Το Τοπικό-Γενικό Αξίωμα

στη Θεωρία Αριθμών

Ευαγγελία Καρτσάκη

Επιβλέπων Καθηγητής:
Ιωάννης Α. Αντωνιάδης

Μεταπτυχιακή εργασία

Πανεπιστήμιο Κρήτης
Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών

Στους γονείς μου, Μανώλη και Νατάσα
και στην αδερφή μου Μαρία

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Ιωάννη Α. Αντωνιάδη, για τις γνώσεις που μου μετέδωσε αλλά και για τον χρόνο που αφιέρωσε ώστε να έχουμε ένα άρτιο αποτέλεσμα. Η βοήθειά του ήταν πραγματικά πολύτιμη. Επίσης ευχαριστώ την κα. Μαρία Λουκάκη και τον κ. Νικόλαο Τζανάκη που μαζί με τον κ. Ιωάννη Α. Αντωνιάδη αποτέλεσαν την επιτροπή αξιολόγησης.

Ευχαριστώ την οικογένεια μου, που με στηρίζει σε κάθε μου επιλογή και που με την καθημερινή τους συμπαράσταση με βοήθησαν να πετύχω τους στόχους μου.

Τέλος, θα ήθελα να ευχαριστήσω την μαθηματικό και δασκάλα μου Έλενα Φακιδαράκη, που με μύησε στον κόσμο των μαθηματικών.

Ευαγγελία Καρτσάκη
Ιούνιος 2022

Περίληψη

Στην παρούσα εργασία μελετούμε το Θεώρημα των Hasse-Minkowski (τοπικό - γενικό αξίωμα), καθώς και τα ιστορικά αντιπαραδείγματά του.

Στο πρώτο κεφάλαιο περιγράφουμε τη διαδικασία κατασκευής του σώματος των p-αδικών αριθμών και μελετούμε αλγεβρικές και τοπολογικές ιδιότητες αυτών. Ιδιαίτερα σημαντικό στα παρακάτω είναι το Λήμμα του Hensel, μέσω του οποίου αποδεικνύουμε την ύπαρξη τοπικών λύσεων (λύσεις στα p-αδικά σώματα $\mathbb{Q}_p$) διοφαντικών εξισώσεων, καθώς και η έννοια του συμβόλου του Hilbert και οι ιδιότητες του, μέσω του οποίου μελετούμε τετραγωνικές μορφές στα σώματα αυτά.

Στο δεύτερο κεφάλαιο αναπτύσσουμε βασικές έννοιες της θεωρίας των τετραγωνικών μορφών και αποδεικνύουμε θεωρήματα χρήσιμα για την απόδειξη του Θεωρήματος των Hasse-Minkowski. Ιδιαίτερα χρήσιμα είναι τα θεωρήματα του Witt αλλά και θεωρήματα που αφορούν τετραγωνικές μορφές στα p-αδικά σώματα.

Τέλος στο τρίτο κεφάλαιο μελετούμε διοφαντικές εξισώσεις για τις οποίες δεν ισχύει το τοπικό - γενικό αξίωμα.

Abstract

In this thesis, we study the Hasse-Minkowski theorem (local - global principle), as well as the historical counterexamples.

In the first chapter, we describe the process of contruction of the p-adic fields and study their algebraic and topological properties. Extremely important is Hensel's Lemma which we use to prove the existence of local solutions of diophantine equations (solutions over p-adic fields), as well as the Hilbert sumbol and it's properties, that we use to study quadratic forms over p-adic fields.

In the second chapter, we develop concepts of quadratic forms theory used in the proof of Hasse-Minkowski theorem. Extremely useful are Witt's theorems as well as theorems concerning quadratic forms over p-adic fields.

Finally, in the third chapter, we study diophantine equations, for which the local global principle fails.

Περιεχόμενα

Εισαγωγή

Ένα από τα κύρια προβλήματα στη Θεωρία Αριθμών είναι η επίλυση διοφαντικών εξισώσεων. Αν $f(x_1, x_2, ..., x_n)$ είναι ένα πολυώνυμο με ακέραιους ή ρητούς συντελεστές, μας ενδιαφέρει να μελετήσουμε αν το πολυώνυμο έχει ρητές ρίζες. Η ιδέα του τοπικού - γενικού αξιώματος είναι η μεταφορά του προβλήματος της επίλυσης μιας διοφαντικής εξίσωσης στα p-αδικά σώματα $\mathbb{Q}_p$ και στο $\mathbb{R}$. Πρόκειται για σώματα με περισσότερες ιδιότητες από το $\mathbb{Q}$, γεγονός που κάνει την επίλυση μιας διοφαντικής εξίσωσης ευκολότερη.

Το τοπικό - γενικό αξίωμα λοιπόν δηλώνει ότι ορισμένοι τύποι διοφαντικών εξισώσεων έχουν ρητή λύση αν και μόνο αν έχουν λύση στα p-αδικά σώματα $\mathbb{Q}_p$ και στο $\mathbb{R}$.

Το κύριο αντικείμενο της παρούσας εργασίας είναι η απόδειξη του Θεωρήματος των Hasse-Minkowski, δηλαδή ότι για οποιαδήποτε τετραγωνική μορφή $f(x_1, x_2, ..., x_n) \in \mathbb{Q}[x_1, x_2, ..., x_n]$ ισχύει το τοπικό γενικό αξίωμα. Πρόκειται για ένα από τα πιο σημαντικά Θεωρήματα της Θεωρίας Αριθμών κατά τον 20ο αιώνα. Το αποτέλεσμα αυτό δικαίωσε πλήρως την άποψη του Kurt Hensel για τη σημαντική χρησιμότητα της θεωρίας των p-αδικών αριθμών και των τοπικών σωμάτων γενικότερα, στη Θεωρία Αριθμών.
Ένα p-αδικό σώμα είναι εξ ορισμού και κατ' αναλογία προς το σώμα των πραγματικών αριθμών, η πλήρωση του $\mathbb{Q}$ ως προς την p-αδική απόλυτη τιμή $|\cdot|_p$, η οποία ορίζεται ως εξής:

Για κάθε ρητό αριθμό $\frac{a}{b} \neq 0$, $a, b \in \mathbb{Z}, b \neq 0$ ορίζουμε $|\frac{a}{b}|_p = p^{-ord_p(\frac{a}{b})}$ όπου $ord_p(\frac{a}{b}) = ord_p(a) - ord_p(b)$, με $ord_p(a), ord_p(b)$ είναι οι μεγαλύτεροι ακέραιοι ώστε $p^{ord_p(a)} \mid a$ και $p^{ord_p(b)} \mid b$.

Ορίζεται η έννοια της ισοδυναμίας μεταξύ απολύτων τιμών του $\mathbb{Q}$ και αποδεικνύεται το θεώρημα του Ostrowski, ότι όλες οι μη-τετριμμένες και μη ισοδύναμες ανά δύο απόλυτες τιμές του $\mathbb{Q}$ είναι οι p-αδικές απόλυτες τιμές $|\cdot|_p$ και η συνήθης απόλυτη τιμή, η οποία συμβολίζεται με $|\cdot|_\infty$.
Το Θεώρημα των Hasse-Minkowski είναι το εξής:

Θεώρημα (Hasse-Minkowski)
Έστω $f(x_1, x_2, ..., x_n) \in \mathbb{Q}[x_1, x_2, ..., x_n]$ τετραγωνική μορφή. Η εξίσωση

$$f(x_1, x_2, ..., x_n) = 0$$

έχει μια μη-μηδενική ρητή λύση ακριβώς τότε όταν έχει μη-μηδενική λύση σε κάθε σώμα $\mathbb{Q}_v$, $v \in P = \mathbb{P} \cup \{\infty\}$.

Μία λύση στα σώματα $\mathbb{Q}_v$ λέγεται τοπική λύση, ενώ μία λύση στο $\mathbb{Q}$ λέγεται γενική λύση.

Η εργασία αποτελείται από τρία κεφάλαια. Στο πρώτο κεφάλαιο αναπτύσσουμε βασικές έννοιες και ιδιότητες των p-αδικών αριθμών. Ιδιαίτερα χρήσιμα είναι το Λήμμα του Hensel, και η δομή της ομάδας $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Επίσης ορίζουμε το σύμβολο του Hilbert και αποδεικνύουμε όλες τις βασικές του ιδιότητες. Το σύμβολο του Hilbert αποτελεί απαραίτητο εργαλείο για τη μελέτη των τετραγωνικών μορφών στα p-αδικά σώματα $\mathbb{Q}_p$.

Στο δεύτερο κεφάλαιο αναπτύσσουμε τη θεωρία των τετραγωνικών μορφών και μελετούμε τις τετραγωνικές μορφές στα p-αδικά σώματα. Αποδεικνύουμε θεωρήματα τα οποία είναι απαραίτητα για την απόδειξη του κεντρικού Θεωρήματος των Hasse-Minkowski, καθώς επίσης και το τοπικό - γενικό αξίωμα για την ισοδυναμία τετραγωνικών μορφών.

Τέλος το τρίτο κεφάλαιο, μελετούμε τα κλασικά αντιπαραδείγματα στο τοπικό - γενικό αξίωμα. Συγκεκριμένα μελετούμε διοφαντικές εξισώσεις οι οποίες έχουν λύσεις τοπικά σε όλα τα p-αδικά σώματα και στο $\mathbb{R}$ αλλά δεν έχουν ρητή λύση. Οι διοφαντικές εξισώσεις στις οποίες αναφερόμαστε στο τρίτο κεφάλαιο είναι η εξίσωση των Lind-Reichardt $X^4 - 17 = 2Y^2$, και η εξίσωση του Selmer $3X^3 + 4Y^3 + 5Z^3 = 0$.

Κεφάλαιο 1

Τα p-αδικά σώματα

1.1 Πλήρωση ενός μετρικού χώρου

Βασική έννοια της τοπολογίας είναι η έννοια του μετρικού χώρου. Στην παρούσα ενότητα θα αναφέρουμε βασικές έννοιες και το θεώρημα της πλήρωσης ενός μετρικού χώρου

Ορισμός 1.1.1. Μετρικός χώρος ονομάζεται ένα ζεύγος (X, d), όπου X είναι ένα μη κενό σύνολο και $d : X \times X \to \mathbb{R}$ μία συνάρτηση με τις ιδιότητες:
(1) $d(x, y) \geq 0$ για κάθε $x, y \in X$ και $d(x, y) = 0 \Leftrightarrow x = y$
(2) $d(x, y) = d(y, x)$ για κάθε $x, y \in X$
(3) $d(x, y) \leq d(x, z) + d(z, y)$ για κάθε $x, y, z \in X$
Η d λέγεται μετρική ή συνάρτηση απόστασης του μετρικού χώρου.

Ορισμός 1.1.2. Μία ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ στοιχείων του X λέγεται ακολουθία Cauchy (ή θεμελιώδης ακολουθία) όταν για κάθε $\varepsilon \in \mathbb{R}, \varepsilon > 0$ υπάρχει φυσικός αριθμός $n_0 = n_0(\varepsilon)$ τέτοιος ώστε για κάθε $m, n > n_0$ να ισχύει $d(a_m, a_n) < \varepsilon$.

Ορισμός 1.1.3. Αν κάθε ακολουθία Cauchy στοιχείων του X συγκλίνει σε κάποιο στοιχείο του X, τότε ο μετρικός χώρος (X, d) λέγεται πλήρης μετρικός χώρος.

Ορισμός 1.1.4. Αν (X, d) είναι ένας μετρικός χώρος και $A \subseteq X$, τότε το A λέγεται πυκνό στον (X, d), όταν κάθε στοιχείο $x \in X$ είναι όριο ακολουθίας στοιχείων του A.

Ορισμός 1.1.5. Μία πλήρωση ενός μετρικού χώρου (X, d) είναι ένας πλήρης μετρικός χώρος $(\tilde{X}, D)$ για τον οποίο υπάρχει μια ισομετρία $\varphi : X \to \tilde{X}$ τέτοια ώστε το σύνολο $\varphi(X)$ να είναι πυκνό στο $\tilde{X}$.
Μια ισομετρία μεταξύ δύο μετρικών χώρων (X_1, d_1) και (X_2, d_2) είναι μία απεικόνιση $\varphi : X_1 \to X_2$, η οποία διατηρεί την απόσταση, δηλαδή

$$d_2(\varphi(x), \varphi(y)) = d_1(x, y)$$

για κάθε $x, y \in X_1$.

Θεώρημα 1.1.6. *Ισχύουν τα εξής:*
(1) Καθε μετρικός χώρος (X, d) επιδέχεται μια πλήρωση.
(2) Η πλήρωση αυτή είναι μοναδική κατα προσέγγιση ισομετρίας.

Για την απόδειξη παραπέμπουμε στο [22] σελ. 2

1.2 Πλήρωση σώματος εφοδιασμένου με απόλυτη τιμή

Στην ενότητα αυτή θα περιγράψουμε τις βασικές ιδιότητες ενός σώματος εφοδιασμένου με απόλυτη τιμή και την διαδικασία της πλήρωσης. Δίνουμε λοιπόν τον ορισμό της απόλυτης τιμής σε ένα σώμα K.

Ορισμός 1.2.1. Έστω σώμα K, μια απόλυτη τιμή στο K είναι μια συνάρτηση $\|\cdot\| : K \to \mathbb{R}_{\geq 0}$ με τις ιδιότητες:
1) $\|x\| \geq 0$ για κάθε $x \in K$ και $\|x\| = 0 \Leftrightarrow x = 0$
2) $\|x.y\| = \|x\|.\|y\|$ για κάθε $x, y \in K$.
3) $\|x + y\| \leq \|x\| + \|y\|$ για κάθε $x, y \in K$.

Παράδειγμα 1.2.2. *Το σώμα $\mathbb{Q}$ με την συνήθη απόλυτη τιμή $|\cdot|$.*

Παρατήρηση 1.2.3. *Ισχύουν τα εξής:*
1) Κάθε σώμα έχει τουλάχιστον την τετριμμένη απόλυτη τιμή με $\|0\| = 0$, $\|x\| = 1$ για κάθε $x \in K^*$.
2) Για κάθε $n \in \mathbb{N}$ έχουμε $n \cdot 1_K = \underbrace{1_K + 1_K + ... + 1_K}_{n\text{-φορές}} \in K$. Ταυτίζουμε το n με το $n \cdot 1_K$, δηλαδή θεωρούμε ότι $n \in K$ για κάθε $n \in \mathbb{N}$.
3) Αν K σώμα με απόλυτη τιμή $\|\cdot\|$, για κάθε $x, y \in K$ ισχύουν:
$(i)\|1\| = \|-1\| = 1$
$(ii)\|x\| = \|-x\|$
$(iii)\|x + y\| \geq |\|x\| - \|y\||$ *όπου στο δεξιό μέλος εμφανίζεται η απόλυτη τιμή του πραγματικού αριθμού $\|x\| - \|y\|$*
$(iv)\|x - y\| \leq \|x\| + \|y\|$
$(v)\|\frac{x}{y}\| = \frac{\|x\|}{\|y\|}$ *για* $y \neq 0$
$(vi)\|n\| \leq n$ *για κάθε* $n \in \mathbb{N}$

Αν το σώμα K έχει απόλυτη τιμή $\|\cdot\|$, η συνάρτηση $d : K \times K \to \mathbb{R}_{\geq 0}$ με $d(x, y) = \|x - y\|$ είναι μια μετρική του K και λέγεται η επαγόμενη μετρική από την $\|\cdot\|$.

Ορισμός 1.2.4. Έστω σώμα K με απόλυτη τιμή $\|\cdot\|$. Η $\|\cdot\|$ λέγεται μη-αρχιμήδεια αν ισχύουν:
1) $\|x\| \geq 0$ για κάθε $x \in K$ και $\|x\| = 0 \Leftrightarrow x = 0$
2) $\|x.y\| = \|x\|.\|y\|$ για κάθε $x, y \in K$.
3) $\|x + y\| \leq max\{\|x\|, \|y\|\}$ για κάθε $x, y \in K$.

Πρόταση 1.2.5. *Έστω K σώμα και $\|\cdot\|$ απόλυτη τιμή στο K. Τα ακόλουθα είναι ισοδύναμα:*
(1) Η $\|\cdot\|$ είναι μη-αρχιμήδεια.
(2) Ισχύει $\|n\| \leq 1$ για κάθε ακέραιο αριθμό n.

Απόδειξη. βλ. [22] Proposition 1.14, [4] □

Πρόταση 1.2.6. *Αν η απόλυτη τιμή $\|\cdot\|$ του K είναι μη-αρχιμήδεια, και $a, x \in K$ με $\|x - a\| < \|a\|$, τότε έχουμε $\|x\| = \|a\|$.*

Απόδειξη. βλ. [22] Proposition 1.15, [4] □

1.2.1 Πλήρωση

Σε αυτή την παράγραφο θα περιγράψουμε την κατασκευή της πλήρωσης ενός σώματος με απόλυτη τιμή. Έστω λοιπόν σώμα K εφοδιασμένο με μια απόλυτη τιμή $\|\cdot\|$.

Ορισμός 1.2.7. Μια ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ στοιχείων του σώματος K λέγεται ακολουθία Cauchy, όταν για κάθε $\varepsilon \in \mathbb{R}, \varepsilon > 0$, υπάρχει φυσικός αριθμός $n_0 = n_0(\varepsilon)$ τέτοιος ώστε για κάθε $m, n \geq n_0$ να ισχύει: $\|a_m - a_n\| < \varepsilon$.

Ορισμός 1.2.8. Η ακολουθία $\{\alpha_n\}_{n\in\mathbb{N}}$ στοιχείων του K λέγεται μηδενική όταν για καθε $\varepsilon > 0$ υπάρχει $n_0 \in \mathbb{N}$ τέτοιο ώστε $\|\alpha_n\| < \varepsilon$ για κάθε $n \geq n_0$.

Πρόταση 1.2.9. *(i) Κάθε μηδενική ακολουθία είναι ακολουθία Cauchy*
(ii) Κάθε ακολουθία Cauchy είναι φραγμένη.

Για την παραπάνω Πρόταση βλ. [22] σελ. 8

Ορισμός 1.2.10. Ένα σώμα K με απόλυτη τιμή $\|\cdot\|$ λέγεται πλήρες αν κάθε ακολουθία Cauchy στοιχείων του K συγκλίνει στο K. Δηλάδη, αν $\{\alpha_n\}_{n\in\mathbb{N}}$ ακολουθία Cauchy στοιχείων του K, υπάρχει ένα $\alpha \in K$ ώστε για κάθε $\varepsilon > 0$ υπάρχει $n_0 \in \mathbb{N}$ ώστε $\|\alpha_n - \alpha\| < \varepsilon$ για κάθε $n \geq n_0$.

Στην συνέχεια θεωρούμε το σύνολο όλων των ακολουθιών Cauchy στο σώμα K.
Έστω $R := \{\{a_n\}_{n\in\mathbb{N}} | \{a_n\}_{n\in\mathbb{N}}$ ακολουθία Cauchy στοιχείων του K$\}$. Στο σύνολο R ορίζουμε πράξεις πρόσθεσης και πολλαπλασιασμού ως εξής:

$$\{a_n\}_{n\in\mathbb{N}} \oplus \{b_n\}_{n\in\mathbb{N}} = \{a_n + b_n\}_{n\in\mathbb{N}} \text{ και,}$$
$$\{a_n\}_{n\in\mathbb{N}} \odot \{b_n\}_{n\in\mathbb{N}} = \{a_n.b_n\}_{n\in\mathbb{N}}$$

Πρόταση 1.2.11. *Το σύνολο R με πράξεις $\oplus$ και $\odot$ αποτελεί αντιμεταθετικό δακτύλιο με μοναδιαίο. Το μηδενικό στοιχείο του R είναι η ακολουθία $\widehat{0} = (0, 0, 0, ...)$ και το μοναδιαίο, η ακολουθία $\widehat{1} = (1, 1, 1, ...)$*

(βλ. [22] σελ. 15)

Έστω τώρα $M := \{\{a_n\}_{n\in\mathbb{N}} | \{a_n\}_{n\in\mathbb{N}}$ μηδενική ακολουθία στοιχείων του K$\}$.

Πρόταση 1.2.12. *Το σύνολο M με πράξεις $\oplus$ και $\odot$ αποτελεί ιδεώδες του R.*

(βλ. [22] σελ. 15, [4])

Ο δακτύλιος πηλίκων R/M αποτελείται από κλάσεις ισοδυναμίας ακολουθιών Cauchy. Δύο ακολουθίες $\{a_n\}_{n\in\mathbb{N}}, \{b_n\}_{n\in\mathbb{N}}$ ανήκουν στην ίδια κλάση αν η $\{a_n - b_n\}_{n\in\mathbb{N}}$ είναι μηδενική ακολουθία.

Πρόταση 1.2.13. *Ο δακτύλιος $\tilde{K} := R/M$ είναι σώμα.*

Απόδειξη. βλ. [22] Theorem 1.19, [4] □

Η απεικόνιση $\begin{cases} K \to \tilde{K} \\ \alpha \mapsto \{\alpha\}_{n\in\mathbb{N}} + M \end{cases}$, είναι μονομορφισμός δακτυλίων και συνεπώς μπορούμε να θεωρήσουμε $K \leq \tilde{K}$.

Για κάθε στοιχείο $\tilde{\alpha} = \{\alpha_n\}_{n\in\mathbb{N}} + M \in \tilde{K}$ ισχύει $\tilde{\alpha} = \lim_{n\to\infty} \alpha_n$. Αν $\tilde{\alpha} = \{\alpha_n\}_{n\in\mathbb{N}} + M \in \tilde{K}$, ορίζουμε:

$$\|\tilde{\alpha}\|_1 = \lim_{n\to\infty} \|\alpha_n\| \qquad (*)$$

Η $\|\cdot\|_1$, όπως ορίστηκε είναι μια απόλυτη τιμή του $\tilde{K}$, το $\tilde{K}$ είναι πλήρες ως προς την απόλυτη τιμή $\|\cdot\|_1$ και το σώμα K είναι πυκνό στο $\tilde{K}$. Επίσης αν $\alpha_n = \alpha \in K$ για κάθε $n \in \mathbb{N}$, τότε $\|\tilde{\alpha}\|_1 = \|\alpha\|$.
Το επόμενο θεώρημα μας λέει ότι η πλήρωση ενός σώματος είναι μοναδική κατά προσέγγιση ισομετρικού ισομορφισμού.

Θεώρημα 1.2.14. *Έστω σώμα K με απόλυτη τιμή $\|\cdot\|$ και $(K_1, \|\cdot\|_1)$, $(K_2, \|\cdot\|_2)$ δύο σώματα πλήρη ως προς τις απόλυτες τιμές $\|\cdot\|_1$ και $\|\cdot\|_2$ αντίστοιχα τα οποία περιέχουν το K, επεκτείνουν την απόλυτη τιμή του $\|\cdot\|$ και το σώμα K είναι πυκνό στα σώματα K_1 και K_2. Τότε υπάρχει ισομετρικός ισομορφισμός $\Phi : K_1 \to K_2$.*

Απόδειξη. βλ [8] σελ 31. □

Παρατήρηση 1.2.15. *Η πλήρωση $(\tilde{K}, \|\cdot\|)$ του σώματος $(K, |\cdot|)$ έχει την ίδια χαρακτηριστική με το K. Επίσης αν η απόλυτη τιμή $|\cdot|$ του K είναι μη-αρχιμήδεια το ίδιο ισχύει και για την απόλυτη τιμή $\|\cdot\|$ του $\tilde{K}$.*

Πρόταση 1.2.16. *Αν $|\cdot|$ είναι μη-αρχιμήδεια απόλυτη τιμή του σώματος K και $\|\cdot\|$ η επέκτασή της στην πλήρωση $\tilde{K}$ του K, τότε*

$$\{|a|, a \in K\} = \{\|\alpha\|, \alpha \in \tilde{K}\}$$

Απόδειξη. βλ. [8] Theorem 1.14 □

1.2.2 Ισοδύναμες απόλυτες τιμές

Στην συνέχεια θα μελετήσουμε την έννοια της ισοδυναμίας απολύτων τιμών.

Ορισμός 1.2.17. Έστω $\|\cdot\|_1, \|\cdot\|_2$ απόλυτες τιμές στο σώμα K. Οι $\|\cdot\|_1$, $\|\cdot\|_2$ λέγονται ισοδύναμες αν μια ακολουθία $\{\alpha_n\}_{n\in\mathbb{N}}$ στοιχείων του K είναι ακολουθία Cauchy ως προς την $\|\cdot\|_1$, αν και μόνον αν είναι ακολουθία Cauchy ως προς την $\|\cdot\|_2$.
Συμβολίζουμε $\|\cdot\|_1 \sim \|\cdot\|_2$.

Παρατήρηση 1.2.18. *Αν η $\|\cdot\|_1$ είναι τετριμμένη απόλυτη τιμή του K και $\|\cdot\|_1 \sim \|\cdot\|_2$ τότε και η $\|\cdot\|_2$ είναι τετριμμένη.*

Παρατήρηση 1.2.19. *Αν οι απόλυτες τιμές $\|\cdot\|_1$ και $\|\cdot\|_2$ του σώματος K είναι ισοδύναμες τότε ισχύουν:*
$(i)\|x\|_1 < 1 \Leftrightarrow \|x\|_2 < 1$
$(ii)\|x\|_1 > 1 \Leftrightarrow \|x\|_2 > 1$
$(iii)\|x\|_1 = 1 \Leftrightarrow \|x\|_2 = 1$

Πόρισμα 1.2.20. *Αν οι απόλυτες τιμές $\|\cdot\|_1, \|\cdot\|_2$ του K είναι ισοδύναμες, τότε ή είναι και οι δύο αρχιμήδειες ή είναι και οι δύο μη αρχιμήδειες.*

Πρόταση 1.2.21. *Έστω σώμα K με απόλυτες τιμές $\|\cdot\|_1, \|\cdot\|_2$. Οι $\|\cdot\|_1$, $\|\cdot\|_2$ είναι ισοδύναμες αν και μόνο αν υπάρχει θετικός πραγματικός αριθμός α τέτοιος ώστε να ισχύει $\|x\|_2 = \|x\|_1^\alpha$ για κάθε $x \in K$.*

Απόδειξη. Υποθέτουμε ότι ισχύει $\|\cdot\|_1 \sim \|\cdot\|_2$. Αν η $\|\cdot\|_1$ είναι τετριμμένη τότε και η $\|\cdot\|_2$ είναι τετριμμένη και άρα το ζητούμενο ισχύει για κάθε πραγματικό αριθμό α. Αν τώρα η $\|\cdot\|_1$ δεν είναι τετριμμένη, υπάρχει $a \in K^*$ ώστε $\|a\|_1 \neq 1$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $\|a\|_1 < 1$. Ορίζουμε

$$\alpha := \frac{\log \|a\|_2}{\log \|a\|_1} \in \mathbb{R}$$

Αφού $\|\cdot\|_1 \sim \|\cdot\|_2$ και $\|a\|_1 < 1$ έχουμε ότι και $\|a\|_2 < 1$. Άρα $\alpha > 0$.
Έστω $x \in K$ με $\|x\|_1 < 1$. Θεωρούμε το σύνολο

$$S = \{r = \frac{m}{n} : m, n \in \mathbb{N}, \|x\|_1^r < \|a\|_1\}$$

Για κάθε $r \in S$ ισχύει $\|x\|_1^r < \|a\|_1 \Rightarrow \|x\|_1^{\frac{m}{n}} < \|a\|_1 \Rightarrow \|x\|_1^m < \|a\|_1^n \Rightarrow \|\frac{x^m}{a^n}\|_1 < 1$ και, επειδή $\|\cdot\|_1 \sim \|\cdot\|_2$ από την Παρατήρηση 1.2.19, προκύπτει $\|\frac{x^m}{a^n}\|_2 < 1 \Rightarrow \|x\|_2^m < \|a\|_2^n \Rightarrow \|x\|_2^r < \|a\|_2$. Με το ίδιο επιχείρημα εναλλάσσοντας τους ρόλους των $\|\cdot\|_1$ και $\|\cdot\|_2$, έχουμε ότι

$$S = \{r = \frac{m}{n} : m, n \in \mathbb{N}, \|x\|_2^r < \|a\|_2\}$$

Αν $r \in S$, τότε $r > \frac{\log\|a\|_1}{\log\|x\|_1}$ και $r > \frac{\log\|a\|_2}{\log\|x\|_2}$ $(*)$. Τότε κατ'ανάγκη

$$\frac{\log\|a\|_1}{\log\|x\|_1} = \frac{\log\|a\|_2}{\log\|x\|_2}$$

διότι αν, χωρίς βλάβη γενικότητας, $\frac{\log\|a\|_1}{\log\|x\|_1} < \frac{\log\|a\|_2}{\log\|x\|_2}$, τότε υπάρχει κάποιος ρητός αριθμός r ωστε $\frac{\log\|a\|_1}{\log\|x\|_1} < r < \frac{\log\|a\|_2}{\log\|x\|_2}$ το οποίο αντιβαίνει στην $(*)$.
Επομένως

$$\frac{\log\|x\|_2}{\log\|x\|_1} = \frac{\log\|a\|_2}{\log\|a\|_1} = \alpha$$

και άρα $\|x\|_2 = \|x\|_1^\alpha$ για κάθε $x \in K$ με $\|x\|_1 < 1$.
Αν $x \in K$ με $\|x\|_1 > 1$, τότε $\|\frac{1}{x}\|_1 < 1 \Rightarrow \|\frac{1}{x}\|_2 = \|\frac{1}{x}\|_1^\alpha \Rightarrow \|x\|_2 = \|x\|_1^\alpha$ και αν $\|x\|_1 = 1 \Rightarrow \|x\|_2 = 1$. Δηλαδή για κάθε $x \in K$ ισχύει $\|x\|_2 = \|x\|_1^\alpha$.

Αντίστροφα έστω ότι υπάρχει $\alpha > 0$ ώστε $\|x\|_2 = \|x\|_1^\alpha$ για κάθε $x \in K$. Έστω $\{a_n\}_{n\in\mathbb{N}}$ ακολουθία στοιχείων του K η οποία είναι Cauchy ως προς την $\|\cdot\|_1$. Έστω $\varepsilon > 0$, τότε υπάρχει $n_0 \in \mathbb{N}$ ώστε για κάθε $n, m \geq n_0$ να ισχύει $\|a_n - a_m\|_1 < \varepsilon^{\frac{1}{\alpha}}$. Τότε $\|a_n - a_m\|_2 < \varepsilon$ και συνεπώς η $\{a_n\}_{n\in\mathbb{N}}$ είναι ακολουθία Cauchy ως προς την $\|\cdot\|_2$. Εναλλάσσοντας τους ρόλους των $\|\cdot\|_1$ και $\|\cdot\|_2$, έχουμε το ζητούμενο. □

Γνωρίζουμε ήδη την συνήθη απόλυτη τιμή $|\cdot|$ στο σώμα $\mathbb{Q}$ των ρητών αριθμών. Μας ενδιαφέρει να μελετήσουμε την υπάρξη άλλων απολύτων τιμών στο $\mathbb{Q}$ και ποιες από αυτές είναι ισοδύναμες.

Ορισμός 1.2.22. Έστω p πρώτος αριθμός. Για $x \in \mathbb{Z}, x \neq 0$, ορίζουμε την τάξη του x ως προς p, $ord_p(x)$ να είναι ο μεγαλύτερος φυσικός αριθμός για τον οποίο ισχύει $p^{ord_p(x)} \mid x$ (όπως την ορίσαμε στην Εισαγωγή). Παρατηρούμε ότι

για τα $x, y \in \mathbb{Z}$ ισχύει $ord_p(x+y) \geq min\{ord_p(x), ord_p(y)\}$.
Για $x \in \mathbb{Q}, x \neq 0$ με $x = \frac{a}{b}$, όπου $a, b \in \mathbb{Z}, b \neq 0$ ορίζουμε

$$ord_p(x) = ord_p(a) - ord_p(b)$$

Έστω $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ με $|x|_p = p^{-ord_p(x)}$ για $x \neq 0$ και $|0|_p = 0$.Τότε έχουμε την παρακάτω Πρόταση.

Πρόταση 1.2.23. *Η συνάρτηση $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ είναι μια μη-αρχιμήδεια απόλυτη τιμή στο $\mathbb{Q}$. Η $|\cdot|_p$ ονομάζεται p-αδική απόλυτη τιμή.*

Απόδειξη. Η ιδιότητα (1) του ορισμού 1.2.4 είναι προφανής. Για την (2) έχουμε:

$$|x \cdot y|_p = p^{-ord_p(x \cdot y)} = p^{-ord_(x)} p^{-ord_p(y)} = |x|_p |y|_p$$

Για την (3), αν $x = 0$ ή $y = 0$ είναι τετριμμένη. Έστω $x, y \neq 0$ με $x = \frac{a}{b}$ και $y = \frac{c}{d}$ όπου $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$. Τότε $x + y = \frac{ad+bc}{bd}$. Άρα:

$$\begin{gathered} ord_p(x+y) = ord_p(ad+bc) - ord_p(b) - ord_p(d) \\ \geq min\{ord_p(ad), ord_p(bc)\} - ord_p(b) - ord_p(d) \\ = min\{ord_p(a) + ord_p(d), ord_p(b) + ord_p(c)\} - ord_p(b) - ord_p(d) \\ = min\{ord_p(x), ord_p(y)\} \end{gathered}$$

Άρα $|x+y|_p = p^{-ord_p(x+y)} \leq max\{p^{-ord_p(x)}, p^{-ord_p(y)}\} = max\{|x|_p, |y|_p\}$. □

Συχνά συμβολίζουμε την συνήθη απόλυτη τιμή $|\cdot|$ του $\mathbb{Q}$ με $|\cdot|_\infty$.

Παρατήρηση 1.2.24. *Αν p και q είναι δύο διαφορετικοί πρώτοι αριθμοί ισχύει $|\cdot|_p \nsim |\cdot|_q$. Επίσης για κάθε πρώτο αριθμό p, $|\cdot|_p \nsim |\cdot|_\infty$.*

Απόδειξη. Άμεση συνέπεια από την Παρατήρηση 1.2.19 □

Πρόταση 1.2.25. *Η συνάρτηση $\|\cdot\| : \mathbb{Q} \to \mathbb{R}$ με $\|x\| = |x|^\alpha$ όπου $\alpha \in \mathbb{R}, \alpha > 0$ και $|\cdot|$ η συνήθης απόλυτη τιμή, είναι απόλυτη τιμή του $\mathbb{Q}$ αν και μόνο αν $\alpha \leq 1$. Μάλιστα τότε η $\|\cdot\|$ είναι ισοδύναμη με την $|\cdot|$.*

Απόδειξη. βλ. [22] Proposition 1.11 . □

Το ερώτημα που προκύπτει είναι αν υπάρχουν άλλες απόλυτες τιμές στο $\mathbb{Q}$ οι οποίες δεν είναι ισοδύναμες με κάποια p-αδική απόλυτη τιμή $|\cdot|_p$ ή με την $|\cdot|_\infty$. Η απάντηση θα δοθεί από το επόμενο θεώρημα.

Θεώρημα 1.2.26. *(Ostrowski)*
Κάθε μη τετριμμένη απόλυτη τιμή του $\mathbb{Q}$ είναι ισοδύναμη προς μία p-αδική απόλυτη τιμή $|\cdot|_p$ για κάποιο πρώτο αριθμό p ή $p = \infty$.

Απόδειξη. Έστω $\|\cdot\|$ απόλυτη τιμή του $\mathbb{Q}$.
Περίπτωση 1: Υποθέτουμε ότι η $\|\cdot\|$ είναι αρχιμήδεια.
Αυτό σημαίνει ότι υπάρχει τουλάχιστον ένας φυσικός αριθμός n για τον οποίο ισχύει $\|n\| > 1$. Έστω n_0 ο ελάχιστος φυσικός αριθμός με αυτή την ιδιότητα. Τότε $\|n_0\| > 1$ και $n_0 > 1$. Αν $\alpha := \frac{\log \|n_0\|}{\log n_0}$, τότε $\alpha > 0$ και $\|n_0\| = n_0^\alpha$. Θα αποδείξουμε ότι για κάθε φυσικό αριθμό n ισχύει $\|n\| = n^\alpha$. Έστω λοιπόν n ένας φυσικός αριθμός. Γράφουμε τον n ως προς βάση το n_0, δηλαδή

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + ... + a_r n_0^r$$

όπου $a_i \in \mathbb{Z}$, $0 \leq a_i < n_0$ για κάθε $i = 0, 1, ..., r$ και $a_r \neq 0$. Επομένως $\|n\| \leq \|a_0\| + \|a_1\|\|n_0\| + ... + \|a_r\|\|n_0\|^r = \|a_0\| + \|a_1\|n_0^\alpha + ... + \|a_r\|n_0^{\alpha r}$
Λόγω της επιλογής του n_0 έχουμε $\|a_i\| \leq 1$ για κάθε $i = 0, 1, ..., r$. Συνεπώς

$$\begin{aligned} \|n\| &\leq 1 + n_0^\alpha + n_0^{2\alpha} + ... + n_0^{\alpha r} \\ &= n_0^{\alpha r}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + ... + n_0^{-\alpha r}) \\ &\leq n_0^{\alpha r}(\textstyle\sum_{i=0}^{\infty} n_0^{-i\alpha}) = n_0^{\alpha r} C \end{aligned}$$

όπου $C := \frac{n_0^\alpha}{n_0^\alpha - 1} > 0$.
Επειδή $a_r \neq 0$, έπεται ότι $n > n_0^r$. Άρα

$$\|n\| \leq n^\alpha C \qquad (1)$$

Η (1) ισχύει για κάθε φυσικό αριθμό n. Την εφαρμόζουμε για φυσικό αριθμό της μορφής n^N όπου $N \in \mathbb{N}$ και παίρνουμε ότι $\|n^N\| \leq C n^{N\alpha} \Rightarrow \|n\| \leq C^{\frac{1}{N}} n^\alpha$
Οπότε για $N \to \infty$ έχουμε

$$\|n\| \leq n^\alpha \qquad (2)$$

Θα αποδείξουμε και την αντίστροφη ανισότητα. Από τον τρόπο γραφής του n προκύπτει ότι $n_0^{r+1} > n \geq n_0^r$. Επομένως

$$\begin{aligned} n_0^{(r+1)\alpha} = \|n_0^{r+1}\| &\leq \|n\| + \|n_0^{r+1} - n\| \\ \Rightarrow \|n\| \geq \|n_0^{r+1}\| - \|n_0^{r+1} - n\| &= n_0^{(r+1)\alpha} - \|n_0^{r+1} - n\| \end{aligned}$$

Εφαρμόζουμε την (2) για το στοιχείο $n_0^{r+1} - n$ και έχουμε

$$\|n_0^{r+1} - n\| \leq (n_0^{r+1} - n)^\alpha$$

οπότε η προηγούμενη ανισότητα γράφεται

$$\|n\| \geq n_0^{(r+1)\alpha} - (n_0^{r+1} - n)^\alpha$$

Επειδή $n \geq n_0^r$, έχουμε

$$\begin{aligned}\|n\| &\geq n_0^{(r+1)\alpha} - (n_0^{r+1} - n_0^r)^\alpha \\ &= n_0^{(r+1)\alpha}[(1 - (1 - \tfrac{1}{n_0})^\alpha] \\ &= n_0^{(r+1)\alpha} C' > n^\alpha C'\end{aligned}$$

όπου $C' := 1 - (1 - \frac{1}{n_0})^\alpha > 0$. Εφαρμόζοντας ξανά το προηγούμενο τέχνασμα παίρνουμε

$$\|n\| \geq n^\alpha$$

και συνεπώς έχουμε την ισότητα $\|n\| = n^\alpha$ για κάθε $n \in \mathbb{N}$.
Από την ιδιότητα (2) του ορισμού της απόλυτης τιμής έπεται ότι $\|x\| = |x|^\alpha$ για κάθε $x \in \mathbb{Q}$ και από την Πρόταση 1.2.21 έπεται οτι η $\|\cdot\|$ είναι ισοδύναμη με την συνήθη απόλυτη τιμή $|\cdot|$.
Περίπτωση 2: Υποθέτουμε ότι η $\|\cdot\|$ είναι μη-αρχιμήδεια.
Τότε για κάθε φυσικό αριθμό n ισχύει $\|n\| \leq 1$. Αφού η $\|\cdot\|$ δεν είναι τετριμμένη, έπεται ότι υπάρχει φυσικός αριθμός n με $\|n\| < 1$. Έστω n_0 ο ελάχιστος φυσικός αριθμός με αυτή την ιδιότητα, τότε ο n_0 είναι πρώτος αριθμός. Πράγματι αν $n_0 = s \cdot t$ με $s < n_0, t < n_0$ τότε λόγω της επιλογής του n_0, έχουμε $\|s\| = 1$ και $\|t\| = 1$, οπότε και $\|n_0\| = \|s \cdot t\| = \|s\|\|t\| = 1$, το οποίο είναι άτοπο. Συνεπώς ο n_0 είναι πρώτος αριθμός και θα τον συμβολίζουμε με p.
Στη συνέχεια θα αποδείξουμε ότι αν ένας φυσικός αριθμός n δεν διαιρείται με p τότε $\|n\| = 1$. Έστω $n = p \cdot q + v$ όπου $q, v \in \mathbb{Z}$ και $0 < v < p$. Τότε $\|v\| = 1$. Επίσης εξ υποθέσεως $\|p\| < 1$, καθώς και $\|q\| \leq 1$. Δηλαδή $\|p \cdot q\| = \|p\|\|q\| < 1$ και άρα

$$\|n - v\| = \|p \cdot q\| < 1 = \|v\|$$

Από την Πρόταση 1.2.6 έχουμε ότι $\|n\| = \|v\| = 1$.
Τώρα κάθε ακέραιος n γράφεται στη μορφή

$$n = p^k m$$

όπου $k \in \mathbb{N}$ και $m \in \mathbb{Z}$, με $p \nmid m$. Σύμφωνα με το προηγούμενο βήμα έχουμε $\|m\| = 1$, δηλαδή

$$\|n\| = \|p\|^k \|m\| = \|p\|^k$$

Έστω $t := \|p\| < 1$. Όπως και στην αρχή της απόδειξης υπάρχει θετικός αριθμός α ώστε να ισχύει $t = (\frac{1}{p})^\alpha$. Επομένως $\|n\| = (\frac{1}{p})^{\alpha k} = |n|_p^\alpha$. Χρησιμοποιώντας την ιδιότητα (2) του ορισμού της απόλυτης τιμής έχουμε $\|x\| = |x|_p^\alpha$ για κάθε $x \in \mathbb{Q}^*$, και από την Πρόταση 1.2.21 έχουμε ότι η $\|\cdot\|$ είναι ισοδύναμη με την p-αδική απόλυτη τιμή $|\cdot|_p$. □

Θεώρημα 1.2.27. *Για κάθε $x \in \mathbb{Q}^*$ ισχύει $\prod_{p \leq \infty} |x|_p = 1$.*

Απόδειξη. Το δείχνουμε αρχικά για $x \in \mathbb{Z}$. Έστω $x = \pm p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ όπου $p_i \in \mathbb{P}, n_i \in \mathbb{N}$ για κάθε $i = 1, 2, ...k$. Τότε $|x|_\infty = |x| = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ και $|x|_{p_i} = p_i^{-n_i}$ για κάθε $i = 1, 2, ..., k$. Επίσης αν $q \in \mathbb{P}$ με $q \nmid x$ τότε $|x|_q = 1$. Άρα $\prod_{p \leq \infty} |x|_p = 1$. Αν τώρα $x \in \mathbb{Q}^*$, τότε ο x γράφεται $x = \frac{a}{b}$ με $a, b \in \mathbb{Z}$ και $a, b \neq 0$. Συνεπώς

$$\prod_{p \leq \infty} |x|_p = \prod_{p \leq \infty} |\tfrac{a}{b}|_p = \prod_{p \leq \infty} \tfrac{|a|_p}{|b|_p} = 1$$

□

1.3 Το σώμα των p-αδικών αριθμών $\mathbb{Q}_p$

Το σώμα $\mathbb{Q}$ των ρητών αριθμών δεν είναι πλήρες ως προς την συνήθη απόλυτη τιμή $|\cdot|$. Μάλιστα γνωρίζουμε ότι η πλήρωση του είναι το σώμα $\mathbb{R}$ των πραγματικών αριθμών. Το ερώτημα είναι αν ισχύει το ίδιο και για τις p-αδικές απόλυτες τιμές $|\cdot|_p$.

Θεώρημα 1.3.1. *Έστω $\|\cdot\|$ μη τετριμμένη απόλυτη τιμή του $\mathbb{Q}$, τότε το $\mathbb{Q}$ δεν είναι πλήρες ως προς την $\|\cdot\|$.*

Απόδειξη. βλ. [15] Lemma 3.2.3 . □

Από το παραπάνω θεώρημα προκύπτει ότι το $\mathbb{Q}$ δεν είναι πλήρες ως προς τις p-αδικές απόλυτες τιμές $|\cdot|_p, p \in \mathbb{P}$.

Ορισμός 1.3.2. Ορίζουμε το σώμα των p-αδικών αριθμών $\mathbb{Q}_p$, ως την πλήρωση του $\mathbb{Q}$, ως προς την απόλυτη τιμή $|\cdot|_p$ για p πρώτο αριθμό. Η απόλυτη τιμή του $\mathbb{Q}_p$ συμβολίζεται επίσης $|\cdot|_p$.

Από τον ορισμό του σώματος $\mathbb{Q}_p$ αν $\alpha \in \mathbb{Q}_p$ υπάρχει ακολουθία Cauchy $\{a_n\}_{n \in \mathbb{N}}$ ρητών αριθμών ώστε $\alpha = \lim_{n \to \infty} a_n$.

1.3.1 Βασικές ιδιότητες του σώματος $\mathbb{Q}_p$

Θεώρημα 1.3.3. *Κάθε $\alpha \in \mathbb{Q}_p$ με $|\alpha|_p \leq 1$ επιδέχεται μονοσήμαντη παράσταση μέσω μιας ακολουθίας Cauchy $\{a_n\}_{n \in \mathbb{N}}$ στοιχείων του $\mathbb{Q}$ για την οποία ισχύουν:*
(1) $a_i \in \mathbb{Z}, 0 \leq a_i < p^i$ για $i \in \mathbb{N}$
(2) $a_i \equiv a_{i+1} mod p^i$ για $i \in \mathbb{N}$
(3) $\alpha = \lim_{n \to \infty} a_n$.

