \zeta_5)\square = (1 + 4\zeta_5)\square$$

και

$$\delta_2([(-1, 0) - \infty]) = (-1 + \zeta_5)\square = (-1)(1 - 2\zeta_5)(1 - 2\zeta_5^2)(1 + 4\zeta_5).$$

Αυτές οι εικόνες παράγουν το $\mathrm{Im}(\delta_2)$. Συνεπάγεται ότι

$$\mathrm{Sel}^2(J(\mathbb{Q})) = \delta(J(\mathbb{Q})[2]) = \langle (-1)(1 - \zeta_5)\square \rangle.$$

Συνεπάγεται ότι $\dim_{\mathbb{F}_2}(\mathrm{Sel}^2(J(\mathbb{Q}))) = 1$. Από τη σχέση

$$\dim_{\mathbb{F}_2}(\delta(J(\mathbb{Q}))) = \dim_{\mathbb{F}_2}(J(\mathbb{Q})[2]) + r$$

προκύπτει ότι $r = 0$. Στο Παράδειγμα 3.35 είδαμε ότι $|J(\mathbb{Q})_{\mathrm{tors}}| = 10$, οπότε $J(\mathbb{Q}) \cong \mathbb{Z}/10\mathbb{Z}$ και παράγεται από το $P = (X(X + 1), X + 1)$. Υπολογίζουμε ότι

$$\begin{aligned} J(\mathbb{Q}) = \{&(1, 0), (X(X + 1), X + 1), (X^2, 1), (X^2 - 2X + 2, -2X + 3), (X - 1), \\ &(X + 1, 0), (X, 1), (X^2 - 2X + 2, 2X - 3), (X^2, -1), (X(X + 1), -X - 1)\} \end{aligned}$$

Στη συνέχεια, ελέγχουμε ποια από αυτά τα 10 σημεία γράφονται στη μορφή $i(P)$ όπου $i : C(\mathbb{Q}) \to J(\mathbb{Q})$ με $i(P) = [P - \infty]$. Τα σημεία της $J(\mathbb{Q})$ αντιστοιχούν σε διαιρέτες βαθμού 2 σε γενική θέση (οπότε το ∞ δεν περιέχεται στο support τους). Καθώς $\deg(P - \infty) = 0$, τα ζητούμενα σημεία είναι αυτά για τα οποία $\deg(a) \leq 1$ (διότι αν $\deg(a) > 1$, το support του διαιρέτη του a περιέχει περισσότερα από ένα σημεία), δηλαδή τα

$$(1, 0), \ \ (X, -1), \ \ (X + 1, 0), \ \ (X, 1),$$

τα οποία αντιστοιχούν στα σημεία

$$\infty, \ \ (0, -1), \ \ (-1, 0), \ \ (0, 1).$$

Συνεπώς, $C(\mathbb{Q}) = \{\infty, (0, -1), (-1, 0), (0, 1)\}$. □

Κεφάλαιο V

Διαφορικά και η μέθοδος του Chabauty

§1 Διαφορικά σε υπερελλειπτικές καμπύλες

5.1 Πρόταση. *Έστω $C : Y^2 = f(X)$ μία υπερελλειπτική καμπύλη γένους g υπέρ το K. Τότε ο χώρος $\Omega^{\mathrm{reg}}_C(K)$ έχει K-βάση το σύνολο*

$$\left\{\frac{dX}{2Y}, \frac{XdX}{2Y}, \frac{X^2dX}{2Y}, ..., \frac{X^{g-1}dX}{2Y}\right\},$$

οπότε κάθε ολόμορφο διαφορικό μπορεί να γραφτεί κατά μοναδικό τρόπο στη μορφή $\dfrac{p(X)dX}{2Y}$ όπου $p(X) \in K[X]$ και $\deg(p) \leq g-1$.

Απόδειξη. Θέτουμε $\omega_0 = \dfrac{dX}{2Y}$. Επίσης, θέτουμε

$$D_\infty = \begin{cases} 2 \cdot \infty, & \deg(f) = 2g+1 \\ \infty_s + \infty_{-s} & \deg(f) = 2g+2. \end{cases}$$

Θα δείξουμε ότι $\mathrm{div}(\omega_0) = (g-1)D_\infty$. Έστω $P = (x, y) \in C_{\mathrm{aff}}(\bar{K})$.

Αν $y \neq 0$ τότε το $t = X - x$ είναι uniformizer στο P και $dt = dX$, δηλαδή $\dfrac{dt}{dX} = 1$, άρα

$$v_P(\omega_0) = v_P\left(\frac{\omega_0}{dt}\right) = v_P\left(\frac{dX}{2Y}\frac{1}{dt}\right) = v_P\left(\frac{dX}{dt}\frac{1}{2Y}\right) = v_P\left(\frac{1}{2Y}\right) = -2v_P(Y) = 0$$

διότι η συνάρτηση Y δεν μηδενίζεται στο P.

Αν $y = 0$ τότε το $t = Y$ είναι uniformizer στο P και $dt = dY$. Από την εξίσωση της καμπύλης $Y^2 = f(X)$, παίρνουμε $2YdY = f'(X)dX$, δηλαδή $\dfrac{dX}{dY} = \dfrac{2Y}{f'(X)}$, άρα

$$\frac{\omega_0}{dt} = \frac{dX}{2Y}\frac{1}{dt} = \frac{dX}{2YdY} = \frac{dX}{dY}\frac{1}{2Y} = \frac{2Y}{f'(X)}\frac{1}{2Y} = \frac{1}{f'(X)}.$$

Η $f'(X)$ δεν μηδενίζεται στο P (αν μηδενιζόταν, το $f(X)$ θα είχε πολλαπλή ρίζα στο P), άρα

$$v_P(\omega_0) = v_P\left(\frac{\omega_0}{dt}\right) = v_P\left(\frac{1}{f'(X)}\right) = 0.$$

Μένει να εξετάσουμε τι γίνεται στα επ'άπειρον σημεία.

Έστω $\deg(f) = 2g+2$. Τότε έχουμε δύο επ'άπειρον σημεία στο $C_{\text{aff}}(\bar{K})$, τα ∞_s και ∞_{-s}, τα οποία έχουν uniformizer το $t = \dfrac{1}{X}$. Είναι $dt = -\dfrac{1}{X^2}$, άρα

$$\frac{\omega_0}{dt} = \frac{dX}{2Ydt} = -\frac{dX \cdot X^2}{2YdX} = -\frac{X^2}{2Y},$$

επομένως,

$$\begin{aligned} v_P(\omega_0) &= v_P\left(\frac{\omega_0}{dt}\right) \\ &= v_P\left(-\frac{X^2}{2Y}\right) \\ &= v_P(X^2) - v_P(2Y) \\ &= v_P(X^2) - v_P(Y) \\ &= -2 - (-g-1) \\ &= g-1. \end{aligned}$$

Έστω $\deg(f) = 2g+1$. Τότε έχουμε ένα επ'άπειρον σημείο, το ∞, και ένας uniformizer είναι ο $dt = \dfrac{Y}{X^{g+1}}$. Έχουμε

$$\begin{aligned} dt &= \frac{X^{g+1}dY - (g+1)X^gYdX}{X^{2g+2}} \\ &= \frac{2YdY \cdot X - 2(g+1)dX \cdot Y^2}{2YX^{g+2}} \\ &= \frac{Xf'(X)dX - 2(g+1)f(X)dX}{2YX^{g+2}} \end{aligned}$$

