ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Οι p-αδικοί αριθμοί και μία εφαρμογή στις Διοφαντικές εξισώσεις

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Ευγενίας Α. Αλεξοπούλου

Επιβλέπουσα: Σοφία Λαμπροπούλου
Καθηγήτρια Ε.Μ.Π.

Αθήνα, Ιούνιος 2007

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Οι p-αδικοί αριθμοί και μία εφαρμογή στις Διοφαντικές εξισώσεις

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Ευγενίας Α. Αλεξοπούλου

Επιβλέπουσα: Σοφία Λαμπροπούλου
Καθηγήτρια Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

.....	.....	.....
Ευγένιος Αγγελόπουλος	Σπύρος Αργυρός	Σοφία Λαμπροπούλου
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αν. Καθηγήτρια Ε.Μ.Π.

Αθήνα, Ιούνιος 2007.

Πρόλογος

Στην παρούσα διπλωματική εργασία μελετώνται οι p-αδικοί αριθμοί και παρουσιάζεται μία εφαρμογή τους στις Διοφαντικές εξισώσεις. Πιο συγκεκριμένα, στο πρώτο κεφάλαιο γίνεται μία ιστορική αναδρομή, στην οποία φαίνεται ο αρχικός ορισμός των p-αδικών αριθμών ως το σύνολο των από αριστερά πεπερασμένων αθροισμάτων δυνάμεων ενός πρώτου p, καθώς και τα κίνητρα που οδήγησαν στην κατασκευή τους. Αυτά ήταν η εύρεση ακεραίων λύσεων κάποιων Διοφαντικών εξισώσεων.

Στο δεύτερο κεφάλαιο εισάγεται η έννοια της μη αρχιμήδειας νόρμας και παρουσιάζονται οι κυριότερες ιδιότητες της, όπως το ότι σε ένα χώρο με μη αρχιμήδεια νόρμα κάθε τρίγωνο είναι ισοσκελές ή το ότι κάθε σημείο μιας μπάλας είναι κέντρο της μπάλας. Επίσης, ορίζεται η p-αδική νόρμα πάνω από το σώμα των ρητών αριθμών, η οποία είναι μη αρχιμήδεια. Σύμφωνα με το *Θεώρημα Ostrowski* (βλ. Θεώρημα 5) κάθε νόρμα που μπορεί να οριστεί πάνω στο $\mathbb{Q}$ είναι ισοδύναμη είτε με τη συνήθη απόλυτη τιμή, είτε με κάποια p-αδική.

Στο τρίτο κεφάλαιο κατασκευάζεται το σώμα των p-αδικών αριθμών $\mathbb{Q}_p$ με μεθόδους ανάλυσης καθώς και με αλγεβρικές μεθόδους, και μελετώνται οι βασικές του ιδιότητες, οι οποίες ξεχωρίζουν για την απλότητά τους σε σχέση με την κλασσική περίπτωση των πραγματικών αριθμών με τη συνήθη απόλυτη τιμή. Για παράδειγμα, μία ακολουθία p-αδικών αριθμών (a_n) είναι Cauchy αν και μόνο αν $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$. Επίσης, είναι πολύ εύκολο να βρίσκουμε στο $\mathbb{Q}_p$ ρίζες πολυωνύμων, όταν αυτά έχουν ρίζες modulo p. Αυτό μας λέει το *Λήμμα του Hensel*, το οποίο διατυπώνουμε στο τέταρτο κεφάλαιο (βλ. Θεώρημα 11).

Στο τέταρτο κεφάλαιο, παρουσιάζεται επίσης μία σημαντική εφαρμογή των p-αδικών αριθμών στην επίλυση Διοφαντικών εξισώσεων που είναι τετραγωνικές μορφές n μεταβλητών. Η επίλυση βασίζεται στο λήμμα του Hensel και στην *Τοπική-Ολική Αρχή*, που λέει ότι: ''μία Διοφαντική εξίσωση έχει λύσεις στο $\mathbb{Q}$ αν και μόνο αν έχει λύσεις σε κάθε $\mathbb{Q}_p$ και στο $\mathbb{R}$''. Η Τοπική-Ολική Αρχή δεν ισχύει πάντα, αλλά ισχύει στην περίπτωση των τετραγωνικών μορφών. Αυτό είναι το *Θεώρημα Hasse-Minkowski*, του οποίου και παραθέτουμε την απόδειξη.