Λήμμα 1.3.4. *Αν $x \in \mathbb{Q}$ και $|x|_p \leq 1$ τότε για κάθε $i \in \mathbb{N}$ υπάρχει $\alpha \in \{0, 1, ..., p^i - 1\}$ ώστε $|\alpha - x|_p \leq p^{-i}$.*

Απόδειξη. Έστω $x = \frac{a}{b}$ με $a, b \in \mathbb{Z}, b \neq 0$ και $(a, b) = 1$. Αφού $|x|_p \leq 1$ έχουμε $p \nmid b$ και άρα $(p^i, b) = 1$ για κάθε $i \in \mathbb{N}$. Συνεπώς για κάθε $i \in \mathbb{N}$ υπάρχουν $m, n \in \mathbb{Z}$ ώστε $mb + np^i = 1$. Έστω $\alpha' := am$, τότε

$$\begin{aligned} |\alpha' - x|_p = |am - \tfrac{a}{b}|_p = |\tfrac{a}{b}|_p |mb - 1|_p \leq |mb - 1|_p \\ = |np^i|_p = |n|_p |p^i|_p \leq p^{-i} \end{aligned}$$

Έστω τώρα $t \in \mathbb{Z}$ ώστε $\alpha := \alpha' + tp^i \in \{0, 1, ..., p^i - 1\}$ τότε $|\alpha - x|_p = |(\alpha' - x) + tp^i|_p \leq max\{|\alpha' - x|_p, |tp^i|_p\} \leq p^{-i}$. □

Απόδειξη. (Θεωρήματος 1.3.3)
Έστω $\{b_n\}_{n\in\mathbb{N}}$ ακολουθία ρητών με $\alpha = \lim_{n\to\infty} b_n$ ως προς την $|\cdot|_p$. Αρκεί να αποδείξουμε ότι υπάρχει ακολουθία Cauchy ρητών $\{a_n\}_{n\in\mathbb{N}}$ ώστε η $\{b_n - a_n\}_{n\in\mathbb{N}}$ να είναι μηδενική ακολουθία.
Αφού $|\alpha|_p \leq 1$ υπάρχει κάποιο $n_0 \in \mathbb{N}$ ώστε $|b_n|_p \leq 1$ για κάθε $n \geq n_0$, οπότε, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $|b_n|_p \leq 1$ για κάθε $n \in \mathbb{N}$. Αφού η $\{b_n\}_{n\in\mathbb{N}}$ είναι ακολουθία Cauchy για κάθε $j \in \mathbb{N}$ υπάρχει $N(j) \in \mathbb{N}$ ώστε για κάθε $n, n' \geq N(j)$ να ισχύει

$$|b_n - b_{n'}|_p \leq p^{-j}$$

και μπορούμε να υποθέσουμε ότι $N(j) \geq j$.
Από το Λήμμα 1.3.4 υπάρχουν $a_j \in \mathbb{Z}$ με $0 \leq a_j < p^j$ ώστε

$$|a_j - b_{N(j)}|_p \leq p^{-j}$$

Τότε

$$\begin{aligned} |a_{j+1} - a_j|_p = |(a_{j+1} - b_{N(j+1)}) + (b_{N(j+1)} - b_{N(j)}) - (a_j - b_{N(j)})|_p \\ \leq max\{|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p\} \leq p^{-j} \end{aligned}$$

και άρα $a_j \equiv a_{j+1} mod p^j$.
Έστω τώρα $j \in \mathbb{N}$ τότε για κάθε $i \geq N(j)$ έχουμε

$$|a_i - b_i|_p = |(a_i - a_j) + (a_j - b_{N(j)}) - (b_i - b_{N(j)})|_p \leq p^{-j}$$

Δηλαδή $\lim_{i\to\infty} |a_i - b_i|_p = 0$ και συνεπώς η ακολουθία $\{b_n - a_n\}_{n\in\mathbb{N}}$ είναι μηδενική.
Απομένει να αποδείξουμε το μονοσήμαντο. Έστω $\{a'_n\}_{n\in\mathbb{N}}$ ακολουθία ρητών η οποία επαληθεύει τις απαιτήσεις του θεωρήματος. Τότε αναγκαστικά η ακολουθία $\{a_n - a'_n\}_{n\in\mathbb{N}}$ είναι μηδενική. Έστω ότι για κάποιο $n_0 \in \mathbb{N}$ ισχύει $a_{n_0} \neq a'_{n_0}$ τότε αφού $a_{n_0}, a'_{n_0} \in \{0, 1, ..., p^{n_0} - 1\}$ έχουμε $a_{n_0} \not\equiv a'_{n_0} mod p^{n_0}$. Όμως, λόγω της (2), για κάθε $n > n_0$ έχουμε

$$a_n \equiv a_{n_0} mod p^{n_0}$$

και

$$a'_n \equiv a'_{n_0} mod p^{n_0}$$

Άρα για κάθε $n > n_0$ έχουμε $a_n \not\equiv a'_n mod p^{n_0}$ και συνεπώς $|a_n - a'_n|_p > \frac{1}{p^{n_0}}$ για κάθε $n > n_0$. Άτοπο. □

Παρατήρηση 1.3.5. *Έστω $\alpha \in \mathbb{Q}_p$ και ακολουθία $\{a_n\}_{n\in\mathbb{N}}$, όπως στο παραπάνω θεώρημα.*
Έχουμε $0 \leq a_1 < p$, $0 \leq a_2 < p^2$ και $a_2 \equiv a_1 mod p$. Άρα $a_2 = a_1 + b_1 p$ με $0 \leq b_1 < p$. Αν ορίσουμε $b_0 := a_1$ και συνεχίσουμε την παραπάνω διαδικασία επαγωγικά για όλους τους όρους της ακολουθίας έχουμε ότι:

$$a_n = b_0 + b_1 p + b_2 p^2 + ... + b_{n-1} p^{n-1} \text{ με } 0 \leq b_i < p$$

Συνεπώς κάθε $\alpha \in \mathbb{Q}_p$ με $|\alpha|_p \leq 1$ γράφεται μονοσήμαντα $\alpha = \sum_{n=0}^{\infty} b_n p^n$, όπου $0 \leq b_n < p$ για κάθε $n \in \mathbb{N}$. Αυτή λέγεται κανονική παράσταση του α.

Αν τώρα $\alpha \in \mathbb{Q}_p$ με $|\alpha|_p \geq 1$, δηλαδή $|\alpha|_p = p^m$ για κάποιο φυσικό αριθμό m τότε αν $\beta = \alpha p^m$ έχουμε $|\beta|_p = |\alpha|_p |p^m|_p = p^m p^{-m} = 1$ και άρα $\beta = \sum_{n=0}^{\infty} b_n p^n$, όπου $0 \leq b_n < p$ για κάθε $n \in \mathbb{N}$. Τότε έχουμε $\alpha = \beta p^{-m} = \sum_{n=-m}^{\infty} b_n p^n$. Αυτή είναι η κανονική p-αδική παράσταση του $\alpha \in \mathbb{Q}_p$.
Αν $\alpha \in \mathbb{Q}_p$ με $|\alpha|_p = p^{-n}$ τότε ο ακέραιος αριθμός n λέγεται τάξη $ord_p(\alpha)$ του α ως προς p.

1.3.2 Ο δακτύλιος των ακεραίων p-αδικών $\mathbb{Z}_p$

Θεωρούμε το σύνολο $\mathbb{Z}_p := \{x \in \mathbb{Q}_p | |x|_p \leq 1\} \subseteq \mathbb{Q}_p$

Πρόταση 1.3.6. *Το $\mathbb{Z}_p$ αποτελεί αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο, ο οποίος είναι και ακέραια περιοχή.*

Απόδειξη. Αν $x, y \in \mathbb{Z}_p$ τότε $|x|_p \leq 1$ και $|y|_p \leq 1$.Τότε

$$|x + y|_p \leq max\{|x|_p, |y|_p\} = 1$$

και

$$|x \cdot y|_p = |x|_p \cdot |y|_p \leq 1$$

Δηλάδη $x + y, x \cdot y \in \mathbb{Z}_p$. Επίσης $|-x|_p = |x|_p \leq 1$ και $|1|_p = 1$. Από τα παραπάνω συμπεραίνουμε ότι ο $\mathbb{Z}_p$ αποτελεί υποδακτύλιο του σώματος $\mathbb{Q}_p$ με μοναδιαίο και συνεπώς έχουμε το ζητούμενο. □

Ορισμός 1.3.7. Η ακέραια περιοχή $\mathbb{Z}_p$ λέγεται δακτύλιος των ακεραίων $p-$αδικών αριθμών.
Ισοδύναμα ο $\mathbb{Z}_p$ ορίζεται ως $\mathbb{Z}_p := \{x \in \mathbb{Q}_p | ord_p(x) \geq 0\}$.

Πρόταση 1.3.8. *Ένα στοιχείο $\varepsilon \in \mathbb{Z}_p$ είναι μονάδα του $\mathbb{Z}_p$ αν και μόνο αν $|\varepsilon|_p = 1$.*

Απόδειξη. Έστω $\varepsilon \in \mathbb{Z}_p$ με $|\varepsilon|_p = 1$, τότε και για το $\varepsilon^{-1} \in \mathbb{Q}_p$ έχουμε $|\varepsilon^{-1}|_p = |\varepsilon|_p^{-1} = 1$. Άρα $\varepsilon^{-1} \in \mathbb{Z}_p$ και συνεπώς το ε είναι μονάδα του δακτυλίου.
Αντίστροφα έστω $\varepsilon \in \mathbb{Z}_p$ μονάδα. Τότε υπάρχει $b \in \mathbb{Z}_p$ ώστε $\varepsilon b = 1$. Άρα

$$|\varepsilon b|_p = 1 \Rightarrow |\varepsilon|_p |b|_p = 1$$

Όμως $|\varepsilon|_p, |b|_p \leq 1$ και συνεπώς κατ'ανάγκη $|\varepsilon|_p = 1$. □

Συμβολίζουμε $\mathbb{Z}_p^* = \{\varepsilon \in \mathbb{Z}_p | \varepsilon \text{ μονάδα του } \mathbb{Z}_p\}$. Από το παραπάνω είναι προφανές ότι $\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p | ord_p(x) = 0\}$.

Πόρισμα 1.3.9. *Έστω $\alpha \in \mathbb{Z}_p$ με $\alpha = \sum_{n=0}^{\infty} a_n p^n$ με $0 \leq a_n < p$. Το α είναι μονάδα του $\mathbb{Z}_p \Leftrightarrow a_0 \neq 0$. Και άρα $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.*

Απόδειξη. Πράγματι $\alpha \in \mathbb{Z}_p^* \Leftrightarrow ord_p(\alpha) = 0 \Leftrightarrow \alpha \in \mathbb{Z}_p \setminus p\mathbb{Z}_p \Leftrightarrow a_0 \neq 0$. □

Πρόταση 1.3.10. *Κάθε $\alpha \in \mathbb{Q}_p^*$ έχει μονοσήμαντη παράσταση της μορφής $\alpha = p^n \varepsilon$ με $n \in \mathbb{Z}, \varepsilon \in \mathbb{Z}_p^*$.*

Απόδειξη. Έστω $\alpha \in \mathbb{Q}_p^*$ τότε το α γράφεται στην μορφή $\alpha = \sum_{i=-m}^{\infty} a_i p^i$. Αν $n = ord_p(\alpha)$ τότε

$$ord_p(a \cdot p^{-n}) = ord_p(\alpha) + ord_p(p^{-n}) = n + (-n) = 0$$

Άρα $\alpha p^{-n} \in \mathbb{Z}_p^*$, δηλαδή υπάρχει $\varepsilon \in \mathbb{Z}_p^*$ ώστε $\alpha p^{-n} = \varepsilon \Rightarrow \alpha = p^n \varepsilon$. Τώρα αν $\alpha = p^n \varepsilon$ με $n \in \mathbb{Z}$ και $\varepsilon \in \mathbb{Z}_p^*$ τότε κατ'ανάγκη $n = ord_p(\alpha)$ και $\varepsilon = \alpha p^{-n}$. Δηλαδή τα n και ε ορίζονται μονοσήμαντα. □

Παρατήρηση 1.3.11. *Το $p\mathbb{Z}_p$ είναι ιδεώδες του $\mathbb{Z}_p$, μάλιστα $p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^*$. Άρα το $p\mathbb{Z}_p$ είναι το μοναδικό μέγιστο ιδεώδες και συνεπώς ο $\mathbb{Z}_p$ είναι τοπικός δακτύλιος.*
Αν $\alpha \in \mathbb{Q}_p^*$ με $\alpha \notin \mathbb{Z}_p$ τότε $|\alpha|_p > 1$ και άρα $|\alpha^{-1}|_p = \frac{1}{|\alpha|_p} < 1$. Δηλαδή $\alpha^{-1} \in \mathbb{Z}_p$. Συνεπώς ο $\mathbb{Z}_p$ είναι ένας δακτύλιος εκτίμησης του $\mathbb{Q}_p$.

Πρόταση 1.3.12. *Τα ιδεώδη του $\mathbb{Z}_p$ είναι ακριβώς τα κύρια ιδεώδη $< p^n >= p^n\mathbb{Z}_p$ με $n \in \mathbb{N}$ και το $< 0 >$. Δηλαδή ο $\mathbb{Z}_p$ είναι περιοχή κυρίων ιδεωδών (Π.Κ.Ι.).*

Απόδειξη. Έστω A ένα μη μηδενικό ιδεώδες του $\mathbb{Z}_p$. Τότε το σύνολο

$$\{ord_p(\alpha) | \alpha \in A\} \subseteq \mathbb{N}$$

και συνεπώς έχει ελάχιστο στοιχείο. Έστω $n = min\{ord_p(\alpha)|\alpha \in A\}$. Αν $\alpha \in A$ με $\alpha \neq 0$ και $\varepsilon := \alpha p^{-ord_p(\alpha)}$ έχουμε $ord_p(\varepsilon) = 0$ και άρα $\varepsilon \in \mathbb{Z}_p^*$. Τότε

$$\alpha = p^n(p^{ord_p(\alpha)-n}\varepsilon)$$

και αφού $ord_p(\alpha) \geq n$ έχουμε $p^{ord_p(\alpha)-n}\varepsilon \in \mathbb{Z}_p$. Άρα $\alpha \in p^n\mathbb{Z}_p$ και συνεπώς $A \subseteq p^n\mathbb{Z}_p$.
Αντίστροφα από τον ορισμό του n υπάρχει κάποιο $\alpha \in A$ ώστε $ord_p(\alpha) = n$. Άρα $\alpha = p^n\varepsilon$ με $\varepsilon \in \mathbb{Z}_p^*$. Τότε $p^n = \alpha\varepsilon^{-1} \in A \Rightarrow p^n\mathbb{Z}_p \subseteq A$. Δηλαδή τελικά $A = p^n\mathbb{Z}_p$. □

Λήμμα 1.3.13. *Το σύνολο $\mathbb{N}$ και συνεπώς και το $\mathbb{Z}$ είναι πυκνό στο $\mathbb{Z}_p$. Δηλαδή για κάθε $\alpha \in \mathbb{Z}_p$ υπάρχει ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ φυσικών αριθμών ώστε $\alpha = \lim_{n\to\infty} a_n$.*

Απόδειξη. Έστω $\alpha \in \mathbb{Z}_p$ με $\alpha \neq 0$. Τότε το α γράφεται $\alpha = \sum_{i=0}^{\infty} b_i p^i$ όπου $0 \leq b_i < p$. Για κάθε $n \in \mathbb{N}$ ορίζουμε $a_n = \sum_{i=0}^{n} b_i p^i \in \mathbb{N}$. Τότε $|\alpha - a_n|_p < \frac{1}{p^n}$ και άρα $\alpha = \lim_{n\to\infty} a_n$. Αν $\alpha = 0$ τότε $\alpha = \lim_{n\to\infty} p^n$. □

Πρόταση 1.3.14. *Για κάθε φυσικό αριθμό n ισχύει $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Απόδειξη. Τα μη μηδενικά ιδεώδη του δακτυλίου $\mathbb{Z}_p$ είναι τα κύρια ιδεώδη

$$p^n\mathbb{Z}_p = \{\alpha \in \mathbb{Z}_p : ord_p(\alpha) \geq 0\} = \{\alpha \in \mathbb{Z}_p : |\alpha|_p \leq p^{-n}\}$$

με $n \in \mathbb{N}$.
Για κάθε φυσικό αριθμό n θεωρούμε τον ομομορφισμό δακτυλίων

$$\varphi_n : \begin{cases} \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p \\ a \mapsto amodp^n\mathbb{Z}_p \end{cases}$$

Τότε $ker\varphi_n = \{a \in \mathbb{Z} : a \in p^n\mathbb{Z}_p\} = p^n\mathbb{Z}$. Επίσης ο φ_n είναι επιμορφισμός δακτυλίων διότι από το Λήμμα 1.3.13 για κάθε $\alpha \in \mathbb{Z}_p$ υπάρχει $a \in \mathbb{Z}$ ώστε $|\alpha - a|_p \leq \frac{1}{p^n} \Leftrightarrow ord_p(\alpha - a) \geq n$, το οποίο σημαίνει ότι $\alpha - a \in p^n\mathbb{Z}_p \Leftrightarrow a \equiv \alpha modp^n\mathbb{Z}_p$. Δηλαδή $\varphi_n(a) = \alpha modp^n\mathbb{Z}_p$. Συνεπώς $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ □

Από την παραπάνω πρόταση είναι προφανές ότι μπορούμε να ταυτίσουμε την κλάση ενός στοιχείου $\alpha \in \mathbb{Z}_p$ $modp^n\mathbb{Z}_p$ με την κλάση ενός ακεραίου $modp^n$.

Λήμμα 1.3.15. *Μια ακολουθία $\{x_n\}_{n\in\mathbb{N}}$ στοιχείων του $\mathbb{Q}_p$ είναι ακολουθία Cauchy αν και μόνο αν $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$.*

Απόδειξη. Έστω m, n φυσικοί αριθμοί με $m > n$. Τότε $m = n + r$ για κάποιο φυσικό αριθμό r. Τότε

$$\begin{aligned}|x_m - x_n|_p &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + ... + x_{n+1} - x_n|_p \\ &\leq max\{|x_{n+r} - x_{n+r-1}|_p, |x_{n+r-1} - x_{n+r-2}|_p, ..., |x_{n+1} - x_n|_p\}\end{aligned}$$

Τότε αν $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$ από την προηγούμενη σχέση έχουμε ότι για κάθε $\varepsilon > 0$ υπάρχει $n_0 \in \mathbb{N}$ ώστε $|x_m - x_n|_p < \varepsilon$ για κάθε $n, m \geq n_0$ και συνεπώς η ακολουθία $\{x_n\}_{n\in\mathbb{N}}$ είναι ακολουθία Cauchy. Η άλλη κατεύθυνση είναι προφανής. □

1.3.3 Το Λήμμα του Hensel

Χρήσιμο για τα επόμενα είναι το Λήμμα:

Λήμμα 1.3.16. *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. Το $f(X + Y) \in \mathbb{Z}_p[X, Y] = \mathbb{Z}_p[X][Y]$. Επομένως μπορούμε να γράψουμε το $f(X + Y)$ στην μορφή

$$f(X + Y) = a_0(X) + a_1(X)Y + ... + a_m(X)Y^m \qquad (1)$$

όπου $a_i(X) \in \mathbb{Z}_p[X]$ για $i = 0, 1, ..., m$.
Για $Y = 0$ από την (1) έχουμε $f(X) = a_0(X)$. Παραγωγίζοντας την σχέση (1) ως προς Y έχουμε

$$f'(X + Y) = a_1(X) + 2a_2(X)Y + ... + ma_m(X)Y^{m-1} \qquad (2)$$

οπότε για $Y = 0$ από την (2) έχουμε $f'(X) = a_1(X)$. Άρα από την (1) έχουμε

$$\begin{aligned}f(X + Y) &= f(X) + f'(X)Y + a_2(X)Y^2 + ... + a_m(X)Y^m \\ &= f(X) + f'(X)Y + Y^2(a_2(X) + ... + a_m(X)Y^{m-2})\end{aligned}$$

Οπότε αν θεωρήσουμε $g(X, Y) = a_2(X)+...+a_m(X)Y^{m-2} \in \mathbb{Z}_p[X, Y]$, έχουμε το ζητούμενο. □

Θεώρημα 1.3.17. *(Το Λήμμα του Hensel)*
Έστω $f(X) \in \mathbb{Z}_p[X]$. Έστω ότι υπάρχει $a_1 \in \mathbb{Z}_p$ ώστε
(1) $f(a_1) \equiv 0 mod p\mathbb{Z}_p$
(2) $f'(a_1) \not\equiv 0 mod p\mathbb{Z}_p$
Τότε υπάρχει μοναδικό $\alpha \in \mathbb{Z}_p$ τέτοιο ώστε $f(\alpha) = 0$ και $\alpha \equiv a_1 mod p\mathbb{Z}_p$.

Απόδειξη. Θα αποδείξουμε την ύπαρξη της ρίζας $\alpha \in \mathbb{Z}_p$ κατασκευάζοντας μια ακολουθία ακεραίων p-αδικών αριθμών με πρώτο όρο το a_1, η οποία συγκλίνει στο α. Συγκεκριμένα θα κατασκευάσουμε ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ ακεραίων p-αδικών αριθμών με τις εξής ιδιότητες:
(1) $f(a_n) \equiv 0 mod p^n\mathbb{Z}_p$
(2) $a_n \equiv a_{n+1} mod p^n\mathbb{Z}_p$
Από την υπόθεση (2) το a_2 θα έχει την μορφή $a_2 = a_1 + pb_1$ με $b_1 \in \mathbb{Z}_p$. Από το Λήμμα 1.3.16 για το $f(X)$ έχουμε $f(a_2) = f(a_1+pb_1) = f(a_1)+f'(a_1)pb_1+p^2R$ όπου $R \in \mathbb{Z}_p$. Άρα

$$f(a_2) = f(a_1 + pb_1) \equiv (f(a_1) + f'(a_1)pb_1) mod p^2\mathbb{Z}_p$$

Για να ισχύει η (1) πρέπει $f(a_2) \equiv 0 mod p^2\mathbb{Z}_p \Leftrightarrow$

$$(f(a_1) + f'(a_1)pb_1) \equiv 0 mod p^2\mathbb{Z}_p$$

Αφού $f(a_1) \equiv 0 mod p\mathbb{Z}_p$ έχουμε ότι $f(a_1) = py$ για κάποιο $y \in \mathbb{Z}_p$. Άρα έχουμε

$$\begin{gathered} py + f'(a_1)b_1p \equiv 0 mod p^2\mathbb{Z}_p \\ \Rightarrow y + f'(a_1)b_1 \equiv 0 mod p\mathbb{Z}_p \end{gathered}$$

Επειδή $f'(a_1) \not\equiv 0 mod p\mathbb{Z}_p$ το $f'(a_1)$ είναι μονάδα του $\mathbb{Z}_p$. Άρα η παραπάνω ισοτιμία γίνεται

$$b_1 \equiv -y(f'(a_1))^{-1} mod p\mathbb{Z}_p$$

Επομένως μπορούμε να επιλέξουμε το b_1 να είναι η λύση της παραπάνω ισοτιμίας με $0 < b_1 < p$ και έτσι για το $a_2 = a_1 + pb_1$ έχουμε $f(a_2) \equiv 0 mod p^2\mathbb{Z}_p$, $f'(a_2) \equiv f'(a_1) mod p\mathbb{Z}_p \not\equiv 0 mod p\mathbb{Z}_p$ και $a_2 \equiv a_1 mod p\mathbb{Z}_p$.
Εντελώς ανάλογα κατασκευάζουμε επαγωγικά το a_{n+1} από το a_n. Η ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ είναι ακολουθία Cauchy ακεραίων p-αδικών αριθμών διότι
$a_{n+1} \equiv a_n mod p^n\mathbb{Z}_p \Rightarrow |a_{n+1} - a_n|_p \leq \frac{1}{p^n}$. Έστω $\alpha \in \mathbb{Q}_p$ το όριο της $\{a_n\}_{n\in\mathbb{N}}$. Τότε υπάρχει $n_0 \in \mathbb{N}$ ώστε $|\alpha - a_{n_0}|_p < 1$ και άρα

$$|\alpha|_p \leq max\{|a_{n_0}|_p, |\alpha - a_{n_0}|_p\} \leq 1$$

δηλαδή $\alpha \in \mathbb{Z}_p$. Επίσης από την σχέση (1) έχουμε $a_{n+1} \equiv a_n mod p^n\mathbb{Z}_p$ για κάθε $n \in \mathbb{N}$. Συνεπώς για κάθε $m > n$ έχουμε $a_m \equiv a_n mod p^n\mathbb{Z}_p$, άρα $\alpha \equiv a_n mod p^n\mathbb{Z}_p$ κάθως $m \to \infty$. Για $n = 1$ έχουμε $\alpha \equiv a_1 mod p\mathbb{Z}_p$.

Για κάθε $n \in \mathbb{N}$ έχουμε $\alpha \equiv a_n mod p^n\mathbb{Z}_p$, άρα

$$f(\alpha) \equiv f(a_n) mod p^n\mathbb{Z}_p \equiv 0 mod p^n\mathbb{Z}_p$$

Δηλαδή $|f(\alpha)|_p \leq p^{-n}$ για κάθε $n \in \mathbb{N}$ και συνεπώς $f(\alpha) = 0$.

Απομένει να δείξουμε ότι το α είναι η μοναδική ρίζα του $f(X)$ στο $\mathbb{Z}_p$ για την οποία ισχύει $\alpha \equiv a_1 mod p\mathbb{Z}_p$. Έστω $\beta \in \mathbb{Z}_p$ ρίζα του $f(X)$ με $\beta \equiv a_1 mod p\mathbb{Z}_p$ και $\alpha \neq \beta$. Τότε $\alpha \equiv \beta mod p\mathbb{Z}_p$ και αφού $\alpha - \beta \neq 0$ έχουμε $\alpha - \beta = p^n\varepsilon$ για κάποιο $\varepsilon \in \mathbb{Z}_p^*$ και $n \in \mathbb{N}$, $n \geq 1$. Τότε, σύμφωνα με το Λήμμα 1.3.16, έχουμε:

$$f(\alpha) = f(\beta + p^n\varepsilon) = f(\beta) + f'(\beta)p^n\varepsilon + g(\beta, p^n\varepsilon)(p^n\varepsilon)^2$$

Αφού $f(\alpha) = f(\beta) = 0$ η παραπάνω σχέση γίνεται:

$$p^n\varepsilon(f'(\beta) + g(\beta, p^n\varepsilon)p^n\varepsilon) = 0$$

Δηλαδή $f'(\beta) = -g(\beta, p^n\varepsilon)p^n\varepsilon \equiv 0 mod p\mathbb{Z}_p$. Όμως αφού $\beta \equiv a_1 mod p\mathbb{Z}_p$ έχουμε $f'(\beta) \equiv f'(a_1) \not\equiv 0 mod p\mathbb{Z}_p$, το οποίο είναι άτοπο. □

Θεώρημα 1.3.18. *(Λήμμα Hensel ισχυρή μορφή)*
Έστω $f(X) \in \mathbb{Z}_p[X]$ και $a \in \mathbb{Z}_p$ ώστε $|f(a)|_p < |f'(a)|_p^2$. Τότε υπάρχει μοναδικό $\alpha \in \mathbb{Z}_p$ για το οποίο ισχύουν $f(\alpha) = 0$ και $|\alpha - a|_p < |f'(a)|_p$.

Απόδειξη. Έστω $b := \frac{f(a)}{f'(a)^2}$, τότε $|b|_p < 1$ και $f(a) = f'(a)^2 b$. Αν υπάρχει $\alpha \in \mathbb{Z}_p$, ώστε $0 < |\alpha - a|_p < |f'(a)|_p$ τότε $ord_p(\alpha - a) > ord_p(f'(a))$ και άρα $\alpha - a = p^{n_1}\varepsilon_1, f'(a) = p^{n_2}\varepsilon_2$ όπου $n_1, n_2 \in \mathbb{N}$ και $\varepsilon_1, \varepsilon_2 \in \mathbb{Z}_p^*$ με $n_1 > n_2$.Τότε

$$\begin{aligned} \alpha - a = p^{n_1}\varepsilon_1 = p^{n_1-n_2}p^{n_2}\varepsilon_1 = p^{n_1-n_2}f'(a)\varepsilon_2^{-1}\varepsilon_1 \\ \Rightarrow \alpha = a + f'(a)p^{n_1-n_2}\varepsilon_2^{-1}\varepsilon_1 \end{aligned}$$

Επομένως αν $\beta := p^{n_1-n_2}\varepsilon_2^{-1}\varepsilon_1$, έχουμε $\alpha = a + f'(a)\beta$ και $|\beta|_p < 1$ διότι $n_1 > n_2$.
Θα αναζητήσουμε $\beta \in \mathbb{Z}_p$ έτσι ώστε το $\alpha = a + f'(a)\beta$ να έχει τις ζητούμενες ιδιότητες. Για το $f(X) \in \mathbb{Z}_p[X]$ από το Λήμμα 1.3.16 έχουμε

$$f(X + Y) = f(X) + f'(X)Y + g(X, Y)Y^2$$

όπου $g(X, Y) \in \mathbb{Z}_p[X]$. Τότε

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

Θεωρούμε το πολυώνυμο $h(X) = b + X + g(a, f'(a)X)X^2 \in \mathbb{Z}_p[X]$. Τότε $h(0) = b$ και $|b|_p < 1 \Rightarrow b \in p\mathbb{Z}_p \Rightarrow b \equiv 0 mod p\mathbb{Z}_p$. Δηλαδή $h(0) \equiv 0 mod p\mathbb{Z}_p$ και $h'(0) = 1 \not\equiv 0 mod p\mathbb{Z}_p$. Άρα απο το λήμμα του Hensel υπάρχει μοναδικό $\beta \in \mathbb{Z}_p$ ώστε $h(\beta) = 0$ και $\beta \equiv 0 mod p\mathbb{Z}_p \Rightarrow |\beta|_p < 1$. Τότε για $\alpha = a + f'(a)\beta$ από την $(*)$ έχουμε $f(\alpha) = 0$ και $|\alpha - a|_p = |f'(a)\beta|_p = |f'(a)|_p|\beta|_p < |f'(a)|_p$. Η μοναδικότητα του α έπεται από την μοναδικότητα του β. □

Λήμμα 1.3.19. *Έστω $f(X) \in \mathbb{Z}_p[X]$, $x \in \mathbb{Z}_p$ ώστε $f(x) \equiv 0 mod p^n$, $ord_p(f'(x)) = k$ και $0 \leq 2k < n$. Τότε υπάρχει $y \in \mathbb{Z}_p$ ώστε*

$$f(y) \equiv 0 mod p^{n+1},\ ord_p(f'(y)) = k \text{ και } y \equiv x mod p^{n-k}.$$

Απόδειξη. Αφού $f(x) \equiv 0 mod p^n$ και $ord_p(f'(x)) = k$, έχουμε $f(x) = p^n b$ και $f'(x) = p^k c$ για κάποια $b \in \mathbb{Z}_p$ και $c \in \mathbb{Z}_p^*$. Τότε υπάρχει $z \in \mathbb{Z}_p$ ώστε $b + zc \equiv 0 mod p$. Έστω $y = x + p^{n-k}z$, τότε $y \equiv x mod p^{n-k}$ και από το Λήμμα 1.3.16 έχουμε

$$f(y) = f(x + p^{n-k}z) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a$$

για κάποιο $a \in \mathbb{Z}_p$. Άρα $f(y) = p^n(b + zc) + p^{2n-2k}a \equiv 0 mod p^{n+1}$ αφού $2n - 2k > n$. Εφαρμόζοντας ξανά το Λήμμα 1.3.16 έχουμε

$$f'(y) = f'(x + p^{n-k}z) \equiv f'(x) mod p^{n-k}$$

Δηλαδή $f'(y) \equiv p^k c mod p^{n-k}$ και αφού $n - k > k$ έχουμε ότι $ord_p(f'(y)) = k$. □

Θεώρημα 1.3.20. *Έστω $f(X_1, ..., X_m) \in \mathbb{Z}_p[X_1, ..., X_m]$, $x = (x_1, ..., x_m) \in \mathbb{Z}_p^m$, $n, k \in \mathbb{Z}$ με $0 < 2k < n$ και $j \in \mathbb{N}$ με $0 < j \leq m$. Έστω ότι ισχύουν*

$$f(x) \equiv 0 mod p^n \text{ και } ord_p(\tfrac{\partial f}{\partial x_j}(x)) = k$$

Τότε υπάρχει $y \in \mathbb{Z}_p^m$ με $f(y) = 0$ και $y \equiv x mod p^{n-k}$.

Απόδειξη. Έστω αρχικά ότι $m = 1$. Εφαρμόζοντας το Λήμμα 1.3.19 για το $x^{(0)} = x$ παίρνουμε $x^{(1)} \in \mathbb{Z}_p$ με $x^{(1)} \equiv x^{(0)} mod p^{n-k}$ ώστε $f(x^{(1)}) \equiv 0 mod p^{n+1}$ και $ord_p(f'(x^{(1)})) = k$.

Εφαρμόζουμε το ίδιο επιχείρημα στο $x^{(1)}$ αντικαθιστώντας το n με $n + 1$ και συνεχίζοντας επαγωγικά κατασκεύαζουμε ακολουθία

$$x^{(0)}, x^{(1)}, ..., x^{(q)}, ...$$

ώστε $x^{(q+1)} \equiv x^{(q)} mod p^{n+q-k}$ και $f(x^{(q)}) \equiv 0 mod p^{n+q}$. Η ακολουθία αυτή είναι ακολουθία Cauchy του $\mathbb{Z}_p$ και για κάθε $q \in \mathbb{N}$ ισχύει $x^{(q)} \equiv x mod p^{n-k}$. Έστω $y \in \mathbb{Z}_p$ το όριο της ακολουθίας, τότε για κάθε $q \in \mathbb{N}_0$ ισχύει $y \equiv x^{(q)} mod p^{n+q-k}$ και άρα $y \equiv x mod p^{n-k}$. Επιλέον για κάθε $q \in \mathbb{N}$ έχουμε

$$f(y) \equiv f(x^{(q)}) mod p^{n+q-k} \equiv 0 mod p^{n+q-k}$$

διότι $f(x^{(q)}) \equiv 0 mod p^{n+q}$. Δηλαδή $|f(y)|_p \leq p^{-(n+q-k)}$ για κάθε $q \in \mathbb{N}$ και άρα $f(y) = 0$.

Έστω τώρα $m > 1$. Θεωρούμε το πολυώνυμο $\tilde{f}(X) = f(x_1, x_2, ..., x_{j-1}, X, x_{j+1}, ..., x_m) \in \mathbb{Z}_p[X]$. Τότε $\tilde{f}(x_j) \equiv 0 mod p^n$ και $ord_p(\tilde{f}'(x_j)) = k$, οπότε σύμφωνα με την περίπτωση $m = 1$ υπάρχει $y_j \in \mathbb{Z}_p$ ώστε $y_j \equiv x_j mod p^{n-k}$ και $\tilde{f}(y_j) = 0$. Τότε για $y = (x_1, ..., x_{j-1}, y_j, x_{j+1}, ..., x_m)$ έχουμε το ζητούμενο. □

1.3.4 Η πολλαπλασιαστική ομάδα $\mathbb{Q}_p^*$ και η ομάδα $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$

Για την πολλαπλασιαστική ομάδα $\mathbb{Q}_p^*$ θεωρούμε την υποομάδα των τετραγώνων $\mathbb{Q}_p^{*2}$ του σώματος $\mathbb{Q}_p$ με $\mathbb{Q}_p^{*2} = \{\alpha^2 | \alpha \in \mathbb{Q}_p^*\}$. Επειδή η ομάδα $\mathbb{Q}_p^*$ είναι αβελιανή μπορούμε να θεωρήσουμε την ομάδα πηλίκο $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.
Αυτό που μας ενδιαφέρει είναι πότε ένα στοιχείο $\alpha \in \mathbb{Q}_p^*$ είναι τετράγωνο στην $\mathbb{Q}_p^*$ και τι μορφή έχει η ομάδα $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Η μελέτη αυτής της ομάδας θα μας είναι ιδιαίτερα χρήσιμη στα επόμενα.
Με βάση την Πρόταση 1.3.14 αν $\varepsilon \in \mathbb{Z}_p$ με $\varepsilon = \sum_{n=0}^{\infty} a_n p^n$ με $0 \leq a_n < p$, μπορούμε να ταυτίσουμε την κλάση $\varepsilon mod p\mathbb{Z}_p$ με την κλάση $a_0 mod p\mathbb{Z}$. Επομένως για $p \neq 2$ μπορούμε να ορίσουμε το σύμβολο του Legendre $(\frac{\varepsilon}{p}) := (\frac{a_0}{p})$.

Πρόταση 1.3.21. *Έστω $\alpha \in \mathbb{Q}_p^*$ με $\alpha = p^n \varepsilon$ όπου $n \in \mathbb{Z}, \varepsilon \in \mathbb{Z}_p^*$. Το α είναι τέλειο τετράγωνο στην $\mathbb{Q}_p^* \Leftrightarrow \begin{cases} 2|n \text{ και } (\frac{\varepsilon}{p}) = 1 \text{ αν } p \neq 2 \\ 2|n \text{ και } \varepsilon \equiv 1 mod 8 \text{ όταν } p = 2 \end{cases}$*

Απόδειξη. Η συνθήκη $2 \mid n$ είναι αναγκαία διότι $n = ord_p \alpha$. Έστω τώρα ότι $2 \mid n$, τότε το α είναι τέλειο τετράγωνο στην ομάδα $\mathbb{Q}_p^*$ αν και μόνο αν το ε είναι τέλειο τετράγωνο στην $\mathbb{Q}_p^*$. Δηλαδή $\varepsilon = \varepsilon_1^2$ με $\varepsilon_1 \in \mathbb{Q}_p^*$. Τότε $|\varepsilon_1|_p = 1$ και άρα $\varepsilon_1 \in \mathbb{Z}_p^*$.
Έστω $p \neq 2$. Αν $\varepsilon = \varepsilon_1^2$ τότε $(\frac{\varepsilon}{p}) = (\frac{\varepsilon_1}{p})^2 = 1$.
Αντίστροφα αν $(\frac{\varepsilon}{p}) = 1$, θεωρούμε το πολυώνυμο $f(X) = X^2 - \varepsilon \in \mathbb{Z}_p[X]$, για το οποίο υπάρχει $a \in \mathbb{Z}_p^*$ ώστε $f(a) \equiv 0 mod p\mathbb{Z}_p$. Επίσης

$$f'(a) = 2a \not\equiv 0 mod p\mathbb{Z}_p$$

αφού $p \neq 2$ και άρα απο το Λήμμα του Hensel, υπάρχει $\varepsilon_1 \in \mathbb{Z}_p$ με $f(\varepsilon_1) = 0$, δηλαδή $\varepsilon = \varepsilon_1^2$.
Έστω $p = 2$. Τότε αν $\varepsilon = \varepsilon_1^2$ με $\varepsilon_1 \in \mathbb{Z}_2^*$, έχουμε $\varepsilon_1 mod 8 \in \{1, 3, 5, 7\}$ και άρα $\varepsilon \equiv 1 mod 8$. Αντίστροφα αν $\varepsilon \equiv 1 mod 8$, για το $f(X) = X^2 - \varepsilon \in \mathbb{Z}_2[X]$ έχουμε $f(3) \equiv 0 mod 2^3\mathbb{Z}_2$ και άρα $|f(3)|_2 \leq \frac{1}{2^3} < \frac{1}{2^2} = |6|_2^2 = |f'(3)|_2^2$. Άρα από την ισχυρή μορφή του Λήμματος Hensel υπάρχει $\varepsilon_1 \in \mathbb{Z}_2$ ώστε $\varepsilon = \varepsilon_1^2$. □

Πρόταση 1.3.22. *Ο ρητός αριθμός $x \in \mathbb{Q}$ είναι τέλειο τετράγωνο ρητού αν και μόνο αν είναι τέλειο τετράγωνο στο $\mathbb{Q}_p$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$.*

Απόδειξη. Αν $x = 0$ δεν έχουμε τίποτα να αποδείξουμε. Έστω λοιπόν $x \in \mathbb{Q}^*$. Γράφουμε το x στην μορφή $x = \pm \prod_{p \in \mathbb{P}} p^{ord_p(x)}$. Αν το x είναι τέλειο τετράγωνο

στο $\mathbb{R}$ έπεται ότι $x > 0$. Στο $\mathbb{Q}_p$ το x γράφεται μονοσήμαντα στην μορφή $x = p^{ord_p(x)}u_p$ με $u_p \in \mathbb{Z}_p^*$. Άρα το x είναι τέλειο τετράγωνο στο $\mathbb{Q}_p$ αν και μόνο αν το $ord_p(x)$ είναι άρτιος και το u_p είναι τέλειο τετράγωνο στο $\mathbb{Q}_p$. Συνεπώς αν το x είναι τέλειο τετράγωνο στα $\mathbb{Q}_p$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$, τότε $x > 0$ και στην ανάλυσή του σε γινόμενο πρώτων παραγόντων όλοι οι εκθέτες είναι άρτιοι. Δηλαδη $x = (\prod_{p\in\mathbb{P}} p^{\frac{ord_p(x)}{2}})^2$, και άρα το x είναι τέλειο τετράγωνο στο $\mathbb{Q}$.
Προφανώς αν το x είναι τέλειο τετράγωνο στο $\mathbb{Q}$, τότε είναι τέλειο τετράγωνο σε όλα τα $\mathbb{Q}_p$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$. □

Παρατήρηση 1.3.23. *Αν $\varepsilon \in \mathbb{Z}_p^*$ με $\varepsilon \equiv 1 mod p^3\mathbb{Z}_p$, τότε το ε είναι τέλειο τετράγωνο στο $\mathbb{Z}_p$.*
Πράγματι αν $p = 2$ και $\varepsilon \equiv 1 mod 8\mathbb{Z}_2$ τότε το ε είναι τέλειο τετράγωνο στο $\mathbb{Z}_2$. Αν $p \neq 2$ και $\varepsilon \equiv 1 mod p^3\mathbb{Z}_p$ τότε $(\frac{\varepsilon}{p}) = (\frac{1}{p}) = 1$, δηλαδή το ε είναι τέλειο τετράγωνο στο $\mathbb{Z}_p$.

Πρόταση 1.3.24. *Για κάθε $x \in \mathbb{Q}_p^*$ υπάρχει $\varepsilon > 0$ ώστε αν $y \in \mathbb{Q}_p$ ισχύει $|y - x|_p < \varepsilon \Rightarrow \frac{y}{x} \in \mathbb{Q}_p^{*2}$.*

Απόδειξη. Έχουμε $x = p^n u$ όπου $n = ord_p(x)$ και $u \in \mathbb{Z}_p^*$. Έστω $\varepsilon := \frac{1}{p^{n+3}}$. Τότε αν $y \in \mathbb{Q}_p$ με $|y - x|_p < \varepsilon$, έχουμε $y - x = p^{n+3}z$ για κάποιο $z \in \mathbb{Z}_p$. Άρα:

$$\frac{y}{x} = \frac{x+p^{n+3}z}{x} = 1 + \frac{p^{n+3}z}{p^n u} = 1 + \frac{z}{u}p^3$$

Δηλαδή $\frac{y}{x} \equiv 1 mod p^3\mathbb{Z}_p$. Άρα $\frac{y}{x} \in \mathbb{Z}_p^*$ και σύμφωνα με την προηγούμενη παρατήρηση $\frac{y}{x} \in \mathbb{Q}_p^{*2}$. □

Πόρισμα 1.3.25. *Το σύνολο $\mathbb{Q}_p^{*2}$ είναι ανοιχτό υποσύνολο του τοπολογικού χώρου $\mathbb{Q}_p$.*

Απόδειξη. Έστω $x \in \mathbb{Q}_p^{*2}$. Απο την Πρόταση 1.3.24 υπάρχει $\varepsilon > 0$ ώστε για κάθε $y \in \mathbb{Q}_p$ με $|x - y|_p < \varepsilon$ να έχουμε $\frac{y}{x} \in \mathbb{Q}_p^{*2}$. Δηλαδή $y = xc^2$ με $c \in \mathbb{Q}_p^*$ και άρα $y \in \mathbb{Q}_p^{*2}$. □

Θεωρούμε τώρα τον ισομορφισμό ομάδων $\log_{-1} : (\{1, -1\}, \cdot) \to (\mathbb{Z}/2\mathbb{Z}, +)$ με $\begin{cases} 1 \mapsto \overline{0} \\ -1 \mapsto \overline{1} \end{cases}$

Πρόταση 1.3.26. *Για κάθε $p \in \mathbb{P}$, $p \neq 2$ η απεικόνιση* $\Phi_{\mathbb{F}_p} : \begin{cases} \mathbb{F}_p^*/\mathbb{F}_p^{*2} \to \mathbb{Z}/2\mathbb{Z} \\ x mod \mathbb{F}_p^{*2} \mapsto \log_{-1}(\frac{x}{p}) \end{cases}$
είναι ισομορφισμός ομάδων. Για $p = 2$ έχουμε $\mathbb{F}_2^*/\mathbb{F}_2^{*2} = \{1\}$

Απόδειξη. Επειδή $\mathbb{F}_2^* = \{1\}$, η περίπτωση $p = 2$ είναι τετριμμένη.
Έστω $p \geq 3$. Εξ'ορισμού της απεικόνισης $\log_{-1}(\frac{\cdot}{p}) : \mathbb{F}_p^* \to \mathbb{Z}/2\mathbb{Z}$, έχουμε $\mathbb{F}_p^{*2} \subseteq ker(\log_{-1}(\frac{\cdot}{p}))$. Επιπλέον τα μισά στοιχεία του $\mathbb{F}_p^*$ είναι τέλεια τετράγωνα και τα άλλα μισά όχι. Συνεπώς η απεικόνιση είναι επιμορφισμός και

$$\#\mathbb{F}_p^*/\mathbb{F}_p^{*2} = 2$$

Άρα η απεικόνιση $\Phi_{\mathbb{F}_p} : \mathbb{F}_p^*/\mathbb{F}_p^{*2} \to \mathbb{Z}/2\mathbb{Z}$ είναι ισομορφισμός ομάδων. □

Πρόταση 1.3.27. *Η απεικόνιση* $\Phi_{\mathbb{R}} : \begin{cases} \mathbb{R}^*/\mathbb{R}^{*2} \to \mathbb{Z}/2\mathbb{Z} \\ x \mapsto \log_{-1}(sgnx) \end{cases}$ *είναι ισομορφισμός ομάδων.*

Απόδειξη. Προφανής διότι το $x \in \mathbb{R}^*$ είναι τέλειο τετράγωνο $\Leftrightarrow sgnx = 1$. □

Παρατήρηση 1.3.28. *Όπως στο $\mathbb{F}_p$, ορίζουμε το σύμβολο του Legendre στο $\mathbb{R} = \mathbb{Q}_\infty$ ως* $\begin{cases} (\frac{\cdot}{\infty}) : \mathbb{R} \to \{-1, 0, 1\} \\ x \mapsto sgn(x) \end{cases}$.