άρα

$$\begin{aligned} v_P(\omega_0) &= v_P\left(\frac{\omega_0}{dt}\right) \\ &= v_P\left(\frac{2YX^{g+2}}{Xf'(X)dX - 2(g+1)f(X)dX}\frac{dX}{2Y}\right) \\ &= v_P\left(\frac{X^{g+2}}{Xf'(X) - 2(g+1)f(X)}\right) \end{aligned}$$

Τα πολυώνυμα $Xf'(X)$ και $2(g+1)f(X)$ έχουν βαθμό $2g+1$. Το πρώτο έχει μεγιστοβάθμιο συντελεστή $2g+1$ και το δεύτερο $2g+2$. Άρα και η διαφορά τους έχει βαθμό $2g+1$ (αφού οι μεγιστοβάθμιοι συντελεστές δεν αλληλοαναιρούνται), που σημαίνει ότι

$$v_P(Xf'(X) - 2(g+1)f(X)) = v_P(X^{2g+1}).$$

Έτσι,

$$\begin{aligned} v_P(\omega_0) &= v_P(X^{2g+2}) - v_P(Xf'(X) - 2(g+1)f(X)) \\ &= v_P(X^{g+2}) - v_P(X^{2g+1}) \\ &= -2(g+2) + 2(2g+1) \\ &= 2g-2 \end{aligned}$$

Δείξαμε λοιπόν ότι $\mathrm{div}(\omega_0) = (g-1)D_\infty$. Αν τώρα $\omega \in \Omega_C^{\mathrm{reg}}(K)$ και $\phi \in K(C)$ τέτοια ώστε $\omega = \phi\omega'$, το ω είναι ολόμορφο αν και μόνο αν $\phi \in \mathscr{L}(\mathrm{div}(\omega_0))$. Πράγματι,

$$\begin{aligned} \phi \in \mathscr{L}((g-1)D_\infty) &\Leftrightarrow \mathrm{div}(\phi) + \mathrm{div}(\omega_0) \geq 0 \\ &\Leftrightarrow \mathrm{div}\left(\frac{\omega}{\omega_0}\right) + \mathrm{div}(\omega_0) \geq 0 \\ &\Leftrightarrow \mathrm{div}(\omega) - \mathrm{div}(\omega_0) + \mathrm{div}(\omega_0) \geq 0 \\ &\Leftrightarrow \mathrm{div}(\omega) \geq 0 \\ &\Leftrightarrow v_P(\omega) \geq 0 \ \text{ για κάθε } \ P \in \mathrm{supp}(\mathrm{div}(\omega)) \\ &\Leftrightarrow \omega \ \text{ ολόμορφο} \end{aligned}$$

Όμως $\mathscr{L}(\mathrm{div}(\omega)) = \mathscr{L}((g-1)D_\infty) = \langle 1, X, X^2, ..., X^{g-1}\rangle$, καθώς οι συναρτήσεις

$$1, X, X^2, ..., X^{g-1}$$

ανήκουν στον χώρο $\mathscr{L}((g-1)D_\infty)$, είναι γραμμικώς ανεξάρτητες και γνωρίζουμε ότι $\dim(\mathrm{div}(\omega)) = g$, αφού $\mathrm{div}(\omega) \in \Omega_C^{\mathrm{reg}}(K)$. ■

§2 Το ολοκλήρωμα του Coleman

Σε αυτήν την παράγραφο, θα αναπτύξουμε εν συντομία μία θεωρία ολοκλήρωσης διαφορικών καμπυλών πάνω από το σώμα των p-αδικών αριθμών, η οποία οφείλεται στον Robert F. Coleman. Στο επόμενο θεώρημα συγκεντρώνουμε τις βασικότερες ιδιότητές του.

5.2 Θεώρημα. *Έστω $p \in \mathbb{P}$ και C μια ομαλή, προβολική και απολύτως ανάγωγη καμπύλη με καλή αναγωγή υπέρ το $\mathbb{Q}_p$. Τότε για κάθε ζεύγος σημείων $P, Q \in C(\bar{\mathbb{Q}}_p)$ και για κάθε ολόμορφο διαφορικό $\omega \in \Omega_C^{\mathrm{reg}}(K)$, υπάρχει ένα ολοκλήρωμα $\int_P^Q \omega \in \bar{\mathbb{Q}}_p$ που ικανοποιεί τις εξής ιδιότητες:*

1) Το ολοκλήρωμα είναι $\bar{\mathbb{Q}}_p$-γραμμικό στο ω, δηλαδή αν $\omega, \omega' \in \Omega_C^{\mathrm{reg}}(K)$ και $a, b \in \bar{\mathbb{Q}}_p$ τότε

$$\int_P^Q (a\omega + b\omega') = a\int_P^Q \omega + b\int_P^Q \omega'.$$

2) Αν τα P και Q ανάγονται στο ίδιο σημείο στο $\bar{C}(\bar{\mathbb{F}}_p)$, δηλαδή $\bar{P} = \bar{Q}$ τότε το ολοκλήρωμα μπορεί να υπολογιστεί γράφοντας $\omega = w(t)dt$ όπου t ένας uniformizer στο P ο οποίος ανάγεται σε uniformizer στο $\bar{P}$ και w μια δυναμοσειρά της οποίας οι συντελεστές έχουν φραγμένη p-αδική απόλυτη τιμή. Ολοκληρώνουμε τυπικά την w και λαμβάνουμε μια δυναμοσειρά l για την οποία $dl(t) = w(t)dt$ και $l(0) = 0$ (δηλαδή η l δεν έχει σταθερό όρο). Υπολογίζουμε το $l(t(Q))$, που συγκλίνει διότι $|t(Q)|_p < 1$ και τελικά,

$$\int_P^Q \omega = l(t(Q)).$$

3) Για τρία σημεία $P, Q, R \in C(\bar{\mathbb{Q}}_p)$,

$$\int_P^Q \omega + \int_R^S \omega = \int_P^S \omega + \int_R^Q \omega$$

Από αυτό, συνεπάγεται και η ισότητα

$$\int_P^Q \omega = \int_P^R \omega + \int_R^Q \omega.$$

για κάθε $P, Q, R, S \in C(\bar{\mathbb{Q}}_p)$. Μπορούμε λοιπόν για έναν διαιρέτη

$$D = \sum_{j=1}^{n} (Q_j - P_j) \in \mathrm{Div}^0(C(\bar{\mathbb{Q}}_p))$$

να ορίσουμε

$$\int^D \omega = \sum_{j=1}^{n} \int_{P_j}^{Q_j}.$$

4) Αν ο D είναι κύριος διαιρέτης, τότε $\int^D \omega = 0$.

5)Το ολοκλήρωμα είναι συμβατό με τη δράση της απόλυτης ομάδας Galois του $\mathbb{Q}_p$, δηλαδή

$$\sigma\left(\int^D \omega\right) = \int^{\sigma(D)} \sigma(\omega)$$

για κάθε $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

6) Σταθεροποιούμε ένα $P_0 \in C(\mathbb{Q}_p)$. Αν $\omega \in \Omega^{\mathrm{reg}}_C(\bar{\mathbb{Q}}_p)$ με $\omega \neq 0$ τότε το σύνολο των σημείων $P \in C(\mathbb{Q}_p)$ που ανάγονται στο ίδιο σημείο του $\bar{C}(\bar{\mathbb{F}}_p)$ με το P_0 και τέτοια ώστε $\int_{P_0}^{P} \omega = 0$ είναι πεπερασμένο.