Τέλος, στο πέμπτο κεφάλαιο, παραθέτουμε κάποιες άλλες εφαρμογές των p-αδικών στη Φυσική, τη Βιολογία και τη Θεωρία Πληροφοριών.

Κλείνοντας αυτή την εισαγωγή θα ήθελα να επισημάνω τη διαφορετικότητα, ως προς τον τρόπο σκέψης, που διέπει τα μαθηματικά των p-αδικών αριθμών σε αντίθεση με τα κλασσικά μαθηματικά. Αυτή η διαφορετικότητα υπήρξε για μένα μία πρόκληση και μία ευχάριστη έκπληξη, καθ' ότι μόνο με τα τελευταία είχα επαφή κατά τη διάρκεια των σπουδών μου. Θα ήθελα λοιπόν να ευχαριστήσω ιδιαίτερα την επιβλέπουσα καθηγήτρια Σοφία Λαμπροπούλου για το όμορφο θέμα που μου πρότεινε, καθώς και για την πολύτιμη βοήθειά της καθ' όλη τη διάρκεια της εκπόνησης της διπλωματικής μου εργασίας.

Introduction

The subject of this diploma thesis is the field of p-adic numbers $\mathbb{Q}_p$ and its use in solving Diophantine equations. We first present the motivation for the invention of p-adic numbers. In the next chapter we introduce the concept of a non-archimedean norm and its corresponding valuation and define the non-archimedean p-adic norm $|\cdot|_p$, where p is a prime number. We also study the properties of a non-archimedean norm on a field.

In chapter 3 we construct the field of p-adic numbers $\mathbb{Q}_p$, both analytically and algebraically. Analytically seen, the field $\mathbb{Q}_p$ is the completion of the rational numbers $\mathbb{Q}$ with respect to the p-adic norm $|\cdot|_p$. Algebraically, after constructing the ring of p-adic integers $\mathbb{Z}_p$ as the inverse limit of the inverse system $(\mathbb{Z}/p^n\mathbb{Z}, \theta_m^n)$, where $\theta_m^n(a) = a \pmod{p^m}$, one may construct $\mathbb{Q}_p$ as the field of fractions of $\mathbb{Z}_p$, $\mathbb{Z}_p[1/p]$. Studying Analysis in $\mathbb{Q}_p$ turns out to be very interesting. Some of the most important results presented are the following:

- Both $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are complete and $\mathbb{Z}_p$ is the completion of the integers $\mathbb{Z}$, with respect to the p-adic norm. Moreover $\mathbb{Z}_p$ is compact, whereas $\mathbb{Q}_p$ is locally compact.

- $\mathbb{Q}_p$ is a totally disconnected Hausdorff topological space. $\mathbb{Q}_p$ is not an ordered field and it is not algebraically closed.

- A sequence of p-adic numbers (a_n) is a Cauchy sequence if and only if $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$.

- A series of p-adic numbers $\sum_{n=1}^{\infty} a_n$ converges, if and only if $\lim_{n\to\infty} |a_n|_p = 0$.

Combining some of the above results with the algebraic structure of $\mathbb{Q}_p$ we obtain *Hensel's Lemma*, a method for approximating the roots of a polynomial within finite time. Hensel's Lemma states that a p-adic integer root of a polynomial with p-adic integer coefficients exists if and only if there exists a simple root modulo p. We present some simple applications of Hensel's

Lemma, like determining the roots of unity and the squares in $\mathbb{Q}_p$, and deciding when a quadratic form has a p-adic solution.

Furthermore, in chapter 4, we analyse the importance of Hensel's Lemma in solving Diophantine equations. More precisely, it can be combined with the *Local-Global Principle*, which states that an equation can be solved over $\mathbb{Q}$ if and only if it can be solved over all the $\mathbb{Q}_p$ and $\mathbb{R}$. We note that the Local-Global Principle does not hold for any equation. But given the Local-Global Principle and having a method for finding p-adic solutions of an equation, rational roots can also be detected. For example, in the case of quadratic forms the Local-Global Principle is successful, as the *Hasse-Minkowski Theorem* states.