Το επόμενο θεώρημα μας δείχνει ότι η ομάδα $\mathbb{Q}^*/\mathbb{Q}^{*2}$ είναι πολύ μεγαλύτερη.

Θεώρημα 1.3.29. *Η απεικόνιση* $\Phi_{\mathbb{Q}} : \begin{cases} \mathbb{Q}^*/\mathbb{Q}^{*2} \to \mathbb{Z}/2\mathbb{Z} \times (\bigoplus_{p\in\mathbb{P}} \mathbb{Z}/2\mathbb{Z}) \\ x\mathbb{Q}^{*2} \mapsto (\log_{-1}(sgnx), (ord_p x + 2\mathbb{Z})_{p\in\mathbb{P}}) \end{cases}$
είναι ισομορφισμός ομάδων.

Απόδειξη. Θεωρούμε την απεικόνιση $\tilde{\Phi}_{\mathbb{Q}} : \mathbb{Q}^* \to \mathbb{Z}/2\mathbb{Z} \times (\bigoplus_{p\in\mathbb{P}} \mathbb{Z}/2\mathbb{Z})$ με $\tilde{\Phi}_{\mathbb{Q}}(x) = (\log_{-1}(sgnx), (ord_p x + 2\mathbb{Z})_{p\in\mathbb{P}})$. Τότε αυτή είναι ομομορφισμός ομάδων. Επίσης αν $(i + 2\mathbb{Z}, (r_p + 2\mathbb{Z})_{p\in\mathbb{P}}) \in \mathbb{Z}/2\mathbb{Z} \times (\bigoplus_{p\in\mathbb{P}} \mathbb{Z}/2\mathbb{Z})$, τότε το $x = (-1)^i \prod_{p\in\mathbb{P}} p^{r_p} \in \mathbb{Q}^*$ απεικονίζεται στο $(i + 2\mathbb{Z}, (r_p + 2\mathbb{Z})_{p\in\mathbb{P}})$. Δηλαδή η $\tilde{\Phi}_{\mathbb{Q}}$ είναι επιμορφισμός. Προφανώς $\mathbb{Q}^{*2} \subseteq ker(\tilde{\Phi}_{\mathbb{Q}})$. Αν τώρα $x \in ker(\tilde{\Phi}_{\mathbb{Q}})$, τότε κατ'ανάγκη $x > 0$ και αν $x = \prod_{p\in\mathbb{P}} p^{r_p}$, πρέπει τα r_p ναι είναι όλα άρτιοι αριθμοί. Δηλαδή $x = (\prod_{p\in\mathbb{P}} p^{\frac{r_p}{2}})^2 \in \mathbb{Q}^{*2}$ και άρα $ker(\tilde{\Phi}_{\mathbb{Q}}) = \mathbb{Q}^{*2}$. □

Τα επόμενα δύο θεωρήματα μας δίνουν το ανάλογο αποτέλεσμα για τις ομάδες $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

Θεώρημα 1.3.30. *Αν $p \in \mathbb{P}$ με $p \neq 2$, ισχύει $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Αν $\varepsilon \in \mathbb{Z}_p^*$ με $(\frac{\varepsilon}{p}) = -1$ το σύνολο $\{1, \varepsilon, p, p\varepsilon\}$ είναι ένα πλήρες σύστημα αντιπροσώπων.*

Απόδειξη. Θεωρούμε την απεικόνιση $\tilde{\Phi}_{\mathbb{Q}_p} : \mathbb{Q}_p^* \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ώστε αν $x \in \mathbb{Q}_p^*$ με $x = p^n u$ για κάποιο $u \in \mathbb{Z}_p^*$, τότε $\tilde{\Phi}_{\mathbb{Q}_p}(x) = (\log_{-1}(\frac{u}{p}), n + 2\mathbb{Z})$. Η $\tilde{\Phi}_{\mathbb{Q}_p}$ είναι ομομορφισμός ομάδων. Μάλιστα είναι επιμορφισμός διότι αν $\varepsilon \in \mathbb{Z}_p^*$ με $(\frac{\varepsilon}{p}) = -1$, τότε $\tilde{\Phi}_{\mathbb{Q}_p}(1) = (\overline{0}, \overline{0}), \tilde{\Phi}_{\mathbb{Q}_p}(p) = (\overline{0}, \overline{1}), \tilde{\Phi}_{\mathbb{Q}_p}(p\varepsilon) = (\overline{1}, \overline{1}), \tilde{\Phi}_{\mathbb{Q}_p}(\varepsilon) = (\overline{1}, \overline{0})$. Ισχύει $\mathbb{Q}_p^{*2} \subseteq ker(\tilde{\Phi}_{\mathbb{Q}_p})$. Θα αποδείξουμε την ισότητα. Έστω

$$x = p^n u \in ker(\tilde{\Phi}_{\mathbb{Q}_p})$$

Αυτό σημαίνει ότι $2 \mid n$ και $(\frac{u}{p}) = 1$. Άρα από την Πρόταση 1.3.21 $x \in \mathbb{Q}_p^{*2}$. □

Θεώρημα 1.3.31. *Η απεικόνιση $\Phi_2 : \begin{cases} \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \to U_8 \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ 2^n\varepsilon\mathbb{Q}_2^{*2} \mapsto (\varepsilon mod 8, n + 2\mathbb{Z}), \varepsilon \in \mathbb{Z}_2^* \end{cases}$ είναι ισομορφισμός ομάδων και το $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ είναι ένα πλήρες σύστημα αντιπροσώπων της $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$.*

Απόδειξη. Η απεικόνιση $\tilde{\Phi}_2 : \mathbb{Q}_2^* \to U_8 \times \mathbb{Z}/2\mathbb{Z}$ με $\tilde{\Phi}_2(2^n\varepsilon) = (\varepsilon mod 8, n + 2\mathbb{Z})$, όπου $\varepsilon \in \mathbb{Z}_2^*$, είναι επιμορφισμός. Επίσης το $2^n\varepsilon$ είναι τέλειο τετράγωνο στο $\mathbb{Q}_2^*$ αν και μόνο αν $2 \mid n$ και $\varepsilon \equiv 1 mod 8$, δηλαδή αν και μόνο αν $2^n\varepsilon \in \ker(\tilde{\Phi}_2)$. Άρα $ker(\tilde{\Phi}_2) = \mathbb{Q}_2^{*2}$ και συνεπώς η Φ_2 είναι ισομορφισμός. □

Χρήσιμο είναι και το Θεώρημα

Θεώρημα 1.3.32. *Έστω $p \neq 2$, $\varepsilon \in \mathbb{Z}_p^*$. Το ε είναι p-οστή δύναμη στο $\mathbb{Q}_p$ αν και μόνο αν είναι p-οστή δύναμη $mod p^2\mathbb{Z}_p$.*

Απόδειξη. Αν $\varepsilon = \varepsilon_1^p$ για κάποιο $\varepsilon_1 \in \mathbb{Q}_p$, τότε $|\varepsilon_1|_p^p = |\varepsilon_1^p|_p = |\varepsilon|_p = 1$, δηλαδή $|\varepsilon_1|_p = 1$ και άρα $\varepsilon_1 \in \mathbb{Z}_p^*$. Άρα αν το ε είναι p-οστή δύναμη στο $\mathbb{Q}_p$ τότε προφανώς είναι p-οστή δύναμη $mod p^2\mathbb{Z}_p$.
Αρκεί να περιοριστούμε σε p-οστές ρίζες του ε στην ομάδα $\mathbb{Z}_p^*$.

Θεωρούμε το πολυώνυμο $f(X) = X^p - \varepsilon$ και θα προσπαθήσουμε να εφαρμόσουμε το ισχυρό Λήμμα του Hensel. Έστω $\alpha \in \mathbb{Z}_p^*$ ώστε $|f(\alpha)|_p < |f'(\alpha)|_p^2$, δηλαδή $|\alpha^p - \varepsilon|_p < |p\alpha^{p-1}|_p^2 = |p|_p^2|\alpha^{p-1}|_p^2 = \frac{1}{p^2}$. Δηλαδή

$$|\alpha^p - \varepsilon| \leq \frac{1}{p^3} \Rightarrow \alpha^p \equiv \varepsilon mod p^3\mathbb{Z}_p$$

Συνεπώς αν το ε είναι p-οστή δύναμη $modp^3\mathbb{Z}_p$, τότε από το ισχυρό Λήμμα του Hensel 1.3.18, το ε είναι p-οστή δύναμη στο $\mathbb{Z}_p$.
Υποθέτουμε τώρα ότι $\varepsilon \equiv \alpha^p modp^2\mathbb{Z}_p$ για κάποιο $\alpha \in \mathbb{Z}_p$. Τότε το α είναι μονάδα του $\mathbb{Z}_p$ διότι αν $\alpha \in p\mathbb{Z}_p$ κατ'ανάγκην και το $\varepsilon \in p\mathbb{Z}_p$. Τότε

$$\frac{\varepsilon}{\alpha^p} \equiv 1 modp^2\mathbb{Z}_p$$

και άρα

$$\frac{\varepsilon}{\alpha^p} \equiv (1+p^2\beta) modp^3\mathbb{Z}_p$$

για κάποιο β με $0 \leq \beta \leq p-1$.

Έχουμε $(1+p\beta)^p = 1 + p(p\beta) + \sum_{k=2}^{p} \binom{p}{k}(p\beta)^k$. Για $k \geq 3$ οι όροι του αθροίσματος διαιρούνται με p^3. Για $k=2$ έχουμε $\binom{p}{2}(p\beta)^2 = \frac{p-1}{2}p^3\beta^2$ που διαιρείται επίσης με p^3. Άρα έχουμε

$$(1+p\beta)^p \equiv (1+p^2\beta) modp^3\mathbb{Z}_p$$

Επομένως $\frac{\varepsilon}{\alpha^p} \equiv (1+p\beta)^p modp^3\mathbb{Z}_p \Rightarrow \varepsilon \equiv \alpha^p(1+p\beta)^p modp^3\mathbb{Z}_p$. Συνεπώς το ε είναι p-οστή δύναμη $modp^3\mathbb{Z}_p$ και άρα το ε είναι p-οστή δύναμη στο $\mathbb{Z}_p$. □

Παρατήρηση 1.3.33. *Αν εφαρμόσουμε το προηγούμενο Θεώρημα για τον πρώτο $p=3$ έχουμε ότι η $\varepsilon \in \mathbb{Z}_3^*$ είναι κύβος στο $\mathbb{Q}_3$ αν και μόνο αν*

$$\varepsilon \equiv (a_0 + a_1 3)^3 mod3^2\mathbb{Z}_3 \equiv a_0^3 mod3^2\mathbb{Z}_3$$

όμως $a_0 \in \{1,2\}$ και άρα το ε είναι κύβος στο $\mathbb{Q}_3$ αν και μόνο αν

$$\varepsilon \equiv \pm 1 mod3^2\mathbb{Z}_3$$

.

Θεώρημα 1.3.34. *(Θεώρημα της σύγχρονης προσέγγισης)*
Έστω $v_1, v_2, \ldots, v_n \in P = \mathbb{P} \cup \{\infty\}$ πεπερασμένου πλήθους και διακεκριμένα, και έστω ότι για κάθε $i = 1,2,\ldots,n$ έχουμε $x_i \in \mathbb{Q}_{v_i}$. Τότε υπάρχει ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ ρητών αριθμών ώστε για κάθε $i=1,2,\ldots,n$ η ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ συγκλίνει στο $x_i \in \mathbb{Q}_{v_i}$.

Απόδειξη. Έστω $S = \{v_1, v_2, \ldots, v_n\}$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι το S περιέχει το ∞. Έστω $p_1, p_2, \ldots, p_n$ διαφορετικοί μεταξύ τους πρώτοι αριθμοί, $x_i \in \mathbb{Q}_{p_i}$ αυθαίρετα δοσμένα στοιχεία και $x_\infty \in \mathbb{R}$. Θα αποδείξουμε ότι υπάρχει ακολουθία $\{a_n\}_{n\in\mathbb{N}}$ ρητων αριθμών η οποία συγκλίνει συγχρόνως στα x_i για $i=1,2,\ldots,n$ και στο x_∞.

Πολλαπλασιάζουμε τα x_i, $i = 1, 2, \ldots, n$ με κατάλληλο φυσικό αριθμό ώστε να μπορούμε να υποθέσουμε ότι $x_i \in \mathbb{Z}_{p_i}$, για κάθε $i = 1, 2, \ldots, n$.
Αρκεί να αποδείξουμε ότι για οποιοδήποτε $N \in \mathbb{N}$ και οποιοδήποτε $\varepsilon > 0$ υπάρχει $x \in \mathbb{Q}$ ώστε $|x - x_\infty| < \varepsilon$ και $ord_{p_i}(x - x_i) \geq N$.
Θεωρούμε το σύστημα των ισοτιμιών:

$$x \equiv x_i mod p_i^N,\ i = 1, 2, \ldots, n$$

Το σύστημα αυτό έχει μία λύση $x_0 \in \mathbb{Z}$, η οποία είναι μοναδική $modm$, όπου $m = \prod_{i=1}^n p_i^N$. Τότε $ord_{p_i}(x_0 - x_i) \geq N$ για κάθε $i = 1, 2, \ldots, n$.
Επιλέγουμε $r \in \mathbb{N}$ ώστε $(m, r) = 1$ και $|\frac{m}{r}| < \varepsilon$. Τότε υπάρχει ακέραιος αριθμός a ώστε $|x_0 - x_\infty - \frac{m}{r}a| < \varepsilon$. Πράγματι αν $z := x_0 - x_\infty$ έχουμε:

$$|z - a\tfrac{m}{r}| < \varepsilon \Leftrightarrow -\varepsilon < z - a\tfrac{m}{r} < \varepsilon \Leftrightarrow \tfrac{r}{m}(z - \varepsilon) < a < \tfrac{r}{m}(z + \varepsilon)$$

Συνεπώς υπάρχει τέτοιος ακέραιος a αν και μόνο αν $\frac{r}{m}(z + \varepsilon) - \frac{r}{m}(z - \varepsilon) > 1 \Leftrightarrow 2\varepsilon\frac{r}{m} > 1 \Leftrightarrow \frac{m}{r} < 2\varepsilon$, που ισχύει.
Τότε για $x = x_0 - \frac{m}{r}a$ έχουμε $x \in \mathbb{Q}$, $|x - x_\infty| < \varepsilon$ και

$$ord_{p_i}(x - x_i) = ord_{p_i}(x_0 - x_i - a\tfrac{m}{r}) \geq min\{ord_{p_i}(x_0 - x_i), ord_{p_i}(a\tfrac{m}{r})\} \geq N$$

καθώς $ord_{p_i}(a\frac{m}{r}) \geq N$ διότι $m = \prod_{i=1}^n p_i^N$, $(r, m) = 1$ και $a \in \mathbb{Z}$. □

Πόρισμα 1.3.35. *Έστω $\upsilon_1, \upsilon_2, \ldots, \upsilon_n \in P = \mathbb{P} \cup \{\infty\}$ πεπερασμένου πλήθους και διακεκριμένα, τότε η φυσική απεικόνιση*

$$\mathbb{Q}^* \to \prod_{i=1}^n \mathbb{Q}^*_{\upsilon_i} / \mathbb{Q}^{*2}_{\upsilon_i}$$
$$x \mapsto (x mod \mathbb{Q}^{*2}_{\upsilon_1}, \ldots, x mod \mathbb{Q}^{*2}_{\upsilon_n})$$

είναι επί. Δηλαδή για οποιεσδήποτε κλάσεις $x_i mod \mathbb{Q}^{*2}_{\upsilon_i}$, $i = 1, 2, \ldots, n$, υπάρχει $x \in \mathbb{Q}^*$ ώστε $x \equiv x_i mod \mathbb{Q}^{*2}_{\upsilon_i}$ για κάθε $i = 1, 2, \ldots, n$.

Απόδειξη. Σύμφωνα με το προηγούμενο Θεώρημα για τα αυθαίρετα δοσμένα $x_i \in \mathbb{Q}^*_{\upsilon_i}$ και για κάθε $\varepsilon > 0$ υπάρχει $x \in \mathbb{Q}^*$ ώστε $|x - x_i|_{\upsilon_i} < \varepsilon$. Για κατάλληλα μικρό ε από την Πρόταση 1.3.24 έχουμε ότι $\frac{x}{x_i} \in \mathbb{Q}^{*2}_{\upsilon_i}$ για κάθε $i = 1, 2, \ldots, n$.
Άρα $x\mathbb{Q}^{*2}_{\upsilon_i} = x_i\mathbb{Q}^{*2}_{\upsilon_i}$ για κάθε $i = 1, 2, \ldots, n$. □

1.4 Το σύμβολο του Hilbert

Έστω $P(x, y, z) \in \mathbb{Q}[x, y, z]$ πολυώνυμο τριών μεταβλητών με συντελεστές στο $\mathbb{Q}$. Θεωρούμε την εξίσωση

$$P(x, y, z) = 0 \qquad (1)$$

Αν υπάρχει $(a,b,c) \in \mathbb{Q}^3$ ώστε $P(a,b,c) = 0$ τότε λέμε ότι το (a,b,c) είναι μια ρητή λύση της εξίσωσης.
Αν K σώμα με $\mathbb{Q} \leq K$ τότε κάθε λύση $(a,b,c) \in K^3$ της (1) θα λέγεται K-ρητή λύση. Είναι προφανές ότι αν η (1) έχει μία ρητή λύση τότε θα έχει και μία K-ρητή λύση για κάθε επέκταση K του $\mathbb{Q}$. Συνεπώς αν έχει ρητή λύση, αυτή θα είναι και $\mathbb{Q}_p$-λύση για κάθε $p \in \mathbb{P} \cup \{\infty\}$.

Ορισμός 1.4.1. Μία λύση της (1) σε κάποιο $\mathbb{Q}_p$, $p \in \mathbb{P} \cup \{\infty\}$ θα λέγεται τοπική λύση (local solution), ενώ μία λύση της στο $\mathbb{Q}$ θα λέγεται γενική λύση (global solution).

Το ερώτημα που θα μας απασχολήσει είναι αν ισχύει και το αντίστροφο, δηλάδη αν η (1) έχει λύση στο $\mathbb{Q}_p$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$, μπορούμε να συμπεράνουμε ότι θα έχει λύση στο $\mathbb{Q}$;
Σύμφωνα με την Πρόταση 1.3.22 για κάθε $a \in \mathbb{Q}$ η εξίσωση $x^2 - a = 0$ έχει λύση στο $\mathbb{Q}$ αν και μόνο έχει λύση στο $\mathbb{Q}_p$ για κάθε $p \in \mathbb{P} \cup \{\infty\}$.

Στη συνέχεια θα ελέγξουμε την επιλυσιμότητα της διοφαντικής εξίσωσης $ax^2 + by^2 = z^2$ $(*)$ στα σώματα $\mathbb{Q}_p$.

Ορισμός 1.4.2. (Το σύμβολο του Hilbert)
Έστω $p \in \mathbb{P} \cup \{\infty\}$ και $a, b \in \mathbb{Q}_p^*$. Ορίζουμε το σύμβολο του Hilbert $(\frac{a,b}{p}) \in \{1, -1\}$, με $(\frac{a,b}{p}) = 1$ αν και μόνο αν η εξίσωση $(*)$ έχει λύση $(x,y,z) \in \mathbb{Q}_p^3 \setminus \{(0,0,0)\}$.

1.4.1 Το σύμβολο του Hilbert στο $\mathbb{R} = \mathbb{Q}_\infty$

Πρόταση 1.4.3. *Έστω $a, b \in \mathbb{R}^*$ τότε $(\frac{a,b}{\infty}) = 1$ αν και μόνο αν $a > 0$ ή $b > 0$.*

Απόδειξη. Αν $a > 0$ τότε $a \cdot 1^2 + b \cdot 0^2 = \sqrt{a}^2$. Δηλαδή η εξίσωση $(*)$ έχει λύση και άρα $(\frac{a,b}{\infty}) = 1$. Ανάλογα αν $b > 0$.
Έστω τώρα ότι $a < 0$ και $b < 0$. Τότε για κάθε $(x,y) \neq (0,0)$, $ax^2 + by^2 < 0$ και άρα η $(*)$ δεν έχει λύση. Συνεπώς $(\frac{a,b}{\infty}) = -1$. □

1.4.2 Το σύμβολο του Hilbert στο $\mathbb{Q}_p$, $p \in \mathbb{P}$

Πρόταση 1.4.4. *Αν $p \in \mathbb{P}$ και $a, b, c, d \in \mathbb{Q}_p^*$ ισχύουν:*
(1) $(\frac{a,b}{p}) = (\frac{b,a}{p})$
(2) $(\frac{a,1}{p}) = (\frac{a,-a}{p}) = 1$

(3) $(\frac{a,1-a}{p}) = 1$ *για* $a \neq 1$
(4) $(\frac{a,b}{p}) = (\frac{ac^2,bd^2}{p})$
(5) $(\frac{ab,ac}{p}) = (\frac{ab,-bc}{p})$
(6) Αν $(\frac{a,c}{p}) = 1$ *τότε* $(\frac{a,b}{p}) = (\frac{a,bc}{p})$

Απόδειξη. Το (1) είναι άμεση συνέπεια του ορισμού. Δηλαδή το σύμβολο του Hilbert είναι συμμετρικό. Τα (2) και (3)προκύπτουν από τις σχέσεις:

$$a \cdot 0^2 + 1 \cdot 1^2 = 1^2, a \cdot 1^2 + (-a) \cdot 1^2 = 0^2 \text{ και } a \cdot 1^2 + (1-a) \cdot 1^2 = 1^2$$

Για το (4) παρατηρούμε ότι η εξίσωση $ac^2X^2 + bd^2Y^2 = a(cX)^2 + b(dY)^2 = Z^2$ με αλλαγή μεταβλητών $X_1 = cX, Y_1 = dY$ γίνεται $aX_1 + bY_1 = Z^2$. Άρα κάθε λύση της μιας εξίσωσης μπορεί να μετατραπεί σε λύση της άλλης.
Για το (5) θα δείξουμε ότι για κάθε λύση της $abX^2 + acY^2 = Z^2$ μπορούμε να πάρουμε μια λύση της $abX^2 - bcY^2 = Z^2$ και αντίστροφα. Έχουμε :

$$\begin{gathered} abx^2 + acy^2 = z^2 \Rightarrow -a^2b^2x^2 - a^2bcy^2 = -abz^2 \\ \Rightarrow abz^2 - bc(ay)^2 = (abx)^2 \end{gathered}$$

και

$$\begin{gathered} abx^2 - bcy^2 = z^2 \Rightarrow a^2b^2x^2 - ab^2cy^2 = abz^2 \\ \Rightarrow abz^2 + ac(by)^2 = (abx)^2 \end{gathered}$$

Το σύμβολο του Hilbert παίρνει μόνο δύο τιμές, τις $+1$ και -1. Άρα για το (6) αρκεί να αποδείξουμε ότι

$$(\tfrac{a,b}{p}) = 1 \Leftrightarrow (\tfrac{a,bc}{p}) = 1$$

Εξ'υποθέσεως $(\frac{a,c}{p}) = 1$. Άρα υπάρχει $(x_1, y_1, z_1) \neq (0,0,0)$ ώστε

$$ax_1^2 + cy_1^2 = z_1^2 \qquad (*)$$

Ας υποθέσουμε τώρα ότι και $(\frac{a,b}{p}) = 1$. Επομένως υπάρχει $(x, y, z) \neq (0,0,0)$ ώστε

$$ax^2 + by^2 = z^2 \qquad (**)$$

Αν $y = 0$ ή $y_1 = 0$ τότε προφανώς η εξίσωση $aX^2 + bcY^2 = Z^2$ έχει λύση.
Αν $y, y_1 \neq 0$ τότε η $(xz_1 + x_1z, 1, zz_1 + axx_1)$ είναι μη τετριμμένη λύση της εξίσωσης $aX^2 + bcY^2 = Z^2$. Πράγματι, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $y = y_1 = 1$ (διαφορετικά διαιρούμε τις σχέσεις $(*)$ και $(**)$ με y_1^2 και y^2 αντίστοιχα). Επομένως $b = z^2 - ax^2$ και $c = z_1^2 - ax_1^2$. Τότε στο σώμα $\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p + \mathbb{Q}_p\sqrt{a}$, έχουμε:

$$\begin{aligned} bc &= (z^2 - ax^2)(z_1^2 - ax_1^2) \\ &= (z + \sqrt{a}x)(z_1 + \sqrt{a}x_1)(z - \sqrt{a}x)(z_1 - \sqrt{a}x_1) \\ &= ((zz_1 + axx_1) + \sqrt{a}(xz_1 + x_1z))((zz_1 + axx_1) - \sqrt{a}(xz_1 + x_1z)) \\ &= (zz_1 + axx_1)^2 - a(xz_1 + x_1z)^2 \end{aligned}$$

Άρα $a(xz_1 + x_1z)^2 + bc1^2 = (zz_1 + axx_1)^2 \Rightarrow (\frac{a,bc}{p}) = 1$.
Αν τώρα $(\frac{a,bc}{p}) = 1$, εφαρμόζοντας την παραπάνω διαδικασία για το σύμβολο $(\frac{a,bc}{p})$, έχουμε $(\frac{a,(bc)c}{p}) = 1$. Όμως $(\frac{a,(bc)c}{p}) = (\frac{a,bc^2}{p}) = (\frac{a,b}{p})$. Δηλαδή

$$(\frac{a,b}{p}) = 1$$

□

Πρόταση 1.4.5. *Έστω $p \in \mathbb{P}$, με $p \neq 2$, $m, n \in \mathbb{Z}$ και $u, v \in \mathbb{Z}_p^*$. Τότε ισχύουν τα εξής:*
(1) $(\frac{u,v}{p}) = 1$
(2) $(\frac{u,vp}{p}) = (\frac{vp,u}{p}) = (\frac{u}{p})$ *και*
(3) $(\frac{up,vp}{p}) = (\frac{-uv}{p})$
Ισοδύναμα σε κλειστή μορφή έχουμε:

$$(\tfrac{up^n,vp^m}{p}) = (-1)^{mn\frac{p-1}{2}}(\tfrac{u}{p})^m(\tfrac{v}{p})^n$$

ή σε μορφή πινάκων

$p \equiv 1 mod 4$

	1	*ε*	*p*	*εp*
1	*+1*	*+1*	*+1*	*+1*
ε	*+1*	*+1*	*-1*	*-1*
p	*+1*	*-1*	*+1*	*-1*
εp	*+1*	*-1*	*-1*	*+1*

$p \equiv 3 mod 4$

	1	*ε*	*p*	*εp*
1	*+1*	*+1*	*+1*	*+1*
ε	*+1*	*+1*	*-1*	*-1*
p	*+1*	*-1*	*-1*	*+1*
εp	*+1*	*-1*	*+1*	*-1*

όπου το $\{1, \varepsilon, p, \varepsilon p\}$ είναι ένα σύστημα αντιπροσώπων της ομάδας $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

Απόδειξη. Δείχνουμε πρώτα ότι $(\frac{u,v}{p}) = 1$. Ψάχνουμε δηλαδή μια λύση $(x, y, z) \neq (0, 0, 0)$, της εξίσωσης $uX^2 + vY^2 = Z^2$. Περιοριζόμαστε σε λύσεις με $y = 1$, αναζητώντας αρχικά λύσεις στο $\mathbb{F}_p$.
Θεωρούμε τα ακόλουθα υποσύνολα του $\mathbb{F}_p$:

$$M_1 = \{u\overline{x}^2 + v mod p \mid \overline{x} \in \mathbb{F}_p\} \subseteq \mathbb{F}_p$$
$$M_2 = \{\overline{z}^2 mod p \mid \overline{z} \in \mathbb{F}_p\} \subseteq \mathbb{F}_p$$

Γνωρίζουμε ότι $\#\mathbb{F}_p^{*2} = \frac{p-1}{2}$ και άρα $\#M_1 = \#M_2 = 1 + \#\mathbb{F}_p^{*2} = \frac{p+1}{2}$. Άρα $\#M_1 + \#M_2 = p + 1 > p = \#\mathbb{F}_p$. Αυτό σημαίνει ότι τα M_1 και M_2 έχουν κάποιο κοινό στοιχείο $w \in \mathbb{F}_p$.
Άρα υπάρχουν $\overline{x}, \overline{z} \in \mathbb{F}_p$ με $u\overline{x}^2 + vmodp = w = \overline{z}^2 modp$, όπου τα $\overline{x}, \overline{z}$ δεν μπορούν να είναι και τα δύο μηδέν. Παίρνουμε $\overline{x} \neq 0$, διαφορετικά χρησιμοποιούμε το ίδιο επιχείρημα εναλλάσσοντας τους ρόλους των $\overline{x}$ και $\overline{z}$.
Για το $\overline{z}$ επιλέγουμε οποιαδήποτε επέκταση του, z στο $\mathbb{Z}_p$. Βρίσκουμε επέκταση $x \in \mathbb{Z}_p$ για το $\overline{x}$, χρησιμοποιώντας το Λήμμα του Hensel.

Πράγματι για το πολυώνυμο $f(X) = uX^2 + v - z^2 \in \mathbb{Z}_p[X]$, έχουμε $f(\overline{x}) \equiv 0 modp$ και $f'(\overline{x}) \not\equiv 0 modp$. Άρα υπάρχει $x \in \mathbb{Z}_p$ ώστε $ux^2 + v = z^2 \Rightarrow (\frac{u,v}{p}) = 1$.

Δείχνουμε τώρα ότι $(\frac{u,vp}{p}) = (\frac{u}{p})$.
Έστω ότι υπάρχει μια μη τετριμμένη λύση (x, y, z) της εξίσωσης

$$uX^2 + vpY^2 = Z^2$$

Αν πολλαπλασιάσουμε τα x, y, z με τον ίδιο αριθμό παίρνουμε μια επιπλέον λύση. Μπορούμε επομένως να πολλαπλασιάσουμε τα x, y, z με κατάλληλη δύναμη του p, ώστε τα $x, y, z \in \mathbb{Z}_p$ και κάποιο από αυτά να ανήκει στο $\mathbb{Z}_p^*$.

Θα δείξουμε ότι $x \in \mathbb{Z}_p^*$. Έστω $x \in p\mathbb{Z}_p$, τότε το x^2 ανήκει στο $p^2\mathbb{Z}_p$ δηλαδή το $z^2 - vpy^2 \in p^2\mathbb{Z}_p$. Άρα έχουμε $z^2 - vpy^2 \in p\mathbb{Z}_p \Rightarrow z^2 \in p\mathbb{Z}_p \Rightarrow z \in p\mathbb{Z}_p \Rightarrow z^2 \in p^2\mathbb{Z}_p \Rightarrow vpy^2 \in p^2\mathbb{Z}_p \Rightarrow y^2 \in p\mathbb{Z}_p \Rightarrow y \in p\mathbb{Z}_p$. Τότε όμως $x, y, z \in p\mathbb{Z}_p$ το οποίο είναι άτοπο.

Από τη σχέση $ux^2 + vpy^2 = z^2$, έχουμε $ux^2 \equiv z^2 modp$ και $ux^2 \not\equiv 0 modp$. Άρα $z^2 \not\equiv 0 modp$ και συνεπώς $z \in \mathbb{Z}_p^*$. Δηλαδή $u \equiv (\frac{z}{x})^2 modp$, και άρα το u είναι τετραγωνικό υπόλοιπο $modp \Rightarrow (\frac{u}{p}) = 1$.

Έστω τώρα $(\frac{u}{p}) = 1$, δηλαδή το u είναι τετραγωνικό υπόλοιπο $modp$. Άρα μπορούμε να βρούμε $\overline{z} \in \mathbb{F}_p$ με $u \equiv \overline{z}^2 modp$. Τότε για το πολυώνυμο $f(X) = X^2 - u \in \mathbb{Z}_p[X]$, έχουμε $f(\overline{z}) \equiv 0 modp$ και $f'(\overline{z}) = 2\overline{z} \not\equiv 0 modp$. Άρα από το Λήμμα του Hensel το $\overline{z}$ επεκτείνεται σε $z \in \mathbb{Z}_p$ ώστε $z^2 = u$. Ισοδύναμα $u \cdot 1^2 + vp \cdot 0^2 = z^2 \Rightarrow (\frac{u,vp}{p}) = 1$.
Δηλαδή δείξαμε ότι $(\frac{u,vp}{p}) = 1 \Leftrightarrow (\frac{u}{p}) = 1 \Rightarrow (\frac{u,vp}{p}) = (\frac{u}{p})$.

Δείχνουμε τώρα ότι $(\frac{up,vp}{p}) = (\frac{-vp}{p})$.
Από την Πρόταση 1.4.4, έχουμε

$$(\tfrac{up,vp}{p}) = (\tfrac{up,-uv}{p}) = (\tfrac{-uv}{p})$$

όπου η τελευταία ισότητα προκύπτει από την προηγούμενη απόδειξη.

Η κλειστή μορφή για το σύμβολο του Hilbert και οι πίνακες επαληθεύονται εύκολα χρησιμοποιώντας την σχέση $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. □

Πρόταση 1.4.6. *Αν* $u2^n, v2^m \in \mathbb{Q}_2^*$ *με* $u, v \in \mathbb{Z}_2^*$, *τότε ισχύει:*

$$(\tfrac{u2^n, v2^m}{2}) = (-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2}}(-1)^{n\frac{v^2-1}{8}}(-1)^{m\frac{u^2-1}{8}}$$

όπου οι ποσότητες $\frac{u-1}{2}, \frac{v-1}{2}, \frac{v^2-1}{8}, \frac{u^2-1}{8}$ *θεωρούνται modulo* 2. *Χρησιμοποιώντας το πλήρες σύστημα αντιπρωσώπων* $\{\pm1, \pm5, \pm2, \pm10\}$ *της* $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, *η παραπάνω σχέση εκφράζεται ισοδύναμα σε μορφή πίνακα ως:*

	1	*-1*	*5*	*-5*	*2*	*-2*	*10*	*-10*
1	*+1*	*+1*	*+1*	*+1*	*+1*	*+1*	*+1*	*+1*
-1	*+1*	*-1*	*+1*	*-1*	*+1*	*-1*	*+1*	*-1*
5	*+1*	*+1*	*+1*	*+1*	*-1*	*-1*	*-1*	*-1*
-5	*+1*	*-1*	*+1*	*-1*	*-1*	*+1*	*-1*	*+1*
2	*+1*	*+1*	*-1*	*-1*	*+1*	*+1*	*-1*	*-1*
-2	*+1*	*-1*	*-1*	*+1*	*+1*	*-1*	*-1*	*+1*
10	*+1*	*+1*	*-1*	*-1*	*-1*	*-1*	*+1*	*+1*
-10	*+1*	*-1*	*-1*	*+1*	*-1*	*+1*	*+1*	*-1*

Απόδειξη. Χρησιμοποιούμε τον συμβολισμό $(a, b)_2$ για το σύμβολο του Hilbert $(\frac{a,b}{2})$, και θα επαληθεύσουμε τις τιμές του πίνακα. Λόγω της συμμετρικότητας του συμβόλου του Hilbert, δεν χρειάζεται να υπολογίσουμε όλα τα στοιχεία του πίνακα. Η πρώτη γραμμή προκύπτει από το (2) της Πρότασης 1.4.4. Για την δεύτερη γραμμή αποδεικνύουμε τις τιμες $+1$, βρίσκοντας λύσεις στις αντίστοιχες εξισώσεις. Έτσι:

$$(-1, 2)_2 = 1 \text{ διότι } -1 \cdot 1^2 + 2 \cdot 1^2 = 1^2$$
$$(-1, 5)_2 = 1 \text{ διότι } -1 \cdot 1^2 + 5 \cdot 1^2 = 2^2$$
$$(-1, 10)_2 = 1 \text{ διότι } -1 \cdot 1^2 + 10 \cdot 1^2 = 3^2$$

Δείχνουμε τώρα ότι $(-1, -2)_2 = -1$.
Έστω ότι δεν ισχύει και υπάρχει μη τετριμμένη λύση (x, y, z) της εξίσωσης $-X^2 - 2Y^2 = Z^2$. Και πάλι όπως στην απόδειξη για την εξίσωση $uX^2 + vpY^2 = Z^2$, μπορούμε να υποθέσουμε ότι $x, y, z \in \mathbb{Z}_2$ και $x, z \in \mathbb{Z}_2^*$. Τότε $x^2 \equiv z^2 \equiv 1 mod 8$, άρα $-2y^2 \equiv z^2 + x^2 \equiv 2 mod 8 \Rightarrow y^2 \equiv -1 mod 4$, το οποίο είναι αδύνατο.
Τώρα χρησιμοποιώντας τα (6) και (2) της Πρότασης 1.4.4, έχουμε:

$$(-1, -1)_2 = (-1, -2^2)_2 = (-1, -2 \cdot 2)_2 = (-1, -2)_2 = -1$$
$$(-1, -5)_2 = (-1, -1 \cdot 5)_2 = (-1, -1)_2 = -1$$
$$(-1, -10)_2 = (-1, -1 \cdot 10)_2 = (-1, -1)_2 = -1 \text{ και}$$
$$(5, -5)_2 = (2, -2)_2 = (10, -10)_2 = 1$$

Από τις σχέσεις $-5\mathbb{Q}_2^{*2} = 3\mathbb{Q}_2^{*2} = 11\mathbb{Q}_2^{*2}$ στην $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ και το (3) της Πρόταση 1.4.4, έχουμε $(-5,-2)_2 = (3,-2)_2 = 1$ και $(-5,-10)_2 = (11,-10)_2 = 1$.
Από το (5) της Πρόταση 1.4.4 ισχύει $(-2,-10)_2 = (-2\cdot 1, -2\cdot 5)_2 = (-2,-5)_2 = 1$ και από το (6) έχουμε:

$$(5,5)_2 = (5,-1\cdot(-5))_2 = (5,-1)_2 = 1$$
$$(-5,-5)_2 = (-1\cdot 5,-5)_2 = (-1,-5)_2 = -1$$
$$(2,2)_2 = (2,-1\cdot(-2))_2 = (2,-1)_2 = 1$$
$$(-2,-2)_2 = (-1\cdot 2,-2)_2 = (-1,-2)_2 = -1$$
$$(10,10)_2 = (10,-1\cdot(-10))_2 = (10,-1)_2 = 1$$
$$(-10,-10)_2 = (-1\cdot 10,-10)_2 = (-1,-10)_2 = -1$$
$$(-5,2)_2 = (-5,-1\cdot(-2))_2 = (-5,-1)_2 = -1$$
$$(5,-2)_2 = (-1\cdot(-5),-2)_2 = (-1,-2)_2 = -1$$
$$(5,-10)_2 = (-1\cdot(-5),-10)_2 = (-1,-10)_2 = -1$$
$$(-5,10)_2 = (-5,-1\cdot(-10))_2 = (-5,-1)_2 = -1$$
$$(2,-10)_2 = (-1\cdot(-2),-10)_2 = (-1,-10)_2 = -1$$
$$(-2,10)_2 = (-2,-1\cdot(-10))_2 = (-2,-1)_2 = -1$$

Τέλος από το (5) της Πρόταση 1.4.4:

$$(2,10)_2 = (2\cdot 1, 2\cdot 5)_2 = (2,-5)_2 = -1$$
$$(2,5)_2 = (1\cdot 2, 1\cdot 5)_2 = (2,-10)_2 = -1$$
$$(5,10)_2 = (5\cdot 1, 5\cdot 2)_2 = (5,-2)_2 = -1.$$

Η κλειστή μορφή επαληθεύεται από τον πίνακα. □

Πόρισμα 1.4.7. *Έστω $p \in \mathbb{P}\cup\{\infty\}$ και $a \in \mathbb{Q}_p^*$. Τότε, $(\frac{a,b}{p}) = 1$ για κάθε $b \in \mathbb{Q}_p \Leftrightarrow a \in \mathbb{Q}_p^{*2}$.*

Απόδειξη. Για $p \in \mathbb{P}$ είναι άμεσο απο τους πίνακες.
Για $p = \infty$ αν $(\frac{a,b}{\infty}) = 1$ για κάθε $b \in \mathbb{R}$ τότε κατ'ανάγκη $a > 0$ και άρα $a \in \mathbb{R}^{*2}$.
Η άλλη κατεύθυνση είναι προφανής. □

Πόρισμα 1.4.8. *Το σύμβολο του Hilbert είναι δι-πολλαπλασιαστικό. Δηλαδή για $p \in \mathbb{P}\cup\{\infty\}, a,b,c \in \mathbb{Q}_p^*$ ισχύουν:*

$$(\tfrac{a,bc}{p}) = (\tfrac{a,b}{p})(\tfrac{a,c}{p}) \text{ και } (\tfrac{ac,b}{p}) = (\tfrac{a,b}{p})(\tfrac{c,b}{p})$$

Απόδειξη. Για $p \in \mathbb{P}$ προκύπτει άμεσα από τους τύπους για το σύμβολο του Hilbert.
Για $p = \infty$ έχουμε:

$$(\tfrac{-1,-1}{\infty})\cdot(\tfrac{-1,-1}{\infty}) = (-1)\cdot(-1) = 1 = (\tfrac{-1,1}{\infty}) = (\tfrac{-1,(-1)\cdot(-1)}{\infty})$$

Τα υπόλοιπα προκύπτουν λόγω συμμετρίας και της Πρόταση 1.4.4. □

Πρόταση 1.4.9. *Για κάθε $a, b \in \mathbb{Q}^*$ ισχύει ο τύπος του γινομένου*

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (\tfrac{a,b}{p}) = 1.$$

Απόδειξη. Το σύμβολο του Hilbert εξαρτάται μόνο από τις κλάσεις των a και b στην ομάδα $\mathbb{Q}_p^* / \mathbb{Q}_p^{*2}$. Οπότε μπορούμε να πολλαπλασιάσουμε τα a, b με κατάλληλα τετράγωνα ακεραίων ώστε να μπορούμε να υποθέσουμε ότι $a, b \in \mathbb{Z}$. Παρατηρούμε ότι μόνο πεπερασμένου πλήθους παράγοντες του γινομένου είναι -1. Αυτό ισχύει διότι για κάθε $p \in \mathbb{P} \setminus \{2\}$, για τον οποίο ισχύει

$$ord_p(a) = ord_p(b) = 0$$

έχουμε $a, b \in \mathbb{Z}_p^*$ και άρα $(\tfrac{a,b}{p}) = 1$.
Από την δι-πολλαπλασιαστικότητα του συμβόλου του Hilbert και επειδή $(\tfrac{1,a}{p}) = 1$ αρκεί να εξετάσουμε τις περιπτώσεις :

$$(a, b) = (-1, -1), (-1, 2), (-1, q), (2, 2), (2, q), (q, q), (q, r)$$

όπου q, r περιττοί πρώτοι με $q \neq r$. Από την ιδιότητα $(\tfrac{ab,ac}{p}) = (\tfrac{ab,-bc}{p})$, έχουμε:

$$(\tfrac{2,2}{p}) = (\tfrac{2\cdot 1, 2\cdot 1}{p}) = (\tfrac{2,-1}{p}) = (\tfrac{-1,2}{p}) \text{ και}$$
$$(\tfrac{q,q}{p}) = (\tfrac{q\cdot 1, q\cdot 1}{p}) = (\tfrac{q,-1}{p})$$

τα οποία ανάγονται στις περιπτώσεις $(a, b) = (-1, 2)$ και $(a, b) = (-1, q)$. Για τις υπόλοιπες 5 περιπτώσεις έχουμε τον πίνακα:

(a, b)	$(\tfrac{a,b}{\infty})$	$(\tfrac{a,b}{2})$	$(\tfrac{a,b}{q})$	$(\tfrac{a,b}{r})$
$(-1, -1)$	-1	-1	$+1$	$+1$
$(-1, 2)$	$+1$	$+1$	$+1$	$+1$
$(-1, q)$	$+1$	$(-1)^{\frac{q-1}{2}}$	$(\tfrac{-1}{q})$	$+1$
$(2, q)$	$+1$	$(-1)^{\frac{q^2-1}{8}}$	$(\tfrac{2}{q})$	$+1$
(q, r)	$+1$	$(-1)^{\frac{q-1}{2}\cdot\frac{r-1}{2}}$	$(\tfrac{r}{q})$	$(\tfrac{q}{r})$

Το γινόμενο των συμβόλων κάθε γραμμής είναι $+1$ λόγω του νόμου τετραγωνικής αντιστροφής και άρα έχουμε το συμπέρασμα. □

Πόρισμα 1.4.10. *Έστω $a, b \in \mathbb{Q}^*$. Αν η εξίσωση $ax^2 + by^2 = z^2$ έχει λύση στο $\mathbb{R}$ και στα $\mathbb{Q}_p$ για όλους του πρώτους αριθμούς $p \in \mathbb{P}$, εκτός ενός πρώτου αριθμού, έστω q, τότε έχει λύση και στο $\mathbb{Q}_q$.*

Απόδειξη. Άμεση από την προηγούμενη Πρόταση. □

Σχόλιο 1.4.11.
(1) Επειδή το σύμβολο του Hilbert $(\frac{a,b}{p})$ *εξαρτάται μόνο από τις κλάσεις των* a, b *στην ομάδα* ${}^{\mathbb{Q}_p^*}\!/_{\mathbb{Q}_p^{*2}}$ *συχνά θα γράφουμε* $(\frac{a,b}{p})$ *για* $a, b \in {}^{\mathbb{Q}_p^*}\!/_{\mathbb{Q}_p^{*2}}$, $p \in \mathbb{P} \cup \{\infty\}$.
(2) Για λόγους ευκολίας συμβολίζουμε με P *το σύνολο* $\mathbb{P} \cup \{\infty\}$. *Επίσης χρησιμοποιούμε τον συμβολισμό* (a, b) *ή* $(a, b)_v$ *για το σύμβολο του Hilbert στο* $\mathbb{Q}_v$ *για* $v \in P$.