Απόδειξη. βλ. [4]. ■

5.3 Σημείωση. Η υπόθεση ότι η καμπύλη έχει καλή αναγωγή στο p δεν είναι απαραίτητη, αλλά απλοποιεί την διατύπωση του (2) θεωρήματος.

5.4 Πόρισμα. *Έστω $p \in \mathbb{P}$ και C μια ομαλή, προβολική και απολύτως ανάγωγη καμπύλη με καλή αναγωγή υπέρ το $\mathbb{Q}_p$. Έστω $P_0 \in C(\mathbb{Q}_p)$, J η Ιακωβιανή της C και $i : C \to J$ η εμφύτευση $P \mapsto [P - P_0]$. Τότε υπάρχει απεικόνιση*

$$J(\mathbb{Q}_p) \times \Omega_C^{\mathrm{reg}}(\mathbb{Q}_p) \to \mathbb{Q}_p, \ \ (P, \omega) \mapsto \langle P, \omega \rangle$$

η οποία είναι προσθετική στην πρώτη συντεταγμένη και $\mathbb{Q}_p$-γραμμική στην δεύτερη συντεταγμένη και $\langle [D], \omega \rangle = \int^D \omega$. Συγκεκριμένα, έχουμε

$$\langle i(P), \omega \rangle = \int_{P_0}^{P} \omega.$$

Απόδειξη. Από τα (1) και (3) του Θεωρήματος 5.2, παίρνουμε μια απεικόνιση

$$\mathrm{Div}^0(C(\bar{\mathbb{Q}}_p)) \times \Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p) \to \bar{\mathbb{Q}}_p, \ \ (D, \omega) \mapsto \int^D \omega$$

η οποία είναι προσθετική στο D και $\bar{\mathbb{Q}}_p$-γραμμική στο ω. Αφού $\int^D \omega = 0$ για κάθε $\omega \in \Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p)$ όταν ο D είναι κύριος διαιρέτης, λαμβάνουμε μια απεικόνιση

$$\alpha : \mathrm{Div}^0(C(\bar{\mathbb{Q}}_p))/\mathrm{Princ}(\bar{\mathbb{Q}}_p) = J(\bar{\mathbb{Q}}_p) \times \Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p) \to \bar{\mathbb{Q}}_p \ \text{ με } \ \alpha([D], \omega) = \int^{[D]} \omega.$$

Όμως,

$$\begin{aligned} \sigma(\alpha([D], \omega)) &= \sigma(\int^D \omega) \\ &= \sigma\left(\int^D \omega\right) \\ &= \int^D \omega \ \text{ (λόγω της συμβατότητας της } \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)) \\ &= \alpha([D], \omega). \end{aligned}$$

Δηλαδή, η εικόνα οποιουδήποτε στοιχείου μέσω του α παραμένει αναλλοίωτο από κάθε στοιχείο $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, που σημαίνει ότι ανήκει στο $\mathbb{Q}_p$. Επομένως, λαμβάνουμε μία απεικόνιση

$$J(\mathbb{Q}_p) \times \Omega_C^{\mathrm{reg}}(\mathbb{Q}_p) \to \mathbb{Q}_p, \ \ ([D], \omega) \mapsto \int^D \omega.$$

Τέλος,

$$\langle i(P), \omega \rangle = \langle [P - P_0], \omega \rangle = \int^{P - P_0} \omega = \int_{P_0}^{P} \omega.$$

■

5.5 Σημείωση. Αν το $P \in J(\mathbb{Q}_p)$ έχει πεπερασμένη τάξη, έστω $n \in \mathbb{N}$, τότε $nP = 0$, οπότε για κάθε $\omega \in \Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p)$ έχουμε

$$\langle P, \omega \rangle = \langle \frac{1}{n} nP, \omega \rangle = \frac{1}{n} \langle 0, \omega \rangle = 0.$$

Αποδεικνύεται ότι αυτήν την ιδιότητα την έχουν μόνο τα σημεία πεπερασμένης τάξης:

5.6 Πρόταση. *Αν το $P \in J(\mathbb{Q}_p)$ έχει πεπερασμένη τάξη, τότε $\langle P, \omega \rangle = 0$ για κάθε $\omega \in \Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p)$ και τα σημεία πεπερασμένης τάξης είναι τα μοναδικά με αυτή την ιδιότητα. Από την άλλη, αν για το ω ισχύει ότι $\langle P, \omega \rangle = 0$ για κάθε $P \in J(\mathbb{Q}_p)$, τότε $\omega = 0$. Αν για το $\omega \in \Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p)$ ισχύει ότι $\langle P, \omega \rangle = 0$ για κάθε $P \in J(\mathbb{Q}_p)$ τότε $\omega = 0$.*

Απόδειξη. βλ. [4, Πρόταση 5.1]. ■

5.7 Πόρισμα. ***(Chabauty).*** *Έστω C μια ομαλή, προβολική και απολύτως ανάγωγη καμπύλη γένους g υπέρ το $\mathbb{Q}$ με Ιακωβιανή J. Υποθέτουμε ότι ο βαθμός (rank) r της Mordell-Weil ομάδας $J(\mathbb{Q})$ είναι γνήσια μικρότερο του g. Τότε το $C(\mathbb{Q})$ είναι πεπερασμένο.*

Απόδειξη. Έστω $p \in \mathbb{P}$ στον οποίο η C έχει καλή αναγωγή. Θέτουμε

$$V = \{\omega \in \Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p) : \langle P, \omega \rangle = 0 \text{ για κάθε } P \in J(\mathbb{Q})\}.$$

Η συνθήκη $\langle P, \omega \rangle = 0$ είναι αληθής για κάθε $P \in J(\mathbb{Q})_{\mathrm{tors}}$. Για τα σημεία του ελεύθερου μέρους της Ιακωβιανής, αρκεί η συνθήκη να ισχύει για τα στοιχεία μιας βάσης της (λόγω της προσθετικότητας της πρώτης συντεταγμένης), έστω $P_1, ..., P_r$. Μεταξύ των $P_1, ..., P_r$ έχουμε το πολύ r γραμμικές σχέσεις. Επειδή $\dim(\Omega_C^{\mathrm{reg}}(\bar{\mathbb{Q}}_p)) = g$, $\dim(V) \geq g - r$ και από την υπόθεση $g > r$, παίρνουμε ότι $\dim(V) > 0$. Άρα το σύνολο V περιέχει μη μηδενικό στοιχείο, έστω ω.

Αν $C(\mathbb{Q}) = \emptyset$ τελειώσαμε.

Αν $C(\mathbb{Q}) \neq \emptyset$, παίρνουμε ένα $P_0 \in C(\mathbb{Q})$ και θεωρούμε την εμφύτευση $i : C \to J$. Αφού $i(P) \in J(\mathbb{Q})$ για κάθε $P \in C(\mathbb{Q})$, έπεται ότι $\langle [P - P_0], \omega \rangle = 0$ για κάθε $P \in C(\mathbb{Q})$, δηλαδή $\int_{P_0}^{P} \omega = 0$ για κάθε $P \in C(\mathbb{Q})$. Από το (6) του Θεωρήματος 5.2, το πλήθος του συνόλου των P με αυτή την ιδιότητα είναι πεπερασμένο σε κάθε «κλάση υπολοίπων» του $C(\mathbb{Q}_p)$ (με τον όρο κλάση υπολοίπων εννοούμε ένα σύνολο σημείων που ανάγονται στο ίδιο σημείο του $C(\mathbb{F}_p)$). Το σύνολο των κλάσεων αυτών είναι πεπερασμένο, άρα και το πλήθος των ρητών σημείων της C είναι και αυτό πεπερασμένο. ■

§3 Άνω φράγμα για το $|C(\mathbb{Q})|$

Σε αυτήν την παράγραφο, θα βρούμε ένα άνω φράγμα για το $|C(\mathbb{Q})|$. Για να το επιτύχουμε, θα χρειαστεί να φράξουμε το πλήθος των σημείων μηδενισμού στο $\mathbb{Z}_p$ μιας δυναμοσειράς με συντελεστές στο $\mathbb{Q}_p$.