Finally, in chapter 5, we describe briefly some of the applications of the fields of p-adic numbers in Physics, in Information Theory and in Biology.

Περιεχόμενα

Κεφάλαιο 1

Μία σύντομη ιστορική αναδρομή

Κατά τη διάρκεια του περασμένου αιώνα οι p-αδικοί αριθμοί και η p-αδική ανάλυση έχουν αναπτυχθεί ιδιαίτερα και πλέον έχουν κεντρικό ρόλο στη θεωρία αριθμών. Αυτό συμβαίνει κυρίως για δύο λόγους: την ευκολία που μας παρέχει η γλώσσα των p-αδικών αριθμών στο να εκφράσουμε σχέσεις ισοτιμίας μεταξύ ακεραίων και την απλούστευση της μελέτης των ρητών από τη σκοπιά της ανάλυσης.

Η ιδέα είναι να εισαχθεί ένας νέος τρόπος μέτρησης της 'απόστασης' μεταξύ ρητών, μία νέα μετρική, και προέκυψε από συγκεκριμένα προβλήματα της Θεωρίας Αριθμών και της Άλγεβρας. Δεν υπάρχει λόγος να θεωρούμε μοναδική δυνατότητα για τους ρητούς να έχουν τη συνήθη μετρική. Για παράδειγμα, μια οποιαδήποτε άλλη συνάρτηση που αντιστοιχίζει σε κάθε ζεύγος ρητών έναν τρίτο και ικανοποιεί τον ορισμό της νόρμας θα ήταν ίσως εξίσου καλή για τη μελέτη τους. Αν ξεκινήσουμε από τη συνήθη νόρμα και τη μετρική που αυτή επάγει στο $\mathbb{Q}$, και πάρουμε την πλήρωση του $\mathbb{Q}$ προσθέτοντας τα όρια των ακολουθιών Cauchy ρητών αριθμών, καταλήγουμε στο σώμα των πραγματικών αριθμών $\mathbb{R}$. Αν διαλέξουμε διαφορετική νόρμα, θα καταλήξουμε σε κάτι άλλο. Αυτό ακριβώς είναι και το αντικείμενο της μελέτης μας.

Ο πρώτος μαθηματικός που εισήγαγε τους p-αδικούς αριθμούς ήταν ο Kurt Hensel στα 1897 , αν και ο E. Kummer χρησιμοποιούσε ήδη τις p-αδικές μεθόδους από το 1894. Ο Kummer κρατούσε καθ' όλη τη διάρκεια της ζωής

του σχέση δι' αλληλογραφίας με το μαθητή του Kronecker, ο οποίος έγραψε και τη διπλωματική του εργασία πάνω σε αυτήν την κατεύθυνση. Ο Kronecker ήταν με τη σειρά του καθηγητής του Hensel. Ο Hensel όχι μόνο σπούδασε με τους Kronecker και Kummer αλλα ήταν επίσης μαθητής του Weierstrass και ήξερε καλά τον ορισμό των πραγματικών αριθμών από τον Cantor και τις ιδέες των Weber και Detekind για την αναλογία μεταξυ σωμάτων αριθμών και σωμάτων συναρτήσεων. Παρακάτω θα δούμε γιατί ακριβώς ένας μαθηματικός που γνώριζε όλα αυτά τα εργαλεία μπόρεσε να εισάγει τις έννοιες και τους συμβολισμούς των p-αδικών αριθμών και των p-αδικών μεθόδων.