Πρόταση 1.4.12. *Για* $a \in {}^{K^*}\!/_{K^{*2}}$ *όπου* K *κάποιο από τα* $\mathbb{Q}_p$, $p \in P$ *και* $\varepsilon = \pm 1$ *ορίζουμε*

$$H_a^\varepsilon = \{b \in {}^{K^*}\!/_{K^{*2}} | (a, b) = \varepsilon\}$$

Τότε ισχύουν τα εξής:
(i) $H_1^1 = {}^{K^*}\!/_{K^{*2}}$ *και* $H_1^{-1} = \emptyset$.
(ii) Για $a \neq 1$,

$$\#H_a^\varepsilon = \begin{cases} 1, & \text{αν } K = \mathbb{R} \\ 2, & \text{αν } K = \mathbb{Q}_p, p \neq 2 \\ 4, & \text{αν } K = \mathbb{Q}_2 \end{cases}$$

(iii) Αν τα H_a^ε *και* $H_{a'}^{\varepsilon'}$ *είναι μη κενά τότε*

$$H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset \Leftrightarrow a = a' \text{και } \varepsilon = -\varepsilon'$$

Απόδειξη. Το (i) είναι άμεσο από την ιδιότητα (2) της Πρότασης 1.4.4. Για το (ii) αν $K = \mathbb{R}$ τότε $H_a^\varepsilon = \{1\}$ αν $\varepsilon = 1$ και $H_a^\varepsilon = \{-1\}$ αν $\varepsilon = -1$.
Για $K = \mathbb{Q}_p$, $p \neq 2$ από τους πίνακες για το σύμβολο του Hilbert βλέπουμε ότι κάθε στήλη εκτός από αυτή του 1, έχει $+1$ σε ακριβώς δύο θέσεις και -1 σε ακριβώς δύο θέσεις. Αντίστοιχα για $p = 2$ κάθε στήλη έχει $+1$ σε ακριβώς τέσσερις θέσεις και το ίδιο ισχύει για το -1.
Για το (iii) παρατηρούμε ότι αν $a = 1$ τότε αφού το σύνολο H_a^ε είναι μη κενό αναγκαστικά πρέπει $\varepsilon = 1$ και άρα $H_a^\varepsilon = {}^{K^*}\!/_{K^{*2}}$. Συνεπώς δεν υπάρχουν a', ε' ώστε $H_{a'}^{\varepsilon'} \neq \emptyset$ και $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$. Οπότε υποθέτουμε ότι $a, a' \neq 1$
Αν $K = \mathbb{R}$ τότε αναγκαστικά $a = a' = -1$ και άρα για να έχουμε $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$ πρέπει $\varepsilon = -\varepsilon'$.
Αν $K = \mathbb{Q}_p$, $p \neq 2$, $p \equiv 1 mod 4$ τότε αν $\{1, u, p, pu\}$ είναι ένα πλήρες σύστημα αντιπροσώπων της ομάδας ${}^{\mathbb{Q}_p^*}\!/_{\mathbb{Q}_p^{*2}}$, έχουμε:

$$H_u^\varepsilon = \begin{cases} \{1, u\}, & \text{αν } \varepsilon = +1 \\ \{p, pu\}, & \text{αν } \varepsilon = -1 \end{cases}$$

$$H_p^\varepsilon = \begin{cases} \{1, p\}, & \text{αν } \varepsilon = +1 \\ \{u, pu\}, & \text{αν } \varepsilon = -1 \end{cases}$$

$$H_{pu}^{\varepsilon} = \begin{cases} \{1, pu\}, & \text{αν } \varepsilon = +1 \\ \{u, p\}, & \text{αν } \varepsilon = -1 \end{cases}$$

Συνεπώς αν $a \neq a'$ έχουμε $H_a^{\varepsilon} \cap H_{a'}^{\varepsilon'} \neq \emptyset$ για οποιαδήποτε επιλογή των $\varepsilon, \varepsilon'$. Άρα αναγκαστικά $a = a'$ και $\varepsilon = -\varepsilon'$.
Οι υπόλοιπες περιπτώσεις είναι εντελώς ανάλογες. □

Θεώρημα 1.4.13. *Έστω $a_1, a_2, \ldots, a_n \in \mathbb{Q}^*$ και $\varepsilon_{i,v} = \pm 1$ για $i = 1, 2, \ldots, n$ και για κάθε $v \in P$. Αν ισχύουν οι υποθέσεις:*
(1) Όλα σχεδόν τα $\varepsilon_{i,v}$ είναι $+1$
(2) Ισχύει $\prod_{v \in P} \varepsilon_{i,v} = 1$ για κάθε $i = 1, 2, \ldots, n$
(3) Για κάθε $v \in P$ υπάρχει $x_v \in \mathbb{Q}_v^*$ ώστε $(a_i, x_v) = \varepsilon_{i,v}$ για κάθε $i = 1, 2, \ldots, n$
Τότε υπάρχει $x \in \mathbb{Q}^*$ ώστε $(a_i, x) = \varepsilon_{i,v}$ για κάθε $i = 1, 2, \ldots, n$ και για κάθε $v \in P$.

Απόδειξη. Πολλαπλασιάζοντας τα $a_1, a_2, \ldots, a_n$ με κατάλληλα τετράγωνα ακεραίων μπορούμε να υποθέσουμε ότι $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ και η τιμή του συμβόλου του Hilbert δεν αλλάζει. Έστω $S = \{p \in \mathbb{P} : p \mid a_i \text{ για κάποιο i}\} \cup \{2, \infty\}$, $T = \{v \in P : \varepsilon_{i,v} = -1 \text{ για κάποιο i}\}$. Τα σύνολα S και T είναι πεπερασμένα, άρα και η ένωσή τους $S \cup T$ είναι πεπερασμένο σύνολο.

Περίπτωση 1: Υποθέτουμε ότι $S \cap T = \emptyset$
Έστω $a := \prod_{l \in T, l \neq \infty} l$ και $m := 8 \prod_{l \in S, l \neq 2, \infty} l$. Αφού $S \cap T = \emptyset$ έχουμε ότι $\mu\kappa\delta(a, m) = 1$. Το θεώρημα του Dirichlet μας λέει ότι αν a, m είναι σχετικά πρώτοι θετικοί ακέραιοι, τότε υπάρχουν άπειροι πρώτοι αριθμοί p ώστε $p \equiv a mod m$. Άρα υπάρχει $p \in \mathbb{P}$ με $p \equiv a mod m$ και $p \notin S \cup T$. Έστω $x := pa \in \mathbb{Q}^*$. Θα αποδείξουμε ότι αυτό το x έχει τις ζητούμενες ιδιότητες.

Για $v \in S$ έχουμε $\varepsilon_{i,v} = +1$ για κάθε $i = 1, 2, \ldots, n$ διότι $S \cap T = \emptyset$. Θα αποδείξουμε ότι $(a_i, x)_v = +1 = \varepsilon_{i,v}$ για κάθε $i = 1, 2, \ldots, n$.
Για το $\infty \in S$ έχουμε $(a_i, x)_\infty = 1$ για κάθε $i = 1, 2, \ldots, n$, διότι $x > 0$. Τώρα $a \equiv p mod m \Rightarrow ap \equiv p^2 mod m \Rightarrow x \equiv p^2 mod m$, επομένως $x \equiv a^2 mod m$. Αν $v = l \in \mathbb{P}$ με $l \in S$, τότε $l \mid m$ και άρα:

$$\text{αν } l \neq 2 \text{ έχουμε } x \equiv a^2 mod l$$
$$\text{αν } l = 2 \text{ έχουμε } x \equiv a^2 mod 8$$

Επίσης για κάθε $l \in S$ $ord_l(x) = 0$, δηλαδή το x είναι μονάδα του $\mathbb{Z}_l$ για κάθε $l \in S$ πρώτο αριθμό.Τότε για $l \neq 2$ από την Πρόταση 1.4.5 έχουμε

$$(a_i, x)_l = \begin{cases} 1, & \text{αν } a_i \equiv \varepsilon mod \mathbb{Q}_l^{*2} \\ (\frac{x}{l}), & \text{αν } a_i \equiv l\varepsilon mod \mathbb{Q}_l^{*2} \end{cases}$$

όπου $\varepsilon \in \mathbb{Z}_l^*$ και $\varepsilon mod\mathbb{Q}_l^{*2}, l\varepsilon mod\mathbb{Q}_l^{*2}$ κλάσεις στην ομάδα $\mathbb{Q}_l^*/\mathbb{Q}_l^{*2}$. Όμως $x \equiv a^2 mod l \Rightarrow (\frac{x}{l}) = 1$ και άρα $(a_i, x)_l = 1$ για κάθε πρώτο αριθμό $l \in S, l \neq 2$ και για κάθε $i = 1, 2, ..., n$.
Επίσης για $l = 2$ έχουμε $(a_i, x)_2 = 1$ διότι, αφού $x \equiv a^2 mod 8 \equiv 1 mod 8$ έχουμε $x \in \mathbb{Q}_2^{*2}$. Δηλαδή για $\upsilon \in S$ έχουμε $(a_i, x)_\upsilon = 1 = \varepsilon_{i,\upsilon}$ για κάθε $i = 1, 2, \ldots, n$.

Έστω τώρα $l \in \mathbb{P}$ με $l \notin S$ Τότε $a_i \in \mathbb{Z}_l^*$ για κάθε $i = 1, 2, \ldots, n$ ($l \neq 2$, αφου $2 \in S$).

- Αν $l \notin T \cup \{p\}$ τότε $ord_l(a) = 0$ και άρα $a \in \mathbb{Z}_l^*$. Επίσης και το $x \in \mathbb{Z}_l^*$ και άρα $(a_i, x)_l = +1$ για κάθε $i = 1, 2, \ldots, n$. Όμως αφού $l \notin T$ έχουμε $\varepsilon_{i,l} = +1$ για κάθε $i = 1, 2, \ldots, n$. Δηλαδή για κάθε $l \notin T \cup \{p\}$ ισχύει $(a_i, x)_l = \varepsilon_{i,l}$ για κάθε $i = 1, 2, \ldots, n$.

- Αν $l \in T$ έχουμε $\varepsilon_{i,l} = -1$ για κάποιο i και $ord_l(x) = 1$. Άρα από την Πρόταση 1.4.5
$$(a_i, x)_l = (\frac{a_i}{l})$$
Από την υπόθεση (3) υπάρχει $x_l \in \mathbb{Q}_l^*$ ώστε $(a_i, x_l)_l = \varepsilon_{i,l}$ για κάθε $i = 1, 2, \ldots, n$.
Αν το i είναι τέτοιο ώστε $\varepsilon_{i,l} = -1$, έχουμε $(a_i, x_l)_l = -1$. Όμως
$$(a_i, x_l)_l = \begin{cases} +1, & \text{αν } 2 | ord_l(x_l) \\ (\frac{a_i}{l}), & \text{αν } 2 \not| ord_l(x_l) \end{cases}$$
Άρα αναγκαστικά $2 \not| ord_l(x_l)$ και $(\frac{a_i}{l}) = -1$. Δηλαδή
$$(a_i, x)_l = (\frac{a_i}{l}) = -1 = \varepsilon_{i,l}$$
Αν το i είναι τέτοιο ώστε $\varepsilon_{i,l} = +1$, αφού $2 \not| ord_l(x_l)$ έχουμε
$$(a_i, x_l)_l = (\frac{a_i}{l})$$
Άρα
$$(a_i, x_l)_l = \varepsilon_{i,l} \Leftrightarrow (a_i, x_l)_l = +1 \Leftrightarrow (\frac{a_i}{l}) = +1$$
Άρα $(a_i, x)_l = +1 = \varepsilon_{i,l}$. Άρα για κάθε $l \in T$ έχουμε $(a_i, x)_l = \varepsilon_{i,l}$ για κάθε $i = 1, 2, \ldots, n$.

- Αν $l = p$ από την υπόθεση (2) έχουμε $\prod_{v\in P} \varepsilon_{i,v} = 1$, για κάθε $i = 1, 2, \ldots, n$ και από τον τύπο του γινομένου για το σύμβολο του Hilbert (Πρόταση 1.4.9), έχουμε $\prod_{v\in P} (a_i, x)_v = 1$. Άρα :

$$(a_i, x)_p = \prod_{v\in P, v\neq p} (a_i, x)_v = \prod_{v\in P, v\neq p} \varepsilon_{i,v} = \varepsilon_{i,p}$$

και συνεπώς έχουμε το ζητούμενο.

Περίπτωση 2:Έστω τώρα ότι $S \cap T \neq \emptyset$
Θα αναγάγουμε το πρόβλημα στην προηγούμενη περίπτωση.
Επειδή το σύνολο S είναι πεπερασμένο, από το Θεώρημα 1.3.34 για κάθε $\varepsilon > 0$ υπάρχει $y \in \mathbb{Q}^*$ ώστε $|y - x_v|_v < \varepsilon$, για κάθε $v \in S$. Αν επιλέξουμε το ε κατάλληλα μικρό από την Πρόταση 1.3.24 έχουμε ότι υπάρχει $y \in \mathbb{Q}^*$ ώστε $\frac{y}{x_v} \in \mathbb{Q}_v^{*2}$ για κάθε $v \in S$.
Συνεπώς $(a_i, y)_v = (a_i, x_v)_v = \varepsilon_{i,v}$ για κάθε $v \in S$ και για κάθε $i = 1, 2, \ldots, n$.

Θέτουμε $\varepsilon'_{i,v} = \varepsilon_{i,v}(a_i, y)_v$ για κάθε $v \in P$ και κάθε $i = 1, 2, \ldots, n$. Τα $\varepsilon'_{i,v}$ επαληθεύουν τις υποθέσεις (1), (2) και (3) του Θεωρήματος. Πράγματι:
(1) Σχεδόν όλα τα $\varepsilon'_{i,v}$ είναι $+1$ διότι μόνο περασμένου πλήθους από τα $\varepsilon_{i,v}$, και τα $(a_i, y)_v$ είναι -1.
(2) $\prod_{v\in P} \varepsilon'_{i,v} = \prod_{v\in P} \varepsilon_{i,v} \prod_{v\in P} (a_i, y)_v = 1$ για κάθε $i = 1, 2, ..., n$
(3) $\varepsilon'_{i,v} = \varepsilon_{i,v}(a_i, y)_v = (a_i, x_v)_v(a_i, y)_v = (a_i, yx_v)_v$, άρα για κάθε $v \in P$ υπάρχει $x'_v := yx_v \in \mathbb{Q}_v^*$ για το οποίο ισχύει $(a_i, x'_v)_v = \varepsilon'_{\iota,v}$ για κάθε $i = 1, 2, ..., n$.

Θεωρούμε $T' = \{v \in P : \varepsilon'_{i,v} = -1$ για κάποιο i$\}$. Τότε αν $v \in S$ έχουμε $(a_i, y)_v = \varepsilon_{i,v}$ για κάθε $i = 1, 2, \ldots, n$ και άρα $\varepsilon'_{i,v} = +1$ για κάθε $i = 1, 2, \ldots, n$. Δηλαδή $S \cap T' = \emptyset$.
Επομένως από την προηγούμενη περίπτωση υπάρχει $x' \in \mathbb{Q}^*$ ώστε

$$(a_i, x')_v = \varepsilon'_{i,v}$$

για κάθε $v \in P, i = 1, 2, \ldots, n$. Τότε το $x := x'y$ είναι λύση του αρχικού προβλήματος. Πράγματι:

$$(a_i, x)_v = (a_i, x'y)_v = (a_i, x')_v(a_i, y)_v = \varepsilon'_{i,v}(a_i, y)_v = \varepsilon_{i,v}$$

για κάθε $v \in P, i = 1, 2, \ldots, n$. □

Πόρισμα 1.4.14. *Έστω $\varepsilon_v = \pm 1$ για $v \in P$ τα οποία ικανοποιούν τις υποθέσεις:*
(1) Όλα σχεδόν τα $\varepsilon_v = +1$ και

(2) $\prod_{\upsilon \in P} \varepsilon_\upsilon = +1$

Τότε υπάρχουν $a, b \in \mathbb{Q}^*$ *ώστε* $(a,b)_\upsilon = \varepsilon_\upsilon$ *για κάθε* $\upsilon \in P$.

Απόδειξη. Έστω $\upsilon_1, \upsilon_2, ..., \upsilon_n$ τα πεπερασμένου πλήθους στοιχεία του P για τα οποία ισχύει $\varepsilon_{\upsilon_i} = -1$ για κάθε $i = 1, 2, ..., n$. Επιλέγουμε $a \in \mathbb{Q}^*$ ώστε $a \notin \mathbb{Q}_{\upsilon_i}^{*2}$ για κάθε $i = 1, 2, ..., n$. Αυτό μπορούμε να το κάνουμε επιλέγοντας $a < 0$ αν $\upsilon_i = \infty$ για κάποιο $i \in \{1, 2, ..., n\}$ και $ord_p(a) \equiv 1 mod 2$ για κάθε πρώτο $p \in \{\upsilon_1, \upsilon_2, ..., \upsilon_n\}$ Τότε για κάθε $i \in \{1, 2, ..., n\}$ υπάρχει $b_{\upsilon_i} \in \mathbb{Q}_{\upsilon_i}^*$ ώστε $(a, b_{\upsilon_i}) = \varepsilon_{\upsilon_i}$ (διαφορετικά από το Πόρισμα 1.4.7 θα έπρεπε $a \in \mathbb{Q}_{\upsilon_i}^{*2}$). Για τα υπόλοιπα $\upsilon \in P$ ορίζουμε $b_\upsilon = 1$. Συνεπώς για κάθε $\upsilon \in P$ ισχύει

$$(a, b_\upsilon) = \varepsilon_\upsilon$$

Επομένως ικανοποιούνται οι υποθέσεις του Θεωρήματος 1.4.13 και άρα υπάρχει $b \in \mathbb{Q}^*$ ώστε

$$(a,b)_\upsilon = \varepsilon_\upsilon$$

για κάθε $\upsilon \in P = \mathbb{P} \cup \{\infty\}$. □

Κεφάλαιο 2

Τετραγωνικές μορφές

2.1 Βασικές Ιδιότητες

Θεωρούμε K ένα σώμα χαρακτηριστικής , $chK \neq 2$.

Ορισμός 2.1.1. Μια τετραγωνική μορφή πάνω από ένα σώμα K είναι ένα ομογενές πολυώνυμο $f(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]$ βαθμού 2.

Παράδειγμα 2.1.2. *Το πολυώνυμο* $f(x, y) = 3x^2 - 2xy + y^2 \in \mathbb{Q}[x, y]$ *είναι μια τετραγωνική μορφή.*

Ο ορισμός της τετραγωνικής μορφής γενικεύεται σε K-διανυσματικούς χώρους πεπερασμένης διάστασης. Συγκεκριμένα:

Ορισμός 2.1.3. Μια τετραγωνική μορφή σε έναν K-διανυσματικό χώρο πεπερασμένης διάστασης V είναι μία συνάρτηση $f : V \to K$ τέτοια ώστε για κάθε επιλογή βάσης $e_1, e_2, ..., e_n$ του V η συνάρτηση

$$f(x_1e_1 + x_2e_2 + ... + x_ne_n) : K^n \to K$$

είναι μια τετραγωνική μορφή των μεταβλητών $x_1, x_2, ..., x_n$.

Ορισμός 2.1.4. Μια διγραμμική μορφή σε έναν K-διανυσματικό χώρο V είναι μια συνάρτηση $B : V \times V \to K$ ώστε να ισχύουν:
(1) $B(v_1 + v_2, w) = B(v_1, w) + B(v_2, w)$ και $B(\lambda v, w) = \lambda B(v, w)$ για κάθε $v_1, v_2, v, w \in V, \lambda \in K$.
(2)$B(v, w_1 + w_2) = B(v, w_1) + B(v, w_2)$ και $B(v, \lambda w) = \lambda B(v, w)$ για κάθε $w_1, w_2, v, w \in V, \lambda \in K$.
Αν επιλέξουμε μία βάση $\{e_1, e_2, ..., e_n\}$ του V τότε:

$$B(v, w) = B(\sum_{i=1}^n x_ie_i, \sum_{i=1}^n y_ie_i) = \sum_{i,j}^n B(e_i, e_j)x_iy_j = x^tAy$$

όπου $A = (B(e_i, e_j))_{i,j} \in M_n(K)$ και x, y είναι τα διανύσματα συντεταγμένων των v και w αντίστοιχα ως προς τη βάση.

Η B λέγεται συμμετρική αν:

$$B(v, w) = B(w, v)$$

για κάθε $v, w \in V$. Είναι προφανές ότι ο πίνακας που αντιστοιχεί σε μια συμμετρική διγραμμική μορφή είναι συμμετρικός.

Ορισμός 2.1.5. Μια διγραμμική μορφή B λέγεται μη-ιδιάζουσα αν για κάθε $v \in V$ με $v \neq 0$ η γραμμική απεικόνιση $T : V \to V$ με $T(w) = B(v, w)$ είναι μη μηδενική. Μια διγραμμική μορφή λέγεται ιδιάζουσα όταν δεν είναι μη-ιδιάζουσα.

Παρατήρηση 2.1.6. *Για κάθε K-διανυσματικό χώρο πεπερασμένης διάστασης V, υπάρχει μια ένα προς ένα αντιστοιχία ανάμεσα στις τετραγωνικές μορφές του V και στις συμμετρικές διγραμμικές μορφές του V. Αν f είναι μια τετραγωνική μορφή τότε η $B : V \times V \to K$, με*

$$B(v, w) := \tfrac{1}{2}(f(v + w) - f(v) - f(w))$$

είναι συμμετρική διγραμμική μορφή. Αν B είναι συμμετρική διγραμμική μορφή, τότε η $f : V \to K$ με

$$f(v) := B(v, v)$$

είναι τετραγωνική μορφή.
Ισοδύναμα σε μορφή πινάκων έχουμε $f(x) = x^t Ax$ και $B(x, y) = x^t Ay$ για έναν μοναδικό συμμετρικό πίνακα $A \in M_n(K)$, και τα x, y είναι τα αντίστοιχα διανύσματα συντεταγμένων των v και w.

Ορισμός 2.1.7. Ορίζουμε τάξη (rank) μιας τετραγωνικής μορφής, την τάξη του αντίστοιχου συμμετρικού πίνακα.

Ορισμός 2.1.8. Η τετραγωνική μορφή f λέγεται μη-ιδιάζουσα αν η αντίστοιχη διγραμμική μορφή B είναι μη-ιδιάζουσα.

Θεώρημα 2.1.9. *Μια τετραγωνική μορφή f είναι μη-ιδιάζουσα αν και μόνο αν ο συμμετρικός πίνακας που αντιστοιχεί στην f είναι αντιστρέψιμος.*

Απόδειξη. Θεωρούμε την τετραγωνική μορφή στο K^n. Έστω B η αντίστοιχη διγραμμική μορφή και A ο πίνακας αναπαράστασης της B.
Υποθέτουμε ότι ο A είναι αντιστρέψιμος, τότε ορίζει ένα ισομορφισμό στον K^n. Έστω $u = (b_1, b_2, ..., b_n) \in K^n$ μη-μηδενικό, δηλαδή $b_i \neq 0$ για κάποιο i. Έστω $w \in K^n$ ώστε $Aw = e_i$, τότε

$$B(u, w) = u^t Aw = b_i \neq 0$$

Άρα η B είναι μη-ιδιάζουσα και συνεπώς και η f.
Έστω τώρα ότι ο A δεν είναι αντιστρέψιμος, τότε ούτε ο A^t είναι αντιστρέψιμος. Άρα υπάρχει $u \in K^n$, $v \neq 0$, ώστε $A^t u = 0$. Τότε για κάθε $w \in K^n$ έχουμε

$$B(u, w) = u^t \cdot Aw = A^t u \cdot w = 0 \cdot w = 0$$

και άρα η B είναι ιδιάζουσα. □

Ορισμός 2.1.10. Δύο τετραγωνικές μορφές $f(x_1, x_2, ..., x_n)$ και $g(x_1, x_2, ..., x_n)$ λέγονται ισοδύναμες αν υπάρχει $n \times n$ αντιστρέψιμος πίνακας $M \in M_n(K)$ ώστε $f(x) = g(Mx)$ όπου $x \in K^n$. Ισόδύναμα αν A, B οι πίνακες που αντιστοιχούν στις f και g αντίστοιχα, έχουμε $A = M^t B M$. Συμβολίζουμε $f \sim g$.

Ορισμός 2.1.11. Έστω f μία τετραγωνική μορφή στον K-δ.χ. V. Ορίζουμε την διακρίνουσα της f:

$$d(f) := det(A)$$

όπου A ο πίνακας που αντιστοιχεί στην f ως προς κάποια βάση $\{e_1, e_2, ..., e_n\}$ του V.

Παρατήρηση 2.1.12. *(1) Αν A_1 είναι ο πίνακας που αντιστοιχεί στην f ως προς την βάση $\{e_1, e_2, ..., e_n\}$ και A_2 ο πίνακας που αντιστοιχεί στην f ως προς την βάση $\{e'_1, e'_2, ..., e'_n\}$, τότε υπάρχει ένας αντιστρέψιμος πίνακας $M \in M_n(K)$ ώστε $A_1 = M^t A_2 M$. Άρα*

$$det(A_1) = det(A_2)(det(M))^2$$

Συνεπώς αν $d(f) \neq 0$, η διακρίνουσα της f είναι μονοσήμαντα ορισμένη αν την θεωρήσουμε ως στοιχείο της K^*/K^{*2}. Οπότε αν η $d(f)$ δεν είναι μηδέν θα την βλέπουμε ως στοιχείο της K^*/K^{*2}.
(2) Αν A είναι ο πίνακας που αντιστοιχεί σε μια τετραγωνική μορφή f όπως στην Παρατήρηση 2.1.6, τότε η f είναι μη-ιδιάζουσα $\Leftrightarrow d(f) \neq 0$.

Πρόταση 2.1.13. *Κάθε τετραγωνική μορφή $f(x_1, x_2, ..., x_n)$ πάνω από ένα σώμα K είναι ισοδύναμη με μία διαγώνια τετραγωνική μορφή*

$$a_1 x_1^2 + a_2 x_2^2 + ... a_n x_n^2$$

Απόδειξη. Θα κάνουμε επαγωγή στην $dim V$. Αν $dim V \leq 1$ δεν έχουμε τίποτα να δείξουμε. Έστω λοιπόν ότι ισχύει για διανυσματικούς χώρους διάστασης $n-1$. Αν $f \equiv 0$ τότε μπορούμε να πάρουμε $a_i = 0$ για κάθε $i = 1, 2, ...n$. Αν η f δεν είναι ταυτοτικά μηδέν υπάρχει κάποιο $v \in V$ με $f(v) \neq 0$. Έστω B η διγραμμική μορφή μου αντιστοιχεί στην f. Τότε η απεικόνιση $T : V \to K$ με $T(x) = B(x, v)$ είναι γραμμική και αφού $T(v) = f(v) \neq 0$, έχουμε $dim(imT) =$

1 και άρα η T είναι επί. Ο πυρήνας της $v^\perp := kerT = \{x \in V | (B(x,v) = 0\}$ έχει διάσταση $dim(v^\perp) = dimV - dim(imT) = n-1$. Επίσης $v \notin v^\perp$ διότι $B(v,v) = f(v) \neq 0$, και άρα $V \cong Kv \oplus v^\perp$. Αν $y \in V$, $y = y_1 + y_2$ με $y_1 \in Kv$ και $y_2 \in v^\perp$, τότε

$$f(y) = f(y_1) + f(y_2) + 2B(y_1, y_2) = f(y_1) + f(y_2)$$

Από την επαγωγική υπόθεση η f περιορισμένη στον $v^\perp$ είναι ισοδύναμη με μία διαγώνια τετραγωνική μορφή και το$f(y_1) = f(x_1 v)$ είναι της μορφής $a_1 x_1^2$ όπου $a_1 = f(v)$. Συνεπώς έχουμε το ζητούμενο. □

Σχόλιο 2.1.14. *Την διαγώνια τετραγωνική μορφή $a_1x_1^2 + a_2x_2^2 + ...a_nx_n^2$ την συμβολίζουμε $< a_1, a_2, ..., a_n >$.*

Ορισμός 2.1.15. Έστω f μια τετραγωνική μορφή στον K-δ.χ. V και $a \in K$. Λέμε ότι η f παριστά το a αν υπάρχει μη μηδενικό $x \in V$ ώστε $f(x) = a$.

Παράδειγμα 2.1.16. *Η τετραγωνική μορφή $x^2 - 2y^2$ πάνω από το $\mathbb{Q}$ παριστά το -7 αλλά όχι το 0.*

Παρατήρηση 2.1.17. *Αν η τετραγωνική μορφή f παριστά το $a \in K$ $a \neq 0$, δηλαδή υπάρχει $v \in V$, $v \neq 0$ ώστε $f(v) = a$, τότε στην διαδικασία που ακολουθήσαμε για την απόδειξη της Πρότασης 2.1.13 επιλέγοντας το συγκεκριμένο v προκύπτει ότι η f είναι ισοδύναμη με την διαγώνια τετραγωνική μορφή $< a_1, a_2, ..., a_n >$ όπου $a_1 = a$.*

Πρόταση 2.1.18. *Κάθε ιδιάζουσα τετραγωνική μορφή παριστά το 0.*

Απόδειξη. Αν η τετραγωνική μορφή f είναι ιδιάζουσα τότε και η αντίστοιχη διγραμμική μορφή B είναι ιδιάζουσα. Αυτό σημαίνει ότι υπάρχει κάποιο μη μηδενικό $v \in V$ ωστε $B(v,w) = 0$ για κάθε $w \in V$. Άρα και $B(v,v) = 0 \Rightarrow f(v) = 0$. □

Πρόταση 2.1.19. *Αν μια μη-ιδιάζουσα τετραγωνική μορφή f παριστά το 0 τότε παριστά κάθε στοιχείο του σώματος K.*

Απόδειξη. Έστω f μη ιδιάζουσα τετραγωνική μορφή που παριστά το 0. Άρα υπάρχει $v \in V$, $v \neq 0$ ώστε $f(v) = 0$. Αν B είναι η διγραμμική μορφή που αντιστοιχεί στην f, υπάρχει $w \in V$ με $B(v,w) \neq 0$ διότι η B είναι μη ιδιάζουσα. Μάλιστα το w είναι γραμμικά ανεξάρτητο από το v, διότι αν $w = kv$ έχουμε $B(v,w) = B(v,kv) = kf(v) = 0$. Τότε έχουμε:

$$\begin{aligned} f(xv + yw) &= f(xv) + f(yw) + 2B(xv, yw) \\ &= x^2 f(v) + y^2 f(w) + 2xyB(v,w) \\ &= axy + by^2 = (ax + by)y \end{aligned}$$

όπου $a := 2B(v,w) \neq 0$ και $b := f(w)$ και $a, b \in K$. Τότε για $c \in K$ μπορούμε να λύσουμε την εξίσωση $(ax+by)y = c$ θέτοντας $y = 1$ και λύνοντας ως προς x. □

Πρόταση 2.1.20. *Έστω $f(x_1, ..., x_n)$ μια μη-ιδιάζουσα τετραγωνική μορφή πάνω από το σώμα K. Για $r \in K^*$ τα ακόλουθα είναι ισοδύναμα.*
(1) Η f παριστά το r
(2) Η τετραγωνική μορφή $g(x_1, x_2, ..., x_n, x_{n+1}) = f(x_1, x_2, ..., x_n) - rx_{n+1}^2$ παριστά το 0.

Απόδειξη. Έστω ότι ισχύει το (1), άρα υπάρχουν $a_1, a_2, ..., a_n \in K$ όχι όλα 0 ώστε $f(a_1, a_2, ..., a_n) = r$. Τότε $g(a_1, a_2, ..., a_n, 1) = r - r = 0$ και συνεπώς η g παριστά το 0.
Αντίστροφα έστω ότι ισχύει το (2), δηλαδή υπάρχουν $a_1, a_2, ..., a_n, a_{n+1} \in K$ όχι όλα 0 ώστε $g(a_1, a_2, ..., a_n, a_{n+1}) = 0$. Δηλαδή

$$f(a_1, a_2, ..., a_n) = ra_{n+1}^2$$

Αν $a_{n+1} \neq 0$ τότε

$$r = \frac{1}{a_{n+1}^2} f(a_1, a_2, ..., a_n) = f(\frac{a_1}{a_{n+1}}, ..., \frac{a_n}{a_{n+1}})$$

και άρα η f παριστά το r.
Αν $a_{n+1} = 0$ τότε $(a_1, a_2, ..., a_n) \neq (0, 0, ..., 0)$ διότι $(a_1, a_2, ..., a_n, a_{n+1}) \neq (0, 0, ..., 0, 0)$ και άρα η f παριστά το 0. Τότε από την Πρόταση 2.1.19 η f παριστά κάθε στοιχείο του σώματος K και συνεπώς και το r. □

2.2 Δύο Θεωρήματα του Witt

Ορισμός 2.2.1. Έστω σώμα K, f μια τετραγωνική μορφή n μεταβλητών με συντελεστές από το K και g μια τετραγωνική μορφή m μεταβλητών με συντελεστές στο K. Με $f \perp g$ θα συμβολίζουμε την τετραγωνική μορφή με $n+m$ μεταβλητές που ορίζεται ως εξής:

$$(f \perp g)(x_1, x_2, ..., x_n, x_{n+1}, ..., x_{n+m}) = f(x_1, x_2, ..., x_n) + g(x_{n+1}, ..., x_{n+m})$$

Παρατήρηση 2.2.2. *(i) Εν γένει $f \perp g \neq g \perp f$. Για παράδειγμα αν $f(x_1, x_2) = x_1^2 + 2x_1x_2$ και $g(x_1, x_2) = 2x_1^2 + 3x_2^2$ τότε*

$$f \perp g = x_1^2 + 2x_1x_2 + 2x_3^2 + 3x_4^2$$

ενώ

$$g \perp f = 2x_1^2 + 3x_2^2 + x_3^2 + 2x_3x_4$$

(ii) Αν σε μια τετραγωνική μορφή εφαρμόσουμε μια μετάθεση των μεταβλητών τότε παίρνουμε μια ισοδύναμη τετραγωνική μορφή. Επομένως και

$$f \perp g \sim g \perp f$$

Με βάση αυτό τον συμβολισμό μια διαγώνια τετραγωνική μορφή γράφεται $< a_1, a_2, ..., a_n >=< a_1 > \perp < a_2 > \perp ... \perp < a_n >$

Παρατήρηση 2.2.3. *Αν f, g, g' είναι τετραγωνικές μορφές και $g \sim g'$ τότε $f \perp g \sim f \perp g'$.*

Απόδειξη. Έστω A_g και $A_{g'}$ οι συμμετρικοί πίνακες που αντιστοιχούν στις g και g' αντίστοιχα, και B ο πίνακας που αντιστοιχεί στην f. Αφού $g \sim g'$ υπάρχει κάποιος αντιστρέψιμος πίνακας $M \in M_n(K)$ ώστε $A_{g'} = MA_gM^t$. Στην τετραγωνική μορφή $f \perp g$ αντιστοιχεί ο πίνακας

$$\left[\begin{array}{c|c} B & 0 \\ \hline 0 & A_g \end{array}\right] \tag{2.1}$$

ενώ στην $f \perp g'$ ο πίνακας

$$\left[\begin{array}{c|c} B & 0 \\ \hline 0 & A_{g'} \end{array}\right] \tag{2.2}$$

Τότε όμως

$$\left[\begin{array}{c|c} B & 0 \\ \hline 0 & A_{g'} \end{array}\right] = \left[\begin{array}{c|c} I & 0 \\ \hline 0 & M \end{array}\right] \cdot \left[\begin{array}{c|c} B & 0 \\ \hline 0 & A_g \end{array}\right] \cdot \left[\begin{array}{c|c} I & 0 \\ \hline 0 & M^t \end{array}\right] \tag{2.3}$$

και συνεπώς

$$\left[\begin{array}{c|c} B & 0 \\ \hline 0 & A_{g'} \end{array}\right] = \left[\begin{array}{c|c} I & 0 \\ \hline 0 & M \end{array}\right] \cdot \left[\begin{array}{c|c} B & 0 \\ \hline 0 & A_g \end{array}\right] \cdot \left[\begin{array}{c|c} I & 0 \\ \hline 0 & M \end{array}\right]^t \tag{2.4}$$

και άρα $f \perp g \sim f \perp g'$. □

Το επόμενο Θεώρημα μας εξασφαλίζει ότι ισχύει και το αντίστροφο.

Παρατήρηση 2.2.4. *Η ισοδυναμία τετραγωνικών μορφών ορίστηκε για τετραγωνικές μορφές με ίδιο πλήθος μεταβλητών. Σιωπηρά λοιπόν όταν γράφουμε $g \sim g'$ έχει ήδη υποτεθεί ότι οι g και g' είναι τετραγωνικές μορφές με ίδιο πλήθος μεταβλητών.*

Θεώρημα 2.2.5. ***(1ο Θεώρημα του Witt)***
Έστω f, g, g' τετραγωνικές μορφές. Αν $f \perp g \sim f \perp g'$ τότε $g \sim g'$.

Απόδειξη. Έστω $f \perp g \sim f \perp g'$. Η απόδειξη θα γίνει σε 4 βήματα.
1ο βήμα Το συμπέρασμα ισχύει όταν $f = n < 0 >$ και η g' είναι μη ιδιάζουσα. Πράγματι έστω M και M' οι συμμετρικοί πίνακες που αντιστοιχούν στις g και g' αντίστοιχα. Τότε στην $f \perp g$ αντιστοιχεί ο πίνακας

$$\left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & M \end{array}\right] \tag{2.5}$$

και στην $f \perp g'$ ο πίνακας

$$\left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & M' \end{array}\right] \tag{2.6}$$

Αφού $f \perp g \sim f \perp g'$ υπάρχει αντιστρέψιμος πίνακας

$$E = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] \tag{2.7}$$

ώστε

$$\left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & M' \end{array}\right] = E^t \cdot \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & M \end{array}\right] \cdot E \tag{2.8}$$

Όμως

$$E^t \cdot \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & M \end{array}\right] \cdot E = \left[\begin{array}{c|c} A^t & C^t \\ \hline B^t & D^t \end{array}\right] \cdot \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & M \end{array}\right] \cdot \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] = \left[\begin{array}{c|c} C^tMC & C^tMD \\ \hline D^tMC & D^tMD \end{array}\right] \tag{2.9}$$

Άρα $M' = D^tMD$.
Αφού η g' είναι μη-ιδιάζουσα έχουμε $det(M') \neq 0$ άρα $det(D)^2 det(M) \neq 0 \Rightarrow det(D) \neq 0$. Δηλαδή ο πίνακας D είναι αντιστρέψιμος και άρα $g \sim g'$.

2ο βήμα Το συμπέρασμα ισχύει όταν $f = n < 0 >$, χωρίς περιορισμό για την g'.
Επειδή οι ρόλοι των g και g' είναι συμμετρικοί, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $rank(g') \leq rank(g)$. Τότε με μία μετάθεση των μεταβλητών μπορούμε να έχουμε

$$g \sim m < 0 > \perp g_1 \text{ και } g' \sim m < 0 > \perp g_1'$$

με m το μέγιστο δυνατό ώστε η g_1' να είναι μη-ιδιάζουσα. Τότε έχουμε:

$$\begin{aligned} f \perp g \sim f \perp g' &\Rightarrow n < 0 > \perp m < 0 > \perp g_1 \sim n < 0 > \perp m < 0 > \perp g_1' \\ &\Rightarrow (n+m) < 0 > \perp g_1 \sim (n+m) < 0 > \perp g_1' \end{aligned}$$

Άρα για $f' := (n+m) < 0 >$ έχουμε $f' \perp g_1 \sim f' \perp g_1'$ και αφού η g_1' είναι μη-ιδιάζουσα, από το πρώτο βήμα παίρνουμε $g_1 \sim g_1'$. Άρα τελικά $g \sim g'$.

3ο βήμα Το συμπέρασμα ισχύει όταν $f =< a >$ για $a \in K^*$.

Έστω M ο συμμετρικός πίνακας που αντιστοιχεί στην g και M' ο πίνακας που αντιστοιχεί στην g'. Τότε στην $f \perp g$ αντιστοιχεί ο πίνακας

$$\left[\begin{array}{c|c} a & 0 \\ \hline 0 & M \end{array}\right] \tag{2.10}$$

και στην $f \perp g'$ ο πίνακας

$$\left[\begin{array}{c|c} a & 0 \\ \hline 0 & M' \end{array}\right] \tag{2.11}$$

και υπάρχει αντιστρέψιμος πίνακας της μορφής

$$\left[\begin{array}{c|c} \alpha & B \\ \hline C & D \end{array}\right] \tag{2.12}$$

ώστε

$$\left[\begin{array}{c|c} a & 0 \\ \hline 0 & M' \end{array}\right] = \left[\begin{array}{c|c} \alpha & B \\ \hline C & D \end{array}\right]^t \cdot \left[\begin{array}{c|c} a & 0 \\ \hline 0 & M \end{array}\right] \cdot \left[\begin{array}{c|c} \alpha & B \\ \hline C & D \end{array}\right] \tag{2.13}$$

$$\Rightarrow \begin{cases} \alpha^2 a + C^t M C = a & (1) \\ \alpha a B + C^t M D = 0 & (2) \\ a B^t B + D^t M D = M' & (3) \end{cases}$$

Αρκεί να αποδείξουμε ότι υπάρχει αντιστρέψιμος πίνακας E ώστε $M' = E^t M E$. Θέτουμε $E = D + sCB$ για κάποιο $s \in K$ το οποίο θα ταυτοποιήσουμε στην συνέχεια. Από τις σχέσεις (1), (2), (3) έχουμε:

$$\begin{aligned} E^t M E = (D + sCB)^t M (D + sCB) &= (D^t + sB^t C^t) M (D + sCB) \\ &= D^t M D + sB^t C^t M D + sD^t M C B + s^2 B^t C^t M C B \\ &= D^t M D + sB^t(-\alpha a B) + s(-\alpha a B)^t B + s^2 B^t (a - \alpha^2 a) B \\ &= D^t M D + a[(1-\alpha^2)s^2 - 2\alpha s] B^t B \end{aligned}$$

Από την (3) για να ισχύει $E^t M E = M'$ πρέπει $(1-\alpha^2)s^2 - 2\alpha s = 1 \Leftrightarrow (\alpha s + 1)^2 = s^2 \Rightarrow s = \begin{cases} \alpha s + 1 \\ \text{ή} \\ -(\alpha s + 1) \end{cases}$

Άρα επιλέγουμε $s = \frac{1}{1-\alpha}$ αν $\alpha \neq 1$ και $s = -\frac{1}{2}$ αν $\alpha = 1$ και έχουμε

$$E^t M E = M'$$

δηλαδή $g \sim g'$.

4ο βήμα Το συμπέρασμα ισχύει αν $f =< a_1, a_2, ..., a_n >$.
Πράγματι η f γράφεται $f =< a_1 > \perp < a_2> \perp \ ... \ \perp < a_n >$ και εφαρμόζοντας διαδοχικά τα βήματα 2 αν $a_i = 0$ και 3 αν $a_i \neq 0$ παίρνουμε $g \sim g'$.

Στην γενική περίπτωση επειδή υπάρχει διαγώνια τετραγωνική μορφή f' ώστε $f \sim f'$ έχουμε $f \perp g \sim f \perp g' \Rightarrow f' \perp g \sim f' \perp g'$, και το συμπέρασμα έπεται από το βήμα 4. □

Ορισμός 2.2.6. Αν $f =< a_1, a_2, ..., a_n >, g =< b_1, b_2, ..., b_n >$ διαγώνιες τετραγωνικές μορφές, οι f και g λέγονται γειτονικές όταν ισχύει μία από τις παρακάτω προτάσεις:
(1) Υπάρχει ακριβώς ένας δείκτης i ώστε $< a_i > \sim < b_i >$ και $a_k = b_k$ για κάθε $k \neq i$
(2) Υπάρχουν ακριβώς δύο δείκτες i, j, $(i \neq j)$ ώστε $< a_i, a_j > \sim < b_i, b_j >$ και $a_k = b_k$ για καθε $k \neq i, j$.

Παρατήρηση 2.2.7. *(1) Είναι προφανές ότι αν οι f και g είναι γειτονικές τότε $f \sim g$.*
(2) Επίσης αν οι f και g μπορούν να συνδεθούν με μία πεπερασμένη αλυσίδα γειτονικών τετραγωνικών μορφών, δηλαδή υπάρχουν τετραγωνικές μορφές $f_1, f_2, ..., f_n$ ώστε η f_i είναι γειτονική με την f_{i+1} για κάθε $i = 1, 2, ..., n-1$ και $f \sim f_1 \sim f_2 \sim ... \sim f_n \sim g$ τότε $f \sim g$.

Θεώρημα 2.2.8. ***(2ο Θεώρημα του Witt)***
Έστω f και g διαγώνιες τετραγωνικές μορφές και $f \sim g$. Τότε υπάρχει αλυσίδα διαγώνιων τετραγωνικών μορφών $f_0, f_1, ..., f_m$ ώστε να ισχύει:
(i) $f_0 = f$, $f_m = g$ και
(ii) Οι f_i, f_{i+1} είναι γειτονικές για κάθε $i = 0, 1, 2, ..., m-1$.