5.8 Λήμμα. *Έστω $l(t) \in \mathbb{Q}_p[\![t]\!]$ με τυπική παράγωγο $w(t) \in \mathbb{Z}_p[\![t]\!]$ τέτοια ώστε η εικόνα $\bar{w}(t) \in \mathbb{F}_p[\![t]\!]$ να έχει τη μορφή $ut^\nu + ...$ με $u \in \mathbb{F}_p^*$. Τότε η l συγκλίνει στο $p\mathbb{Z}_p$. Αν $p > \nu + 2$ τότε*

$$|\{\tau \in p\mathbb{Z}_p : l(\tau) = 0\}| \leq \nu + 1.$$

Απόδειξη. [37, σελ. 43]. ■

5.9 Θεώρημα. ***(Coleman.)*** *Έστω C μία ομαλή, προβολική και απολύτως ανάγωγη καμπύλη γένους g υπέρ το $\mathbb{Q}$ με Ιακωβιανή J. Υποθέτουμε ότι το rank r της Mordell-Weil ομάδας $J(\mathbb{Q})$ είναι γνήσια μικρότερο του g. Έστω $p \in \mathbb{P}$ τέτοιος ώστε η C να έχει καλή αναγωγή με $p > 2g$. Τότε*

$$|C(\mathbb{Q})| \leq |\bar{C}(\mathbb{F}_p)| + 2g - 2.$$

Απόδειξη. Αν $C(\mathbb{Q}) = \emptyset$, η ανισότητα είναι προφανής. Έστω λοιπόν $P_0 \in C(\mathbb{Q})$. Όπως στην απόδειξη του Πορίσματος 5.7, υπάρχει μη μηδενικό $\omega \in \Omega_C^{\mathrm{reg}}(\mathbb{Q}_p)$ τέτοιο ώστε $\int_{P_0}^{P} \omega = 0$ για κάθε $P \in C(\mathbb{Q})$. Έστω $\bar{Q} \in \bar{C}(\mathbb{F}_p)$ και $Q \in C(\mathbb{Q}_p)$ η ανύψωσή του. Επιλέγουμε έναν uniformizer $t \in \mathbb{Q}_p(C)^*$ στο $\mathbb{Q}$ τέτοιο ώστε το t να ανάγεται σε uniformizer $\bar{t} \in \mathbb{F}_p(\bar{C})^*$ στο $\bar{Q}$ (π.χ. αν η C είναι υπερελλειπτική και $\bar{Q} = (\bar{x}, \bar{y})$ τότε παίρνουμε $Q = (x, y)$ και $t = X - x$ αν $\bar{x} \neq 0$ και $Q = (x, 0)$ και $t = Y$ αν $\bar{y} = 0$). Μπορούμε να κλιμακώσουμε το ω έτσι ώστε η αναγωγή του $\bar{\omega}$ να ορίζεται και να είναι μη μηδενική. Τότε $\bar{\omega} \in \Omega_C^{\mathrm{reg}}(\mathbb{F}_p)$. Υπενθυμίζουμε ότι ο διαιρέτης $\mathrm{div}(\bar{\omega})$ είναι effective και έχει βαθμό $2g-2$. Γράφουμε $\omega = w(t)dt$ όπου $w(t) \in \mathbb{Z}_p[\![t]\!]$ (οι συντελεστές είναι στο $\mathbb{Z}_p$ επειδή το $\bar{\omega}$ ορίζεται). Τότε $\bar{\omega} = \bar{w}(\bar{t})d\bar{t}$ όπου $\bar{w}(\bar{t}) = t^{v_{\bar{Q}}(\bar{\omega})}(u_0 + u_1\bar{t} + ...)$ με $u_0 \in \mathbb{F}_p^*$. Από το (6) του Θεωρήματος 5.2, $\int_{P_0}^{P} \omega = l(t(P))$ για κάθε $P \in C(\mathbb{Q}_p)$ με $\bar{P} = \bar{Q}$, όπου $l(t) \in \mathbb{Q}_p[\![t]\!]$ με $l'(t) = w(t)$. Τα σημεία μηδενισμού της l είναι τα σημεία $P \in C(\mathbb{Q}_p)$ που ανάγονται στο $\bar{Q}$ και ικανοποιούν την $\int_{P_0}^{P} \omega = 0$, τα οποία είναι το πολύ $v_{\bar{Q}}(\bar{\omega}) + 1$, από το Λήμμα 5.8. Άρα

$$\begin{aligned}
|C(\mathbb{Q})| &\leq |\{P \in C(\mathbb{Q}_p) : \int_{P_0}^{P} \omega = 0\}| \\
&\leq \sum_{\bar{Q} \in \bar{C}(\mathbb{F}_p)} (v_{\bar{Q}}(\bar{\omega}) + 1) \\
&= \sum_{\bar{Q} \in \bar{C}(\mathbb{F}_p)} v_{\bar{Q}}(\bar{\omega}) + \sum_{\bar{Q} \in \bar{C}(\mathbb{F}_p)} 1 \\
&\leq \deg(\mathrm{div}(\bar{\omega})) + |\bar{C}(\mathbb{F}_p)| \\
&= 2g - 2 + |\bar{C}(\mathbb{F}_p)|.
\end{aligned}$$

■

5.10 Παράδειγμα. Θεωρούμε την καμπύλη

$$C : Y^2 = X(X-1)(X-2)(X-5)(X-6)$$

υπέρ το $\mathbb{Q}$. Στο Παράδειγμα 4.14 είχαμε δεί ότι η $J(\mathbb{Q})$ έχει rank 1 που είναι μικρότερο του $g = 2$. Πάνω στην καμπύλη βρίσκουμε τα ρητά σημεία

$$(0,0), (1,0), (2,0), (5,0), (6,0), (3,-6), (3,-6), (10,-120) \text{ και } (10,120),$$

οπότε μαζί με το επ'άπειρον σημείο έχουμε 10 ρητά σημεία, άρα $|C(\mathbb{Q})| \geq 10$.

Η C έχει καλή αναγωγή στον πρώτο $p = 7$. Εύκολα βρίσκουμε ότι

$$\bar{C}(\mathbb{F}_7) = \{\infty, (0,0), (1,0), (2,0), (3,-1), (3,1), (5,0), (6,0)\},$$

άρα $|\bar{C}(\mathbb{F}_7)| = 8$. Από το Θεώρημα 5.9,

$$|C(\mathbb{Q})| \leq |\bar{C}(\mathbb{F}_p)| + 2g - 2 = 8 + 4 - 2 = 10.$$

Συνεπώς $|C(\mathbb{Q})| = 10$ και

$$C(\mathbb{Q}) = \{\infty, (0,0), (1,0), (2,0), (5,0), (6,0), (3,-6), (3,-6), (10,-120), (10,120)\}.$$

□

Επίλογος

Το παράδειγμά μας αποδείχθηκε για πρώτη φορά από τον David Grand στο [14]. Σε προηγούμενή τους εργασία, οι D. Gordon και D. Grant ([13]) είχαν αποδείξει ότι η Ιακωβιανή της συγκεκριμένης καμπύλης είναι

$$J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}.$$

Την 2-κάθοδο του Selmer εφάρμοσε και η Jaclyn Lang στο [19] για την υπερελλειπτική καμπύλη

$$Y^2 = X(X-3)(X-4)(X-6)(X-7).$$

Ο Jan Steffen Müller στο [23], μελετά, εντελώς ανάλογα την καμπύλη

$$Y^2 = f(X) = X(X-2)(X+2)(X+3)(X+7).$$

Εφαρμόζει τη μέθοδο της 2-καθόδου για την ομάδα του Selmer και υπολογίζει τον βαθμό (rank) αυτής. Επειδή ο rank είναι 2 και το γένος της καμπύλης είναι δύο, δεν μπορούμε να εφαρμόσουμε τη μέθοδο του Chabauty.