1.1 Η αναλογία του Hensel

Το κίνητρο του Hensel ήταν κυρίως η αναλογία μεταξύ του δακτυλίου $\mathbb{Z}$ των ακεραίων, με το σώμα-πηλίκο του, τους ρητούς $\mathbb{Q}$, και του δακτυλίου $\mathbb{C}[x]$ των πολυωνύμων με μιγαδικούς συντελεστες με το σώμα-πηλίκο τους $\mathbb{C}(x)$. Ας γίνουμε πιο συγκεκριμένοι: ένα στοιχείο $f(x) \in \mathbb{C}(x)$ είναι μία ρητή συνάρτηση, δηλ. το πηλίκο δύο πολυωνύμων $p(x), q(x) \in \mathbb{C}[x]$ με $q(x) \neq 0$:

$$f(x) = \frac{p(x)}{q(x)}.$$

Αντίστοιχα, ένας ρητός αριθμός $x \in \mathbb{Q}$ είναι το πηλίκο δύο ακεραίων $a, b \in \mathbb{Z}$ με $b \neq 0$:

$$x = \frac{a}{b}.$$

Επίσης, οι ιδιότητες των δύο δακτυλίων είναι αρκετά παρόμοιες. Και οι δύο είναι περιοχές μονοσήμαντης παραγοντοποίησης, όπου στον μεν $\mathbb{Z}$ έχουμε ότι κάθε ακέραιος μπορεί να εκφραστεί μοναδικά ως ± 1 επί ένα γινόμενο πρώτων, στον δε $\mathbb{C}(x)$ κάθε πολυώνυμο μπορεί να εκφραστεί μοναδικά ως

$$p(x) = a(x - a_1)(x - a_2)\dots(x - a_n),$$

με τους $a, a_1, a_2, \dots, a_n$ να είναι μιγαδικοί αριθμοί. Τα παραπάνω μας δίνουν το πρώτο στοιχείο της αναλογίας που διερεύνησε ο Hensel: *Οι πρώτοι αριθμοί $p \in Z$ είναι ανάλογοι των γραμμικών πολυωνύμων $(x - a) \in \mathbb{C}(x)$.*

Η αναλογία πάει ακόμα παραπέρα αν σκεφτεί κανείς ότι δοθέντος ενός πολυωνύμου $P(x)$ και ενός συγκεκριμένου $a \in \mathbb{C}$ μπορούμε, κάνοντας το ανάπτυγμα Taylor, να γράψουμε το πολυώνυμο στη μορφή:

$$P(x) = a_0 + a_1(x-a) + a_2(x-a)^2 + \ldots + a_n(x-a)^n$$

$$= \sum_{i=0}^{n} a_i(x-a)^i, a_i \in \mathbb{C}.$$

Προφανώς και για τους ακεραίους (τουλάχιστον για τους θετικούς ακεραίους για αρχή) έχουμε ότι δοθέντος θετικού ακεραίου m και πρώτου αριθμού p, μπορούμε να γράψουμε τον m σε βάση p, δηλ. στη μορφή:

$$m = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n = \sum_{i=0}^{n} a_i p^i,$$

$a_i \in \mathbb{Z},\ 0 \leq a_i \leq p-1$.

Αυτές οι εκφράσεις είναι ενδιαφέρουσες γιατί μας δίνουν 'τοπικές' πληροφορίες: για παράδειγμα το ανάπτυγμα σε δυνάμεις του $(x-a)$ μας δείχνει αν το a είναι ρίζα του $P(x)$ και τι βαθμού. Παρόμοια το ανάπτυγμα σε βάση p δείχνουν αν ο m διαιρείται από τον p και με ποιά πολλαπλότητα.

Τώρα, για τα πολυώνυμα και τα πηλίκα τους μπορούμε να πούμε περισσότερα πράγματα. Αν πάρουμε κάποιο πολυώνυμο $f(x)$ στο $\mathbb{C}(x)$ και ένα $a \in \mathbb{C}$, υπάρχει πάντα ανάπτυγμα της μορφής:

$$f(x) = \frac{p(x)}{q(x)} = a_{n_0}(x-a)^{n_0} + a_{n_0+1}(x-a)^{n_0+1} + \ldots = \sum_{i \geq n_0} a_i(x-a)^i,$$

το γνωστό από τη μιγαδική ανάλυση ανάπτυγμα Laurent του $f(x)$, με τους συντελεστές $a_i \in \mathbb{C}$ και τους εκθέτες $n_i \in \mathbb{Z}$. Όμως αυτό είναι ένα πιο πολύπλοκο αντικείμενο από το ανάπτυγμα Taylor που χρησιμοποιήσαμε πριν:

- Το n_0 μπορεί κάλλιστα να είναι και αρνητικό, γεγονός που μας δείχνει ότι το a είναι ρίζα του $q(x)$ και όχι του $p(x)$, ή διαφορετικά, αν το κλάσμα δεν είναι σε ανηγμένη μορφή, ότι η πολλαπλότητα του a ως ρίζας του $q(x)$ είναι μεγαλύτερη από αυτήν ως ρίζας του $p(x)$. Με όρους της Ανάλυσης θα λέγαμε ότι η $f(x)$ έχει *πόλο* τάξης $-n_0$ στο a.