Για την απόδειξη του Θεωρήματος θα χρειαστούμε το επόμενο Λήμμα

Λήμμα 2.2.9. *Έστω σώμα K και f, g δύο μη ιδιάζουσες τετραγωνικές μορφές βαθμού (rank) 2 πάνω από το K. Οι f, g είναι ισοδύναμες $\Leftrightarrow$ έχουν την ίδια διακρίνουσα και παριστούν ένα κοινό στοιχείο $a \in K^*$.*

Απόδειξη. Έστω ότι $f \sim g$, A είναι ο πίνακας που αντιστοιχεί στην f και B είναι ο πίνακας που αντιστοιχεί στην g. Τότε υπάρχει αντιστρέψιμος πίνακας M ώστε $A = M^t B M$ και άρα

$$det(A) = det(B) det(M)^2$$

Δηλάδη $d(f) = d(g)$ (ως στοιχεία της ${}^{K^*}\!/_{K^{*2}}$). Επίσης αφού $f(x) = g(Mx)$ οι f και g παριστούν τα ίδια στοιχεία.
Έστω τώρα ότι οι f και g έχουν την ίδια διακρίνουσα και παριστούν ένα κοινό στοιχείο $a \in K^*$. Τότε $f \sim < a, b >$ για κάποιο $b \in K^*$. Πράγματι η f είναι ισοδύναμη με μια μη-ιδιάζουσα τετραγωνική μορφή $< a_1, a_2 >$ και
$a_1, a_2 \in K^*$. Τότε η $< a_1, a_2 >$ παριστά το a. Δηλαδή υπάρχουν $x_1, x_2 \in K^*$

ώστε $a_1x_1^2 + a_2x_2^2 = a$. Τότε για $b := a_1a_2^2x_2^2 + a_2a_1^2x_1^2$, και τον αντιστρέψιμο πίνακα

$$S = \begin{bmatrix} x_1 & a_2x_2 \\ x_2 & -a_1x_1 \end{bmatrix} \tag{2.14}$$

□

έχουμε

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = S^t \cdot \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} \cdot S \tag{2.15}$$

Δηλαδή $< a_1, a_2 > \sim < a, b >$ και συνεπώς $f \sim < a, b >$. Όμοια υπάρχει $b' \in K$ ώστε $g \sim < a, b' >$. Εξ υποθέσεως οι f, g έχουν την ίδια διακρίνουσα και άρα υπάρχει $c \in K^*$ ώστε $ab = ab'c^2 \Rightarrow b = b'c^2$ και άρα $< b > \sim < b' >$. Άρα τελικά

$$f \sim < a, b > = < a > \perp < b > \sim < a > \perp < b' > = < a, b' > \sim g$$

Ορισμός 2.2.10. Δύο τετραγωνικές μορφές f και g οι οποίες συνδέονται μέσω μιας πεπερασμένης αλυσίδας γειτονικών τετραγωνικών μορφών τις ονομάζουμε αλυσιδο-ισοδύναμες και συμβολίζουμε $f \approx g$.

Παρατήρηση 2.2.11. *Οι τετραγωνικές μορφές οι οποίες συνδέονται μέσω μιας μετάθεσης των μεταβλητών είναι αλυσιδο-ισοδύναμες. Αυτό ισχύει διότι κάθε μετάθεση του συνόλου $\{1, 2, ..., n\}$ είναι γινόμενο αντιμεταθέσεων, επομένως σε κάθε βήμα της πεπερασμένης αλυσίδας εναλλάσονται δύο μεταβλητές.*

Απόδειξη. (Θεωρήματος 2.2.8)
Έχουμε $f \sim g$ και συνεπώς οι f και g έχουν τον ίδιο βαθμό. Άρα μέσω μιας μετάθεσης των μεταβλητών έχουμε

$$f \approx f_1 \perp s < 0 >$$

και

$$g \approx g_1 \perp s < 0 >$$

όπου οι f_1, g_1 είναι μη-ιδιάζουσες. Τότε από το 1ο Θεώρημα του Witt έχουμε $f_1 \sim g_1$ και άρα το πρόβλημα ανάγεται για μη-ιδιάζουσες τετραγωνικές μορφές.

Έστω λοιπόν $f = < a_1, a_2, ..., a_n >, g = < b_1, b_2, ..., b_n >$ μη-ιδιάζουσες τετραγωνικές μορφές με $a_i, b_i \in K^*$ για κάθε $i = 1, 2, ..., n$. Θα εφαρμόσουμε επαγωγή στον n. Για $n = 1, 2$ δεν έχουμε τίποτα να δείξουμε. Έστω ότι το Θεώρημα ισχύει για τετραγωνικές μορφές με $n - 1$ μεταβλητές, $(n \geq 3)$. Προφανώς η g παριστά το b_1 και αφού $f \sim g$ και η f παριστά το b_1. Από

όλες τις αλυσιδο-ισοδύναμες τετραγωνικές μορφές με την f επιλέγουμε την $f' =< c_1, c_2, ..., c_n >$ για την οποία ισχύει ότι η $< c_1, c_2, ..., c_r >$ παριστά το b_1 και το r είναι το ελάχιστο δυνατό. Θα δείξουμε ότι $r = 1$.

Έστω ότι $r \geq 2$. Θα καταλήξουμε σε άτοπο. Έστω $b_1 = c_1x_1^2+c_2x_2^2+...+c_rx_r^2$. Επειδή το r είναι το ελάχιστο πλήθος μεταβλητών που μπορούμε να έχουμε μία τέτοια αναπαράσταση του b_1, όλα τα υποαθροίσματα της παράστασης $c_1x_1^2 + c_2x_2^2 + ... + c_rx_r^2$, είναι μη μηδενικά. Άρα το $d := c_1x_1^2 + c_2x_2^2 \neq 0$. Επειδή οι τετραγωνικές μορφές $< c_1, c_2 >$ και $< d, c_1c_2d >$ έχουν την ίδια διακρίνουσα και παριστούν και οι δύο το $d \in K^*$, από το Λήμμα 2.2.9 έχουμε $< c_1, c_2 > \sim < d, c_1c_2d >$. Τότε

$$f \approx f' =< c_1, c_2, ..., c_n > \approx < d, c_1c_2d, c_3, ..., c_n > \approx < d, c_3, c_4, ..., c_n, c_1c_2d >$$

όπου η τελευταία σχέση ισχύει λόγω της Παρατήρησης 2.2.11 και

$$b_1 = c_1x_1^2 + c_2x_2^2 + ... + c_rx_r^2 = d1^2 + c_3x_3^2 + ... + c_rx_r^2$$

Δηλαδή βρήκαμε μια τετραγωνική μορφή, η οποία είναι αλυσιδο-ισοδύναμη με την f και παριστά το b_1 από $r - 1$ όρους. Άτοπο.
Συνεπώς $r = 1$, δηλαδή η $< c_1 >$ παριστά το b_1 και άρα $< b_1 > \sim < c_1 >$. Επομένως

$$f' =< c_1, c_2, ..., c_n > \approx < b_1, c_2, ..., c_n >$$

Όμως $f' \sim f \sim g$

$$\Rightarrow < b_1, c_2, ..., c_n > \sim < b_1, b_2, ..., b_n >= g$$

Από το 1ο Θεώρημα του Witt έχουμε $< c_2, c_3, ..., c_n > \sim < b_2, b_3, ..., b_n >$ και από την επαγωγική υπόθεση

$$\Rightarrow < c_2, c_3, ..., c_n > \approx < b_2, b_3, ..., b_n >$$

Άρα τελικά

$$f \approx < b_1, c_2, ..., c_n > \approx < b_1, b_2, ..., b_n >= g$$

□

2.3 Πραγματικές τετραγωνικές μορφές

Έχουμε ήδη δει ότι κάθε τετραγωνική μορφή $f(x_1, x_2, ..., x_n)$ είναι ισοδύναμη με μία διαγώνια τετραγωνική μορφή. Επίσης κάθε θετικός πραγματικός αριθμός είναι τέλειο τετράγωνο στο $\mathbb{R}$, επομένως $f \sim f_{(r,s)}$ όπου

$$f_{(r,s)} = x_1^2 + x_2^2 + ... + x_r^2 - x_{r+1}^2 - ... - x_{r+s}^2$$

με $r, s \in \mathbb{N}_0$ και $r + s \leq n$

Θεώρημα 2.3.1. *(Θεώρημα του Sylvester)*
Ισχύει:

$$f_{(r,s)} \sim f_{(r',s')} \Leftrightarrow (r,s) = (r',s')$$

Απόδειξη. Έστω $f_{(r,s)} \sim f_{(r',s')}$ τότε $r+s = rank(f_{(r,s)}) = rank(f_{(r',s')}) = r'+s'$. Άρα αρκεί να δείξουμε ότι $r = r'$.
Αφού $f_{(r,s)} \sim f_{(r',s')}$ υπάρχει ένας αντιστρέψιμος πίνακας $S \in M_n(\mathbb{R})$ ώστε $f_{(r',s')}(x) = f_{(r,s)}(Sx)$ για κάθε $x \in \mathbb{R}^n$. Έστω $x_1, x_2, ..., x_r \in \mathbb{R}^n$ τα οποία αποτελούν τις πρώτες r στήλες του πίνακα S^{-1}. Τότε για κάθε $i = 1, 2, ..., r$ ισχύει

$$f_{(r',s')}(x_i) = f_{(r,s)}(Sx_i) = f_{(r,s)}(e_i) = 1$$

όπου $e_i \in \mathbb{R}^n$ το οποίο έχει 1 στην i-θέση και 0 στις υπόλοιπες.
Ανάλογα αν $a_1, a_2, ..., a_r$ οποιοιδήποτε πραγματικοί αριθμοί ισχύει

$$f_{(r',s')}(\sum_{i=1}^{r} a_i x_i) = f_{(r,s)}(a_1, a_2, ..., a_r, 0, 0, ..., 0) = a_1^2 + a_2^2 + ... + a_r^2$$

Έστω ότι $r > r'$, τότε το σύνολο $\{x_1, x_2, ..., x_r, e_{r'+1}, ..., e_n\}$ αποτελείται από $r + (n - r') > n$ διανύσματα του $\mathbb{R}^n$. Άρα τα διανύσματα αυτά είναι γραμμικώς εξαρτημένα. Δηλαδή υπάρχουν $a_1, a_2, ..., a_r, b_1, b_2, ..., b_{n-r'} \in \mathbb{R}$, όχι όλα ίσα με το 0, ώστε

$$a_1x_1 + a_2x_2 + ... + a_rx_r + b_1e_{r'+1} + b_2e_{r'+2} + ... + b_{n-r'}e_n = 0$$

Επειδή τα διανύσματα $e_{r'+1}, ..., e_n$ είναι γραμμικώς ανεξάρτητα δεν γίνεται $a_i = 0$ για κάθε $i = 1, ..., r$. Συνεπώς $a_i \neq 0$ για κάποιο i. Άρα

$$f_{(r',s')}(\sum_{i=1}^{r} a_i x_i) = a_1^2 + a_2^2 + ... + a_r^2 > 0$$

Όμως

$$f_{(r',s')}(\sum_{i=1}^{r} a_i x_i) = f_{(r',s')}(-\sum_{i=1}^{n-r'} b_i e_{r'+i}) = -b_1^2 - b_2^2 - ... - b_{n-r'}^2 \leq 0$$

το οποίο είναι άτοπο. Συνεπώς $r \leq r'$.
Για λόγους συμμετρίας έχουμε $r' \leq r$ και άρα $r = r'$. Η αντίστροφη κατεύθυνση είναι προφανής. □

Από το προηγούμενο θεώρημα έπεται ότι κάθε πραγματική τετραγωνική μορφή καθορίζεται μονοσήμαντα από το ζεύγος (r, s).

Ορισμός 2.3.2. Έστω f μη-ιδιάζουσα πραγματική τετραγωνική μορφή με $rank(f) = n$. Τότε το μονοσήμαντα ορισμένο διατεταγμένο ζεύγος (r, s) για το οποίο ισχύει $f \sim f_{(r,s)}$ λέγεται υπογραφή της f.

- Η f λέγεται θετικά ορισμένη $\Leftrightarrow n = r$
- Η f λέγεται αρνητικά ορισμένη $\Leftrightarrow n = s$
- Η f λέγεται μη ορισμένη $\Leftrightarrow rs \neq 0$

2.4 Τετραγωνικές μορφές στα p-αδικά σώματα $\mathbb{Q}_p$

Έχουμε ήδη μελετήσει το σύμβολο του Hilbert στα σώματα $\mathbb{Q}_p$ για $p \in P$. Αν K είναι κάποιο από τα $\mathbb{Q}_p$, $p \in P$ τότε είναι άμεσο ότι αν $a, b \in K^*$, τότε η μη-ιδιάζουσα τετραγωνική μορφή $< a, b >$ παριστά το 1 στο K αν και μόνο αν το σύμβολο του Hilbert $(a, b) = 1$. Πράγματι αν η $< a, b >$ παριστά το 1 τότε προφανώς $(a, b) = 1$. Αντίστροφα αν $(a, b) = 1$ τότε υπάρχει $(x, y, z) \in K^3$ με $(x, y, z) \neq (0, 0, 0)$ ώστε

$$ax^2 + by^2 = z^2$$

Αν $z \neq 0$ τότε $a(\frac{x}{z})^2 + b(\frac{y}{z})^2 = 1$ και άρα η $< a, b >$ παριστά το 1.
Αν $z = 0$ τότε η $< a, b >$ παριστά το 0 και από την Πρόταση 2.1.19 παριστά κάθε στοιχείο του K και συνεπώς και το 1.

Ορισμός 2.4.1. Έστω f μια μη-ιδιάζουσα διαγώνια τετραγωνική μορφή με $f =< a_1, a_2, ..., a_n >$. Ορίζουμε την αναλλοίωτη του Hasse

$$\varepsilon(< a_1, a_2, ..., a_n >) = \prod_{1 \leq i < j \leq n} (a_i, a_j)$$

όπου (a_i, a_j) το σύμβολο του Hilbert, και $\varepsilon(< a >) = 1$.

Θεώρημα 2.4.2. *Αν* $f =< a_1, a_2, ..., a_n > \sim g =< b_1, b_2, ..., b_n >$ *τότε* $\varepsilon(f) = \varepsilon(g)$.

Απόδειξη. Σύμφωνα με το 2ο Θεώρημα του Witt μπορούμε να υποθέσουμε ότι οι f και g είναι γειτονικές τετραγωνικές μορφές.
Έστω ότι ισχύει η πρώτη περίπτωση του ορισμού των γειτονικών τετραγωνικών μορφών. Δηλαδή υπάρχει κάποιο $i_0 \in \{1, 2, ..., n\}$ ώστε $< a_{i_0} > \sim < b_{i_0} >$ και $a_i = b_i$ για κάθε $i \in \{1, 2, ..., n\}, i \neq i_0$. Τότε $a_{i_0} = b_{i_0} c^2$ για κάποιο $c \in K^*$

και άρα $(x, a_{i_0}) = (x, b_{i_0})$ για κάθε $x \in K^*$. Άρα $\varepsilon(f) = \varepsilon(g)$.
Έστω ότι ισχύει η δεύτερη περίπτωση του ορισμού των γειτονικών τετραγωνικών μορφών. Τότε, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $a_i = b_i$ για κάθε $i \geq 3$ (αυτό είναι εφικτό αν εφαρμόσουμε μια μετάθεση των δεικτών) και $< a_1, a_2 > \sim < b_1, b_2 >$.
Αφού $< a_1, a_2 > \sim < b_1, b_2 > \Rightarrow d(< a_1, a_2 >) = d(< b_1, b_2 >) \Rightarrow a_1 a_2 = b_1 b_2 d^2$ για κάποιο $d \in K^*$. Επίσης η $< a_1, a_2 >$ παριστά το 1 αν και μόνο αν η $< b_1, b_2 >$ παριστά το 1 και άρα $(a_1, a_2) = (b_1, b_2)$. Επομένως

$$\begin{aligned}
\varepsilon(f) = \varepsilon(< a_1, a_2, ..., a_n >) &= \prod_{1 \leq i < j \leq n} (a_i, a_j) \\
&= (a_1, a_2)(a_1, a_3)...(a_1, a_n)(a_2, a_3)...(a_2, a_n). \prod_{3 \leq i < j \leq n} (a_i, a_j) \\
&= (a_1, a_2)(a_1, a_3 a_4 ... a_n)(a_2, a_3 a_4 ... a_n) \prod_{3 \leq i < j \leq n} (a_i, a_j) \\
&= (a_1, a_2)(a_1 a_2, b_3 b_4 ... b_n) \prod_{3 \leq i < j \leq n} (b_i, b_j) \\
&= (b_1, b_2)(b_1 b_2, b_3 b_4 ... b_n) \prod_{3 \leq i < j \leq n} (b_i, b_j) = \varepsilon(g)
\end{aligned}$$

□

Ορισμός 2.4.3. Έστω f μια μη-ιδιάζουσα τετραγωνική μορφή με $rank(f) = n$. Ορίζουμε την αναλλοίωτη του Hasse $\varepsilon(f) = \varepsilon(< a_1, a_2, ..., a_n >)$ όπου $< a_1, a_2, ..., a_n >$ είναι οποιαδήποτε διαγώνια τετραγωνική μορφή ισοδύναμη προς την f.

Θα δώσουμε τώρα δύο κριτήρια για το πότε μια μη-ιδιάζουσα τετραγωνική μορφή πάνω από το $\mathbb{Q}_p$, $p \in \mathbb{P}$ παριστά το 0 ή κάποιο στοιχείο $a \in \mathbb{Q}_p^* / \mathbb{Q}_p^{*2}$.

Θεώρημα 2.4.4. *Έστω $p \in \mathbb{P}$ και f μια μη-ιδιάζουσα τετραγωνική μορφή με συντελεστές στο $\mathbb{Q}_p$, με $rank(f) = n$ και $d := d(f) \in \mathbb{Q}_p^* / \mathbb{Q}_p^{*2}$, και $\varepsilon := \varepsilon(f) \in \{\pm 1\}$. Η f παριστά το 0 στις ακόλουθες περιπτώσεις:*
(i) $n = 2$ και $d = -1$
(ii) $n = 3$ και $(-1, -d) = \varepsilon$
(iii) $n = 4$ και $d \neq 1$ ή ($d = 1$ και $\varepsilon = (-1, -1)$)
(iv) $n \geq 5$

Πόρισμα 2.4.5. *Έστω $p \in \mathbb{P}$ και f μια μη-ιδιάζουσα τετραγωνική μορφή με συντελεστές στο $\mathbb{Q}_p$, με $rank(f) = n$ και $d := d(f) \in \mathbb{Q}_p^* / \mathbb{Q}_p^{*2}$, και $\varepsilon := \varepsilon(f) \in \{\pm 1\}$. Η f παριστά το $a \in \mathbb{Q}_p^* / \mathbb{Q}_p^{*2}$ στις ακόλουθες περιπτώσεις:*
(i) $n = 1$ και $a = d$
(ii) $n = 2$ και $(a, -d) = \varepsilon$

(iii) $n = 3$ *και* $a \neq -d$ *ή* $(a = -d$ *και* $\varepsilon = (-1, -d))$
(iv) $n \geq 4$

Οι αποδείξεις του Θεωρήματος 2.4.4 και του Πορίσματος 2.4.5 θα γίνουν παράλληλα. Θυμίζουμε, από την Πρόταση 2.1.20, ότι μια μη-ιδιάζουσα τετραγωνική μορφή f παριστά το $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \Leftrightarrow$ η τετραγωνική μορφή $f \perp < -a >$ παριστά το 0.

Παρατήρηση 2.4.6. *Αν* f *είναι μια μη ιδιάζουσα τετραγωνική μορφή με συντελεστές στο* $\mathbb{Q}_p^*$, *με* $rank(f) = n$ *και* $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, *τότε η τετραγωνική μορφή* $f \perp < -a >$ *είναι μη-ιδιάζουσα με* $rank(f \perp < -a >) = n+1$. *Επίσης αν* $d := d(f), \varepsilon := \varepsilon(f)$ *τότε* $d(f \perp < -a >) = -da$ *και* $\varepsilon(f \perp < -a >) = (-a, d)\varepsilon$.
Πράγματι τα αποτελέσματα για τον βαθμό και την διακρίνουσα είναι προφανή. Θα αποδείξουμε ότι $\varepsilon(f \perp < -a >) = (-a, d)\varepsilon$.
Έστω ότι $f \sim < a_1, a_2, ..., a_n >$, *δηλαδή* $\varepsilon = \varepsilon(< a_1, a_2, ..., a_n >)$. *Έστω* $a_{n+1} := -a$ *τότε*

$$\varepsilon(f \perp < -a >) = \varepsilon(< a_1, a_2, ..., a_n, a_{n+1} >) = \prod_{1 \leq i < j \leq n+1} (a_i, a_j)$$
$$= (a_1, a_2)(a_1, a_3)...(a_1, a_n)(a_1, a_{n+1})(a_2, a_3)...(a_2, a_n)(a_2, a_{n+1})$$
$$...(a_{n-1}, a_n)(a_{n-1}, a_{n+1})(a_n, a_{n+1})$$
$$= \varepsilon(f)(a_1 a_2 ... a_n, a_{n+1}) = \varepsilon(d, -a) = (-a, d)\varepsilon$$

Απόδειξη. (Θεωρήματος 2.4.4 - Πορίσματος 2.4.5)
Μια μη-ιδιάζουσα τετραγωνική μορφή βαθμού 1 δεν παριστά ποτέ το μηδέν διότι έχει την μορφή $f = ax^2$ με $a \neq 0$. Χωρίς βλάβη της γενικότητας, θεωρούμε ότι η f είναι διαγώνια τετραγωνική μορφή $f =< a_1, a_2, ..., a_n >, a_1, a_2, ..., a_n \in \mathbb{Q}_p^*$.

- Απόδειξη του (i) του Θεωρήματος:
  Έστω $f =< a_1, a_2 >$. Η f παριστά το μηδέν αν και μόνο αν υπάρχουν $x_1, x_2 \in \mathbb{Q}_p^*$ ώστε $a_1 x_1^2 + a_2 x_2^2 = 0$. Ισοδύναμα

$$(\tfrac{x_2}{x_1})^2 = -\tfrac{a_1}{a_2} \Leftrightarrow -\tfrac{a_1}{a_2} \in \mathbb{Q}_p^{*2} \Leftrightarrow -a_1 a_2 \in \mathbb{Q}_p^{*2} \Leftrightarrow -d = 1 \Leftrightarrow d = -1$$

- Απόδειξη (i) του Πορίσματος:
  Αν f μη-ιδιάζουσα τετραγωνική μορφή βαθμού 1, τότε η f παριστά το $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ αν και μόνο αν η $f \perp < -a >$ παριστά το μηδέν. Όμως η $f \perp < -a >$ έχει βαθμό 2 οπότε από το (i) του Θεωρήματος 2.4.4

$$d(f \perp < -a >) = -1 \Leftrightarrow -ad = -1 \Leftrightarrow ad = 1 \Leftrightarrow ad^2 = d \Leftrightarrow a = d$$

- Απόδειξη του (ii) του Θεωρήματος:
Έστω $f =< a_1, a_2, a_3 >$. Τότε η f παριστά το μηδέν αν και μόνο αν η $-a_3 f \sim< -a_3a_1, -a_3a_2, -1 >$ παριστά το μηδέν. Από τον ορισμό του συμβόλου του Hilbert η $< -a_3a_1, -a_3a_2, -1 >$ παριστά το μηδέν $\Leftrightarrow (-a_3a_1, -a_3a_2) = 1$. Όμως
$(-a_3a_1, -a_3a_2) =$
$(-1,-1)(-1,a_3)(-1,a_2)(a_3,-1)(a_3,a_3)(a_3,a_2)(a_1,-1)(a_1,a_3)(a_1,a_2) =$
$(-1,-1)(-1,a_3)(a_3,a_3)[(-1,a_1)(-1,a_2)(-1,a_3)][(a_1,a_2)(a_1,a_3)(a_2,a_3)] =$
$(-1,-1)(-1,a_3)(a_3,a_3)(-1,a_1a_2a_3)\varepsilon =$
$(-1,-1)(-a_3,a_3)(-1,d)\varepsilon = (-1,-d)\varepsilon$
Άρα η f παριστά το μηδέν $\Leftrightarrow (-1,-d)\varepsilon = 1 \Leftrightarrow \varepsilon = (-1,-d)$.

- Απόδειξη του (ii) του Πορίσματος:
Η f παριστά το $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ αν και μόνο αν η $f \perp< -a >$ παριστά το μηδέν. Επειδή η $f \perp< -a >$ έχει βαθμό 3 από το (ii) του Θεωρήματος 2.4.4 αυτό συμβαίνει $\Leftrightarrow (-1, -d(f \perp< -a >) = \varepsilon(f \perp< -a >)$. Όμως
$(-1, -d(f \perp< -a >)) = \varepsilon(f \perp< -a >) \Leftrightarrow$
$(-1, ad) = (-a, d)\varepsilon \Leftrightarrow$
$(-1, ad)(-a, d) = \varepsilon \Leftrightarrow$
$(-1, a)(-1, d)(-a, d) = \varepsilon \Leftrightarrow$
$(-1, a)(a, d) = \varepsilon \Leftrightarrow$
$(a, -d) = \varepsilon$

- Απόδειξη του (iii) του Θεωρήματος:
Η $f =< a_1, a_2, a_3, a_4 >$ παριστά το μηδέν αν και μόνο αν οι τετραγωνικές μορφές $< a_1, a_2 >$ και $< -a_3, -a_4 >$ παριστούν κάποιο κοινό στοιχείο $x \in \mathbb{Q}_p$. Αν $x = 0$ τότε από την Πρόταση 2.1.19 οι $< a_1, a_2 >$ και $< -a_3, -a_4 >$ παριστούν όλα τα στοιχεία του $\mathbb{Q}_p$. Συνεπώς η f παριστά το μηδέν αν και μόνο αν οι $< a_1, a_2 >$ και $< -a_3, -a_4 >$ παριστούν κάποιο κοινό στοιχείο $x \in \mathbb{Q}_p^*$.
Από το (ii) του Πορίσματος η $< a_1, a_2 >$ παριστά το x

$$\Leftrightarrow (x, -d(< a_1, a_2 >) = \varepsilon(< a_1, a_2 >) \Leftrightarrow (x, -a_1a_2) = (a_1, a_2)$$

Όμοια η $< -a_3, -a_4 >$ παριστά το x

$$\Leftrightarrow (x - a_3a_4) = (-a_3, -a_4)$$

Τελικά η f παριστά το 0 αν και μόνο αν υπάρχει κάποιο $x \in \mathbb{Q}_p^*$ ώστε

$$(x, -a_1a_2) = (a_1, a_2) \text{ και } (x - a_3a_4) = (-a_3, -a_4)$$

Σύμφωνα με την Πρόταση 1.4.12 δεν υπάρχει τέτοιο x αν

$$H_{-a_1a_2}^{(a_1,a_2)} \cap H_{-a_3a_4}^{(-a_3,-a_4)} = \emptyset$$

Τα σύνολα $H_{-a_1a_2}^{(a_1,a_2)}, H_{-a_3a_4}^{(-a_3,-a_4)}$ είναι μη κενά διότι:

$$(a_1, -a_1a_2) = (a_1, -a_1)(a_1, a_2) = (a_1, a_2)$$

και άρα $a_1 \in H_{-a_1a_2}^{(a_1,a_2)}$. Όμοια

$$(-a_3, -a_3a_4) = (-a_3, a_3)(-a_3, -a_4) = (-a_3, -a_4)$$

και άρα $-a_3 \in H_{-a_3a_4}^{(-a_3,-a_4)}$. Επομένως, από την Πρόταση 1.4.12, έπεται ότι δεν υπάρχει το ζητούμενο x αν και μόνο αν $a_1a_2 = a_3a_4$ και $(a_1, a_2) = -(-a_3, -a_4)$. Όμως $a_1a_2 = a_3a_4 \Leftrightarrow d = 1$ και τότε από την δι-πολλαπλασιαστικότητα του συμβόλου του Hilbert και την ιδιότητα $(a, a) = (-1, a)$ έχουμε:

$$\begin{aligned}
&\varepsilon(f) = \prod_{1\le i<j\le 4} (a_i, a_j) = \\
&(a_1, a_2)(a_1, a_3)(a_1, a_4)(a_2, a_3)(a_2, a_4)(a_3, a_4) = \\
&(a_1, a_2)(a_1, a_3a_4)(a_2, a_3a_4)(a_3, a_4) = \\
&(a_1, a_2)(a_3, a_4)(a_1a_2, a_3a_4) = \\
&(a_1, a_2)(a_3, a_4)(a_3a_4, a_3a_4) = \\
&(a_1, a_2)(a_3, a_4)(-1, a_3a_4) = \\
&(a_1, a_2)(a_3, a_4)(-1, -a_3a_4)(-1, -1) = \\
&(a_1, a_2)(a_3, -a_3a_4)(-1, -a_3a_4)(-1, -1) = \\
&(a_1, a_2)(-a_3, -a_3a_4)(-1, -1) = \\
&(a_1, a_2)(-a_3, -a_4)(-1, -1)
\end{aligned}$$

Οπότε $(a_1, a_2) = -(-a_3, -a_4) \Leftrightarrow \varepsilon(f) = -(-1, -1)$. Άρα το x δεν υπάρχει

$$\Leftrightarrow d = 1 \text{ και } \varepsilon = -(-1, -1)$$

Άρα η f παριστά το 0 αν και μόνο αν $d \neq 1$ ή $(d = 1$ και $\varepsilon = (-1, -1))$.

- Απόδειξη (iii) του Πορίσματος:
  Η f παριστά το a αν και μόνο αν η $f \perp< -a >$ παριστά το μηδέν. Από το (iii) του Θεωρήματος αυτό συμβαίνει $\Leftrightarrow d(f \perp< -a >) \neq 1$ ή $d(f \perp< -a >) = 1$ και $\varepsilon(f \perp< -a >) = (-1, -1)$. Όμως

$$d(f \perp < -a >) = -ad \text{ και } \varepsilon(f \perp < -a >) = (-a, d)\varepsilon$$

Άρα $d(f \perp < -a >) = 1 \Leftrightarrow -ad = 1 \Leftrightarrow a = -d$ και τότε
$\varepsilon(f \perp < -a >) = (-1, -1) \Leftrightarrow \varepsilon = (-a, d)(-1, -1) = (-1, d)(a, d)(-1, -1) = (-1, -d)(a, d) = (-1, -d)(-d, d) = (-1, -d)$.

- Απόδειξη του (iv) του Θεωρήματος:
Αρκεί να δείξουμε ότι μία τετραγωνική μορφή f με $rank(f) = 5$ παριστά το μηδέν.
Από το Πόρισμα 2.4.5 μία τετραγωνική μορφή $q =< b_1, b_2 >$ βαθμού 2 παριστά το $x \in {}^{\mathbb{Q}_p^*}\!/_{\mathbb{Q}_p^{*2}}$ αν και μόνο αν $(x, -d(q)) = \varepsilon(q)$. Δηλαδή αν $x \in H_{-d(q)}^{\varepsilon(q)}$ (όπως στην Πρόταση 1.4.12).
Αν $d(q) = -1$, τότε $\varepsilon(q) = (b_1, b_2) = (b_1, b_2)(b_1, -b_1) = (b_1, -b_1 b_2) = (b_1, -d) = (b_1, 1) = +1$, και άρα, σύμφωνα με την Πρόταση 1.4.12, $H_{-d(q)}^{\varepsilon(q)} = {}^{\mathbb{Q}_p^*}\!/_{\mathbb{Q}_p^{*2}}$.
Αν $d(q) \neq -1$ τότε ξανά από την Πρόταση 1.4.12 $\#H_{-d(q)}^{\varepsilon(q)} \geq 2$ το οποίο σημαίνει ότι η q παριστά τουλάχιστον δύο μη μηδενικά στοιχεία. Αφού λοιπόν κάθε τετραγωνική μορφή βαθμού 2 παριστά τουλάχιστον δύο μη μηδενικά στοιχεία, το ίδιο ισχύει και για την f. Άρα υπάρχει $a \in {}^{\mathbb{Q}_p^*}\!/_{\mathbb{Q}_p^{*2}}$, $a \neq d$ ώστε η f να παριστά το a. Τότε $f \sim < a > \perp g$ όπου η g είναι μία τετραγωνική μορφή βαθμού 4. Η διακρίνουσα της g είναι

$$d(g) = \frac{d}{a} \neq 1$$

οπότε από το (iii) του Θεωρήματος η g παριστά το 0. Συνεπώς και η f παριστά το 0.
Η περίπτωση (iv) του Πορίσματος είναι άμεση.

□

Θεώρημα 2.4.7. *Έστω f, g δύο μη-ιδιάζουσες τετραγωνικές μορφές πάνω από το $\mathbb{Q}_p$, $p \in \mathbb{P}$ με $rank(f) = rank(g) = n$. Τότε:*

$$f \sim g \Leftrightarrow d(f) = d(g) \text{ και } \varepsilon(f) = \varepsilon(g).$$

Απόδειξη. Η μία κατεύθυνση είναι προφανής. Έστω ότι $d(f) = d(g)$ και $\varepsilon(f) = \varepsilon(g)$. Θα κάνουμε επαγωγή στο βαθμό n.
Για $n = 1$ είναι προφανές. Υποθέτουμε ότι ισχύει για τετραγωνικές μορφές βαθμού $n - 1$. Αφού $d(f) = d(g)$ και $\varepsilon(f) = \varepsilon(g)$ σύμφωνα με το Πόρισμα

2.4.5 οι f και g παριστούν τα ίδια στοιχεία του $\mathbb{Q}_p^*$. Έστω $a \in \mathbb{Q}_p^*$, το οποίο παριστούν οι f, g. Τότε $f \sim < a > \perp f_1$ και $f \sim < a > \perp g_1$, όπου οι f_1, g_1 είναι μη-ιδιάζουσες βαθμού $n-1$. Τότε

$$d(f_1) = \frac{d(f)}{a} = \frac{d(g)}{a} = d(g_1)$$

και

$$\varepsilon(f_1) = \varepsilon(f)(a, d(f_1)) = \varepsilon(g)(a, d(g_1)) = \varepsilon(g_1)$$

Άρα από την επαγωγική υπόθεση $f_1 \sim g_1$ και συνεπώς $f \sim g$. □

2.5 Το Θεώρημα των Hasse-Minkowski

Έστω f μία τετραγωνική μορφή με συντελεστές στο σώμα $\mathbb{Q}$. Για κάθε $v \in P = \mathbb{P} \cup \{\infty\}$, $\mathbb{Q} \subset \mathbb{Q}_v$, οπότε η f μπορεί να θεωρηθεί ως τετραγωνική μορφή στο $\mathbb{Q}_v$ για κάθε $v \in P$. Συμβολίζουμε την f θεωρούμενη στο $\mathbb{Q}_v$ με f_v.
Είναι προφανές ότι αν η f παριστά το 0 στο $\mathbb{Q}$, τότε η f_v παριστά το 0 στο $\mathbb{Q}_v$ για κάθε $v \in P$. Το ερώτημα που μας ενδιαφέρει να απαντήσουμε είναι αν ισχύει το αντίστροφο. Η απάντηση θα δοθεί από το επόμενο Θεώρημα.

Θεώρημα 2.5.1. *(Hasse-Minkowski)*
Έστω f μία τετραγωνική μορφή με συντελεστές στο $\mathbb{Q}$. Η f παριστά το 0 στο $\mathbb{Q}$ αν και μόνο αν η f_v παριστά το 0 στο $\mathbb{Q}_v$ για κάθε $v \in P = \mathbb{P} \cup \{\infty\}$.

Πόρισμα 2.5.2. *Έστω f μία τετραγωνική μορφή στο $\mathbb{Q}$. Η f παριστά το $a \in \mathbb{Q}$ αν και μόνο αν η f_v παριστά το a στο $\mathbb{Q}_v$ για κάθε $v \in P$.*

Απόδειξη. Αν $a = 0$ ισχύει από το Θεώρημα Hasse-Minkowski. Αν η f είναι ιδιάζουσα τότε $f \sim m < 0 > \perp g$ όπου g είναι μη ιδιάζουσα τετραγωνική μορφή, και άρα η f παριστά το a αν και μόνο αν η g παριστά το a. Οπότε το πρόβλημα ανάγεται σε μη-ιδιάζουσες τετραγωνικές μορφές.
Έστω λοιπόν f μια μη-ιδιάζουσα τετραγωνική μορφή στο $\mathbb{Q}$ και $a \in \mathbb{Q}^*$. Από την Πρόταση 2.1.20, η f παριστά το a στο $\mathbb{Q}$ αν και μόνο αν η τετραγωνική μορφή $f \perp < -a >$ παριστά το 0 στο $\mathbb{Q}$. Όμως από το Θεώρημα των Hasse-Minkowski η $f \perp < -a >$ παριστά το 0 στο $\mathbb{Q}$ αν και μόνο αν η $f_v \perp < -a >$ παριστά το 0 στο $\mathbb{Q}_v$ για κάθε $v \in P$ και αυτό ισχύει αν και μόνο αν η f_v παριστά το a στο $\mathbb{Q}_v$ για κάθε $v \in P$. □

Πόρισμα 2.5.3. *Αν f είναι μια μη-ιδιάζουσα τετραγωνική μορφή στο $\mathbb{Q}$ με $rank(f) \geq 5$, τότε η f παριστά το 0 στο $\mathbb{Q}$ αν και μόνο αν είναι μη ορισμένη ως πραγματική τετραγωνική μορφή.*

Απόδειξη. Αφού η f είναι μη-ιδιάζουσα, για κάθε πρώτο αριθμό p η τετραγωνική μορφή f_p είναι μη-ιδιάζουσα. Έχουμε ήδη αποδείξει ότι κάθε μη-ιδιάζουσα τετραγωνική μορφή στο $\mathbb{Q}_p$, $p \in \mathbb{P}$ βαθμού μεγαλύτερου είτε ίσου του 5 παριστά πάντα το 0 στο $\mathbb{Q}_p$. Συνεπώς σύμφωνα με το Θεώρημα των Hasse-Minkowski, Η f παριστά το 0 στο $\mathbb{Q}$ αν και μόνο αν παριστά το 0 στο $\mathbb{R}$, δηλαδή αν και μόνο αν είναι μη ορισμένη. □

Προχωράμε τώρα στην απόδειξη του Θεωρήματος Hasse-Minkowski.

Απόδειξη. (Θεωρήματος Hasse-Minkowski)
Αφού κάθε ιδιάζουσα τετραγωνική μορφή παριστά το μηδέν, χωρίς βλάβη της γενικότητας, υποθέτουμε ότι η f είναι μη-ιδιάζουσα. Θα ξεχωρίσουμε περιπτώσεις ανάλογα με τον βαθμό n $(rank(f))$ της f.

- **Περίπτωση 1:** $n = 1$
  Τότε $f =< a >$ με $a \neq 0$. Μια μη-ιδιάζουσα τετραγωνική μορφή βαθμού 1 δεν παριστά ποτέ το 0 στο σώμα $\mathbb{Q}$ αλλά ούτε στα $\mathbb{Q}_\upsilon$, $\upsilon \in P$.

  Μπορούμε να υποθέσουμε ότι η f είναι διαγώνια, οπότε για τις επόμενες περιπτώσεις θεωρούμε $f =< a_1, a_2, ..., a_n >$ με $a_i \in \mathbb{Q}^*$ για κάθε $i = 1, 2, ..., n$.

- **Περίπτωση 2:** $n = 2$
  Η $f =< a_1, a_2 >$ παριστά το $\mathbb{Q}$ αν και μόνο αν υπάρχουν $x_1, x_2 \in \mathbb{Q}^*$ ώστε

  $$a_1 x_1^2 + a_2 x_2^2 = 0 \Leftrightarrow -\tfrac{a_1}{a_2} = (\tfrac{x_2}{x_1})^2$$

  Δηλαδή ακριβώς τότε όταν $-\frac{a_1}{a_2} \in \mathbb{Q}^{*2}$.Όμως ένας ρητός αριθμός είναι τέλειο τετράγωνο στο $\mathbb{Q}^*$ αν και μόνο αν είναι τέλειο τετράγωνο στα $\mathbb{Q}_\upsilon$ για κάθε $\upsilon \in P$. Άρα

  $$-\tfrac{a_1}{a_2} \in \mathbb{Q}^{*2} \Leftrightarrow -\tfrac{a_1}{a_2} \in \mathbb{Q}_\upsilon^{*2} \text{ για κάθε } \upsilon \in P$$

  και το τελευταίο ισχύει αν και μόνο αν η f_υ παριστά το 0 στο $\mathbb{Q}_\upsilon$ για κάθε $\upsilon \in P$.

- **Περίπτωση 3:** $n = 3$
  Έστω $f =< a_1, a_2, a_3 >$, με $a_1, a_2, a_3 \in \mathbb{Q}^*$. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι:
  (i) $a_1, a_2, a_3 \in \mathbb{Z}$
  (ii) τα a_1, a_2, a_3 είναι ελεύθερα τετραγώνου
  (iii) τα a_1, a_2, a_3 είναι πρώτα μεταξύ τους ανά δύο

Πράγματι αν υπάρχει πρώτος p ώστε $p \mid a_1, a_2$, η τετραγωνική μορφή $< a_1, a_2, a_3 >$ παριστά το 0 αν και μόνο αν η $< pa_1, pa_2, pa_3 >$ παριστά το 0. Όμως η $< pa_1, pa_2, pa_3 >$ είναι ισοδύναμη με την $< \frac{a_1}{p}, \frac{a_2}{p}, pa_3 >$ και άρα τότε και η $< \frac{a_1}{p}, \frac{a_2}{p}, pa_3 >$ παριστά το 0. Όμως αφού τα a_1, a_2, a_3 είναι ελεύθερα τετραγώνου $p \nmid \frac{a_1}{p}, \frac{a_2}{p}$. (Αν $p \mid a_3$ αντικαθιστούμε το pa_3 με $\frac{a_3}{p}$.)

Για να παριστά η f το 0 στο $\mathbb{R}$ πρέπει τουλάχιστον ένα από τα a_1, a_2, a_3 να είναι αρνητικός αριθμός και τουλάχιστον ένα να είναι θετικός αριθμός, και επειδή αν η f παριστά το 0 και η $-f$ παριστά το 0 μπορούμε τελικά να θεωρήσουμε ότι $f =< a, b, -c >$ με $a, b, c \in \mathbb{N}$. Αν $a = b = c = 1$ τότε προφανώς η εξίσωση

$$x^2 + y^2 - z^2 = 0$$

έχει λύση $(x, y, z) = (1, 0, 1)$ στο $\mathbb{Q}$ καθώς και στα $\mathbb{Q}_v$ για κάθε $v \in P$. Υποθέτουμε λοιπόν ότι $abc > 1$ και ότι η f παριστά το 0 στα $\mathbb{Q}_v$ για κάθε $v \in P$.

Έστω $p \in \mathbb{P}$ με $p \mid c$ τότε η $f =< a, b, -c >$ παριστά το 0 στο $\mathbb{Q}_p$. Δηλαδή υπάρχουν $\alpha, \beta, \gamma \in \mathbb{Q}_p$ όχι όλα μηδέν και $a\alpha^2 + b\beta^2 = c\gamma^2$. Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι $\alpha, \beta, \gamma \in \mathbb{Z}_p$ και τουλάχιστον ένα από αυτά είναι μονάδα του $\mathbb{Z}_p$. Θα δείξουμε ότι $\beta \in \mathbb{Z}_p^*$. Πράγματι αν $\beta \in p\mathbb{Z}_p$ τότε $c\gamma^2 - a\alpha^2 \in p^2\mathbb{Z}_p$ και άρα $a\alpha^2 \in p\mathbb{Z}_p$. Όμως $p \nmid a$ και άρα αναγκαστικά $\alpha \in p\mathbb{Z}_p$. Τότε $c\gamma^2 = a\alpha^2 + b\beta^2 \in p^2\mathbb{Z}_p \Rightarrow \gamma \in p\mathbb{Z}_p$. Δηλαδή $\alpha, \beta, \gamma \in p\mathbb{Z}_p$ που είναι άτοπο.
Από την σχέση

$$a\alpha^2 + b\beta^2 = c\gamma^2$$

έχουμε $b \equiv -a\frac{\alpha^2}{\beta^2} mod p$. Άρα

$$ax^2 + by^2 - cz^2 \equiv a\beta^{-2}(\beta x + \alpha y)(\beta x - \alpha y) mod p$$

Δηλαδή η τετραγωνική μορφή f αναλύεται σε γινόμενο δύο γραμμικών παραγόντων $mod p$ για κάθε πρώτο p με $p \mid c$. Επειδή το c είναι ελεύθερο τετραγώνου από το Κινέζικο Θεώρημα Υπολοίπων η τετραγωνική μορφή f αναλύεται σε γινόμενο δύο γραμμικών παραγόντων $mod c$ (βλ. [3] σελ. 86).
Εργαζόμενοι ανάλογα για τους πρώτους παράγοντες των a, b παίρνουμε ότι η f αναλύεται σε γινόμενο δύο γραμμικών παραγόντων $mod a$ και

$modb$, και, επειδή τα a, b, c είναι πρώτα μεταξύ τους ανά δύο, από το Κινέζικο Θεώρημα Υπολοίπων υπάρχουν $A, B, C, A', B', C' \in \mathbb{Z}$ ώστε

$$ax^2 + by^2 - cz^2 \equiv (Ax + By + Cz)(A'x + B'y + C'z) mod(abc)$$

Για κάθε θετικό πραγματικό αριθμό r στο διάστημα $[0, r)$ υπάρχουν ακριβώς $[r] + 1 > r$ ακέραιοι αν $r \notin \mathbb{N}$ και ακριβώς r αν $r \in \mathbb{N}$. Επειδή οι φυσικοί αριθμοί a, b, c είναι ελεύθεροι τετραγώνου και τουλάχιστον ένας είναι μεγαλύτερος του 1, τουλάχιστον ένας από τους πραγματικούς αριθμούς $\sqrt{ab}, \sqrt{ac}, \sqrt{bc}$, δεν είναι ακέραιος. Επομένως υπάρχουν περισσότερες από abc τριάδες ακεραίων (x, y, z) στο καρτεσιανό γινόμενο $S := [0, \sqrt{bc}) \times [0, \sqrt{ac}) \times [0, \sqrt{ab})$. Όμως

$$\#\{(Ax + By + Cz) mod(abc) | (x, y, z) \in S \cap \mathbb{Z}\} \leq abc$$

Άρα υπάρχουν $(x_1, y_1, z_1), (x_2, y_2, z_2) \in S \cap \mathbb{Z}$ με $(x_1, y_1, z_1) \neq (x_2, y_2, z_2)$ ώστε να ισχύει η ισοτιμία

$$Ax_1 + By_1 + Cz_1 \equiv (Ax_2 + By_2 + Cz_2) mod(abc)$$

Έστω $(x_0, y_0, z_0) = (x_1, y_1, z_1) - (x_2, y_2, z_2) \neq (0, 0, 0)$. Τότε

$$Ax_0 + By_0 + Cz_0 \equiv 0 mod(abc)$$

Άρα

$$ax_0^2 + by_0^2 - cz_0^2 \equiv (Ax_0 + By_0 + Cz_0)(A'x_0 + B'y_0 + C'z_0) mod(abc)$$

$$\Rightarrow ax_0^2 + by_0^2 - cz_0^2 \equiv 0 mod(abc)$$

Συνεπώς υπάρχει $N \in \mathbb{Z}$ ώστε $ax_0^2 + by_0^2 - cz_0^2 = Nabc$.
Τώρα $0 \leq x_1, x_2 < \sqrt{bc} \Rightarrow -\sqrt{bc} < x_1 - x_2 < \sqrt{bc} \Rightarrow |x_0| < \sqrt{bc}$.
Όμοια $|y_0| < \sqrt{ac}$ και $|z_0| < \sqrt{ab}$. Άρα

$$ax_0^2 < abc, \qquad by_0^2 < abc, \qquad -cz_0^2 > -abc$$

Τότε έχουμε

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc$$

$$\Leftrightarrow -abc < Nabc < 2abc$$

$$\Leftrightarrow -1 < N < 2$$

Άρα $N = 0$ ή $N = 1$.
Αν $N = 0$ τότε $ax_0^2 + by_0^2 - cz_0^2 = 0$ και αφού $(x_0, y_0, z_0) \neq (0, 0, 0)$ η f

παριστά το 0 στο $\mathbb{Q}$.
Αν $N = 1$ έχουμε

$$ax_0^2 + by_0^2 - cz_0^2 = abc$$

$$\Rightarrow a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0$$

και αφού $z_0^2 + ab > 0$ η f παριστά το 0 στο $\mathbb{Q}$.