Το Παράδειγμα 4.33 της εργασίας, στο οποίο απαιτείται γνώση τόσο αλγεβρικής θεωρίας αριθμών όσο και θεωρίας τοπικών σωμάτων είναι του Michael Stoll, στο [37]. Ανάλογο παράδειγμα διαπραγματεύεται και ο C.D. Lazda στο [20]. Πρόκειται για την υπερελλειπτική καμπύλη

$$Y^2 = (X^2-5)(X^3+10)$$

της οποίας με χρήση της 2-καθόδου του Selmer υπολογίζει τον βαθμό (rank) της Ιακωβιανής, ο οποίος στο συγκεκριμένο παράδειγμα είναι 1.

Οι E. V. Flynn, Bjorn Poonen και Edward F. Schaefer στο [9], αποδεικνύουν ότι τα ρητά σημεία της υπερελλειπτικής καμπύλης

$$Y^2 = X^6 + 8X^5 + 22X^4 + 22X^3 + 5X^2 + 6X + 1$$

υπέρ το $\mathbb{Q}$ είναι ακριβώς τα (0,1),(0,-1),(-3,1),(-3,-1) (και τα επ΄άπειρον σημεία).

Τέλος, ο J. L. Wetherell στο [41] παίρνει ως κίνητρο το πρόβλημα 17 του έκτου βιβλίου του Διόφαντου (βλ. [32, σελ. 149 και σελ. 255]). Από την εξίσωση αυτή προκύπτει η υπερελλειπτική καμπύλη υπέρ το $\mathbb{Q}$, $Y^2 = X^6 + X^2 + 1$. Ο Διόφαντος

υπολογίζει ότι η εξίσωση έχει μοναδική θετική λύση την $\left(\frac{1}{2}, \frac{9}{8}\right)$. Επισυνάπτουμε τα σχετικά αποσπάσματα από το βιβλίο [32], σελ. 149 και σελ. 255.

---

17. We wish to find three square numbers which, when added, give a square, and such that the first of these (three square) numbers equals the side of the second, and the second equals the side of the third.

150 Part Two Translation

Let us put x^2 as the first, so that the second is x^4—for x^4 is the square of x^2, and x^2 is equal to the side of the second—, and the third is x^8, —which equals the square of the second, and the second is its side.[24] The three numbers, when added, give $x^8 + x^4 + x^2$, and this has to be a square number. Let us put as its side $x^4 + \frac{1}{2}$; this when multiplied by itself gives $x^8 + x^4 + \frac{1}{4}$, which is equal to $x^8 + x^4 + x^2$. We remove the identical common (terms); so x^2 is equal to $\frac{1}{4}$. We had put x^2 as the first of the three numbers, so it is $\frac{1}{4}$. This $\frac{1}{4}$ is equal to the side of the second, (so) the second is $\frac{1}{2} \cdot \frac{1}{8}$. Again, the second equals the side of the third, (so) the third is one part of 256 parts of 1. These three numbers, when added, give 81 parts of 256 parts of the unit, which is a square number with side 9 parts of 16.

Therefore, we have found three numbers fulfilling the condition imposed upon us, and these are $\frac{1}{4}, \frac{1}{2} \cdot \frac{1}{8}$, (and) one part of 256 parts of 1. This is what we intended to find.

Problem VI,17.

$$\begin{cases} a^2 + b^2 + c^2 = \square, \\ a^2 = b, \\ b^2 = c. \end{cases}$$

The magnitude to be raised to the highest exponent, a, is taken as unknown x; hence

$$x^2 + x^4 + x^8 = \square.$$

Putting $$\square = (x^4 + \tfrac{1}{2})^2 = x^8 + x^4 + \tfrac{1}{4},$$

we have immediately $$x^2 = \tfrac{1}{4}.$$

So $a^2 = x^2 = \frac{1}{4}$, $b^2 = (\frac{1}{4})^2 = \frac{1}{16}$, $c^2 = (\frac{1}{16})^2 = \frac{1}{256}$, $\square = \frac{81}{256} = (\frac{9}{16})^2$.

Εντελώς φυσιολογικά τίθεται το ερώτημα αν αυτή η υπερελλειπτική καμπύλη έχει άλλα ρητά σημεία. Η απάντηση δόθηκε από τον J. L. Wetherell. Εδώ η υπερελλειπτική καμπύλη έχει γένος 2 αλλά και ο βαθμός (rank) της Ιακωβιανής είναι 2. Συνεπώς δεν μπορούμε να εφαρμόσουμε (τουλάχιστον απευθείας) την μέθοδο του Chabauty.

Ο Wetherell συνδύασε τη μέθοδο του Chabauty με άλλες μεθόδους και κατάφερε να αποδείξει ότι η μοναδική θετική ρητή λύση είναι η λύση του Διόφαντου.

Φυσιολογικά, τίθεται το ερώτημα αν το φράγμα του Coleman του Θεωρήματος 5.9 είναι το καλύτερο δυνατό. Υπό τις προϋποθέσεις του Θεωρήματος 5.9, η απάντηση είναι θετική (βλ. Παράδειγμα 5.10). Τα παρακάτω θεωρήματα που οφείλονται στον Michael Stoll, δίνουν άνω φράγμα για το $C(\mathbb{Q})$ το οποίο εμπλέκει μόνο το γένος της καμπύλης και τον βαθμό της Ιακωβιανής.

Θεώρημα. Αν C υπερελλειπτική καμπύλη ορισμένη υπέρ το $\mathbb{Q}$ με γένος g και Mordell-Weil rank $r \leq g-3$ τότε

$$C(\mathbb{Q}) \leq 8(r+4)(g-1) + \max\{1, 4r\}g.$$

Το παραπάνω φράγμα, βελτιώθηκε τον Ιούλιο του 2019 από τον ίδιο (βλ. [39]):

Θεώρημα. Έστω C υπερελλειπτική καμπύλη γένους g υπέρ το $\mathbb{Q}$ με Ιακωβιανή J. Υποθέτουμε ότι ο βαθμός r της Ιακωβιανής ικανοποιεί την $r \leq g-3$. Τότε

$$|C(\mathbb{Q})| \leq 33(g-1) + \max\{1, 8rg-1\}.$$

Σχετικά με φράγματα του βαθμού (rank) της Ιακωβιανής μιας υπερελλειπτικής καμπύλης, παραπέμπουμε στη μεταπτυχιακή εργασία [8].

Τελικά, τι μπορεί να πάει στραβά στην προσέγγισή μας για την εύρεση των ρητών σημείων μιας καμπύλης; Υπάρχουν διάφορα σημεία στα οποία η προσέγγισή μας μπορεί να αποτύχει:

1. Είναι αδύνατο να υπολογίσουμε ένα άνω φράγμα για τον βαθμό r. Ο λόγος μπορεί να είναι ότι οι υπολογισμού της 2-ομάδας του Selmer είναι ακατόρθωτοι.