- Το ανάπτυγμα συνήθως δεν είναι πεπερασμένο. Μάλιστα θα είναι πεπερασμένο τότε και μόνο τότε αν το κλάσμα είναι σε ανηγμένη μορφή και το $q(x)$ τυχαίνει να είναι κάποια δύναμη του $(x-a)$. Δηλαδή, συνήθως θα είναι ένα άπειρο άθροισμα, και μπορεί να αποδειχθεί ότι η σειρά $f(\lambda)$ θα συγκλίνει όποτε το λ είναι αρκετά κοντά αλλά όχι ίσο με το a.

Το σημαντικό είναι ότι κάθε ρητή συνάρτηση μπορεί να εκφραστεί μέσω ενός αναπτύγματος τέτοιας μορφής για κάθε έναν από τους 'πρώτους' $(x-a)$. Από την άλλη μεριά δεν αντιστοιχεί κάθε τέτοια σειρά σε ρητή συνάρτηση. Για παράδειγμα οι σειρές για το $sin(x)$, $exp(x)$ δεν αποτελούν αναπτύγματα ρητών συναρτήσεων. Δηλαδή έχουμε δύο σώματα, το $\mathbb{C}(x)$ και το σώμα όλων των σειρών Laurent $\mathbb{C}(x-a)$, με το πρώτο να εμπεριέχεται γνήσια στο δεύτερο. Η συνάρτηση:

$$f(x) \mapsto \text{ανάπτυγμα του } f(x) \text{ γύρω από το } (x-a)$$

ορίζει τον ακόλουθο εγκλεισμό των σωμάτων

$$\mathbb{C}(x) \hookrightarrow \mathbb{C}(x-a).$$

Υπάρχουν βέβαια άπειρες τέτοιες απεικονίσεις, μία για κάθε a, και κάθε μία μας δίνει 'τοπικές' πληροφορίες για τη συμπεριφορά των ρητών συναρτήσεων κοντά στο a.

Ο Hensel σκέφτηκε να επεκτείνει την αναλογία μεταξύ $\mathbb{C}[x]$ και $\mathbb{Z}$ ώστε να συμπεριλάβει την κατασκευή τέτοιων αναπτυγμάτων και στο $\mathbb{Q}$. Αν θυμηθούμε ότι το ανάλογο του να επιλέξουμε ένα a είναι να επιλέξουμε έναν πρώτο p, και ότι για τους θετικούς ακεραίους το ζητούμενο ανάπτυγμα είναι η έκφρασή του σε βάση p, μένει μόνο να περάσουμε στους θετικούς ρητούς. Το πέρασμα αυτό γίνεται με φυσικό τρόπο, γράφοντας αριθμητή και παρονομαστή σε βάση p και μετά διαιρώντας φορμαλιστικά. Το μόνο πράγμα στο οποίο πρέπει να είμαστε προσεκτικοί είναι η 'μεταφορά', με την έννοια ότι δύο συντελεστές a_{n_i}, a_{m_i} για τον όρο p^i μπορούν να αθροίζουν σε κάτι μεγαλύτερο του p, οπότε και μεταφέρουν κάποιο κρατούμενο στον επόμενο όρο p^{i+1}. Δηλαδή πρέπει να σκεφτόμαστε modulo p για τους συντελεστές και να μην ξεχνάμε τα κρατούμενα.