- **Περίπτωση 4:** $n = 4$
Έστω $f =< a_1, a_2, a_3, a_4 >$ η οποία παριστά το 0 θεωρούμενη στο $\mathbb{Q}_v$ για κάθε $v \in P$. Άρα οι τετραγωνικές μορφές $< a_1, a_2 >$ και $< -a_3, -a_4 >$ θεωρούμενες στα $\mathbb{Q}_v$ παριστούν ένα κοινό στοιχείο στο $\mathbb{Q}_v$ για κάθε $v \in P$. Αρκεί να δείξουμε ότι παριστούν ένα κοινό στοιχείο και στο $\mathbb{Q}$. Αν οι $< a_1, a_2 >$ και $< -a_3, -a_4 >$ παριστούν το 0 στο $\mathbb{Q}_v$, αφού είναι μη-ιδιάζουσες από την Πρόταση 2.1.19 παριστούν κάθε στοιχείο του $\mathbb{Q}_v$. Άρα οι $< a_1, a_2 >, < -a_3, -a_4 >$ παριστούν ένα κοινό στοιχείο $x_v \in \mathbb{Q}_v^*$ για κάθε $v \in P = \mathbb{P} \cup \{\infty\}$.
Τότε, σύμφωνα με το Πόρισμα 2.4.5, για κάθε πρώτο $p \in \mathbb{P}$ ισχύει

$$(x_p, -a_1a_2)_p = (a_1, a_2)_p$$

και

$$(x_p, -a_3a_4)_p = (-a_3, -a_4)_p$$

Επίσης υπάρχει $x_\infty \in \mathbb{R}$ το οποίο παριστούν οι $< a_1, a_2 >$ και $< -a_3, -a_4 >$ θεωρούμενες ως πραγματικές τετραγωνικές μορφές. Σύμφωνα με τις ιδιότητες του συμβόλου του Hilbert στο $\mathbb{R}$ $(a, b)_\infty = -1 \Leftrightarrow a < 0$ και $b < 0$. Επομένως:

$$\begin{gathered}(a_1, a_2)_\infty = -1 \Leftrightarrow a_1 < 0 \text{ και } a_2 < 0 \\ \Leftrightarrow x_\infty = a_1x_1^2 + a_2x_2^2 < 0 \text{ και } -a_1a_2 < 0 \\ \Leftrightarrow (x_\infty, -a_1a_2)_\infty = -1\end{gathered}$$

Δηλαδή $(x_\infty, -a_1a_2)_\infty = (a_1, a_2)_\infty$. Όμοια έχουμε $(x_\infty, -a_3a_4)_\infty = (-a_3, -a_4)_\infty$. Τελικά έχουμε:

$$(x_v, -a_1a_2)_v = (a_1, a_2)_v \text{ και } (x_v, -a_3a_4)_v = (-a_3, -a_4)_v \qquad (*)$$

για κάθε $v \in P$.
Θα χρησιμοποιήσουμε τώρα το Θεώρημα 1.4.13 για $\varepsilon_{1,v} = (a_1, a_2)_v$ και $\varepsilon_{2,v} = (-a_3, -a_4)_v$. Από την σχέση $(*)$ έχουμε την υπόθεση (3) του

Θεωρήματος. Επίσης από τον τύπο του γινομένου για το σύμβολο του Hilbert έχουμε:

$$\prod_{v\in P}(a_1,a_2)_v = 1 = \prod_{v\in P}(-a_3,-a_4)_v$$

Τέλος για κάθε $p \in \mathbb{P}$, $p \neq 2$ με $ord_p(a_1) = ord_p(a_2) = ord_p(a_3) = ord_p(a_4) = 0$ έχουμε $a_1, a_2, a_3, a_4 \in \mathbb{Z}_p^*$ και άρα $(a_1,a_2)_p = (-a_3,-a_4)_p = +1$. Οι πρώτοι αριθμοί p για τους οποίους ισχύει $ord_p(a_i) \neq 0$ για κάποιο $i \in \{1,2,3,4\}$ είναι πεπερασμένου πλήθους και συνεπώς όλα σχεδόν τα $(a_1,a_2)_v$ και $(-a_3,-a_4)_v$ έχουν την τιμή $+1$. Άρα από το Θεώρημα 1.4.13 υπάρχει $x \in \mathbb{Q}^*$ ώστε:

$$(x, -a_1a_2)_v = (a_1,a_2)_v$$

και

$$(x,-a_3a_4)_v = (-a_3,-a_4)_v$$

για κάθε $v \in P = \mathbb{P}\cup\{\infty\}$. Τότε, σύμφωνα με το Πόρισμα 2.4.5, και τις ιδιότητες του συμβόλου του Hilbert στο $\mathbb{R}$ έχουμε ότι οι τετραγωνικές μορφές $< a_1, a_2 >_v$ και $< -a_3, -a_4 >_v$ παριστούν το $x \in \mathbb{Q}^*$ για κάθε $v \in P$. Επειδή έχουμε ήδη αποδείξει το Θεώρημα Hasse-Minkowski για $n \leq 3$ μπορούμε να εφαρμόσουμε το Πόρισμα 2.5.2 για τετραγωνικές μορφές βαθμού 2. Άρα οι $< a_1, a_2 >$ και $< -a_3, -a_4 >$ παριστούν το $x \in \mathbb{Q}$ στο $\mathbb{Q}$ και συνεπώς η f παριστά το 0 στο $\mathbb{Q}$.

- **Περίπτωση 5:** $n \geq 5$
  Θα εφαρμόσουμε επαγωγή στο n. Έστω ότι το θεώρημα Hasse-Minkowski ισχύει για τετραγωνικές μορφές βαθμού το πολύ $n-1$. Θα αποδείξουμε ότι ισχύει για τετραγωνικές μορφές βαθμού n.
  Έστω λοιπόν ότι για κάθε $v \in P$ η f_v παριστά το 0. Όπως και στην προηγούμενη περίπτωση αυτό σημαίνει ότι για κάθε $v \in P$ υπάρχει $x_v \in \mathbb{Q}_v^*$ ώστε οι τετραγωνικές μορφές $< a_1, a_2 >_v$ και $< -a_3, -a_4, ..., -a_n >_v$ παριστούν το x_v. Δηλαδή υπάρχουν $\alpha_{1,v}, \alpha_{2,v}, ..., \alpha_{n,v} \in \mathbb{Q}_v$ ώστε

$$x_v = a_1\alpha_{1,v}^2 + a_2\alpha_{2,v}^2$$

και

$$x_v = -a_3\alpha_{3,v}^2 - a_4\alpha_{4,v}^2 - ... - a_n\alpha_{n,v}^2$$

Έστω $S := \{p \in \mathbb{P} | ord_p(a_i) \neq 0 \text{ για κάποιο } i = 1,2,...,n\} \cup \{2,\infty\}$. Το S είναι πεπερασμένο σύνολο. Από το Θεώρημα σύγχρονης Προσέγγισης για τα $v \in S$ υπάρχει ακολουθία ρητών αριθμών $\{A_n\}_{n\in\mathbb{N}}$ η οποία συγκλίνει στο $\alpha_{1,v}$ και ακολουθία ρητών $\{B_n\}_{n\in\mathbb{N}}$ η οποία συγκλίνει στο $\alpha_{2,v}$ για κάθε $v \in S$.
Για κάθε $v \in S$ η συνάρτηση:

$$\Phi_v : \mathbb{Q}_v \times \mathbb{Q}_v \to \mathbb{Q}_v \text{ με } \Phi_v(x_1, x_2) = a_1x_1^2 + a_2x_2^2$$

είναι συνεχής. Επομένως η ακολουθία $a_1A_n^2 + a_2B_n^2$ συγκλίνει στο

$$a_1\alpha_{1,v}^2 + a_2\alpha_{2,v}^2 = x_v$$

για κάθε $v \in S$. Άρα για κάθε $\varepsilon > 0$ υπάρχουν $x_1, x_2 \in \mathbb{Q}$ ώστε για το $x = a_1x_1^2 + a_2x_2^2 \in \mathbb{Q}$ να έχουμε

$$|x_v - x|_v < \varepsilon$$

για κάθε $v \in S$. Από την Πρόταση 1.3.24 για τα x_v με $v \in S$ υπάρχει $\varepsilon_v > 0$ ώστε $|x_v - y|_v < \varepsilon_v \Rightarrow \frac{y}{x_v} \in \mathbb{Q}_v^{*2}$. Οπότε αν $\varepsilon = min\{\varepsilon_v | v \in S\}$ για αυτό το ε υπάρχει $x = a_1x_1^2 + a_2x_2^2 \in \mathbb{Q}$ ώστε $|x_v - x|_v < \varepsilon$ και άρα $\frac{x}{x_v} \in \mathbb{Q}_v^{*2}$ για κάθε $v \in S$. Δηλαδή $x = x_vy_v^2$ στο $\mathbb{Q}_v$ για κάθε $v \in S$.
Η τετραγωνική μορφή $g =< -a_3, -a_4, ..., -a_n >$ παριστά το x_v για κάθε $v \in P$ και αφού για $v \in S$ το $x = x_vy_v^2$, η g παριστά το $x \in \mathbb{Q}$ στο $\mathbb{Q}_v$ για κάθε $v \in S$. Θα αποδείξουμε ότι η g παριστά το x και στα σώματα $\mathbb{Q}_v$ για κάθε $v \notin S$.
Για $n \geq 6$ αυτό είναι άμεσο διότι η $rank(g) = n - 2 \geq 4$ και από το Πόρισμα 2.4.5 κάθε τετραγωνική μορφή βαθμού μεγαλύτερου είτε ίσου του 4 παριστά κάθε στοιχείο του $\mathbb{Q}_p^*$ για κάθε πρώτο p.

Έστω τώρα $n = 5$. Για $v \notin S$ έχουμε $ord_v(a_i) = 0$ για κάθε $i = 1, ..., 5$. Άρα $a_3, a_4, a_5 \in \mathbb{Z}_v^*$ και $d(g) = -a_3a_4a_5 \in \mathbb{Z}_v^*$. Υπολογίζουμε την αναλλοίωτη της g στα $\mathbb{Q}_v, v \notin S$.

$$\begin{aligned}\varepsilon(g) &= (-a_3, -a_4)_v(-a_3, -a_5)_v(-a_4, -a_5)_v \\ &= (-1, -1)_v(-1, a_4)_v(a_3, -1)_v(a_3, a_4)_v \\ &\cdot(-1, -1)_v(-1, a_5)_v(a_3, -1)_v(a_3, a_5)_v \\ &\cdot(-1, -1)_v(-1, a_5)_v(a_4, -1)_v(a_4, a_5)_v \\ &= (-1, -1)_v(a_3, a_4)_v(a_3, a_5)_v(a_4, a_5)_v\end{aligned}$$

Όμως αφού $-1, a_3, a_4, a_5 \in \mathbb{Z}_v^*$ και $v \in \mathbb{P} \setminus \{2\}$ για το σύμβολο του Hilbert έχουμε

$$(-1, -1)_v = 1,\ (a_3, a_4)_v = 1,\ (a_3, a_5)_v = 1 \text{ και } (a_4, a_5)_v = 1$$

Επίσης

$$(-1, -d(g))_v = (-1, -1)_v(-1, d(g))_v = (-1, d(g))_v = 1$$

διότι $d(g) \in \mathbb{Z}_v^*$ για $v \notin S$. Δηλαδή για κάθε $v \notin S$ ισχύει $(-1, -d(g))_v = 1 = \varepsilon(g)$. Τότε από το Πόρισμα 2.4.5 έχουμε ότι η g παριστά το $x \in \mathbb{Q}^*$

στο $\mathbb{Q}_v$ για κάθε $v \notin S$.

Αποδείξαμε λοιπόν ότι για κάθε $v \in P$ η τετραγωνική μορφή

$$g =< -a_3, -a_4, ..., -a_n >$$

παριστά το x στο $\mathbb{Q}_v$. Επίσης, εκ κατασκευής, και η τετραγωνική μορφή $< a_1, a_2 >$ παριστά το x στα $\mathbb{Q}_v$ για κάθε $v \in P$. Από την επαγωγική υπόθεση το θεώρημα Hasse-Minkowski ισχύει για τετραγωνικές μορφές βαθμού έως $n-1$ οπότε το Πόρισμα 2.5.2 εφαρμόζεται για τις $< a_1, a_2 >$ και $< -a_3, -a_4, ..., -a_n >$. Δηλαδή οι $< a_1, a_2 >$ και $< -a_3, -a_4, ..., -a_n >$ παριστούν το x στο $\mathbb{Q}$ και συνεπώς η f παριστά το 0 στο $\mathbb{Q}$.

□

Θεώρημα 2.5.4. *Δύο ρητές τετραγωνικές μορφές f και f' είναι ισοδύναμες αν και μόνο αν οι f_v, f'_v είναι ισοδύναμες για κάθε $v \in P$.*

Απόδειξη. Αν $f \sim f'$ τότε προφανώς $f_v \sim f'_v$ για κάθε $v \in P$. Έστω τώρα ότι $f_v \sim f'_v$ για κάθε $v \in P$. Θα κάνουμε επαγωγή στο πλήθος n των μεταβλητών. Για $n = 0$ δεν υπάρχει τίποτα να δείξουμε.
Για $n = 1$, αν οι f, f' είναι ιδιάζουσες τότε το συμπέρασμα ισχύει. Έστω ότι οι f και f' είναι μη-ιδιάζουσες, τότε υπάρχουν $a, b \in \mathbb{Q}^*$ ώστε $f =< a >$ και $f' =< b >$. Αφού $f_v \sim f'_v$ για κάθε $v \in P$, για κάθε $v \in P$ υπάρχει $x_v \in \mathbb{Q}_v$ ώστε $a = bx_v^2$ στο $\mathbb{Q}_v$. Δηλαδή ο ρητός αριθμός $\frac{a}{b}$ είναι τέλειο τετράγωνο στο $\mathbb{Q}_v$ για κάθε $v \in P$ και συνεπώς είναι τέλειο τετράγωνο και στο $\mathbb{Q}$ (από την Πρόταση 1.3.22). Δηλαδή υπάρχει $c \in \mathbb{Q}^*$ ώστε $\frac{a}{b} = c^2$ και άρα οι f και f' είναι ισοδύναμες στο $\mathbb{Q}$.

Έστω τώρα $n \geq 1$ και ότι το θεώρημα ισχύει για τετραγωνικές μορφες με $n-1$ μεταβλητές. Οι f και f' έχουν την ίδια τάξη. Αν οι f, f' είναι ιδιάζουσες υπάρχουν ρητές τετραγωνικές μορφές g και g' ώστε $f \sim g \perp < 0 >$ και $f' \sim g' \perp < 0 >$ και οι g, g' έχουν $n-1$ μεταβλητές. Αν οι f, f' είναι μή ιδιάζουσες τότε υπάρχει $a \in \mathbb{Q}^*$ ώστε η f να παριστά το a στο $\mathbb{Q}$. Τότε η f_v παριστά το a στα $\mathbb{Q}_v$ για κάθε $v \in P$ και αφού $f_v \sim f'_v$ και η f'_v παριστά το a στα $\mathbb{Q}_v$ για κάθε $v \in P$. Τότε από το Πόρισμα 2.5.2 η f' παριστά το a στο $\mathbb{Q}$ και άρα $f \sim g \perp < a >$ και $f' \sim g' \perp < a >$ για κάποιες ρητές τετραγωνικές μορφές g και g' με $n-1$ μεταβλητές.
Όμως $f_v \sim f'_v$ για κάθε $v \in P \Rightarrow g_v \sim g'_v$ για κάθε $v \in P$, και από την επαγωγική υπόθεση έχουμε $g \sim g'$ στο $\mathbb{Q}$. Άρα τελικά $f \sim f'$. □

2.6 Εφαρμογές

Ορισμός 2.6.1. Για $a \in \mathbb{Q}_p^*$, $p \in \mathbb{P}$ ορίζουμε το σύνολο

$$\mathcal{N}_a := \{z \in \mathbb{Q}_p^* | \text{ υπάρχουν } x, y \in \mathbb{Q}_p \text{ ώστε } z = x^2 - ay^2\}$$

Παρατήρηση 2.6.2. *Για $a, b \in \mathbb{Q}_p^*$ ισχύει $b \in \mathcal{N}_a \Leftrightarrow (\frac{a,b}{p}) = 1$.*

Απόδειξη. Έστω $b \in \mathcal{N}_a$ δηλαδή υπάρχουν $x, y \in \mathbb{Q}_p$ ώστε $b = x^2 - ay^2 \Rightarrow ay^2 + b1^2 = x^2 \Rightarrow (\frac{a,b}{p}) = 1$.
Αντίστροφα αν $(\frac{a,b}{p}) = 1$ υπάρχουν $x, y, z \in \mathbb{Q}_p$ με $(x, y, z) \neq (0, 0, 0)$ ώστε $ax^2 + by^2 = z^2$. Αν $y \neq 0$ τότε $b = (\frac{z}{y})^2 - a(\frac{x}{y})^2$ και άρα $b \in \mathcal{N}_a$. Αν $y = 0$ τότε κατ'ανάγκη $x \neq 0$ και άρα $a = (\frac{z}{x})^2 \in \mathbb{Q}_p^{*2}$. Τότε $b = (\frac{b+1}{2})^2 - a(\frac{(b-1)x}{2z})^2$ και άρα $b \in \mathcal{N}_a$. □

Από την προηγούμενη παρατήρηση προκύπτει ότι:

$$b \in \mathcal{N}_a \Leftrightarrow (\frac{a,b}{p}) = 1 \Leftrightarrow (\frac{b,a}{p}) = 1 \Leftrightarrow a \in \mathcal{N}_b$$

Λήμμα 2.6.3. *Έστω $a \in \mathbb{Q}_p^*$ ισχύουν:*
(i) $\mathcal{N}_a \leq \mathbb{Q}_p^*$.
(ii) $a \in \mathbb{Q}_p^{*2} \Leftrightarrow \mathcal{N}_a = \mathbb{Q}_p^*$.

Απόδειξη. (i) Έστω $z_1, z_2 \in \mathcal{N}_a$ με $z_1 = x_1^2 - ay_1^2$ και $z_2 = x_2^2 - ay_2^2$ τότε $z_1 z_2 = (x_1 x_2 + a y_1 y_2)^2 - a(x_1 y_2 + y_1 x_2)^2$ και άρα $z_1 z_2 \in \mathcal{N}_a$.
Επίσης αν $z = x^2 - ay^2 \in \mathcal{N}_a$ τότε $z^{-1} = (xz^{-1})^2 - a(yz^{-1})^2$ και άρα $z^{-1} \in \mathcal{N}_a$.
(ii)Από το Πόρισμα 1.4.7, έχουμε:
$a \in \mathbb{Q}_p^{*2} \Leftrightarrow (\frac{a,b}{p}) = 1$ για κάθε $b \in \mathbb{Q}_p^* \Leftrightarrow b \in \mathcal{N}_a$ για κάθε $b \in \mathbb{Q}_p^* \Leftrightarrow$

$$\mathcal{N}_a = \mathbb{Q}_p^*$$

□

Σύμφωνα με τα παραπάνω για $p \neq 2$ έχουμε $\mathbb{Q}_p^{*2} \subseteq \mathcal{N}_a \subseteq \mathbb{Q}_p^*$ και $\mathcal{N}_a \neq \mathbb{Q}_p^* \Leftrightarrow a \notin \mathbb{Q}_p^{*2}$. Άρα για $a \notin \mathbb{Q}_p^{*2}$ ο δείκτης της $\mathcal{N}_a$ στην ομάδα $\mathbb{Q}_p^*$ μπορεί να είναι είτε 2 είτε 4, ενώ για $p = 2$ ο δείκτης μπορεί να είναι 2,4 ή 8.

Πόρισμα 2.6.4. *Έστω $a \in \mathbb{Q}_p^* \setminus \mathbb{Q}_p^{*2}$. Τότε $\mathbb{Q}_p^*/\mathcal{N}_a \cong \mathbb{Z}/2\mathbb{Z}$.*

Απόδειξη. Ορίζουμε την απεικόνιση $\varphi : \mathbb{Q}_p^* \to \mathbb{Z}/2\mathbb{Z}$ με $\varphi(x) = \log_{-1}(\frac{x,a}{p})$. Η φ είναι ομομορφισμός ομάδων, ο οποίος είναι επί διότι $\varphi(1) = 0$ και αφού $a \in \mathbb{Q}_p^* \setminus \mathbb{Q}_p^{*2}$ υπάρχει $b \in \mathbb{Q}_p^*$ ώστε $(\frac{a,b}{p}) = -1$, δηλαδή $\varphi(b) = 1$. Τέλος ο πυρήνας της φ είναι $ker\varphi = \{x \in \mathbb{Q}_p^* | (\frac{x,a}{p}) = 1\} = \mathcal{N}_a$ και άρα έχουμε το ζητούμενο. □

Ορισμός 2.6.5. Έστω $d \in \mathbb{Q}^*$, το οποίο δεν είναι τέλειο τετράγωνο ρητού. Στο σώμα $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$ ορίζουμε την *norm* $N_d : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ με $N_d(a + b\sqrt{d}) = a^2 - db^2$.

Έστω $d \in \mathbb{Q}^*$ και θεωρούμε το d στο $\mathbb{R}$. Αν $d < 0$ τότε $d \notin \mathbb{R}^{*2}$ και άρα $\mathbb{R}(\sqrt{d}) = \{x + y\sqrt{d} | x, y \in \mathbb{R}\} = \mathbb{C}$. Αν $z \in \mathbb{C}$ με $z = x + y\sqrt{d}$ τότε $N_d(z) = x^2 - dy^2 \geq 0$. Ειδικότερα $\mathcal{N}_d := \{a \in \mathbb{R}^* | a = N_d(z), z \in \mathbb{C}\} = \mathbb{R}_{>0}$. Μάλιστα $\mathcal{N}_d = \{r \in \mathbb{R}^* | (\frac{r,d}{\infty}) = 1\}$.
Αν $d > 0$ τότε $\mathbb{R}(\sqrt{d}) = \mathbb{R}$ και κάθε $x \in \mathbb{R}$ είναι norm στοιχείου του $\mathbb{R}(\sqrt{d})$. Αυτό ανταναλκλάται στο γεγονός ότι $(\frac{r,d}{\infty}) = 1$ για κάθε $r \in \mathbb{R}^*$.

Τώρα στο $\mathbb{Q}_p$ θεωρούμε την εξίσωση $x^2 - d = 0$ για $d \in \mathbb{Q}_p$. Αν αυτή έχει λύση στο $\mathbb{Q}_p$ δηλαδή $d \in \mathbb{Q}_p^{*2}$ τότε $\mathbb{Q}_p(\sqrt{d}) = \mathbb{Q}_p$ και $(\frac{x,d}{p}) = 1$ για κάθε $x \in \mathbb{Q}_p^*$. Δηλαδή για κάθε $x \in \mathbb{Q}_p^*$ υπάρχει $y \in \mathbb{Q}_p^*$ ώστε $x = N_d(y)$.
Αν $d \notin \mathbb{Q}_p^{*2}$ τότε αν $\sqrt{d}$ είναι μία ρίζα του πολυωνύμου $x^2 - d$ σε κάποια επέκταση του $\mathbb{Q}_p$ έχουμε $\mathbb{Q}_p \subsetneq \mathbb{Q}_p(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}_p\}$ και στο $\mathbb{Q}_p(\sqrt{d})$ ορίζεται η norm $N_d(a + b\sqrt{d}) = a^2 - db^2$. Η $N_d : \mathbb{Q}_p(\sqrt{d})^* \to \mathbb{Q}_p^*$ είναι ομομορφισμός ομάδων. Η εικόνα της

$$\mathcal{N}_d = N_d(\mathbb{Q}_p(\sqrt{d})^*) = \{x \in \mathbb{Q}_p^* | (\tfrac{x,d}{p}) = 1\}$$

Θεώρημα 2.6.6. *Έστω $a, d \in \mathbb{Q}^*$, d ελεύθερο τετραγώνου. Το a είναι norm στοιχείου του σώματος $\mathbb{Q}(\sqrt{d})$ αν και μόνο αν είναι τοπικά norm στα $\mathbb{Q}_p$, $p \in \mathbb{P}$ και στο $\mathbb{R}$, δηλαδή το a ως στοιχείο του $\mathbb{Q}_v$, $v \in P$, είναι norm στοιχείου του σώματος $\mathbb{Q}_v(\sqrt{d})$.*

Απόδειξη. Το a είναι norm του σώματος $\mathbb{Q}(\sqrt{d})$ αν και μόνο αν υπάρχουν $x, y \in \mathbb{Q}$ ώστε $a = x^2 - dy^2$. Ισοδύναμα το a είναι norm του σώματος $\mathbb{Q}(\sqrt{d})$ αν και μόνο αν η τετραγωνική μορφή $f(x, y) = x^2 - dy^2$ παριστά το a στο $\mathbb{Q}$.

Όμως από το Θεώρημα των Hasse-Minkowski η f παριστά το a στο $\mathbb{Q} \Leftrightarrow$ η f_v παριστά το a στο $\mathbb{Q}_v$ για κάθε $v \in P$. Δηλαδή αν για κάθε $v \in P$ υπάρχουν $x_v, y_v \in \mathbb{Q}_v$ ώστε $a = x_v^2 - dy_v^2$ το οποίο ισχύει αν και μόνο αν το a είναι norm του σώματος $\mathbb{Q}_v(\sqrt{d})$ για κάθε $v \in P$. Τελικά:

Το a είναι norm του σώματος $\mathbb{Q}(\sqrt{d}) \Leftrightarrow$ το a είναι norm του σώματος $\mathbb{Q}_v(\sqrt{d})$ για κάθε $v \in P$.

□

Αποδεικνύεται ότι το τοπικό-γενικό αξίωμα σχετικά με την norm ισχύει για κυκλικές επεκτάσεις.

Για το δεύτερο κεφάλαιο της εργασίας συμβουλευτήκαμε τα συγγράμματα [31], [32] και [10].

2.7 Ιστορικά στοιχεία

Ο μαθηματικός Kurt Hensel ήταν ο δημιουργός της θεωρίας των p-αδικών αριθμών. Μετέφερε τη μέθοδο της μιγαδικής ανάλυσης κατά την οποία μελετώνται μιγαδικές συναρτήσεις τοπικά, προκειμένου να προκύψουν γενικά αποτελέσματα και ιδιότητες αυτών, στη Θεωρία Αριθμών. Η βασική παρατήρηση του ήταν ότι οι γραμμικοί παράγοντες $(x-a)$ που παράγουν τα πρώτα ιδεώδη του $\mathbb{C}[x]$ παίζουν ρόλο στο σώμα $\mathbb{C}(x)$, ανάλογο με αυτόν που παίζουν οι πρώτοι αριθμοί p στο $\mathbb{Q}$. Με τη βοήθεια της θεωρίας του προσπάθησε να αποδείξει την υπερβατικότητα του e. Έδωσε μάλιστα μια σχετική διάλεξη το 1905 στο Merano της Ιταλίας, αλλά σύντομα διαπιστώθηκε ότι η απόδειξη δεν ήταν ορθή. Ίσως αυτός ήταν ο κύριος λόγος που δεν βοήθησε στη "νομιμοποίηση " της μεθόδου στους μαθηματικούς κύκλους της τότε εποχής.
Εδώ ας μας επιτραπεί να αναφέρουμε ότι όχι μόνο η υπερβατικότητα του e αλλά γενικότερα το Lindemann-Weierstrass θεώρημα αποδείχθηκε τελικά με p-αδικές μεθόδους πολύ αργότερα, το 1987, από τους J.-P. Bezivin και Phillipe Robba [9].

Η δικαίωση της θεωρίας των p-αδικών σωμάτων του Kurt Hensel προέκυψε πολύ νωρίτερα από την απόδειξη του τοπικού - γενικού αξιώματος για τετραγωνικές μορφές, από τον Helmut Hasse. Το 1920, ο Helmut Hasse, ένας νεαρός φοιτητής μόλις 22 ετών, αποφάσισε να διακόψει τις σπουδές του στο τότε σημαντικότερο κέντρο μαθηματικών σπουδών του κόσμου, το Göttingen και να εγγραφεί για να συνεχίσει τις σπουδές του στο Marburg για να μελετήσει τη θεωρία των p-αδικών αριθμών κοντά στο δημιουργό της, τον K. Hensel. Αφορμή και κίνητρο αυτής της απόφασής του ήταν το βιβλίο του Hensel, "Zahlentheorie " (1913), το οποίο βρήκε και αγόρασε ο Hasse από ένα παλαιοπωλείο του Göttingen (στις 20 Μαρτίου του 1920).

Στον πρόλογο στα άπαντά του ο Hasse [17], γράφει (σε μετάφραση του P.Roquette, [28]):

" From the first moment, this book was particularly appealing to me because of his completely new methods, and certainly it seemed to be worth of detailed study... I felt strongly attracted to it, and hence I went to the " small" Marburg."

Στα άπαντά του ο Hasse αναφέρει ότι το τοπικό-γενικό αξίωμα του υποδείχθηκε από τον δάσκαλο του Hensel. Αναφέρεται σε μία κάρτα που του έστειλε ο Hensel και την οποία κράτησε ως ιδιαίτερα σημαντικό αναμνηστικό. Ο Hensel έγραφε:

" Dear Mr. Hasse!... I am always harboring the idea that there is a particular question at the bottom of these things. If I know of an analytic function that it is of rational type at each point, then it is a rational fuction. If I know the same of a number, that it is p-adic for each prime number p and for p_∞, then I do not yet know that it is rational. How would this have to be amended?"

Ο Hasse γράφει στο [17]:

" It was this question at the end of this message which opened my eyes...From this seed there grew quickly...the Local-Global Principle for all representation and equivalence relations for quadratic forms with rational and also with algebraic coefficients. Thus I owe the discovery of this principle, like so many other things, to my respected teacher and later my paternal friend Kurt Hensel."

Το άρθρο του Hasse δημοσιεύθηκε στο Crelle's Journal, το 1923, [19]. Πρόκειται για το θεώρημα της εργασίας μας. Ακολούθησε το τοπικό - γενικό αξίωμα σχετικά με την ισοδυναμία τετραγωνικών μορφών,[18], καθώς και το τοπικό - γενικό αξίωμα για την norm κυκλικών επεκτάσεων του $\mathbb{Q}$, [20].

Φυσικά λίγο αργότερα, το 1924 ο Hasse [16], απέδειξε το τοπικό - γενικό αξίωμα για οποιοδήποτε αλγεβρικό σώμα αριθμών. Η απόδειξη αυτή ξεπερνάει σε απαιτήσεις θεωρίας το περιεχόμενο της παρούσας εργασίας. Απαιτεί τη θεωρία των p-αδικών τοπικών σωμάτων και τοπική θεωρία κλάσεων σωμάτων. Δεν υπάρχει μέχρι σήμερα στοιχειώδης απόδειξη του αποτελέσματος. Από τα βιβλία θεωρίας τετραγωνικών μορφών, μόνο ο O'Meara [26], το προσπάθησε αλλά και αυτός περιορίζεται μόνο στην τοπική θεωρία κλάσεων για τετραγωνικές επεκτάσεις. Τέλος αναφέρουμε τα ακόλουθα από το βιβλίο του Winfried Scharlau [29]:

We will prove the Hasse-Minkowski theorem which classifies quadratic forms over global fields. This is one of the deepest and most difficult results of the theory of quadratic forms. However, it is difficult only because the algebraic number theory involved in the proof is difficult. What is needed from the theory of quadratic forms is easy in comparison. In keeping with our

established practice we only quote the needed number theoretic results and only carry out that part of the proof which belongs to the realm of quadratic forms.

Κεφάλαιο 3

Τα κλασικά αντιπαραδείγματα

Σε αυτό το κεφάλαιο θα μελετήσουμε μερικά αντιπαραδείγματα του τοπικού-γενικού αξιώματος. Συγκεκριμένα θα μελετήσουμε εξισώσεις οι οποίες έχουν λύσεις στα σώματα $\mathbb{Q}_v$ για κάθε $v \in P = \mathbb{P} \cup \{\infty\}$, αλλά δεν έχουν ρητές λύσεις.

3.1 Η εξίσωση $(X^2-2)(X^2-17)(X^2-34)=0$

Σε αυτή την ενότητα θα ασχοληθούμε με ένα απλό αντιπαράδειγμα στο τοπικό-γενικό αξίωμα. Συγκεκριμένα θα δείξουμε ότι η εξίσωση

$$(X^2-2)(X^2-17)(X^2-34)=0$$

έχει λύση στο $\mathbb{Q}_v$ για κάθε $v \in P$ αλλά δεν έχει καμία ρητή λύση.

Θεώρημα 3.1.1. *Η εξίσωση $(X^2-2)(X^2-17)(X^2-34)=0$ έχει λύση στο $\mathbb{Q}_v$ για κάθε $v \in P$ αλλά δεν έχει λύση στο $\mathbb{Q}$.*

Απόδειξη. Στο $\mathbb{Q}$ προφανώς δεν έχει λύση διότι οι πραγματικές ρίζες της εξίσωσης είναι οι $\pm\sqrt{2}, \pm\sqrt{17}, \pm\sqrt{34} \in \mathbb{R} \setminus \mathbb{Q}$.
Σύμφωνα με την Πρόταση 1.3.21 για $p \neq 2$ μία μονάδα $\varepsilon \in \mathbb{Z}_p^*$ είναι τέλειο τετράγωνο αν και μόνο αν $(\frac{\varepsilon}{p}) = 1$, ένω για $p = 2$ αν και μόνο αν $\varepsilon \equiv 1 mod 8$.

Το $2 \in (\mathbb{Q}_{17}^*)^2$ διότι $(\frac{2}{17}) = +1$. Συνεπώς η εξίσωση στο $\mathbb{Q}_{17}$, έχει λύση την $\sqrt{2} \in \mathbb{Q}_{17}$
Το $17 \in (\mathbb{Q}_2^*)^2$ διότι $17 \equiv 1 \mod 8$ και άρα η εξίσωση έχει λύση και στο $\mathbb{Q}_2$.
Αν τώρα p πρώτος αριθμός με $p \neq 2, 17$ τότε τα $2, 17, 34 \in \mathbb{Z}_p^*$.

- Αν $(\frac{2}{p}) = 1$ τότε $2 \in (\mathbb{Q}_p^*)^2$

- Αν $(\frac{17}{p}) = 1$ τότε $17 \in (\mathbb{Q}_p^*)^2$
- Αν $(\frac{2}{p}) = -1$ και $(\frac{17}{p}) = -1$, τότε $(\frac{34}{p}) = (\frac{2}{p})(\frac{17}{p}) = +1$. Δηλαδή $34 \in (\mathbb{Q}_p^*)^2$.

Συνεπώς η εξίσωση έχει λύση στο $\mathbb{Q}_p$ για κάθε πρώτο p. □

3.2 Η εξίσωση Lind, Reichardt $X^4 - 17 = 2Y^2$

3.2.1 Τοπική μελέτη της εξίσωσης $X^4 - 17 = 2Y^2$

Στα επόμενα θα χρησιμοποιήσουμε το

Θεώρημα 3.2.1. *Έστω $p \in \mathbb{P}$ με $p \equiv 1 mod 4$, $a, b, c \in \mathbb{Z}$ τα οποία δεν διαιρούνται με p. Τότε η εξίσωση*

$$aX^4 + bY^4 = c$$

έχει λύση $mod p$ για $p > 41$.

Η απόδειξη του Θεωρήματος χρησιμοποιεί αθροίσματα Gauss και αθροίσματα Jacobi τετάρτου βαθμού. (βλ. [31] σελ 142)

Λήμμα 3.2.2. *Η εξίσωση $X^4 - 17 = 2Y^2$ $(*)$ έχει λύση στο $\mathbb{Q}_p$, για κάθε περιττό πρώτο p.*

Απόδειξη. Θα εξετάσουμε τις περιπτώσεις $p \equiv 1, 3, 7, 5 mod 8$.

Περίπτωση 1: $p \equiv 1, 7 mod 8$
Έχουμε $(\frac{2}{p}) = 1$, δηλαδή το 2 είναι τετραγωνικό υπόλοιπο $mod p$ και άρα υπάρχει $b \in \mathbb{Z}$ ώστε $b^2 \equiv 2 mod p$. Τότε

$$3^4 - 17 \equiv 2(4b)^2 mod p$$

Θεωρούμε το πολυώνυμο $f(X) = 2X^2 + 17 - 3^4 \in \mathbb{Z}_p[X]$, τότε $f(4b) \equiv 0 mod p$ και $f'(4b) = 16b \not\equiv 0 mod p$ αφού $b \not\equiv 0 mod p$. Από το Λήμμα του Hensel υπάρχει $y \in \mathbb{Z}_p$ ώστε $f(y) = 0$. Δηλαδή

$$3^4 - 17 = 2y^2$$

και άρα η $(3, y)$ είναι λύση της εξίσωσης $(*)$ στο $\mathbb{Z}_p$.

Περίπτωση 2: $p \equiv 3 mod 8$

Έχουμε $(\frac{-1}{p}) = -1$ και $(\frac{2}{p}) = -1$. Άρα $(\frac{-2}{p}) = 1$ και υπάρχει $b \in \mathbb{Z}$ ώστε $b^2 \equiv -2 mod p$. Τότε

$$1^4 - 17 \equiv 2(2b)^2 mod p$$

Εφαρμόζοντας το Λήμμα του Hensel για το πολυώνυμο $f(X) = 2X^2 + 17 - 1^4 \in \mathbb{Z}_p[X]$ παίρνουμε ότι υπάρχει $y \in \mathbb{Z}_p$, ώστε $f(y) = 0$. Δηλαδή

$$1^4 - 17 = 2y^2$$

και άρα η $(1, y)$ είναι λύση της εξίσωσης $(*)$.

Περίπτωση 3: $p \equiv 5 mod 8$
Σε αυτή την περίπτωση έχουμε $p \equiv 1 mod 4$ και άρα σύμφωνα με το Θεώρημα 3.2.1 η εξίσωση $X^4 - 17 = 2Y^2$ έχει λύση $mod p$ για $p > 41$. Θα δείξουμε ότι έχει λύση $mod p$ και για $p = 5, 13, 29, 37$.

Αφού $p \equiv 5 mod 8$ έχουμε $(\frac{2}{p}) = -1$ και $(\frac{-1}{p}) = 1$. Έστω $a \in \mathbb{Z}$ ώστε $2a \equiv 1 mod p$, τότε $(\frac{a}{p}) = -1$.
Αν $(\frac{17}{p}) = -1$ τότε $(\frac{-17a}{p}) = (\frac{-1}{p})(\frac{17}{p})(\frac{a}{p}) = 1$ και άρα υπάρχει $t \in \mathbb{Z}$ ώστε

$$-17a \equiv t^2 mod p$$

Ισοδύναμα $-17 \equiv 2t^2 mod p$ και άρα

$$0^4 - 17 \equiv 2t^2 mod p$$

Δηλαδη η εξίσωση $(*)$ έχει λύση $mod p$.

Έχουμε:
$(\frac{17}{5}) = (\frac{2}{5}) = -1$,
$(\frac{17}{29}) = (\frac{29}{17}) = (\frac{12}{17}) = (\frac{3}{17}) = (\frac{17}{3}) = (\frac{2}{3}) = -1$ και
$(\frac{17}{37}) = (\frac{37}{17}) = (\frac{3}{17}) = -1$
και άρα για $p = 5, 29, 37$ η εξίσωση $(*)$ έχει λύση $mod p$. Μένει η περίπτωση $p = 13$. Τότε όμως

$$4^4 - 17 = 239 \equiv 18 \equiv 2(3)^2 mod 13$$

Τελικά η εξίσωση $(*)$ έχει λύση $mod p$ για κάθε πρώτο $p \equiv 5 mod 8$.
Έστω $x, y \in \mathbb{Z}$ ώστε

$$x^4 - 17 \equiv 2y^2 mod p$$

Τότε τουλάχιστον ένα από τα x, y δεν διαιρείται με p διότι διαφορετικά θα έχουμε $-17 \equiv 0 mod p$ το οποίο δεν γίνεται διότι $17 \equiv 1 mod 8$ ενώ $p \equiv 5 mod 8$

Αν $x \not\equiv 0 mod p$ για το $f(X) = X^4 - 17 - 2y^2 \in \mathbb{Z}_p$ έχουμε $f(x) \equiv 0 mod p$ και $f'(x) \not\equiv 0 mod p$, οπότε από το Λήμμα του Hensel η εξίσωση $(*)$ έχει λύση. Όμοια αν $y \not\equiv 0 mod p$ εφαρμόζοντας το Λήμμα του Hensel για το πολυώνυμο $f(X) = 2X^2 + 17 - x^4$ παίρνουμε λύση της $(*)$ στο $\mathbb{Z}_p$. □

Παρατήρηση 3.2.3. *Προφανώς η εξίσωση $X^4 - 17 = 2Y^2$ έχει λύσεις στο $\mathbb{R}$. Για παράδειγμα η $(x, y) = (\sqrt[4]{17}, 0)$ είναι μια λύση.*

Λήμμα 3.2.4. *Η εξίσωση $X^4 - 17 = 2Y^2$ $(*)$ έχει λύση στο $\mathbb{Q}_2$.*

Απόδειξη. Θα αναζητήσουμε λύση της $(*)$ για $Y = 4$, δηλαδή λύση της εξίσωσης $X^4 = 49$. Έστω $f(X) = X^4 - 49 \in \mathbb{Z}_p[X]$, τότε για $x = 3$ έχουμε $f(3) = 3^4 - 49 = 32 \equiv 0 mod 2^5$ και $f'(3) = 4(3)^3$, δηλαδή $ord_2(f'(3)) = 2$. Άρα ικανοποιούνται οι προϋποθέσεις του Θεωρήματος 1.3.20 για $m = 1$, $n = 5$ και $k = 2$ και άρα υπάρχει $a \in \mathbb{Z}_2$ ώστε $f(a) = 0$. Άρα

$$a^4 - 17 = 2(3)^2$$

και συνεπώς η $(*)$ έχει λύση στο $\mathbb{Z}_2$. □

3.2.2 Γενική μελέτη της εξίσωσης $X^4 - 17 = 2Y^2$

Θα αποδείξουμε τώρα ότι η εξίσωση των Lind, Reichardt $X^4 - 17 = 2Y^2$ δεν έχει ρητή λύση.

Θεώρημα 3.2.5. *Η εξίσωση $X^4 - 17Y^4 = 2Z^2$ δεν έχει μη μηδενική ακέραια λύση.*

Απόδειξη. Έστω $(x, y, z) \neq (0, 0, 0)$ ακέραια λύση. Αν $z = 0$ τότε $x^4 = 17y^4$ και αφού $x, y \in \mathbb{Z}$ αναγκαστικά $x = y = 0$. Όμοια αν $x = 0$ ή $y = 0$. Άρα $x, y, z \neq 0$. Οι τριάδες $(\pm x, \pm y, \pm z)$ είναι επίσης λύσεις, έτσι χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $x, y, z \geq 1$. Αν $p \in \mathbb{P}$ με $p|x, z$ τότε $p^2|17y^4 \Rightarrow p|y$. Άρα $p^4|2z^2 \Rightarrow p^2|z$, και η $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2})$ είναι επίσης λύση. Όμοια αν $p|y, z$ ή $p|x, y$. Επομένως μπορούμε να υποθέσουμε οτι τα x, y, z είναι ανά δύο σχετικά πρώτα. Παρατηρούμε ότι το z δεν μπορεί να διαιρείται με 17 διότι τότε $17|x$ το οποίο αντιβαίνει στο ότι τα x, z είναι σχετικά πρώτα. Επίσης $17 \nmid x$ διότι αν $17|x \Rightarrow 17|z$.

Υποθέτουμε ότι $z > 1$ και έστω $z = p_1^{e_1} ... p_r^{e_r}$ η ανάλυση του z σε πρώτους παράγοντες. Τότε για $i = 1, ..., r$ έχουμε

$$x^4 \equiv 17y^4 mod p_i$$

και άρα το 17 είναι τετραγωνικό υπόλοιπο $mod p_i$ για κάθε $i = 1, ..., r$. Τότε για $p_i \neq 2$ έχουμε

$$(\tfrac{p_i}{17}) = (-1)^{\frac{p_i-1}{2}\frac{17-1}{2}}(\tfrac{17}{p_i}) = 1$$

Επίσης $(\frac{2}{17}) = 1$ και από την πολλαπλασιαστικότητα του συμβόλου του Legendre έχουμε $(\frac{z}{17}) = 1$. Το ίδιο ισχύει και αν $z = 1$.