2. Βρίσκουμε πολύ λίγα ανεξάρτητα σημεία της Ιακωβιανής ώστε να πλησιάσουμε το άνω φράγμα. Δύο από τις πιθανές αιτίες είναι είτε επειδή το άνω φράγμα είναι μεγάλο είτε το ότι υπάρχουν σημεία με πολύ μεγάλες συντεταγμένες.

3. Ισχύει $r \geq g$.

Στις περιπτώσεις (1),(2) και στην υποπερίπτωση $r = g$ του (3), μπορούμε να τα καταφέρουμε ίσως με άλλες μεθόδους. Αν $r > g$, η κατάσταση γίνεται αρκετά πολύπλοκη.

Παράρτημα: SAGE

Σε αυτό το παράρτημα περιλαμβάνουμε μια σειρά από συναρτήσεις στο SAGE, κατασκευασμένες από την Jaclyn Lang όπως παρατίθενται στην εργασία [19, σελ. 32] της ίδιας, με ελάχιστες τροποποιήσεις. Είναι πολύ χρήσιμες για την περάτωση των υπολογισμών που γίνονται στα παραδείγματα των κεφαλαίων III και IV.

conj: Δέχεται ως είσοδο μία τετραγωνική επέκταση K του $\mathbb{F}_p$ για κάποιον πρώτο p και ένα στοιχείο $x \in K$. Αν επιλέξουμε μια βάση $\{1, \alpha\}$ για την επέκταση $K/\mathbb{F}_p$ και γράψουμε $x = a + b\alpha$, η συνάρτηση conj επιστρέφει το συζυγές στοιχείο του x, δηλαδή το $a + b\sigma(\alpha)$ όπου σ ο αυτομορφισμός του Frobenius.

```
def conj(x,K):
    p=K.characteristic()
    for i in GF(p):
        if x−i∗(K.gen()) in GF(p):
            b=i
            a=x−i∗(K.gen())
    return a+b∗(K.gen()^p)
```

cp_multiplication: Δέχεται ως είσοδο δύο n-άδες a, b στοιχείων της πολλαπλασιαστικής ομάδας $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ (σε μορφή λίστας) και επιστρέφει την n-άδα $a \cdot b$ όπου κάθε εγγραφή λαμβάνεται $\bmod (\mathbb{Q}^*)^2$. Καλεί την συνάρτηση **square_free_part**.

```
def cp_multiplication(a,b):
    P=[]
    for j in range(len(a)):
        P.append(square_free_part(a[j]∗b[j]))
    return P
```

cp_product: Δέχεται ως είσοδο μία λίστα με πεπερασμένο αριθμό στοιχείων της ομάδας και επιστρέφει $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^n$ το γινόμενό τους με τις εγγραφές να είναι $\bmod (\mathbb{Q}^*)^2$. Καλεί τη συνάρτηση **cp_multiplication**.

```
def cp_product(list):
    p=[]
    for i in list [0]:
```

```
        p.append(1)
    for i in range(len(list)):
        p=cp_multiplication(p,list[i])
    return p
```

cp_span: Δέχεται ως είσοδο μία λίστα με στοιχεία της ομάδας $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^n$ και επιστρέφει την υποομάδα που παράγουν (υπέρ το $\mathbb{F}_2$). Καλεί την συνάρτηση του SAGE **Combinations()** καθώς και την **cp_product**. Αφού όλα τα στοιχεία της $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^n$ έχουν τάξη 2, η υποομάδα που παράγεται από μία λίστα στοιχείων της, λαμβάνεται πολλαπλασιάζοντας όλους τους δυνατούς συνδυασμούς των γεννητόρων χωρίς πολλαπλότητα. Η εντολή **len(cp_span())** επιστρέφει το πλήθος της υποομάδας.

```
def cp_span(gens):
    L=[]
    for i in range(1,len(gens)+1):
        M=Combinations(gens,i)
        if M==[[]]:
            for j in gens[0]:
                M[0].append(1)
            M=[M]

        for j in M:
            if cp_product(j) not in L:
                L.append(cp_product(j))
    if cp_product([gens[0],gens[0]]) not in L:
        L.append(cp_product([gens[0],gens[0]]) )
    return L
```

find_new_gens: Δέχεται ως είσοδο ένα πολυώνυμο F, τέσσερις ρίζες a_1, a_2, a_3, a_4, έναν πρώτο αριθμό p, δύο φυσικούς αριθμούς i και n, μία λίστα reps που περιέχει ένα πλήρες σύστημα αντιπροσώπων της ομάδας $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ και μία λίστα gen_knowns, που περιέχει τους γνωστούς γεννήτορες της $J(\mathbb{Q}_p)[2]$. Η συνάρτηση υπολογίζει την υποομάδα που παράγεται από τις εικόνες μέσω της δ_p των γνωστών ρητών σημείων. Έπειτα, καλεί τη συνάρτηση **find_possibilities** και υπολογίζει τις εικόνες των σημείων της λίστας που επιστρέφει μέσω της δ_p. Αν η εικόνα αυτή δεν ανήκει στην υποομάδα που παράγεται από τα γνωστά ρητά σημεία, προσθέτει έναν νέο πιθανό γεννήτορα στην λίστα. Επιστρέφει μία λίστα στοιχείων της $\mathrm{Im}(\delta_p)$ που δεν ανήκουν στην υποομάδα που παράγουν οι εικόνες των γνωστών ρητών σημείων. Πέρα από την **find_possibilities**, καλεί τις **cp_span** και **Q_p_mod_squares**.

```
def find_new_gens(F,a1,a2,a3,a4,p,i,reps,n,gen_knowns):
    known_elements=cp_span(gen_knowns)
    new_gens=[]
    for x in  find_possibilities (F,p,i):
```

```
        x=ZZ(x)
        ex_bar=[Q_p_mod_squares(x−a1, p, reps, n),
            Q_p_mod_squares(x−a2, p, reps, n),
            Q_p_mod_squares(x−a3, p, reps, n),
            Q_p_mod_squares(x−a4, p, reps, n)]
        if not ex_bar in known_elements and not x in new_gens:
            if 0 not in ex_bar:
                new_gens.append(x)
    return new_gens
```

find_possibilities: Η συνάρτηση δέχεται ως είσοδο ένα πολυώνυμο F, έναν πρώτο p και έναν φυσικό αριθμό i. Επιστρέφει μία λίστα με στοιχεία x έτσι ώστε το (x, y) να είναι σημείο της καμπύλης $Y^2 = F(X)$ με $x, y \in \mathbb{Q}_p$. Εξετάζει όλα τα στοιχεία του $\mathbb{Z}/p^i\mathbb{Z}$. Καλεί τις συναρτήσεις **squares_mod_with_roots, squares_mod**, **val**, καθώς και την συνάρτηση Integers(x) του SAGE

```
def find_possibilities (F,p,i):
    possibilities =[]
    for x in Integers(p^i):
        if (F(x)%(p^i)) in squares_mod(p^i):
            x=ZZ(x)
            for y in squares_mod_with_roots(p^i):
                if y[0]==(F(x)%(p^i)):
                    if y[1]^2−F(x)==0 and not x in possibilities:
                        if not y[1]==0:
                            possibilities .append(x)

                    if not y[1]^2−F(x)==0 and x not in possibilities:
                        if not y[1]==0:
                            if val(y[1]^2−F(x),p)>2*val(2*y[1],p):
                                possibilities .append(x)
    return possibilities
```

intersect: Δέχεται ως είσοδο δύο λίστες X, Y που αναπαριστούν σύνολα. Επιστρέφει το σύνολο $X \cap Y$ σε μορφή λίστας. Προφανώς, δεν έχει σημασία η σειρά που δίνονται τα X και Y στη συνάρτηση.

```
def intersect (X,Y):
    intersection =[]
    for x in X:
        if x in Y:
            intersection .append(x)
    return intersection
```