Δίνουμε ένα παράδειγμα τέτοιας διαίρεσης. Θα βρούμε την 3-αδική έκφραση του ρητού $r = \frac{32}{7}$:

$$r = \frac{32}{7} = \frac{2 + 1 \times 3 + 1 \times 3^3}{1 + 2 \times 3}$$

Εκτελούμε τη διαίρεση και προσέχουμε ότι $-1 \equiv 2 \pmod 3$:

$2 + 1 \times 3 + 1 \times 3^3$	$1 + 2 \times 3$
$- \quad (2 + 4 \times 3)$	$2 + 0 \times 3 + 2 \times 3^2 + 2 \times 3^3 + \cdots$
$= \quad 0 \quad - 3 \times 3$	
$= \qquad -1 \times 3^2 + 1 \times 3^3$	
$- \qquad (2 \times 3^2 + 4 \times 3^3)$	
$= \qquad -3 \times 3^2 - 3 \times 3^3$	
$= \qquad -1 \times 3^3 - 1 \times 3^4$	
$\vdots$	

Η σκέψη για την παραπάνω διαίρεση είναι ανάλογη αυτής της διαίρεσης πολυωνύμων. Οι όροι του πηλίκου a_n συμπληρώνονται ως εξής: πρέπει να επαληθεύουν την εξίσωση:

$$1 \cdot a_n \equiv b_n \pmod 3,$$

όπου b_n οι συντελεστές που προκύπτουν κατά τη διαδικασία της διαίρεσης. Στην παραπάνω διαίρεση, όπου $b_0 = 2,\ b_1 = 0,\ b_2 = -1,\ b_3 = -1$ κ.λ.π. έχουμε ότι για τα $a_0 = 2,\ a_1 = 0,\ a_2 = 2,\ a_3 = 2$ κ.λ.π. επαληθεύονται οι ακόλουθες εξισώσεις:

$1 \cdot 2 = 2 \pmod 3$
$1 \cdot 0 \equiv 0 \pmod 3$
$1 \cdot 2 = -1 \pmod 3$
$1 \cdot 2 = -1 \pmod 3$

κ.ο.κ

Συνεχίζουμε τη διδικασία επ' άπειρον
Έτσι έχουμε την έκφραση για τον r:

$$r = 2 + 2 \times 3^2 + 2 \times 3^3 + \cdots$$

Δεχόμενοι όλη αυτή τη διαδικασία φορμαλιστικά, μπορούμε να δούμε ότι είναι εφαρμόσιμη σε κάθε θετικό ρητό $x = a/b$ και ότι η τελική σειρά μας

δείχνει τις ιδιότητες του x σε σχέση με τον πρώτο p. Έτσι, για κάθε πρώτο p μπορούμε να γράψουμε κάθε (θετικό μέχρι τώρα) ρητό αριθμό a/b στη μορφή:

$$x = \frac{a}{b} = \sum_{n \geq n_0} a_n p^n, \ n_0 \in \mathbb{Z}.$$

Αν θεωρήσουμε ότι το κλάσμα a/b είναι σε ανηγμένη μορφή, παρατηρούμε τα ακόλουθα:

- $n_0 \geq 0$ αν και μόνο αν $p \nmid b$,
- $n_0 > 0$ αν και μόνο αν $p \nmid b$ και $p|a$
- $n_0 < 0$ αν και μόνο αν $p|b$ και $p \nmid a$

Δηλαδή το n_0 είναι κάτι παρόμοιο με την πολλαπλότητα μίας ρίζας ή πόλου στις ρητές συναρτήσεις, και σε αυτό αντανακλάται η 'πολλαπλότητα' του p στο a/b. Χαρακτηρίζεται δε από τη σχέση:

$$x = p^{n_0} \frac{a_1}{b_1} \ \mu\epsilon \ p \nmid a_1 b_1.$$

Μένει να δούμε πώς μπορούμε να πάρουμε τους αρνητικούς ρητούς αριθμούς. Αλλά, αν σκεφτούμε ότι οι σειρές μας μπορούν να πολλαπλασιαστούν, αρκεί να βρούμε ένα ανάπτυγμα για το -1. Βρίσκουμε ότι για κάθε p ισχύει:

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots,$$

αφού εάν προσθέσουμε 1 παίρνουμε:

$$\begin{aligned}
&\underbrace{1 + (p-1)}_{p} + (p-1)p + (p-1)p^2 + \cdots = \\
&= \underbrace{p + (p-1)p}_{p^2} + (p-1)p^2 + (p-1)p^3 + \cdots = \\
&= \underbrace{p^2 + (p-1)p^2}_{p^3} + (p-1)p^3 + \cdots = \\
&= \cdots \\
&= 0
\end{aligned}$$

Το συμπέρασμα είναι ότι μπορούμε –τουλάχιστον τυπικά, καθώς ακόμα δεν έχουμε ιδέα αν οι σειρές μας συγκλίνουν– να αντιστοιχίσουμε σε κάθε ρητό μία πεπερασμένη από τα αριστερά 'σειρά Laurent' δυνάμεων του p:

$$x = a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \ldots,\ n_0 \in \mathbb{Z}$$

Αυτή η σειρά καλείται *p-αδικό ανάπτυγμα του x*.

Δεν είναι δύσκολο να δείξει κανείς ότι το σύνολο όλων των από αριστερά πεπερασμένων σειρών Laurent δυνάμεων του p είναι σώμα, όπως και το $\mathbb{C}(x-a)$, που είναι σώμα.

Θεωρούμε τις ακόλουθες πράξεις της πρόσθεσης και του πολλαπλασιασμού στο σύνολο των p-αδικών αναπτυγμάτων ρητών αριθμών:

Για $x = \sum_{i\geq n_0} a_i p^i$ και $y = \sum_{i\geq m_0} b_i p^i$ ορίζουμε:

$$x + y = \sum_{i\geq min\{n_0,m_0\}} (a_i + b_i)p^i$$

$$xy = \sum_{i\geq 2min\{n_0,m_0\}} c_i p^i$$

με τους συντελεστές c_i να είναι

$$c_i = \sum_{i_1+i_2=i} a_{i_1} b_{i_2}.$$

Χωρίς βλάβη της γενικότητας, μπορούμε να ''γεμίσουμε'' κάποιο από τα δύο αναπτύγματα (αυτό με το μεγαλύτερο από τα $n_0,\ m_0$) με όρους με μηδενικούς συντελεστές. Πετυχαίνουμε έτσι και οι δύο σειρές να ξεκινάνε από το $min\{n_0, m_0\}$. Βέβαια δεν πρέπει να ξεχνάμε τη μεταφορά κρατουμένων, όπου είναι απαραίτητο. Με τις πράξεις αυτές το σύνολό μας γίνεται σώμα, το οποίο θα συμβολίζουμε με $\mathbb{Q}_p$ και θα το καλούμε *σώμα των p-αδικών αριθμών*.

Αυτός είναι ένας τρόπος να πάρουμε το $\mathbb{Q}_p$, και είναι αυτός που οδήγησε στην ανάπτυξη της θεωρίας των p-αδικών αριθμών. Θα παρουσιάσουμε αργότερα δύο ακόμα κατασκευές, οι οποίες θμελιώνουν τη διαισθητική θεωρία που αναπτύξαμε ως τώρα.

Όπως και πριν με τα σώματα $\mathbb{C}(x)$ και $\mathbb{C}(x-a)$, η συνάρτηση:

$$x \mapsto p\text{-αδικό ανάπτυγμα του } x$$

ορίζει έναν εγκλεισμό μεταξύ των δύο σωμάτων:

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p.$$

Το γεγονός ότι το $\mathbb{Q}_p$ είναι γνήσια μεγαλύτερο του $\mathbb{Q}$ θα το δείξουμε στην αμέσως επόμενη ενότητα.