Άρα υπάρχει $t \in \mathbb{Z}$ ώστε $z \equiv t^2 mod 17$ και $t \not\equiv 0 mod 17$. Τότε έχουμε

$$x^4 - 17y^4 \equiv 2t^4 mod 17 \Rightarrow x^4 \equiv 2t^4 mod 17$$

Άρα $x^{16} \equiv 2^4 t^{16} mod 17$. Από το μικρό Θεώρημα Fermat $x^{16} \equiv t^{16} \equiv 1 mod 17$ και άρα από την προηγούμενη σχέση $1 \equiv 16 mod 17$, το οποίο είναι άτοπο. □

Πρόταση 3.2.6. *Η εξίσωση $X^4 - 17 = 2Y^2$ δεν έχει ρητές λύσεις.*

Απόδειξη. Έστω $x, y \in \mathbb{Q}$ ώστε $x^4 - 17 = 2y^2$. Μπορούμε να γράψουμε τα x, y στην μορφή $x = \frac{a}{b}$, $y = \frac{c}{d}$ με $a, b, c, d \in \mathbb{Z}$, $b, d > 0$ και $(a, b) = (c, d) = 1$. Άρα από την προηγούμενη σχέση έχουμε

$$a^4 d^2 - 17b^4 d^2 = 2c^2 b^4$$

Τότε $d^2 \mid 2c^2 b^4 \Rightarrow d^2 \mid 2b^4$ (διότι $(d, c) = 1$) και άρα $d | b^2$.
Επίσης $b^4 \mid a^4 d^2 \Rightarrow b^4 \mid d^2$ (διότι $(a, b) = 1$) και άρα $b^2 \mid d$. Δηλαδή $d = b^2$ και άρα η εξίσωση γίνεται

$$a^4 - 17b^4 = 2c^2$$

Όμως από το προηγούμενο Θεώρημα η εξίσωση $X^4 - 17Y^4 = 2Z^2$ δεν έχει μη μηδενική ακέραια λύση, άρα αναγκαστικά $a = b = c = 0$ το οποίο είναι άτοπο διότι $b \neq 0$. □

Αποδείξαμε λοιπόν το

Θεώρημα 3.2.7. *Η εξίσωση των Lind, Reichardt $X^4 - 17 = 2Y^2$ έχει λύση τοπικά στο σώμα $\mathbb{Q}_v$ για κάθε $v \in P = \mathbb{P} \cup \{\infty\}$ αλλά δεν έχει ρητή λύση.*

Ακολουθεί μία εντελώς στοιχειώδης απόδειξη της Πρότασης 3.2.6 από το βιβλίο του Cassels [13] σελ. 57-59

Απόδειξη. Έστω ότι υπάρχουν $x, y \in \mathbb{Q}$ ώστε $x^4 - 17 = 2y^2$. Τότε, όπως αποδείχθηκε, μπορούμε να γράψουμε τα x, y στην μορφή $x = \frac{a}{c}$ και $y = \frac{d}{c^2}$, με $a, b, c \in \mathbb{Z}$ και $(a, b, c) = 1$. Τότε $a^4 - 17c^4 = 2b^2$ η οποία γράφεται ως

$$(5a^2 + 17c^2)^2 - 17(a^2 + 5c^2)^2 = (4b)^2 \qquad (1)$$

ή ισοδύναμα

$$(5a^2 + 17c^2 + 4b)(5a^2 + 17c^2 - 4b) = 17(a^2 + 5c^2)^2 \qquad (2)$$

Αν p είναι περιττός πρώτος ο οποίος διαιρεί και τους δύο παράγοντες στο αριστερό μέλος της σχέσης (2), τότε $p \mid 8b \Rightarrow p \mid b$. Άρα $p \mid (5a^2 + 17c^2)$ και από την (2) $p \mid (a^2 + 5c^2)$. Άρα

$$p \mid (5a^2 + 17c^2) - 5(a^2 + 5c^2) = -8c^2$$

Δηλαδή $p \mid c$. Όμοια $p \mid a$, το οποίο αντιβαίνει στο ότι $(a, b, c) = 1$. Συνεπώς ο μόνος πρώτος αριθμός που μπορεί να διαιρεί και τους δύο παράγοντες στο αριστερό μέλος της (2) είναι ο $p = 2$.

Από την σχέση (2) υπάρχουν $u, v \in \mathbb{Z}$ ώστε να ισχύει μια από τις επόμενες περιπτώσεις:
Περίπτωση 1:
$5a^2 + 17c^2 \pm 4b = 17u^2$
$5a^2 + 17c^2 \mp 4b = v^2$
$a^2 + 5c^2 = uv$
Περίπτωση 2:
$5a^2 + 17c^2 \pm 4b = 34u^2$
$5a^2 + 17c^2 \mp 4b = 2v^2$
$a^2 + 5c^2 = 2uv$
Στην Περίπτωση 1 έχουμε:

$$10a^2 + 34c^2 = 17u^2 + v^2 \qquad (3)$$

και

$$a^2 + 5c^2 = uv \qquad (4)$$

Θα αποδείξουμε ότι το παραπάνω σύστημα δεν έχει μη τετριμμένη λύση στο $\mathbb{Q}_{17}$. Επειδή το σύστημα των εξισώσεων (3)-(4) είναι ομογενές πολλαπλασιάζοντας τα a, c, u, v με $(17)^n$ για κατάλληλο ακέραιο n μπορούμε να υποθέσουμε ότι $a, c, u, v \in \mathbb{Z}_{17}$ και κάποιο από αυτά είναι μονάδα του $\mathbb{Z}_{17}$. Άρα

$$max\{|a|_{17}, |c|_{17}, |u|_{17}, |v|_{17}\} = 1$$

Τότε από την (3) έχουμε $10a^2 \equiv v^2 mod 17$ και αφού το 10 δεν είναι τετραγωνικό υπόλοιπο $mod 17$ αναγκαστικά $17 \mid a, v$, δηλαδή $|a|_{17}, |v|_{17} < 1$ (ειδικότερα $|a|_{17}, |v|_{17} \leq \frac{1}{17}$).
Τότε από την (4) έχουμε $|5c^2|_{17} \leq max\{|uv|_{17}, |a^2|_{17}\} < 1 \Rightarrow |c|_{17} < 1$, και από την (3)

$$|17u^2|_{17} = |10a^2 + 34c^2 - v^2|_{17} \leq max\{|10a^2|_{17}, |34c^2|_{17}, |v^2|_{17}\} \leq \frac{1}{17^2}$$

και άρα $|u|_{17} < 1$, το οποίο αντιβαίνει στην σχέση:

$$max\{|a|_{17}, |c|_{17}, |u|_{17}, |v|_{17}\} = 1$$

Με όμοιο τρόπο δείχνουμε και στην Περίπτωση 2, ότι το σύστημα

$$\begin{cases} 5a^2 + 17c^2 = 34u^2 + 2v^2 \\ a^2 + 5c^2 = 2uv \end{cases}$$

δεν έχει μη τετριμμένη λύση στο $\mathbb{Q}_{17}$. □

Ακολουθεί απόδειξη της Πρότασης 3.2.6 με χρήση Αλγεβρικής Θεωρίας Αριθμών.

Απόδειξη. Έστω $K = \mathbb{Q}(\sqrt{17})$, και υποθέτουμε ότι η εξίσωση $X^4 - 17 = 2Y^2$ έχει ρητή λύση (x, y). Τότε $x = \frac{a}{c}$, $y = \frac{b}{c^2}$ με $(a, c) = (b, c) = (a, b) = 1$ και

$$a^4 - 17c^4 = 2b^2 \qquad (*)$$

Από την παραπάνω εξίσωση έπεται ότι $a \equiv c mod 2$. Όμως δεν γίνεται $a \equiv c \equiv 0 mod 2$ διότι τότε $2 \mid (a, c) = 1$ και άρα οι a και c είναι και οι δύο περιττοί.

Επειδή $17 \equiv 1 mod 4$, η βάση ακεραιότητας του σώματος K είναι το $\{1, \frac{1+\sqrt{17}}{2}\}$. Επομένως αφου a, c είναι περιττοί το $\frac{a+c\sqrt{17}}{2}$ είναι ακέραιος αλγεβρικός του K, διότι αν $a = 2k + 1$, $c = 2l + 1$ με $k, l \in \mathbb{Z}$ τότε

$$\frac{a + c\sqrt{17}}{2} = (k - l) + (2l + 1)\frac{1 + \sqrt{17}}{2}$$

Αφού τα a^2, c^2 είναι επίσης περιττοί, τα $\frac{a^2+c^2\sqrt{17}}{2}$ και $\frac{a^2-c^2\sqrt{17}}{2}$ είναι ακέραιοι αλγεβρικοί του K.

Ισχυρισμός: Τα κύρια ιδεώδη $I_1 =< \frac{a^2+c^2\sqrt{17}}{2} >$ και $I_2 =< \frac{a^2-c^2\sqrt{17}}{2} >$ του δακτυλίου R_K των ακεραίων αλγεβρικών, είναι σχετικά πρώτα.
Πράγματι αν $P \neq < \sqrt{17} >$ είναι πρώτο ιδεώδες με $P \mid I_1$, $P \mid I_2$, τότε $\frac{a^2+c^2\sqrt{17}}{2}, \frac{a^2-c^2\sqrt{17}}{2} \in P$ και άρα $a^2 \in P \Rightarrow a \in P$.
Επίσης $c^2\sqrt{17} \in P$ και αφού $\sqrt{17} \notin P$ έχουμε $c^2 \in P \Rightarrow c \in P$. Όμως $(a, c) = 1$ και άρα $1 \in P$. Άτοπο αφού το P είναι πρώτο ιδεώδες.
Αν P είναι το πρώτο ιδεώδες $< \sqrt{17} >$ και $P \mid I_1, I_2$ τότε έχουμε

$$\frac{a^2 + c^2\sqrt{17}}{2}, \frac{a^2 - c^2\sqrt{17}}{2} \in < \sqrt{17} >$$

και άρα $a^2 \in < \sqrt{17} > \Rightarrow \sqrt{17} \mid a^2$ στον R_K. Άρα υπάρχουν $w, z \in \mathbb{Z}$ ώστε

$$a^2 = \sqrt{17}(w + z\frac{1+\sqrt{17}}{2})$$

δηλαδή $2a^2 = \sqrt{17}(2w + z + z\sqrt{17}) = 17z + \sqrt{17}(2w + z)$. Συνεπώς $w = -\frac{z}{2}$ και $2a^2 = 17z \Rightarrow 17 \mid 2a^2 \Rightarrow 17 \mid a \Rightarrow (17)^4 \mid a^4$. Τότε από την σχέση

$$a^4 - 17c^4 = 2b^2$$

έχουμε $17 \mid 2b^2 \Rightarrow 17 \mid b \Rightarrow (17)^2 \mid b^2$ και άρα αναγκαστικά $17 \mid c$, άτοπο αφού $(a, c) = 1$.

Από την $(*)$ έχουμε

$$\frac{a^4 - 17c^4}{4} = (\frac{a^2 + c^2\sqrt{17}}{2})(\frac{a^2 - c^2\sqrt{17}}{2}) = \frac{b^2}{2}$$

Δηλαδή $N_{K/\mathbb{Q}}(\frac{a^2+c^2\sqrt{17}}{2}) = \frac{b^2}{2}$. Όμως το $\frac{a^2+c^2\sqrt{17}}{2}$ είναι ακέραιος αλγεβρικός και άρα $N_{K/\mathbb{Q}}(\frac{a^2+c^2\sqrt{17}}{2}) \in \mathbb{Z}$. Δηλαδή $\frac{b^2}{2} \in \mathbb{Z} \Rightarrow b = 2b_0$ και η παραπάνω σχέση γράφεται

$$(\frac{a^2 + c^2\sqrt{17}}{2})(\frac{a^2 - c^2\sqrt{17}}{2}) = 2b_0^2$$

Ο αριθμός κλάσεων ιδεωδών του K είναι 1 και συνεπώς ο R_K είναι $\Pi.K.I.$ Το 2 αναλύεται στον R_K ως εξής

$$2 = (\frac{5 + \sqrt{17}}{2})(\frac{5 - \sqrt{17}}{2})$$

και άρα

$$< \frac{a^2 + c^2\sqrt{17}}{2} >< \frac{a^2 - c^2\sqrt{17}}{2} >=< \frac{5 + \sqrt{17}}{2} >< \frac{5 - \sqrt{17}}{2} >< b_0 >^2$$

Τα ιδεώδη $< \frac{5+\sqrt{17}}{2} >, < \frac{5-\sqrt{17}}{2} >$ είναι πρώτα διότι έχουν norm 2. Άρα $< \frac{5+\sqrt{17}}{2} > | < \frac{a^2+c^2\sqrt{17}}{2} >$ ή $< \frac{5-\sqrt{17}}{2} > | < \frac{a^2+c^2\sqrt{17}}{2} >$ και άρα

$$\frac{a^2 + c^2\sqrt{17}}{2} = \frac{5 \pm \sqrt{17}}{2}\varepsilon\alpha^2$$

όπου $\alpha \in R_K$ και το ε είναι μονάδα του R_K, $\varepsilon > 0$.

Ισχύουν $N_{K/\mathbb{Q}}(\frac{5\pm\sqrt{17}}{2}) = 2 > 0$, $N_{K/\mathbb{Q}}(\alpha^2) > 0$ καθώς και $N_{K/\mathbb{Q}}(\frac{a^2+c^2\sqrt{17}}{2}) =$

$2b_0^2 > 0$. Επομένως $\varepsilon > 0$ και $N_{K/\mathbb{Q}}(\varepsilon) > 0$. Από το Θεώρημα των μονάδων του *Dirichlet* η ομάδα των μονάδων R_K^* του R_K είναι ελεύθερη αβελιανή ομάδα με rank 1 (βλ [1] σελ.179). Μία θεμελιώδης μονάδα του R_K είναι η $\varepsilon_0 = 4 + \sqrt{17}$ και επόμενως $\varepsilon = \varepsilon_0^n > 0$ για κάποιο $n \in \mathbb{Z}$.

$N_{K/\mathbb{Q}}(\varepsilon_0) = -1$ και άρα αν ο n είναι περιττός τότε $N_{K/\mathbb{Q}}(\varepsilon) = N_{K/\mathbb{Q}}(\varepsilon_0)^n = (-1)^n = -1$. Όμως $N_{K/\mathbb{Q}}(\varepsilon) > 0$ και άρα ο n είναι άρτιος. Δηλαδή $\varepsilon = \varepsilon_0^{2l}$ για κάποιο $l \in \mathbb{Z}$ και αν $\alpha' = \varepsilon_0^l \alpha$ έχουμε

$$\frac{a^2 + c^2\sqrt{17}}{2} = \frac{5 \pm \sqrt{17}}{2}\alpha'^2$$

έστω $\alpha' = \frac{u+v\sqrt{17}}{2} \in R_K$ τότε

$$\frac{a^2 + c^2\sqrt{17}}{2} = \frac{5 \pm \sqrt{17}}{2}(\frac{u + v\sqrt{17}}{2})^2 = \frac{5(u^2 \pm 34uv + 17v^2) + \sqrt{17}(10uv \pm u^2 \pm 17v^2)}{8}$$

Άρα $4a^2 = 5(u^2 \pm 34uv + 17v^2) \Rightarrow (2a)^2 \equiv 5u^2 mod 17$. Δηλαδή το 5 είναι τετραγωνικό υπόλοιπο $mod 17$. Όμως αυτό δεν ισχύει διότι ,$(\frac{5}{17}) = (-1)^{\frac{5-1}{2}\frac{17-1}{2}}(\frac{17}{5}) = (\frac{2}{5}) = -1$ και συνεπώς καταλήξαμε σε άτοπο. □

Οι W. Aitken, F.Lemmermeyer στο άρθρο τους [6] εφαρμόζουν μία πολύ στοιχειώδη διαδικασία , την παραμέτριση κωνικών τομών και γενικεύουν στο

Θεώρημα 3.2.8. *Το σύστημα $U^2 - qW^2 = dZ^2$, $UW = V^2$ για το οποίο ισχύουν:*
(1) Το q είναι πρώτος αριθμός με $q \equiv 1 mod 16$
(2) Το d είναι μη μηδενικό, ελεύθερο τετραγώνου και $q \nmid d$
(3) Το d είναι τετραγωνικό υπόλοιπο $mod q$ αλλά όχι τέταρτη δύναμη $mod q$
(4) Το q είναι τέταρτη δύναμη $mod p$ για κάθε περιττό p, με $p \mid d$
είναι τοπικά επιλύσιμο στα $\mathbb{Q}_v$, $v \in \mathbb{P} \cup \{\infty\}$, αλλά όχι στο $\mathbb{Q}$.

Το παράδειγμα των Lind, Reichardt είναι ειδική περίπτωση του θεωρήματος αυτού. Πράγματι το σύστημα γράφεται

$$U^4 - qV^4 = d(ZU)^2, \qquad UW = V^2$$

και για $q = 17$ και $d = 2$ έχουμε την εξίσωση των Lind, Reichardt. Επομένως το αντιπαράδειγμα των Lind, Reichardt ισχύει διότι $17 \equiv 1 mod 16$, και το 2 είναι τετραγωνικό υπόλοιπο $mod 17$ αλλά όχι τέταρτη δύναμη $mod 17$ και άρα ικανοποιούνται οι απαιτήσεις του θεωρήματος.
Γενικότερα αν $q \in \mathbb{P}$ με $q \equiv 1 mod 16$ τέτοιος ώστε το 2 να μην είναι τέταρτη δύναμη $mod q$ τότε το σύστημα $U^2 - qW^2 = dZ^2$, $UW = V^2$ είναι επίσης αντιπαράδειγμα στο αξίωμα του Hasse. Μάλιστα το σύστημα πάλι γίνεται

$U^4 - qV^4 = d(ZU)^2, UW = V^2$, δηλαδή η εξίσωση $X^4 - qY^4 = 2Z^2$ είναι αντιπαράδειγμα.
Επίσης για $q = 17$ και $d = 19$ έχουμε $(\frac{19}{17}) = (\frac{2}{17}) = (-1)^{\frac{289-1}{8}} = (-1)^{36} = +1$. Δηλαδή το 19 είναι τετραγωνικό υπόλοιπο $mod17$ αλλά όχι τέταρτη δύναμη $mod17$ καθώς η ισοτιμία $x^4 \equiv 19 mod 17$ δεν έχει λύση. Το 17 είναι τέταρτη δύναμη $mod19$ διότι $5^4 \equiv 17 mod 19$. Δηλαδή ικανοποιούνται οι απαιτήσεις του Θεωρήματος και άρα και η εξίσωση $X^4 - 17Y^4 = 19Z^2$ είναι αντιπαράδειγμα στο αξίωμα του Hasse.

3.2.3 Ιστορικά στοιχεία

Το άρθρο του H.Reichardt [27] υποβλήθηκε προς δημοσίευση στο περιοδικό, στις 16 Σεπτεμβρίου του 1940 και ήταν το πρώτο σημαντικό αντιπαράδειγμα. Αργότερα το 1951 ακολούθησε το αντιπαράδειγμα του Selmer στο οποίο θα αναφερθούμε στην επόμενη παράγραφο. Όταν το 1966 δημοσιεύθηκε το σημαντικό αρθρο του Cassels [11], ο Birch ενημέρωσε τον Cassels, ότι ο Lind [24] είχε αποδείξει μεταξύ άλλων ότι η ίδια εξίσωση, είναι αντιπαράδειγμα στο τοπικό-γενικό αξίωμα. Την πληροφορία αυτήν την πρόσθεσε την τελευταία στιγμή ως Appendix A στην προαναφερθείσα εργασία του ο Cassels.
Τέλος από το άρθρο το H. Reichardt συνάγεται ότι και οι "συνοδεύουσες" εξισώσεις

$$X^4 - 68Y^4 = Z^2, \qquad 68X^4 - Y^4 = Z^2, \qquad 17X^4 - Y^4 = 2Z^2$$

είναι επίσης αντιπαραδείγματα στο τοπικό-γενικό αξίωμα.

Οι εξισώσεις

$$X^4 - 17Y^4 = 2Z^2, \qquad 68X^4 - Y^4 = Z^2, \qquad 17X^4 - Y^4 = 2Z^2$$

είναι ειδικές περιπτώσεις της Πρότασης 6.5 σελ. 316 του [33], για $p = 17$. Συγκεκριμένα ισχύει:

Πρόταση 3.2.9. *Έστω p πρώτος αριθμός, $p \equiv 1 mod 8$ ώστε το 2 να μην είναι τέταρτη δύναμη $mod p$. Τότε οι καμπύλες*

$$w^2 + 1 = 4pz^4 \qquad w^2 + 2 = 2pz^4, \qquad w^2 + 2pz^4 = 2$$

έχουν μη-τετριμμένα σημεία σε κάθε πλήρωση του $\mathbb{Q}$, αλλά δεν έχουν ρητά σημεία.

Πράγματι για $p = 17$ η πρώτη εξίσωση γίνεται

$$w^2 + 1 = 68z^4 \Rightarrow 68z^4 - 1 = w^2$$

η οποία αντιστοιχεί στην $68X^4 - Y^4 = Z^2$. Η δεύτερη εξίσωση

$$w^2 + 2 = 2 \cdot 17z^4 \Rightarrow 2(2w)^2 + 2^4 = 17 \cdot 2^4 z^4 \Rightarrow 17(2z)^4 - 2^4 = 2(2w)^2$$

η οποία αντιστοιχεί στην $17X^4 - Y^4 = 2Z^2$ και η τρίτη εξίσωση

$$w^2 + 2 \cdot 17z^4 = 2 \Rightarrow 2(2w)^2 + 17(2z)^4 = 2^4 \Rightarrow 2^4 - 17(2z)^4 = 2(2w)^2$$

που αντιστοιχεί στην $X^4 - 17Y^4 = 2Z^2$.

3.3 Η εξίσωση του Selmer $3X^3+4Y^3+5Z^3=0$

3.3.1 Τοπική μελέτη της εξίσωσης $3X^3+4Y^3+5Z^3=0$

Θεώρημα 3.3.1. *Η εξίσωση του Selmer $3X^3+4Y^3+5Z^3=0$ $(*)$ έχει μη μηδενική λύση στο σώμα $\mathbb{Q}_p$ για κάθε πρώτο p.*

Απόδειξη. Θα διακρίνουμε τις περιπτώσεις $p=3$, $p=5$ και $p\neq 3,5$.

Περίπτωση 1: $p=3$
Θέτουμε στην εξίσωση $(*)$ $X=0$ και $Z=-1$ και άρα αναζητούμε λύση της εξίσωσης $4Y^3=5$ ή ισοδύναμα $Y^3=\frac{5}{4}$.
Έστω $t\in\mathbb{Z}$ με $t\equiv 7 mod 9$, τότε $4t\equiv 1 mod 9$. Άρα $\frac{5}{4}\equiv 5.7\equiv -1 mod 3^2\mathbb{Z}_3$ και άρα από την Παρατήρηση 1.3.33 το $\frac{5}{4}$ είναι κύβος στο $\mathbb{Q}_3$. Άρα υπάρχει $y\in\mathbb{Q}_3$ ώστε $y^3=\frac{5}{4}$ και άρα η $(0,y,-1)$ είναι λύση της $(*)$ στο $\mathbb{Q}_3$.

Έστω τώρα $p\neq 3$, $a,b\in\mathbb{Z}_p^*$ ώστε $a\equiv b^3 mod p$. Τότε από το Λήμμα του Hensel για το πολυώνυμο $F(X)=X^3-a$, έχουμε ότι το a είναι κύβος στο $\mathbb{Z}_p$. Ειδικότερα:
Περίπτωση 2: $p=5$
Για $X=1$, $Z=0$ η εξίσωση γίνεται $3+4Y^3=0\Leftrightarrow Y^3=-\frac{3}{4}$. Αρκεί να δείξουμε ότι το $-\frac{3}{4}\in\mathbb{Z}_p^*$ είναι κύβος $mod 5\mathbb{Z}_5$. Αφού $4\cdot 4\equiv 1 mod 5\mathbb{Z}_5$ έχουμε

$$-\frac{3}{4}\equiv(-3)\cdot 4\equiv 3 mod 5\mathbb{Z}_5\equiv 2^3 mod 5\mathbb{Z}_5$$

Άρα υπάρχει $y\in\mathbb{Z}_5$, ώστε $y^3=-\frac{3}{4}$ στο $\mathbb{Z}_5$ και άρα η $(1,y,0)$ είναι λύση της $(*)$ στο $\mathbb{Z}_5$.

Περίπτωση 3: $p\neq 3,5$
Η ομάδα $(\mathbb{Z}/p\mathbb{Z})^*$ είναι κυκλική τάξης $p-1$. Έστω $\overline{a}$ ένας γεννήτορας, τότε $(\mathbb{Z}/p\mathbb{Z})^{*3}=<\overline{a}^3>$ και άρα $|(\mathbb{Z}/p\mathbb{Z})^{*3}|=ord(\overline{a}^3)$. Όμως

$$ord(\overline{a}^3)=\frac{ord(\overline{a})}{(3,p-1)}=\frac{p-1}{(3,p-1)}$$

Αν $p\equiv 2 mod 3\Rightarrow 3\nmid p-1\Rightarrow(3,p-1)=1$ και άρα $ord(\overline{a}^3)=p-1$, ένω αν $p\equiv 1 mod 3$ τότε $(3,p-1)=3$ και άρα $ord(\overline{a}^3)=\frac{p-1}{3}$.
Συνεπώς $[(\mathbb{Z}/p\mathbb{Z})^*:(\mathbb{Z}/p\mathbb{Z})^{*3}]=\begin{cases}1, & \text{αν } p\equiv 2 \mod 3\\ 3, & \text{αν } p\equiv 1 \mod 3\end{cases}$

- Έστω $\overline{3}=3+p\mathbb{Z}\in(\mathbb{Z}/p\mathbb{Z})^{*3}$.
  Τότε υπάρχει $b\in\mathbb{Z}$, $(b,p)=1$ ώστε $b^3\equiv 3 \mod p$. Έστω $t\in\mathbb{Z}$

ώστε $bt \equiv 1 \mod p$, τότε αφού $3 \in \mathbb{Z}_p^*$, έχουμε $\frac{1}{3} \in \mathbb{Z}_p^*$ και μάλιστα $t^3 \equiv \frac{1}{3} \mod p\mathbb{Z}_p$. Τότε από το Λήμμα του Hensel για το πολυώνυμο $f(X) = X^3 - \frac{1}{3}$ υπάρχει $x \in \mathbb{Z}_p$ ώστε $x^3 = \frac{1}{3}$ και η $(x, 1, -1)$ είναι λύση της εξίσωσης $(*)$ στο $\mathbb{Q}_p$.

- Έστω $\overline{3} = 3 + p\mathbb{Z} \notin (\mathbb{Z}/p\mathbb{Z})^{*3}$. Έστω $H := (\mathbb{Z}/p\mathbb{Z})^* / (\mathbb{Z}/p\mathbb{Z})^{*3}$, τότε $|H| = 3$ και $p \equiv 1 \mod 3$. Το $\{\overline{1}, \overline{3}, \overline{9}\}$ είναι ένα πλήρες σύστημα αντιπροσώπων της H και άρα για κάθε $a \in \mathbb{Z}$ με $p \nmid a$, υπάρχει $b \in \mathbb{Z}$ ώστε να ισχύει μία από τις ισοτιμίες:

$$a \equiv b^3 \mod p, \qquad a \equiv 3b^3 \mod p, \qquad a \equiv 9b^3 \mod p$$

Αν $5 \equiv b^3 \mod p$ τότε από το Λήμμα του Hensel για το πολυώνυμο $f(X) = X^3 - 5$ υπάρχει $x \in \mathbb{Z}_p$ ώστε $x^3 = 5$ και τότε η $(-x, x, -1)$ είναι λύση της $(*)$.

Αν $5 \equiv 3b^3 \mod p$ τότε υπάρχει $x \in \mathbb{Z}_p$ ώστε $x^3 = \frac{5}{3}$ και η $(x, 0, -1)$ είναι λύση της $(*)$.

Τέλος αν $5 \equiv 9b^3 \mod p$ τότε $(3b)^3 \equiv 15 \mod p$ και από το Λήμμα του Hensel για το πολυώνυμο $f(X) = X^3 - 15$ υπάρχει $x \in \mathbb{Z}_p$ ώστε $x^3 = 15$ και άρα η $(3x, 5, -7)$ είναι λύση της $(*)$.

□

Δείξαμε λοιπόν ότι η εξίσωση του Selmer έχει μη τετριμμένη λύση στο $\mathbb{Q}_p$ για κάθε $p \in \mathbb{P}$. Προφανώς έχει λύση και στο $\mathbb{R}$ (π.χ. $(x, y, z) = (\sqrt[3]{5}, 0, \sqrt[3]{3})$).

3.3.2 Γενική μελέτη της εξίσωσης $3X^3 + 4Y^3 + 5Z^3 = 0$

Θεώρημα 3.3.2. *Η εξίσωση του Selmer $3X^3 + 4Y^3 + 5Z^3 = 0$ δεν έχει μη μηδενική ρητή λύση.*

Απόδειξη. Πολλαπλασιάζοντας την εξίσωση του Selmer με 2 παίρνουμε $(2Y)^3 + 6X^3 = 10(-Z)^3$. Επομένως αρκεί να δείξουμε ότι η εξίσωση

$$X^3 + 6Y^3 = 10Z^3 \qquad (1)$$

δεν έχει μη-μηδενική ρητή λύση. Έστω λοιπόν (x, y, z) μη-μηδενική ρητή λύση. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $x, y, z \in \mathbb{Z}$. Επειδή οι αριθμοί $6, 10, \frac{10}{6}$ δεν είναι τέλειοι κύβοι στο $\mathbb{Q}$ κανένα από τα x, y, z δεν μπορεί να είναι 0. Επίσης αν p είναι ένας πρώτος αριθμός ο οποίος διαιρεί

δύο από τους x, y, z τότε θα διαιρεί και τον τρίτο διότι οι ακέραιοι 6 και 10 δεν διαιρούνται από κύβο πρώτου αριθμού. Άρα, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι τα x, y, z είναι ανα δύο σχετικά πρώτα, δηλαδή $(x, y) = (x, z) = (y, z) = 1$.
Προφανώς από την (1) ο x είναι άρτιος. Αν κάποιο από τα y, z ήταν άρτιος τότε επειδή $2^3 \nmid 6, 10$ κατ'ανάγκη και ο άλλος θα ήταν άρτιος το οποίο αντιβαίνει στο ότι τα x, y, z είναι ανά δύο σχετικά πρώτα. Άρα ο x είναι άρτιος και οι y, z περιττοί.

Από την (1) έπεται ότι

$$x^3 \equiv z^3 \mod 3 \text{ και } x^3 + y^3 \equiv 0 \mod 5$$

Άρα αν $3 \mid x$ τότε $3 \mid z$ και αφού $3^3 \nmid 6$ έχουμε $3 \mid y$ το οποίο είναι άτοπο. Επίσης αν $5 \mid x \Rightarrow 5 \mid y$ και αφού $5^3 \nmid 10$ έχουμε $5 \mid z$ το οποίο είναι επίσης άτοπο. Συνεπώς $3 \nmid x, z$ και $5 \nmid x, y$.

Στην συνέχεια θα εργαστούμε στο σώμα $K = \mathbb{Q}(\alpha)$ με $\alpha = \sqrt[3]{6}$. Η (1) γράφεται ισοδύναμα:

$$(x + y\alpha)(x^2 - xy\alpha + y^2\alpha^2) = 10z^3 \qquad (2)$$

Βάση ακεραιότητας του σώματος K είναι το σύνολο $\{1, \sqrt[3]{6}, \sqrt[3]{36}\}$. Άρα ο δακτύλιος των ακεραίων αλγεβρικών του K είναι ο $R_K = \mathbb{Z}[\sqrt[3]{6}]$ και η διακρίνουσα του σώματος είναι $D_K = -3^3 6^2 = -972$. (βλ. [1] σελ. 66, [7] σελ. 176) και $N_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2) = a^3 + 6b^3 + 36c^3 - 18abc$

Εφαρμόζοντας τον νόμο ανάλυσης για τους πρώτους αριθμούς $2, 3, 5, 7$ έχουμε:
$< 2 >= P_2^3$ με $P_2 =< 2, \alpha >=< \alpha - 2 >$ όπου το P_2 είναι πρώτο ιδεώδες με $N_K(P_2) = 2$.
$< 3 >= P_3^3$ όπου $P_3 =< 3, \alpha >$ πρώτο ιδεώδες με $N_K(P_3) = 3$.
$< 5 >= P_5 P_{25}$ με $P_5 =< 5, \alpha - 1 >=< \alpha - 1 >$, $P_{25} =< 5, \alpha^2 + \alpha + 1 >$ και $N_K(P_5) = 5$, $N_K(P_{25}) = 5^2$.
$< 7 >= P_7 P_7' P_7''$ με $P_7 =< 7, \alpha + 1 >, P_7' =< 7, \alpha + 2 >, P_7'' =< 7, \alpha - 3 >$ και $N_K(P_7) = N_K(P_7') = N_K(P_7'') = 7$.
Τότε $< 10 >=< 2 >< 5 >= P_2^3 P_5 P_{25}$. Τα ιδεώδη P_2, P_3, P_5 του δακτυλίου R_K είναι τα μοναδικά ιδεώδη με norm 2,3 και 5 αντίστοιχα και τα P_7, P_7', P_7'' τα μοναδικά ιδεώδη με norm 7.

Θα υπολογίσουμε τώρα τον αριθμό κλάσεων ιδεωδών στου K. Η ταυτότητα του σώματος είναι $[r_1, r_2] = [1, 1]$ και η σταθερά του Minkowski είναι $M_K = (\frac{4}{p})^{r_2} \frac{n!}{n^n} \sqrt{|D_K|} \simeq 8,82$. Άρα σε κάθε κλάση υπάρχει ακέραιο ιδεώδες

με norm το πολύ 8.
Τα ιδεώδη P_2 και P_5 είναι κύρια. Επίσης

$$P_2P_3 =< 2, \alpha >< 3, \alpha >=< \alpha >$$

και άρα και το P_3 είναι κύριο.
Τώρα $N_{K/\mathbb{Q}}(\alpha+1) = 7$ και άρα $N_K(< \alpha+1 >) = 7$ και αφού $< \alpha+1 > \subseteq P_7$ αναγκαστικά $P_7 =< \alpha+1 >$, δηλαδη το P_7 είναι κύριο ιδεώδες.
Επίσης $N_{K/\mathbb{Q}}(\alpha+2) = 2^3 + 6 = 14 = 2 \cdot 7$, άρα $< \alpha+2 >= P_2P_7'$ και συνεπώς και το P_7' είναι κύριο. Τέλος αφού $< 7 >= P_7P_7'P_7''$, έχουμε ότι και το ιδεώδες P_7'' είναι κύριο. Άρα ο αριθμός κλάσεων ιδεωδών του K είναι $h_K = 1$. Εισάγοντας στο SAGE τις εντολές
$K. < a >= NumberField(x^3 - 6)$
$h = K.class\_number()$
μας επιστρέφει τον αριθμό κλάσεων ιδεωδών του K.

Η (2) σε μορφή ιδεωδών γράφεται

$$< x + y\alpha >< x^2 - xy\alpha + y^2\alpha >=< 10 >< z^3 >= P_2^3P_5P_{25} < z^3 > \quad (3)$$

Έστω P ένα πρώτο ιδεώδες το οποίο διαιρεί τα κύρια ιδεώδη $< x + y\alpha >$ και $< x^2 - xy\alpha + y^2\alpha >$. Θα δείξουμε ότι $P = P_2$. Αρχικά $P_2 |< x + y\alpha >$ και $P_2 |< x^2 - xy\alpha + y^2\alpha >$ διότι $P_2 |< \alpha >$ και $P_2 |< x >$ καθώς ο x είναι άρτιος. Αφού $x + y\alpha \in P$ και $x^2 - xy\alpha + y^2\alpha \in P$ έχουμε

$$3xy\alpha = (x + y\alpha)^2 - (x^2 - xy\alpha + y^2\alpha) \in P$$

Άρα $P |< 3 >< x >< y >< \alpha >$.

- Αν $P |< 3 >= P_3^3$ τότε $P = P_3$.
  Όμως τα ιδεώδη P_3, P_2, P_5 και P_{25} είναι διαφορετικά μεταξύ τους και άρα από την (3) έχουμε $P_3 |< z >$. Άρα $3 = N_K(P_3) \mid N_{K/\mathbb{Q}}(z) = z^3$. Δηλαδή $3 \mid z$ το οποίο δεν ισχύει. Άρα $P \neq P_3$

- Αν $P |< x >$, τότε $x \in P$ και $x + y\alpha \in P$, άρα $y\alpha \in P$, δηλαδή $P |< y >< \alpha >$. Όμως αφού $(x, y) = 1$ και $P |< x >$ έχουμε $P \nmid < y >$ και άρα $P |< \alpha >= P_2P_3$ και αφού $P \neq P_3$ αναγκαστικά $P = P_2$.

- Αν $P |< y >$, τότε αφού $x + y\alpha \in P$ έχουμε $P |< x >$ το οποίο δεν μπορεί να ισχύει αφού $(x, y) = 1$.

- Τέλος αν $P \mid < \alpha >$ αναγκαστικά $P = P_2$.

Συνεπώς το μόνο πρώτο ιδεώδες που μπορεί να διαιρεί τα $< x + y\alpha >$ και $< x^2 - xy\alpha + y^2\alpha >$ είναι το P_2.
Επειδή ο x είναι άρτιος έχουμε $< 2 >= P_2^3 \mid < x >$, όμως ο y είναι περιττός και το $< \alpha >= P_2P_3$, άρα το $< y\alpha >$ διαιρείται με P_2 ακριβώς μία φορά. Άρα και το ιδεώδες $< x + y\alpha >$ διαιρείται με P_2 ακριβώς μία φορά. Δηλαδή:

$$< x + y\alpha >= P_2A \text{ και } < x^2 - xy\alpha + y^2\alpha^2 >= P_2B$$

όπου $P_2 \nmid A$ και τα ιδεώδη A, B είναι πρώτα μεταξύ τους.
Από την (3) έχουμε

$$P_2^2AB = P_2^3P_5P_{25} < z >^3$$

δηλαδή

$$AB = P_2P_5P_{25} < z >^3$$

και άρα το P_2 διαιρεί το B.
Επειδή η συνάρτηση $x \mapsto x^3$ είναι ένα προς ένα στο $\mathbb{F}_5$ και $x^3 \equiv (-y)^3 \mod 5$ έχουμε $x \equiv -y \mod 5$ και άρα $x + y \in < 5 > \subseteq P_5 =< \alpha - 1 >$ και άρα $x + y\alpha = (x + y) + y(\alpha - 1) \in P_5$. Δηλαδή

$$P_5 \mid < x + y\alpha >$$

Αν τώρα $P_{25} \mid < x + y\alpha >$ τότε $< 5 >= P_5P_{25} \mid < x + y\alpha >$. Άρα το 5 διαιρεί το $x + y\alpha$ στον $R_K = \mathbb{Z}[\alpha]$, δηλαδή υπάρχουν $a, b, c \in \mathbb{Z}$ ώστε

$$x + y\alpha = 5(a + b\alpha + c\alpha^2)$$

από το οποίο προκύπτει ότι $5 \mid x, y$ το οποίο δεν ισχύει. Άρα το P_{25} είναι παράγοντας του $< x^2 - xy\alpha + y^2\alpha >$.
Συνεπώς $A = P_5M$ και $B = P_2P_{25}M'$ και τα ιδεώδη M, M' είναι πρώτα μεταξύ τους. Τότε

$$< x + y\alpha >= P_2P_5M \text{ και } < x^2 - xy\alpha + y^2\alpha >= P_2^2P_{25}M'.$$

και αφού $AB = P_2P_5P_{25} < z >^3$ έχουμε

$$P_5P_{25}MM' = P_5P_{25} < z >^3$$

Δηλαδή $< z >^3= MM'$ και αφού τα M, M' είναι σχετικά πρώτα είναι και τα δύο κύβοι ιδεωδών του R_K. Έστω $M = I^3$ και $M' = I'^3$.

Έχουμε δείξει λοιπόν ότι $< x + y\alpha >= P_2P_5I^3$ και αφού $h_K = 1$ υπάρχει $\beta \in R_K$ ώστε $I =< \beta >$. Δηλαδή $< x + y\alpha >=< \alpha - 2 >< \alpha - 1 >< \beta^3 >$ και συνεπώς

$$x + y\alpha = (\alpha - 2)(\alpha - 1)\beta^3v$$

για κάποια μονάδα $v \in R_K^*$. Επειδή $r_1 = 1$, $r_2 = 1$ από το Θεώρημα των μονάδων του Dirichlet η ομάδα των μονάδων είναι $R_K^* = \{\pm 1\} \times < \varepsilon_0 >$ για κάποια μονάδα ε_0. Άρα η ομάδα $R_K^* / (R_K^*)^3$ έχει τάξη 3. Αν βρούμε μία μονάδα η οποία δεν είναι κύβος τότε έχουμε ένα πλήρες σύστημα αντιπροσώπων της $R_K^* / (R_K^*)^3$.
Το $u = 1 - 6\alpha + 3\alpha^2 = \frac{(2-\alpha)^3}{2}$ έχει $N_{K/\mathbb{Q}}(u) = 1$ και άρα είναι μονάδα. Θα δείξουμε ότι το u δεν είναι κύβος.

Επειδή το ιδεώδες $< 7 >$ αναλύεται πλήρως στον R_K, το ιδεώδες

$$P_7 =< \alpha + 1 >$$

έχει norm 7 έχουμε $f(P_7/7\mathbb{Z}) = 1$, άρα $[R_K/P_7 : \mathbb{Z}/7\mathbb{Z}] = 1$ δηλαδή $R_K / P_7 \cong \mathbb{Z} / 7\mathbb{Z}$.
Θεωρούμε τον $\varphi : R_K \to \mathbb{Z} / 7\mathbb{Z}$ με $\varphi(\alpha) = 6 \mod 7$ και για κάθε $k \in \mathbb{Z}$, ισχύει $\varphi(k) = k mod 7$. Τότε $\varphi : R_K^* \to (\mathbb{Z} / 7\mathbb{Z})^*$ και ο φ είναι επιμορφισμός ομάδων. Τότε $\varphi(u) = (1 - 6 \cdot 6 + 3 \cdot 6^2) \mod 7 \equiv 3 \mod 7$. Συνεπώς το u δεν μπορεί να είναι κύβος στην R_K^* διότι το 3 δεν είναι κύβος $\mod 7$, και άρα το $\{1, u, u^2\}$ είναι ένα πλήρες σύστημα αντιπροσώπων της $R_K^* / (R_K^*)^3$. Άρα η μονάδα v γράφεται $v = u^k w^3$ για κάποια $k \in \{0, 1, 2\}$ και $w \in R_K^*$. Δηλαδή

$$x + y\alpha = (\alpha - 2)(\alpha - 1)(\beta w)^3 (\frac{(2-a)^3}{2})^k = (\alpha - 2)(\alpha - 1)\frac{(\beta w (2-\alpha)^k)^3}{2^k}$$

Έστω $\beta w (2-\alpha)^k = A + B\alpha + C\alpha^2 \in R_K$. Αφού $\beta w (2-\alpha)^k \neq 0$, τα A, B, C δεν είναι όλα 0 . Τότε

$$2^k x + 2^k y\alpha = (\alpha - 2)(\alpha - 1)(A + B\alpha + C\alpha)^3$$

Εξισώνοντας τους συντελεστές του α^2 και στα δύο μέλη παίρνουμε:

$$0 = A^3 + 6B^3 + 36C^3 + 36ABC - 9(A^2B + 6AC^2 + 6B^2C) + 6(AB^2 + A^2C + 6BC^2) \quad (4)$$

Άρα $A^3 \equiv 0 \mod 3$ και επομένως $3 \mid A$. Τότε όλοι οι όροι στην παραπάνω σχέση εκτός από το $6B^3$ διαιρούνται με 9 και άρα $6B^3 \equiv 0 mod 9$, δηλαδή $3 \mid B$. Συνεπώς όλοι οι όροι εκτός από το $36C^3$ διαιρούνται με 27, άρα αναγκαστικά $36C^3 \equiv 0 \mod 27$, δηλαδή $3 \mid C$.
Αφού λοιπόν τα A, B και C διαιρούνται και τα τρία με 3 και το δεξί μέλος της (4) είναι ομογενές, όλοι οι όροι διαιρούνται με 27. Επομένως διαιρώντας την (4) με 27 έχουμε ότι τα $(A', B', C') = (A/3, B/3, C/3)$ ικανοποιούν επίσης την (4). Συνεπώς μπορούμε να εφαρμόσουμε την παραπάνω διαδικασία άπειρες φορές οπότε αναγκαστικά $A = B = C = 0$, το οποίο είναι αντίφαση. □

Αναλυτικά η απόδειξη έχει δοθεί στο άρθρο του Conrad [14] το οποίο αποτελεί εμπεριστατωμένη έρευνα των ιδεών του Cassels [13] σελ.220-222

Θα αποδείξουμε τώρα ότι η εξίσωση του Selmer δεν έχει μη-τετριμμένη ρητή λύση με μία διαφορετική προσέγγιση. Είναι προφανές ότι αν έχει μη-τετριμμένη ρητή λύση τότε έχει και μη-τετριμμένη ακέραια λύση.

Θεώρημα 3.3.3. *Η κυβική καμπύλη του Selmer* $3X^3 + 4Y^3 + 5Z^3 = 0$ *δεν έχει μη-τετριμμένα ρητά σημεία.*

Λήμμα 3.3.4. *Έστω* $K = \mathbb{Q}(\omega)$*, όπου* ω *πρωταρχική 3η ρίζα της μονάδος και* $G = Gal(\mathbb{Q}(\omega)/\mathbb{Q})$*. Θεωρούμε την καμπύλη* $C : X^3 + Y^3 + d = 0$*,* $d \in \mathbb{Z}$*. Αν* $A, B \in K^2$ *δύο διακεκριμένα σημεία της καμπύλης* C *συζυγή ως προς την* G*, τότε η ευθεία που τα συνδέει είναι ρητή και το τρίτο σημείο τομής με την* C *έχει ρητές συντεταγμένες.*

Απόδειξη. Η ομάδα G είναι κυκλική, $G =< \sigma >$ με $\sigma(\omega) = \omega^2$. Έστω $A = (x_1, y_1), B = (x_2, y_2)$, τότε $\sigma(x_1) = x_2, \sigma(x_2) = x_1, \sigma(y_1) = y_2$ και $\sigma(y_2) = y_1$. Η ευθεία L που συνδέει τα A και B έχει κλίση $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. Τότε

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

και άρα $\lambda \in \mathbb{Q}$ και $L : Y = \lambda X + \mu$. Όμως $\mu = y_1 - \lambda x_1$ και άρα $\sigma(\mu) = \sigma(y_1) - \lambda\sigma(x_1) = y_2 - \lambda x_2 = \mu$, δηλαδή $\mu \in \mathbb{Q}$ και συνεπώς η ευθεία L είναι ρητή.