J(L,F): Δέχεται ως είσοδο τη μοναδική επέκταση L βαθμού 2 του $\mathbb{F}_p$ για κάποιον $p \in \mathbb{P}$

και το πολυώνυμο $F(x)$ βαθμού 5 μιας υπερελλειπτικής καμπύλης $C : Y^2 = F(X)$. Επιστρέφει μία λίστα με τα σημεία της $J(\mathbb{F}_p)$. Η εντολή **len(J(L,F)):** δίνει το πλήθος του συνόλου.

```
def J(L,F):
    p=L.characteristic()
    elements=['O']
    for x in points_in(GF(p),F):
        elements.append([x,'infty'])
    for x in points_in(GF(p),F):
        for y in points_in(GF(p),F):
            if not x[0]==y[0] and [y,x] not in elements:
                elements.append([x,y])
            if x[0]==y[0] and not x[1]==-y[1]:
                if not [y,x] in elements:
                    elements.append([x,y])
    for x in points_not_in_ground_field (L,F):
        for y in points_not_in_ground_field (L,F):
            if not x[0]==conj(x[0],L):
                if conj(x[0],L)==y[0] and conj(x[1],L)==y[1]:
                    if [y,x] not in elements:
                        elements.append([x,y])
    return elements
```

multi_intersect: Δέχεται ως είσοδο μία λίστα με λίστες, όπου κάθε εσωτερική λίστα αντιπροσωπεύει ένα σύνολο. Επιστρέφει μία λίστα που περιέχει την συνολοθεωρητική τομή των συνόλων. Καλεί τη συνάρτηση **intersect**.

```
def multi_intersect(list):
    set=list[0]
    for j in range(len(list)):
        set=intersect(set, list[j])
    return set
```

points_in: Δέχεται ως είσοδο ένα σώμα K και ένα πολυώνυμο F. Στην περίπτωσή μας, το $F(X)$ είναι το πολυώνυμο που ορίζει την υπερελλειπτική καμπύλη $C : Y^2 = F(X)$. Επιστρέφει μία λίστα με τα σημεία (x, y) της C όπου $x, y \in K$. Δεν περιλαμβάνει τα επ΄άπειρον σημεία. Για κάθε στοιχείο $i \in K$, ελέγχει αν το $F(i)$ είναι τέλειο τετράγωνο μέσω της συνάρτησης **squares**. Έπειτα, προσθέτει στη λίστα τα σημεία $(x, y) = (i, \sqrt{F(i)})$ και $(x, -y) = (i, -\sqrt{F(i)})$. Χρησιμοποιώντας την εντολή **len(points_in(K,F))** βρίσκουμε πόσα ρητά σημεία έχει η καμπύλη, εξαιρώντας τα επ΄άπειρον σημεία.

```
def points_in(K,F):
    points=[]
    for i in K:
```

```
        if K(F(i)) in squares(K) and [i, sqrt(F(i))] not in points:
            points.append([i, sqrt(F(i))])
            if not sqrt(F(i))==0:
                points.append([i, -sqrt(F(i))])
    return points
```

points_not_in_ground_field: Δέχεται ως είσοδο ένα σώμα K θετικής χαρακτηριστικής και ένα πολυώνυμο F, όπως στη συνάρτηση **points_in**. Επιστρέφει όλα τα σημεία (x, y) της καμπύλης με $x, y \in K$ αλλά όχι και τα δύο να βρίσκονται στο πρώτο υπόσωμα. Χρησιμοποιεί τη συνάρτηση **characteristic()** του SAGE για να καθορίσει τη χαρακτηριστική του K και επίσης καλεί τη συνάρτηση **points_in**.

```
def points_not_in_ground_field(K,F):
    p=K.characteristic()
    v=[]
    for x in points_in(K,F):
        if x[0] not in GF(p) or x[1] not in GF(p):
            v.append(x)
    return v
```

Δέχεται ως είσοδο έναν μη μηδενικό ρητό αριθμό x και επιστρέφει τη λίστα με τους πρώτους αριθμούς στους οποίους ο x έχει μη μηδενική p-αδική εκτίμηση. Χρησιμοποιεί τη συνάρτηση **factor** του SAGE.

```
def prime_divisors(x):
    primes=[]
    F=factor(x)
    for i in F:
        primes.append(i[0])
    return primes
```

Q_p_mod_squares: Δέχεται ως είσοδο τέσσερις τιμές: έναν ρητό αριθμό x, έναν πρώτο αριθμό p, μία λίστα από αντιπροσώπους της ομάδας $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ και έναν θετικό ακέραιο n. Χρησιμοποιεί το Λήμμα του Hensel για να βρεί τον αντιπρόσωπο από την λίστα του συμμπλόκου που περιέχει τον x στην $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. Η συνάρτηση ψάχνει μέχρι την δύναμη p^n. Παίρνοντας το n αρκετά μεγάλο, πάντα θα βρίσκουμε τον επιθυμητό αντιπρόσωπο. Αν $x = 0$, η συνάρτηση επιστρέφει το 0. Καλεί τις συναρτήσεις **squares_mod_with_roots** και **val**. Η ιδέα είναι ότι το x βρίσκεται σε ακριβώς ένα σύμπλοκο της ομάδας $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. Αφού κάθε σύμπλοκο έχει τάξη 2, το γινόμενο $x \cdot j$ για έναν αντιπρόσωπο j από τη λίστα των αντιπροσώπων, θα είναι τετράγωνο στο $\mathbb{Q}_p$ αν και μόνο αν τα x και j είναι στο ίδιο σύμπλοκο. Η συνάρτηση διατρέχει όλα τα δυνατά γινόμενα $x \cdot j$ και χρησιμοποιεί το κριτήριο του Λήμματος του Hensel για να καθορίσει το πότε έχει βρεθεί ο κατάλληλος αντιπρόσωπος.

```
def Q_p_mod_squares(x, p, reps, n):
    for i in range(1,n+1):
        for j in reps:
            if ((x*j)%(p^i)) in squares_mod(p^i):
                for y in squares_mod_with_roots(p^i):
                    if y[0]==((x*j)%(p^i)) and not y[1]==0:
                        if y[1]^2-x*j==0:
                            return j
                            break
                        if val(y[1]^2-x*j, p) > 2*val(2*y[1],p):
                            return j
                            break
    return 0
```

same_set: Δέχεται ως είσοδο δύο λίστες X και Y που αντιπροσωπεύουν σύνολα και επιστρέφει «True» αν $X = Y$ ως σύνολα και «False» αλλιώς. Καλεί τη συνάρτηση **multi_intersect**.

```
def same_set(X,Y):
    for x in X:
        if not x in Y:
            return False
            break
    for y in Y:
        if not y in X:
            return False
            break
    return True
```