Έστω τώρα $\Gamma = (x_3, y_3)$ το τρίτο σημείο τομής της L με την C. Τότε τα A,B,Γ είναι λύσεις του συστήματος

$$\begin{cases} X^3 + Y^3 + d = 0 \\ Y = \lambda X + \mu \end{cases}$$

Δηλαδή τα x_1, x_2, x_3 είναι λύσεις της εξίσωσης

$$X^3 + (\lambda X + \mu)^3 + d = 0$$

Άρα $X^3 + (\lambda X + \mu)^3 + d = (\lambda^3 + 1)(X - x_1)(X - x_2)(X - x_3)$. Εξισώνοντας τους συντελεστές του X^2 έχουμε $3\lambda^2\mu = -(\lambda^3 + 1)(x_1 + x_2 + x_3)$, δηλαδή

$$x_1 + x_2 + x_3 = -\frac{3\lambda^2\mu}{\lambda^3 + 1} \in \mathbb{Q}$$

Όμως $\sigma(x_1 + x_2) = \sigma(x_1) + \sigma(x_2) = x_2 + x_1$, άρα $x_1 + x_2 \in \mathbb{Q}$ οπότε $x_3 \in \mathbb{Q}$. Τότε $y_3 = \lambda x_3 + \mu \in \mathbb{Q}$ και άρα το $\Gamma = (x_3, y_3)$ είναι ρητό σημείο. □

Θεώρημα 3.3.5. *Έστω $a, b, c \geq 1$ διακεκριμένοι ακέραιοι και έστω $d = abc$ ελεύθερο κύβου. Υποθέτουμε ότι υπάρχουν ακέραιοι u, v, w όχι όλοι μηδέν ώστε*

$$au^3 + bv^3 + cw^3 = 0$$

Τότε υπάρχουν $x, y, z \in \mathbb{Z}$ για τους οποίους ισχύει $x^3 + y^3 + dz^3 = 0$ και $z \neq 0$.

Απόδειξη. Έστω $K = \mathbb{Q}(\omega)$ όπου ω πρωταρχική 3η ρίζα της μονάδος,

$$G = Gal(K/\mathbb{Q}) =< \sigma >$$

με $\sigma(\omega) = \omega^2$. Θεωρούμε τα στοιχεία του σώματος K

$$\alpha = au^3 + \omega bv^3 + \omega^2 cw^3 \text{ και } \beta = au^3 + \omega^2 bv^3 + \omega cw^3$$

Τότε

$$\alpha + \beta = 2au^3 + (\omega^2 + \omega)bv^3 + (\omega^2 + \omega)cw^3 = 2au^3 - bv^3 - cw^3 = 3au^3$$

Όμοια, $\omega\alpha + \omega^2\beta = 3cw^3$ και $\omega^2\alpha + \omega\beta = 3bv^3$. Άρα

$$(\alpha + \beta)(\omega\alpha + \omega^2\beta)(\omega^2\alpha + \omega\beta) = 27abc(uvw)^3 = d(3uvw)^3$$

Όμως

$$(\alpha + \beta)(\omega\alpha + \omega^2\beta)(\omega^2\alpha + \omega\beta) = \alpha^3 + \beta^3$$

$\Rightarrow \alpha^3 + \beta^3 = d(3uvw)^3 \Rightarrow \alpha^3 + \beta^3 + d(-3uvw)^3 = 0$. Άρα για το $\gamma = -3uvw \in \mathbb{Z}$ έχουμε

$$\alpha^3 + \beta^3 + d\gamma^3 = 0 \qquad (1)$$

Ισχυρισμός: Κανένα από τα u, v, w δεν είναι μηδέν.
Πράγματι ισχύει $au^3 + bv^3 + cw^3 = 0$ και το $d = abc$ είναι ελεύθερο κύβου. Έστω ότι $w = 0$ τότε $au^3 + bv^3 = 0$ και $u, v \neq 0$ διότι δεν είναι και τα τρία u, v, w μηδέν. Έστω $u' = \frac{u}{(u,v)}$ και $v' = \frac{v}{(u,v)}$, $u', v' \neq 0$. Τότε $au'^3 + bv'^3 = 0$ και $(u', v') = 1$
Έστω $v' \neq \pm 1$ και p πρώτος αριθμός με $p \mid v'$. Τότε $p^3 \mid au'^3 \Rightarrow p^3 \mid a$ διότι $p \nmid u'$. Αυτό όμως είναι άτοπο διότι το $d = abc$ είναι ελεύθερο κύβου.
Αν $v' = 1$ τότε το u' δεν μπορεί να είναι 1 ή -1 διότι τότε $a \pm b = 0$ το οποίο δεν ισχύει διότι τα a, b είναι διακριτά και $a, b \geq 1$. Το ίδιο ισχύει και αν $v' = -1$. Συνεπώς αν $v' = \pm 1$ υπάρχει πρώτος p με $p \mid u'$. Τότε $p^3 \mid bv'^3 = \pm b$ το οποίο είναι άτοπο διότι το $d = abc$ είναι ελεύθερο κύβου. Δηλαδή $w \neq 0$. Ανάλογα αποδεικνύεται ότι $u \neq 0$ και $v \neq 0$.

Συνεπώς $\gamma = -3uvw \neq 0$ και η (1) γίνεται $(\frac{\alpha}{\gamma})^3 + (\frac{\beta}{\gamma})^3 + d = 0$ (2).

Θεωρούμε την καμπύλη $C := X^3 + Y^3 + d = 0$ και τα σημεία $A = (\frac{\alpha}{\gamma}, \frac{\omega\beta}{\gamma}), B = (\frac{\beta}{\gamma}, \frac{\omega^2\alpha}{\gamma})$. Τα A και B είναι σημεία της καμπύλης C συζυγή ως προς την G. Από το Λήμμα 3.3.4 η ευθεία που τα συνδέει είναι ρητή και τέμνει την C σε ένα ρητό σημείο $\Gamma = (x, y)$. Δηλαδή

$$x^3 + y^3 + d = 0$$

και τα $x, y \neq 0$ διότι $d > 1$ και ελεύθερο κύβου. Αν $x = \frac{k_1}{l_1}$ και $y = \frac{k_2}{l_2}$, πολλαπλασιάζοντας την παραπάνω σχέση με το $EK\Pi(l_1, l_2)^3$ παίρνουμε

$$x'^3 + y'^3 + dz^3 = 0$$

όπου $x', y', z \in \mathbb{Z}$ και $z \neq 0$.. □

Στην συνέχεια θα αποδείξουμε ότι η εξίσωση $X^3 + Y^3 + 60Z^3 = 0$ δεν έχει ρητή λύση (x, y, z) με $z \neq 0$. Τότε έχουμε την απόδειξη του Θεωρήματος 3.3.3.

Απόδειξη. (Θεωρήματος 3.3.3)
Έστω ότι η εξίσωση $3X^3 + 4Y^3 + 5Z^3 = 0$ έχει μη-τετριμμένη ρητή λύση, τότε έχει και μη-τετριμμένη ακέραια λύση. Τότε όμως από το Θεώρημα 3.3.5 η εξίσωση $X^3 + Y^3 + 60Z^3 = 0$ έχει μη-τετριμμένη ακέραια λύση (x, y, z) με $z \neq 0$ το αποίο είναι άτοπο. □

Παρατήρηση 3.3.6. *Στην καμπύλη* $X^3 + Y^3 + dZ^3 = 0$ (1) *αν θέσουμε* $X = U + V$ *και* $Y = U - V$, *έχουμε*

$$2U^3 + 6UV^2 + dZ^3 = 0$$

και για $X_1 = -6dZ$, $Y_1 = 6^2dV$ *και* $Z_1 = U$ *έχουμε*

$$Y_1^2 Z_1 = X_1^3 - 2^4 3^3 d^2 Z_1^3$$

Για $d = 60$ *θέτοντας* $Y_1 = 2^3 Y$, $X_1 = 2^2 X$ *και* $Z = Z_1$ *στην παραπάνω σχέση έχουμε*

$$Y^2 Z = X^3 - 3^3(30)^2 Z^3 \quad (2)$$

Άρα η (1) *είναι αμφίρρητα ισόμορφη με την* (2), *συνεπώς υπάρχει αμφιμονοσήμαντη αντιστοιχία ανάμεσα στα ρητά σημεία της* (1) *και της* (2). *Η προβολική καμπύλη* $Y^2Z = X^3 - 3^3(30)^2Z^3$, *έχει μόνο ένα επ'άπειρον σημείο το* $[0, 1, 0]$. *Τα υπόλοιπα σημεία της καμπύλης αντιστοιχούν σε αφινικά σημεία. Θα εργαστούμε λοιπόν με την καμπύλη* $Y^2 = X^3 - 3^3(30)^2$ *που είναι η αντίστοιχη αφινική για την* (2). *Η παραπάνω είναι μία αφινική ελλειπτική καμπύλη.*

Θεώρημα 3.3.7. *(Θεώρημα του Mordell)*
Η ομάδα των ρητών σημείων $E(\mathbb{Q})$ μιας ρητής ελλειπτικής καμπύλης E είναι πεπερασμένα παραγόμενη αβελιανή ομάδα.

Για την απόδειξη του Θεωρήματος παραπέμπουμε στο [2]

Παρατήρηση 3.3.8. *Από το Θεώρημα του Mordell έχουμε ότι υπάρχει ακέραιος $r \geq 0$ ώστε $E(\mathbb{Q}) \cong E(\mathbb{Q})_{torsion} \oplus \mathbb{Z}^r$.*
Αν

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}) \oplus ... \oplus (\mathbb{Z}/p_s^{\nu_s}\mathbb{Z})$$

οπότε

$$2E(\mathbb{Q}) \cong (2\mathbb{Z})^r \oplus 2(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}) \oplus ... \oplus 2(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z})$$

και άρα

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r \oplus (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})/2(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}) \oplus ... \oplus (\mathbb{Z}/p_s^{\nu_s}\mathbb{Z})/2(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z})$$

Αν p είναι περιττός, τότε $2(\mathbb{Z}/p^\nu\mathbb{Z}) \cong \mathbb{Z}/p^\nu\mathbb{Z}$.
Αν $p = 2$ τότε $2(\mathbb{Z}/2^\nu\mathbb{Z}) \cong \mathbb{Z}/2^{\nu-1}\mathbb{Z}$
Άρα για p περιττό έχουμε $(\mathbb{Z}/p^\nu\mathbb{Z})/2(\mathbb{Z}/p^\nu\mathbb{Z}) = \{0\}$, ενώ αν $p = 2$, τότε έχουμε $(\mathbb{Z}/2^\nu\mathbb{Z})/2(\mathbb{Z}/2^\nu\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Έστω $t = \#\{j \in \{1, 2, ..., s\} | p_j = 2\}$ τότε

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{r+t}$$

και συνεπώς $|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+t}$

Θεώρημα 3.3.9. *Έστω $E_{|\mathbb{Q}}$ μια ελλειπτική καμπύλη σε μορφή Weierstrass $Y^2 = X^3 + k$, $k \in \mathbb{Z}$. Η ομάδα των ρητών σημείων της καμπύλης πεπερασμένης τάξης είναι*

$$E(\mathbb{Q})_{torsion} = \begin{cases} \mathbb{Z}/6\mathbb{Z}, & \text{αν } k = 1 \\ \mathbb{Z}/3\mathbb{Z}, & \text{αν } k = -432 \text{ ή αν το } k \text{ είναι τέλειο τετράγωνο και } k \neq 1 \\ \mathbb{Z}/2\mathbb{Z}, & \text{αν το } k \text{ είναι τέλειος κύβος και } k \neq 1 \\ \{O\}, & \text{αλλιώς} \end{cases}$$

Για την απόδειξη βλ. [23] σελ.134

Για την καμπύλη $Y^2 = X^3 - 3^3(30)^2$ λοιπόν έχουμε $E(\mathbb{Q})_{torsion} = \{O\}$. Αν αποδείξουμε ότι η ${}^{E(\mathbb{Q})}\!/_{2E(\mathbb{Q})}$ είναι τετριμμένη, τότε $r = 0$ και άρα $E(\mathbb{Q}) = \{O\}$. Δηλαδή η $Y^2 = X^3 - 3^3(30)^2$ δεν έχει ρητά σημεία και συνεπώς ούτε και η $U^3 + V^3 + 60 = 0$

Παρατήρηση 3.3.10. *Έστω $E(\mathbb{Q})$, η ομάδα των ρητών σημείων της ελλειπτικής καμπύλης $Y^2 = F(X)$ όπου $F(X) = X^3 + AX + B$ με $4A^3 + 27B^2 \neq 0$. Θεωρούμε τον μεταθετικό δακτύλιο $\mathbb{Q}[\Theta] = {}^{\mathbb{Q}[X]}\!/_{< F(X) >}$.*
Αν Το $F(X)$ είναι ανάγωγο πολυώνυμο, το $\mathbb{Q}[\Theta]$ είναι σώμα.
Αν το $F(X)$ αναλύεται σε γινόμενο δύο αναγώγων πολυωνύμων, έστω $F(X) = g_1(X)g_2(X)$ τότε $\mathbb{Q}[\Theta] = {}^{\mathbb{Q}[X]}\!/_{< g_1(X) >} \oplus {}^{\mathbb{Q}[X]}\!/_{< g_2(X) >}$.
Τέλος αν το $F(X)$ αναλύεται πλήρως στο $\mathbb{Q}$, δηλαδή έχει τρεις ρητές ρίζες e_1, e_2, e_3, τότε $\mathbb{Q}[\Theta] = {}^{\mathbb{Q}[X]}\!/_{< X - e_1 >} \oplus {}^{\mathbb{Q}[X]}\!/_{< X - e_2 >} \oplus {}^{\mathbb{Q}[X]}\!/_{< X - e_3 >} \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$. Θα θεωρήσουμε μόνο τις περιπτώσεις που το $F(X)$ έχει τρεις ρητές ρίζες ή καμία ρητή ρίζα.

Ορισμός 3.3.11. Ορίζουμε την απεικόνιση $\mu : E(\mathbb{Q}) \to {}^{\mathbb{Q}[\Theta]^*}\!/_{(\mathbb{Q}[\Theta]^*)^2}$.
Περίπτωση 1: Το $F(X) = X^3 + aX + b$ έχει τρεις ρητές ρίζες e_1, e_2, e_3, τότε $\mathbb{Q}[\Theta] \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$ και ${}^{\mathbb{Q}[\Theta]^*}\!/_{(\mathbb{Q}[\Theta]^*)^2} \cong {}^{\mathbb{Q}^*}\!/_{\mathbb{Q}^{*2}} \oplus {}^{\mathbb{Q}^*}\!/_{\mathbb{Q}^{*2}} \oplus {}^{\mathbb{Q}^*}\!/_{\mathbb{Q}^{*2}}$.
$\mu : E(\mathbb{Q}) \to {}^{\mathbb{Q}^*}\!/_{\mathbb{Q}^{*2}} \oplus {}^{\mathbb{Q}^*}\!/_{\mathbb{Q}^{*2}} \oplus {}^{\mathbb{Q}^*}\!/_{\mathbb{Q}^{*2}}$ με
$\mu(O) = (1(\mathbb{Q}^*)^2, 1(\mathbb{Q}^*)^2, 1(\mathbb{Q}^*)^2)$
$\mu(x, y) = ((x - e_1)(\mathbb{Q}^*)^2, (x - e_2)(\mathbb{Q}^*)^2, (x - e_3)(\mathbb{Q}^*)^2)$ για $y \neq 0$
$\mu(e_1, 0) = ((e_2 - e_1)(e_3 - e_1)(\mathbb{Q}^*)^2, (e_1 - e_2)(\mathbb{Q}^*)^2, (e_1 - e_3)(\mathbb{Q}^*)^2)$, ανάλογα ορίζονται τα $\mu(e_2, 0)$ και $\mu(e_3, 0)$.

Περίπτωση 2: Το $F(X) = X^3 + aX + b$ δεν έχει καμία ρητή ρίζα.
$\mu : E(\mathbb{Q}) \to {}^{\mathbb{Q}[\Theta]^*}\!/_{(\mathbb{Q}[\Theta]^*)^2}$ με
$\mu(O) = 1(\mathbb{Q}[\Theta]^*)^2$, $\mu(x, y) = (x - \Theta)(\mathbb{Q}[\Theta]^*)^2$.

Θεώρημα 3.3.12. *Η απεικόνιση $\mu : E(\mathbb{Q}) \to {}^{\mathbb{Q}[\Theta]^*}\!/_{(\mathbb{Q}[\Theta]^*)^2}$, είναι ομομορφισμός ομάδων και $ker\mu = 2E(\mathbb{Q})$.*

Για την απόδειξη βλ. [12] σελ. 67-69, [5] σελ. 12.

Δίνουμε τώρα μία άλλη απόδειξη της Παρατήρησης 3.3.8.

Θεώρημα 3.3.13. *Έστω $E_{|\mathbb{Q}} : Y^2 = F(X) = X^3 + aX + b$ μια ελλειπτική καμπύλη με $a, b \in \mathbb{Z}$. Η ομάδα ${}^{E(\mathbb{Q})}\!/_{2E(\mathbb{Q})}$ είναι πεπερασμένη.*

Απόδειξη. Θα το αποδείξουμε μόνο στην περίπτωση που το $F(X) = X^3 + aX + b$ έχει τρεις ρίζες $e_1, e_2, e_3 \in \mathbb{Q}$.
Έστω $(x, y) \in E(\mathbb{Q})$, $y \neq 0$, τότε τα x, y έχουν την μορφή $x = \frac{r}{t^2}$ και $y = \frac{s}{t^3}$ με $r, s, t \in \mathbb{Z}$ και $(r, t) = (s, t) = 1$.
Πράγματι έστω $x = \frac{m}{np^r}$ και $y = \frac{d}{ep^s}$ όπου $r > 0$ και $p \nmid mnde$. Τότε από την εξίσωση της καμπύλης έχουμε

$$\frac{d^2}{e^2p^{2s}} = \frac{m^3}{(np^r)^3} + a\frac{m}{np^r} + b = \frac{m^3 + amn^2p^{2r} + bn^3p^{3r}}{n^3p^{3r}}$$

Έχουμε $ord_p(\frac{d^2}{e^2}p^{2s}) = -2s$. Αφού $r > 0$ και $p \nmid m$ έπεται ότι

$$p \nmid (m^3 + amn^2p^{2r} + bn^3p^{3r})$$

Επομένως $ord_p(\frac{m^3+amn^2p^{2r}+bn^3p^{3r}}{n^3p^{3r}}) = -3r$. Άρα $2s = 3r$ και αφού $r > 0$ έπεται ότι $s > 0$ και συνεπώς το p διαιρεί και τον παρονομαστή του y. Μάλιστα $3 \mid s$ άρα $s = 3q$ για κάποιο $q \in \mathbb{Z}$, και άρα $r = 2q$. Δηλαδή

$$x = \frac{m}{n(p^q)^2} \qquad y = \frac{d}{e(p^q)^3}$$

Αν τώρα υποθέσουμε ότι ο p διαιρεί τον παρονομαστή του y τότε με όμοιο τρόπο βρίσκουμε ότι ο p διαιρεί και τον παρονομαστή του x και $r = 2q, s = 3q$, συνεπώς έχουμε το ζητούμενο. Δηλαδή $x = \frac{r}{t^2}$ και $y = \frac{s}{t^3}$.
Από την εξίσωση έπεται ότι

$$s^2 = r^3 + art^4 + bt^6$$

Αφού οι ρίζες e_1, e_2, e_3 του $F(X) = X^3 + aX + b$ είναι ρητοί αριθμοί και το $F(X)$ είναι μονικό, τα e_1, e_2, e_3 είναι ακέραιοι. Συνεπώς

$$s^2 = (r - e_1t^2)(r - e_2t^2)(r - e_3t^2) \qquad (1)$$

με $e_1, e_2, e_3 \in \mathbb{Z}$.
Έστω $d = \mu\kappa\delta((r-e_1t^2), (r-e_2t^2))$ τότε $d \mid (e_1-e_2)t^2 = (r-e_2t^2)-(r-e_1t^2)$ και $d \mid (e_1 - e_2)r = e_1(r - e_2t^2) - e_2(r - e_1t^2)$, και αφού $\mu\kappa\delta(t, r) = 1$ έπεται ότι $d \mid (e_1 - e_2)$. Ανάλογα ο $\mu\kappa\delta((r - e_1t^2), (r - e_3t^2))$ διαιρεί το $(e_1 - e_3)$ και ο $\mu\kappa\delta((r - e_2t^2), (r - e_3t^2))$ διαιρεί το $(e_2 - e_3)$. Μπορούμε να γράψουμε:

$$\begin{aligned} r - e_1t^2 &= d_1v_1^2 \\ r - e_2t^2 &= d_2v_2^2 \\ r - e_3t^2 &= d_3v_3^2 \end{aligned}$$

με μοναδικό τρόπο, όπου τα d_j είναι ελεύθερα τετραγώνου. Τότε λόγω της (1) το $d_1d_2d_3$ είναι τέλειο τετράγωνο. Έστω $d_1d_2d_3 = (p_1^{s_1}p_2^{s_2}...p_\kappa^{s_k})^2$ η ανάλυση του $d_1d_2d_3$ σε πρώτους παράγοντες. Τότε $p_i^{2s_i} \mid d_1d_2d_3$ και τα d_1, d_2, d_3 είναι ελεύθερα τετραγώνου, άρα $1 \leq 2s_i \leq 3$ δηλαδή $s_i = 1$ για κάθε $i = 1, ..., k$. Έστω $p \in \{p_1, p_2, ..., p_k\}$, αφού τα d_1, d_2, d_3 είναι ελεύθερα τετραγώνου το p διαιρεί ακριβώς δύο από τα d_1, d_2 και d_3. Αν $p \mid d_i, d_j$ για $i \neq j$ τότε $p \mid (r - e_it^2), (r - e_jt^2)$ και συνεπώς ο p διαιρεί και τον μέγιστο κοινό διαιρέτη τους και άρα το $(e_i - e_j)$. Τελίκα $p \mid (e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$ και αυτό για κάθε $p \in \{p_1, p_2, ..., p_k\}$. Συνεπώς

$$d_j \mid (e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$$

για κάθε $j = 1, 2, 3$. Άρα υπάρχουν πεπερασμένου πλήθους σύνολα $\{d_1, d_2, d_3\}$. Τότε για την απεικόνιση μ έχουμε:

$$\begin{aligned}\mu(x, y) &= ((x - e_1)(\mathbb{Q}^*)^2, (x - e_2)(\mathbb{Q}^*)^2, (x - e_3)(\mathbb{Q}^*)^2) \\ &= ((\tfrac{r}{t^2} - e_1)(\mathbb{Q}^*)^2, (\tfrac{r}{t^2} - e_2)(\mathbb{Q}^*)^2, (\tfrac{r}{t^2} - e_3)(\mathbb{Q}^*)^2) \\ &= ((r - e_1t^2)(\mathbb{Q}^*)^2, (r - e_2t^2)(\mathbb{Q}^*)^2, (r - e_3t^2)(\mathbb{Q}^*)^2) \\ &= (d_1v_1^2(\mathbb{Q}^*)^2, d_2v_2^2(\mathbb{Q}^*)^2, d_3v_3^2(\mathbb{Q}^*)^2) \\ &= (d_1(\mathbb{Q}^*)^2, d_2(\mathbb{Q}^*)^2, d_3(\mathbb{Q}^*)^2)\end{aligned}$$

Δηλαδή η εικόνα της μ είναι πεπερασμένη και συνεπώς και η ομάδα $E(\mathbb{Q})/2E(\mathbb{Q})$. □

Θεώρημα 3.3.14. *Για την καμπύλη $Y^2 = X^3 - 3^3(30)^2$ η ομάδα $E(\mathbb{Q})/2E(\mathbb{Q})$ είναι τετριμμένη.*

Απόδειξη. Έστω $\alpha = \sqrt[3]{30}$, οι ρίζες του πολυωνύμου $F(X) = X^3 - 3^3(30)^2$ είναι οι $e_1 = 3\alpha^2, e_2 = 3\omega\alpha^2, e_3 = 3\omega^2\alpha^2$, όπου ω είναι μία πρωταρχική 3η ρίζα της μονάδος. Έστω $K = \mathbb{Q}(\alpha)$ και $\tilde{K} = K(\omega)$. Έστω $(x, y) \in E(\mathbb{Q})$, τα x, y έχουν την μορφή $x = \frac{r}{t^2}$ και $y = \frac{s}{t^3}$ με $r, s, t \in \mathbb{Z}$ και $(r, t) = (s, t) = 1$. Τότε η εξίσωση γίνεται

$$s^2 = (r - e_1t^2)(r - e_2t^2)(r - e_3t^2)$$

και άρα

$$< s >^2 = < r - e_1t^2 >< r - e_2t^2 >< r - e_3t^2 > \qquad (1)$$

ως ιδεώδη του $R_{\tilde{K}}$. Όπως και στην περίπτωση με τις ρητές ρίζες αν Q είναι ένα πρώτο ιδεώδες του $R_{\tilde{K}}$ που διαιρεί δύο από τα $< r - e_1t^2 >, < r - e_2t^2 >$ $, < r - e_3t^2 >$, έστω τα $< r - e_it^2 >, < r - e_jt^2 >$ τότε διαιρεί και το

$< e_i - e_j >$. Άρα θα διαιρεί και την διακρίνουσα του πολυωνύμου $F(X)$. Η διακρίνουσα του $F(X)$ είναι $D(F) = -27(3^3(30)^2)^2 = -3^{13}2^45^4$. Συνεπώς $Q \mid < 3 >< 2 >< 5 >$.

Το ιδεώδες $< r - 3\alpha^2t^2 >$ του $R_K = \mathbb{Z}[\alpha]$ μπορεί να γραφεί

$$< r - 3\alpha^2t^2 >=< cb^2 >$$

για κάποια $c, b \in R_K$. Συγκεκριμένα θα αποδείξουμε ότι το $< r-3\alpha^2t^2 >$ είναι τέλειο τετράγωνο ιδεώδους του R_K. Έστω Q ένα πρώτο ιδεώδες του $R_{\tilde{K}}$ που διαιρεί το $< r - 3\alpha^2t^2 >$ αλλά όχι τα $< r - 3\omega\alpha^2t^2 >, < r - 3\omega^2\alpha^2t^2 >$ τότε από την σχέση (1), ο εκθέτης με τον οποίο εμφανίζεται το Q στην ανάλυση του $< r - 3\alpha^2t^2 >$ είναι άρτιος. Άρα και ο εκθέτης του $Q \cap R_K$ στην ανάλυση του $< r - 3\alpha^2t^2 >$ ως ιδεώδες του R_K είναι επίσης άρτιος.

Αν Q είναι ένα πρώτο ιδεώδες του $R_{\tilde{K}}$ που διαιρεί το $< r - 3\alpha^2t^2 >$ και κάποιο από τα $< r - 3\omega\alpha^2t^2 >, < r - 3\omega^2\alpha^2t^2 >$ τότε με βάση τα παραπάνω το $Q \mid < 2 >< 3 >< 5 >$. Όμως στον R_K τα ιδεώδη $< 2 >, < 3 >, < 5 >$ διακλαδίζονται πλήρως, δηλαδή $< 2 >= P_2^3$, $< 3 >= P_3^3$ και $< 5 >= P_5^3$ όπου τα P_2, P_3, P_5 είναι πρώτα ιδεώδη του R_K με $N_K(P_2) = 2$, $N_K(P_3) = 3$ και $N_K(P_5) = 5$. Συνεπώς $Q \mid P_2P_3P_5$.

Παρατηρούμε ότι $N_{K/\mathbb{Q}}(r - 3\alpha^2t^2) = \prod_{i=0}^{2}(r - 3\omega^i\alpha^2t^2) = s^2$. Αν $Q \mid P_2$ τότε $P_2 = Q \cap R_K$ και συνεπώς το P_2 διαιρεί το $< r - 3\alpha^2t^2 >$ στον R_K. Έστω l ο μεγαλύτερος εκθέτης ώστε $P_2^l \mid < r - 3\alpha^2t^2 >$. Τότε

$$N_K(P_2)^l \mid N_K(< r - 3\alpha^2t^2 >) = s^2$$

δηλαδή $2^l \mid s^2$ και το l είναι το μέγιστο δυνατό. Άρα ο l είναι άρτιος. Ανάλογα αν $Q \mid P_3$ ή $Q \mid P_5$ τότε τα P_3, P_5 εμφανίζονται στην ανάλυση του $< r-3\alpha^2t^2 >$ με άρτιο εκθέτη. Συνεπώς όλα τα πρώτα ιδεώδη του R_K που διαιρούν το $< r - 3\alpha^2t^2 >$ στον R_K εμφανίζονται με άρτιο εκθέτη στην ανάλυση του και άρα το $< r - 3\alpha^2t^2 >$ είναι τέλειο τετράγωνο ιδεώδους του R_K. Άρα υπάρχει ιδεώδες I του R_K ώστε

$$< r - 3\alpha^2t^2 >= I^2$$

Εισάγωντας στο SAGE τις εντολές
$K. < a >= NumberField(x^3 - 30)$
$h = K.class\_number()$
μας επιστρέφει τον αριθμό κλάσεων ιδεωδών του K, ο οποίος είναι $h_K = 3$.
Αφού $< r-3\alpha^2t^2 >= I^2$ και $(2, h_K) = 1$ το I είναι κύριο ιδεώδες, άρα υπάρχει $\beta \in K$ ώστε

$$< r - 3\alpha^2t^2 >=< \beta^2 >$$

Άρα $r - 3\alpha^2 t^2 = \varepsilon\beta^2$ για κάποια μονάδα $\varepsilon \in R_K$.

Η ταυτότητα του σώματος K είναι $[r_1, r_2] = [1, 1]$, οπότε σύμφωνα με το Θεώρημα των μονάδων του Dirichlet η ομάδα των μονάδων R_K^* έχει $rank$, $r = r_1 + r_2 - 1 = 1$, και επειδή οι ρίζες της μονάδος στο K είναι οι $\{\pm 1\}$ αν ε_0 είναι μία θεμελιώδης μονάδα έχουμε $\varepsilon = \pm\varepsilon_0^n$ για κάποιο $n \in \mathbb{Z}$.
Εισάγωντας στο SAGE τις εντολες:
$K.< a >= NumberField(x^3 - 30)$
$G.gens\_values()$
μας επιστρέφει την θεμελιώδη μονάδα $\varepsilon_0 = 1 + 9\alpha - 3\alpha^2 > 0$. Επειδή ισχύει $r - 3\alpha^2 t^2 > 0$ έπεται ότι $\varepsilon > 0$ και άρα $\varepsilon = \varepsilon_0^n$ για κάποιο $n \in \mathbb{Z}$. Συνεπώς

$$r - 3\alpha^2 t^2 = \varepsilon_0^n \beta^2$$

Ανάλογα με το αν ο n είναι άρτιος ή περιττός έχουμε:

$$r - 3\alpha^2 t^2 = \gamma^2 \quad \text{ή} \quad r - 3\alpha^2 t^2 = \varepsilon_0 \gamma^2$$

για κάποιο $\gamma \in R_K$.
Έστω ότι ισχύει η δεύτερη σχέση δηλαδή $r - 3\alpha^2 t^2 = \varepsilon_0 \gamma^2$, όπου

$$\varepsilon_0 = 1 + 9\alpha - 3^2 > 0$$

Έστω $\gamma = u + v\alpha + w\alpha^2$ για κάποια $u, v, w \in \mathbb{Q}$. Τότε

$\varepsilon_0\gamma^2 = (u^2 + 60wv + 360uv + 270v^2 - 3(30)^2 w^2) + (9u^2 + 2uv - 180uv - 90v^2 + 540vw + 30w^2)\alpha + (-3u^2 + 18uv + v^2 + 2uw - 180vw + 270w^2)\alpha^2$.
Εξισώνοντας τους συντελεστές του α και του α^2 για τα $\varepsilon_0\gamma^2$ και $r - 3\alpha^2 t^2$ έχουμε

$$9u^2 + 2uv - 180uv - 90v^2 + 540vw + 30w^2 = 0 \quad (2)$$

και

$$-3u^2 + 18uv + v^2 + 2uw - 180vw + 270w^2 = -3t^2 \quad (3)$$

Θέτουμε:

$$u = -28e + 90f$$
$$v = -9e + 29f$$
$$w = q - 3e + 9f$$

τότε η εξίσωση (2) γίνεται $30q^2 - 4ef = 0$. Το προβολικό σημείο $[e, f, q] = [4e^2, 4ef, 4eq] = [4e^2, 30q^2, 4eq]$, οπότε για $m = 2e, n = q$ έχουμε $[e, f, q] = [m^2, 30n^2, 2mn]$. Αντικαθιστώντας στην εξίσωση (3) παίρνουμε ότι για κάποιο l:

$$-3l^2 = 3m^4 - 112m^3 n + 1620m^2 n^2 - 10800mn^3 + 27900n^4$$

με $m, n, l \in \mathbb{Q}$. Όμως αυτή η εξίσωση δεν έχει λύση στο $\mathbb{Q}_2$ και συνεπώς ούτε και στο $\mathbb{Q}$.
Άρα ισχύει η $r-3\alpha^2t^2 = \gamma^2$. Τότε για την απεικόνιση $\mu : E(\mathbb{Q}) \to {\mathbb{Q}[\Theta]^*}/{(\mathbb{Q}[\Theta]^*)^2}$, έχουμε:
$\mu(x,y) = (x-\Theta)(\mathbb{Q}[\Theta]^*)^2 = (\frac{r}{t^2} - 3\alpha^2)(\mathbb{Q}[\Theta]^*)^2$
$= (r - 3\alpha^2t^2)(\mathbb{Q}[\Theta]^*)^2 = \gamma^2(\mathbb{Q}[\Theta]^*)^2 = (\mathbb{Q}[\Theta]^*)^2$.
Άρα $(x,y) \in ker\mu = 2E(\mathbb{Q})$ για κάθε $(x,y) \in E(\mathbb{Q})$, δηλαδή $E(\mathbb{Q}) = 2E(\mathbb{Q})$ και άρα η ομάδα ${E(\mathbb{Q})}/{2E(\mathbb{Q})}$ είναι τετριμμένη. □

Αποδείξαμε λοιπόν ότι η καμπύλη $Y^2 = X^3 - 3^3(30)^2$ δεν έχει ρητά σημεία. Άρα το μόνο ρητό σημείο της καμπύλης $X^3+Y^3+60Z^3 = 0$ είναι το $[1,-1,0]$ και συνεπώς η εξίσωση του Selmer $3X^3+4Y^3+5Z^3 = 0$ δεν έχει μη-μηδενική ρητή λύση.
Ανάλογο αποτέλεσμα ισχύει και για τις καμπύλες

$$12X^3+Y^3+5Z^3 = 0 \quad 15X^3+4Y^3+Z^3 = 0 \quad 3X^3+20Y^3+Z^3 = 0$$

(βλ. [25]). Μάλιστα δουλεύοντας ακριβώς όπως για την καμπύλη του Selmer αποδεικνύεται ότι δεν έχουν μη-μηδενική ρητή λύση. Η καμπύλη

$$X^3+22Y^3+3Z^3 = 0$$

είναι επίσης ένα αντιπαράδειγμα. (βλ. [13] σελ. 222)

3.4 Παρατηρήσεις

Όπως έχουμε ήδη αναφέρει, ο έλεγχος ύπαρξης λύσης στα σώματα $\mathbb{Q}_p$, ανάγεται στο πρόβλημα της ύπαρξης λύσης στο πεπερασμένο σώμα $\mathbb{F}_p$ και στη δυνατότητα εφαρμοφής του Λήμματος του Hensel στη συνέχεια.
Στην εργασία αποφύγαμε τη χρήση σχετικών αποτελεσμάτων και προσπαθήσαμε, κατά το δυνατόν, με στοιχειώδεις μεθόδους, να έχουμε τα αντίστοιχα αποτελέσματα. Εδώ θα αναφερθούμε στα θεωρητικά αυτά αποτελέσματα .

Η εξίσωση του Selmer

$$3X^3+4Y^3+5Z^3$$

είναι μια μη-ιδιάζουσα κυβική καμπύλη. Επομένως έχει γένος 1 στο $\mathbb{F}_p$ για κάθε πρώτο αριθμό p, ο οποίος δεν διαιρεί το γινόμενο $2 \cdot 3 \cdot 5$.

Το γεγονός ότι κάθε μη-ιδιάζουσα κυβική καμπύλη (γένους 1) ορισμένη υπεράνω του σώματος $\mathbb{F}_p$, έχει τουλάχιστον ένα $\mathbb{F}_p$-ρητό σημείο, είναι αποτέλεσμα του F.K.Schmidt. Ο Cassels [12] , σελ. 120 θεωρεί την ιδέα που βρίσκεται πίσω από την απόδειξη " amusing"

" He used analytic means to estimate the number of points defined over the extension fields $\mathbb{F}_{q^n}$. In particular, he showed that the number is > 0 for all large enough n.
Let $b_1, ..., b_n$ be n conjugate points defined over F_{q^n} and $c_1, ..., c_{n+1}$ be similar conjugates defined over $F_{q^{n+1}}$. Then by Riemann-Roch there is a function whose poles are simple poles at the c_i and which has simple zeros at the b_j . It has one further zero; which must be defined over F_q. "

Με χρήση αυτού του Θεωρήματος θα ήταν αρκετό για την απόδειξη ύπαρξης τοπικής λύσης μόνο ο επιπλέον έλεγχος για τους πρώτους $p = 2, 3, 5$

Για ελλειπτικές καμπύλες υπεράνω ενός πεπερασμένου σώματος $\mathbb{F}_q$ ισχύει το ακόλουθο θεώρημα του Hasse.

Θεώρημα 3.4.1. *("Εικασία του Riemann " για ελλειπτικές καμπύλες)*
Έστω $C : Y^2 = X^3 + AX + B$ ελλειπτική καμπύλη ορισμένη υπεράνω του πεπερασμένου σώματος $\mathbb{F}_q$. Ο αριθμός $N = N(C)$ των $\mathbb{F}_q$-σημείων της C (συμπεριλαμβανομένου και του επ'άπειρου σημείου της καμπύλης) επαληθεύει την ανισότητα

$$|N - (q + 1)| \leq 2\sqrt{q}$$

Με χρήση του Θεωρήματος και πάλι, θα έπρεπε να ελέγξουμε την ύπαρξη λύσης στο $\mathbb{Q}_p$ μόνο για τούς πρώτους p που διαιρούν την διακρίνουσα του πολυωνύμου $f(X) = X^3 + AX + B$ και, ίσως, και αυτούς που δεν επαληθεύουν την ανισότητα $p + 1 - 2\sqrt{p} \geq 1$, δηλαδή τους $p = 2, 3$.

Αντίστοιχο παράδειγμα αποτελεί το Θεώρημα 8.3.4 του Alex Schmidt [31] σελ. 142 το οποίο χρησιμοποιήσαμε για την ύπαρξη παντού τοπικής λύσης της διοφαντικής εξίσωσης των Lind-Reichardt. Εδώ η μεθοδολογία είναι αναλυτική και περιλαμβάνει βασικές έννοιες Θεωρίας χαρακτήρων Dirichlet, αθροισμάτων Gauss και αθροισμάτων Jacobi, ως προς δύο χαρακτήρες Dirichlet χ και ψ *modp*.

Η παρατήρηση ότι η εξίσωση του Selmer είναι μία διαγώνια εξίσωση μας οδηγεί επίσης να υπενθυμίσουμε ότι για διαγώνιες εξισώσεις υπάρχει γενικότερο Θεώρημα.

Θεώρημα 3.4.2. *Έστω η διαγώνια εξίσωση*

$$a_1X_1^{l_1} + a_2X_2^{l_2} + ... + a_rX_r^{l_r} = 0$$

με $a_i \in \mathbb{F}_p^*$ *για κάθε* $i = 1, ..., r$, *και* N_p *το σύνολο των λύσεων της εξίσωσης στο* $\mathbb{F}_p$. *Έστω* $M = \#\{(\chi_1, \chi_2, ..., \chi_r)\}$ *όπου* χ_i *είναι μη τετριμμένοι χαρακτήρες, τέτοιοι ώστε* $\chi_i^{l_i} = \varepsilon$ *και* $\chi_1\chi_2...\chi_r = \varepsilon$ *όπου* ε *ο ταυτοτικός χαρακτήρας. Τότε ισχύει*

$$|N_p - p^{r-1}| \leq M(p-1)p^{\frac{r}{2}-1}$$

(βλ. [21] σελ. 103)

Πόρισμα 3.4.3. *Το πλήθος* N_p *των* $\mathbb{F}_p$ *ρητών σημείων της καμπύλης*

$$aX^3 + bY^3 + cZ^3 = 0$$

όπου $a, b, c \in \mathbb{F}_p^*$ *επαληθεύει την ανισότητα*

$$|N_p - p^2| \leq 2(p-1)\sqrt{p}$$

Απόδειξη. Εφαρμόζουμε το προηγούμενο Θεώρημα για $r = 3$ και $l_1, l_2, l_3 = 3$.

- Αν $p \not\equiv 1 mod 3$ τότε δεν υπάρχουν χαρακτήρες στο $\mathbb{F}_p^*$ τάξης 3 και άρα $M = 0$.
- Αν $p \equiv 1 mod 3$ τότε υπάρχουν ακριβώς τρεις χαρακτήρες στο $\mathbb{F}_p^*$ με τάξη που διαιρεί το 3. Πράγματι αν $\mathbb{F}_p^* =< g >$, αυτοί είναι οι $\varepsilon, \chi_1, \chi_2$ με $\varepsilon(g^k) = 1$, $\chi_1(g^k) = e^{\frac{2\pi ik}{3}}$ και $\chi_2(g^k) = e^{\frac{4\pi ik}{3}}$. Παρατηρούμε ότι $\chi_1\chi_2 = \varepsilon$ και άρα οι μόνες τριάδες που ικανοποιούν τις απαιτήσεις του Θεωρήματος είναι οι (χ_1, χ_1, χ_1) και (χ_2, χ_2, χ_2). Δηλαδή $M = 2$.

Συνεπώς

$$|N_p - p^2| \leq M(p-1)\sqrt{p} \leq 2(p-1)\sqrt{p}$$

□

Επειδή για κάθε περιττό πρώτο αριθμό p ισχύει $-2(p-1)\sqrt{p} + p^2 \geq 2$, για $a, b, c \in \mathbb{F}_p^*$ η εξίσωση

$$aX^3 + bY^3 + cZ^3 = 0$$

έχει τουλάχιστον μία μη μηδενική λύση στο $\mathbb{F}_p$, για τους περιττούς πρώτους p με $a, b, c \in \mathbb{F}_p^*$.

Βιβλιογραφία

[1] Ιωάννης Α. Αντωνιάδης, Αριστείδης Ι. Κοντογεώργης, *Αλγεβρική Θεωρία Αριθμών*, ΚΑΛΛΙΠΟΣ, 2021
beta.kallipos.gr/jspui/handle/11419/8007

[2] Ιωάννης Α. Αντωνιάδης, *Αριθμητική Ελλειπτικών Καμπυλών-Το Θεώρημα του Mordell*, Ηράκλειο, 1999

[3] Ιωάννης Α. Αντωνιάδης, *Θεωρία Αριθμών κατά τον 17ο και 18ο αιώνα*, Ηράκλειο, 1999

[4] Ιωάννης Α. Αντωνιάδης, *Τοπικά Σώματα*, χειρόγραφες σημειώσεις

[5] Αλέξανδρος Γαλανάκης *Mordel-Weil Theorem for elliptic curves defined over number fields*, Μεταπτυχιακή εργασία, Ηράκλειο, 2017

[6] W. Aitken, F.Lemmermeyer, *Counterexamples to the Hasse Principle*, American Mathematical Monthly 118, (2011), 1-18

[7] Saban Alaca, Kenneth S. Williams, *Introductory Algebraic Number Theory*, CUP, Cambridge, 2004

[8] George Bachman, *Introduction to p-adic Numbers and Valuation Theory*, Academic Press, New York, 1964

[9] J.-P. Bezivin, Phillipe Robba, *A new p-adic method for proving irrationality and transcendence results*, Ann. Math. II, ser 129 (1989), 151-160

[10] Z.I. Borevic and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966

[11] J.W.Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Sac. 41, (1966), 193-291 και 42 (1967), 183

[12] J.W.S. Cassels, *Lectures on Elliptic Curves*, CUP, Cambridge, 1991

[13] J.W.S. Cassels *Local Fields*, CUP, Cambridge, 1986

[14] Keith Conrad,, *Selmer's Example*. Αναζητήστε "Keith Conrad expository" ή επισκεφθείτε
https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf

[15] Fernando Q. Gouvea, *p-adic Numbers, An Introduction*, Third Edition, Springer, 2020

[16] H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper.*, Journ. f. d. reine u. angewandte Math. 153 (1924) 113-130

[17] H. Hasse, *Mathematische Abhandlungen*, Hrsg.von H.W.Leopoldt and P.Roquette, 1975

[18] H. Hasse, *Über die Äquivalenz quadratischer Formen im Körper den rationalen Zahlen.*, Journ.f.d. reine u. angewandte Math. 152 (1923) 205-224

[19] H. Hasse, *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper den rationalen Zahlen.*,Journ.f.d. reine u. angewandte Math. 152 (1923) 129-148

[20] H. Hasse, K.Hensel, *Über die Normenreste eined relativ zyklischen Körpers von Primzahlgrad l nach einem Primteiler ľ von l.* , Math. Annalen 90 (1923) 262-278

[21] K. Ireland and M. Rosen *A Classical Introduction to Modern Number Theory*, Second Edition, Springer-Verlag, New York, 1990

[22] Svetlana Katok, *p-adic Analysis Compared with Real*, Student Mathematical Library vol.37, 2007.

[23] Anthony W. Knapp, *Elliptic Curves*, PUP, Princeton, 1992

[24] Carl Eric Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven von Geschlecht Eins*, PHD, Uppsala 1940

[25] B.Mazur, *On the passage from local to global in Number Theory*, Bulletin of the A.M.S, 29 (1), (1993), 14-50

[26] O.T.O'Meara, *Introduction to quadratic forms*, Springer-Verlag, 1963

[27] Hans Reichardt, *Einige im Kleinen überall lösbare in Grössen unlösbare diophantische Gleichungen* , J.reine angew. Math. 184, (1942), 12-18

[28] P. Roquette, *History of Valuation Theory, Part I, 23.7.2003*

[29] Winfried Scharlau, *Quadratic and Hermiitian Forms*, Springer-Verlag, Berlin 1985

[30] Amelie Schinck, *The Local-Global Principle in Number Theory*, Master Thesis, Concordia University, Montreal Canada, 2001

[31] Alexander Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer, Berlin Heidelberg, 2007

[32] Jean-Pierre Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973

[33] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986