square_free_part: Δέχεται ως είσοδο έναν ρητό αριθμό x και επιστρέφει τον ελεύθερο τετραγώνου αντιπρόσωπό του στην ομάδα $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Καλεί τη συνάρτηση **factor()** του SAGE, η οποία επιστρέφει μία λίστα με tuples της μορφής (p, e) όπου $p \in \mathbb{P}$ και $e \in \mathbb{Z}$ η p-αδική εκτίμηση του x και αποθηκεύει το πρόσημο του x ως **factor(x).unit()**.

```
def square_free_part (x):
    F=factor(x)
    u=F.unit()
    for i in F:
        if i[1]%2==1:
            u=u*i[0]
    return u
```

squares: Δέχεται ως είσοδο ένα πεπερασμένο σώμα K και επιστρέφει μία λίστα με

τα στοιχεία που είναι τέλεια τετράγωνα. Ελέγχει αν ένα στοιχείο του K είναι τέλειο τετράγωνο μέσω της συνάρτησης του SAGE **is_square**.

```
def squares(K):
    squares=[]
    for a in K:
        if a.is_square():
            squares.append(a)
    return squares
```

squares_mod: Δέχεται ως είσοδο έναν φυσικό αριθμό n και επιστρέφει τα τετράγωνα mod n. Είναι παρόμοια με την **squares**, αλλά δεν απαιτεί να εργαζόμαστε πάνω από σώμα.

```
def squares_mod(n):
    v=[]
    for i in range(n):
        if i^2%n not in v:
            v.append(i^2%n)
    return v
```

squares_mod_with_roots: Δέχεται ως είσοδο έναν φυσικό αριθμό n και επιστρέφει μία λίστα με ζεύγη, όπου η πρώτη συντεταγμένη είναι τετράγωνο mod n και η δεύτερη είναι μια τετραγωνική ρίζα της πρώτης, mod n. Κάθε δυνατό τέτοιο ζεύγος εμφανίζεται μόνο μία φορά στη λίστα.

```
def squares_mod_with_roots(n):
    v=[]
    for i in range(n):
        v.append([i^2%n, i])
    return v
```

val: Δέχεται ως είσοδο έναν μη μηδενικό ρητό αριθμό x και έναν πρώτο αριθμό p. Επιστρέφει την p-αδική εκτίμηση του x. Καλεί τη συνάρτηση **prime_divisors**.

```
def val(x, p):
    v=0
    while p in prime_divisors(x):
        v=v+1
        x=ZZ(x/p)
    return v
```

Βιβλιογραφία

[1] George Bachman, *Introduction to p-adic numbers and valuation theory*, Academic Paperbacks, New York, 1964.

[2] David G. Cantor, *Computing in the Jaobian of a Hyperelliptic Curve*, Math. Comp., **48**(1987)95-101.

[3] J.W.S Cassels, *Local Fields*, Cambridge University Press, Cambridge, 1986.

[4] Robert F. Coleman, *Torsion Points on Curves and p-adic Abelian Integrals*, Ann. Math, v. 121, pp. 111-168, 1985.

[5] Keith Conrad, *Hensel's Lemma*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf

[6] Gabriel Daniel, Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Birkhäuser, Boston, 2008.

[7] Giulio Di Piazza, *Arithmetic on Jacobians of algebraic curves*, Master Thesis, Université Bordeaux 1, Università degli Studi di Padova, 2012-13

[8] Gürka Dogen, *Rank bounds of some hyperelliptic Jacobians*, Master Thesis, Universität Regensburg, Universität Leiden, 2018.

[9] E.V. Flynn, Bjorn Poonen, Edward F. Schaeffer, *Cycles of Quadratic Polynomials and Rational Points on a genus 2-curve, Duke Mathematical Journal*, **90**(3)1997, 435-463.

[10] Gerhard Frey, *Elementare Zahlentheorie*, Vieweg Verlag, 1984.

[11] William Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, 2008, http://www.math.lsa.umich.edu/ wfulton/CurveBook.pdf

[12] Fernando Q. Gouvea, *p-adic Numbers, An Introduction*, Springer-Verlag, 1993.

[13] D. Gordon, D.Grant, *Computing the Mordel-Weil rank of Jacobians of curves of genus 2*, Trans. Amer. Math. Society, **337**(1993), 807-824.

[14] David Grant, *A curve for which Coleman's effective Chabauty bound is short*, Proc. Amer. Math. Society, **122**(1994), 317-319.

[15] Marc Hindry, Joseph H. Silverman, *Diophantine Geometry (An Introduction)*, Springer-Verlag, New York, 2000.

[16] Klaus Hulek, *Elementary Algebraic Geometry*, AMS, 2000.

[17] Svetlana Katok, *p-adic Analysis Compared with Real*, AMS, 2007.

[18] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, New York, 1977.

[19] Jaclyn Lang, *Two-Descent on the Jacobians of Hyperelliptic Curves*, Churchill College, 2010,
http://guests.mpim-bonn.mpg.de/jlang/partiiiessay.pdf

[20] Christopher D. Lazda, *2-Descent on the Jacobians of Hyperelliptic Curves*, University of Cambridge, 2010
https://staff.fnwi.uva.nl/c.d.lazda/resources/Preprints/Essay.pdf

[21] David Mumford, *Tata lectures on theta II*, Vol. 43, Progress in Mathematics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Boston, MA: Birkh¨auser Boston Inc., 1984, pp. xiv+272. isbn: 0-8176-3110-0

[22] Stefan Müller-Stach, Jens Piontkowski, *Elementare und algebraische Zahlentheorie, 2.Auflage*, Vieweg and Teubner, Berlin, 2011.

[23] Jan Steffen Müller, *Rational points on Jacobians of hypperelliptic curves*, Institut für Mathematik, Carl von Ossietzky Universität Oldenburg, 2014.

[24] Wladyslaw Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warsaw, 1973.

[25] Jürgen Neukirch, *Algebraic Number Theory*, Springer, Berlin, Heidelberg, 1999.

[26] Grace Orzech, Morris Orzech, *Plane Algebraic Curves*, Marcel Dekker, 1981.

[27] Daniel Perrin, *Algebraic Geometry (An Introduction)*, Springer-Verlag, London, 2008.

[28] Alexander Schmidt, *Einfürung in die algebraische Zahlentheorie*, Springer-Verlag, Berlin, 2007.

[29] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[30] Jean-Pierre Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.

[31] Samir Siksek, *Chabauty and the Mordell-Weil Sieve*, University of Warwick, 2014
https://homepages.warwick.ac.uk/staff/S.Siksek/papers/ohrid.pdf

[32] Jacques Sesiano, *Books IV to VII of Diophantus' Arithmetica*, Springer, New York, 1982

[33] Igor R. Shafarevich, Basic Algebraic Geometry, Springer-Verlag, Berlin, 1994

[34] Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, William Traves, *An Invitation to Algebraic Geometry*, Springer-Verlag, New York, 2000.

[35] Henning Stichtenoth, *Algebraic Function Fields and Codes*, Springer Verlag, Berlin, 1993.

[36] Michael Stoll, *Arithmetic of Hyperelliptic Curves*, Lecture Notes, University of Bayreuth, 2014.

[37] Michael Stoll, *Arithmetic of Hyperelliptic Curves*, Lecture Notes, University of Bayreuth, 2019.
http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2019/Skript-ArithHypCurves-pub-print.pdf

[38] Michael Stoll, *Algebraische Kurven*, Lecture Notes, 2001.

[39] Michael Stoll, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank*, J. Eur. Math. Soc., **21**, 923-956, 2019

[40] Robert J. Walker, *Algebraic Curves*, Springer-Verlag, New York, 1991.

[41] Joseph L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph. D. Thesis, University of California at Berkeley, 1997.

[42] Anthi Zervou, *Profinite Groups and Cohomology*, Master Thesis, University of Crete, 2017.