Συνοψίζουμε την αναλογία που μελέτησε ο Hesnel στον ακόλουθο πίνακα:

$\mathbb{Z} \subset \mathbb{Q} \hookrightarrow \mathbb{Q}_p$	$\mathbb{C}[x] \subset \mathbb{C}(x) \hookrightarrow \mathbb{C}(x-a)$
πρώτοι $p \in \mathbb{Z}$	πολυώνυμα $(x-a) \in \mathbb{C}[x]$
$a \in \mathbb{Z} \Leftrightarrow a = \pm 1\, p_1 \cdot p_2 \cdots p_n$ p_i πρώτοι $\in \mathbb{Z}$	$p(x) \in \mathbb{C}[x] \Leftrightarrow p(x) = a(x-a_1)\cdots(x-a_m)$ με $a, a_i \in \mathbb{C}$
$r \in \mathbb{Q} \Leftrightarrow r = a/b$ με $a,\ b \in \mathbb{Z},\ b \neq 0$	$f(x) \in \mathbb{C}(x) \Leftrightarrow f(x) = p(x)/q(x)$ με $p(x),\ q(x) \in \mathbb{C}[x],\ q(x) \neq 0$
δοθέντος πρώτου $p \in \mathbb{Z}$ και $m \in \mathbb{Z}$ $m = a_0 + a_1 p + \ldots + a_n p^n,$ $a_i \in \mathbb{Z},\ 0 \leq a_i \leq p-1$	δοθέντος $a \in \mathbb{C}$ και $p(x) \in \mathbb{C}[x]$ $p(x) = a_0 + a_1(x-a) + \ldots + a_m(x-a)^m$ $a_j \in \mathbb{C}$
δοθέντος πρώτου $p \in \mathbb{Z}$ και $q \in \mathbb{Q}$ $q = a_{n_0} p^{n_0} + a_{n_0+1} p^{n_0+1} + \ldots,$ $a_i \in \mathbb{Z},\ 0 \leq a_i \leq p-1,\ n_0 \in \mathbb{Z}$	δοθέντος $a \in \mathbb{C}$ και $f(x) \in \mathbb{C}(x)$ $f(x) = a_{m_0}(x-a)^{m_0} + a_{m_0+1}(x-a)^{m_0+1} + \ldots,$ $a_j \in \mathbb{C},\ m_0 \in \mathbb{Z}$

1.2 Εξισώσεις modulo p^n

Οι p-αδικοί αριθμοί είναι στενά συνδεδεμένοι με το πρόβλημα της επίλυσης εξισώσεων modulo δυνάμεις του p. Θα δούμε μερικά ενδιαφέροντα παραδείγματα πάνω σε αυτό το θέμα.

1. Μία εξίσωση με λύσεις στο $\mathbb{Q}$

Θα ψάξουμε να βρούμε τις λύσεις της εξίσωσης

$$x^2 \equiv 25 \pmod{p^n} \tag{1.1}$$

για κάθε $n \in \mathbb{N}$. Γνωρίζουμε ότι η εξίσωση έχει τις ακέραιες λύσεις ± 5. Από αυτές αυτόματα παίρνουμε μία λύση για κάθε n: απλά παίρνουμε την $x \equiv \pm 5 \pmod{p^n}$ για κάθε n.

Κατ' αρχήν σημειώνουμε ότι πράγματι για $p \neq 2, 5$ οι μόνες δυνατές λύσεις ως προς ισοδυναμία της εξίσωσης $x^2 \equiv 25 \pmod{p^n}$ είναι οι ± 5. Αυτό προκύπτει από τη Θεωρία Αριθμών μελετώντας την περίπτωση $n = 1$ και διεξάγοντας τα συμπεράσματά μας και για μεγαλύτερα n:

Η τετραγωνική εξίσωση ισοτιμίας της μορφής $x^2 \equiv a \pmod{p}$, $a \in \mathbb{Z}$ με $p \nmid a$, $p \neq 2$ έχει είτε δύο είτε καμμία λύσεις. Στην προκειμένη περίπτωση ο 25 είναι τέλειο τετράγωνο, και άρα έχει ακριβώς δύο λύσεις, τις ± 5. Στη συνέχεια, με επαγωγή στο n, αποδεικνύεται ότι για την $x^2 \equiv a \pmod{p^n}$ με p περιττό πρώτο που δε διαιρεί το a, η εξίσωση επιδέχεται είτε δύο είτε καμμία λύσεις, ανάλογα με τη συμπεριφορά της modulo p.

Στις ειδικές περιπτώσεις όπου είτε $p|a$ ($p = 5$ για το δικό μας παράδειγμα) ή $p = 2$ έχουμε ότι η εξίσωση έχει πάνω από δύο ρίζες, το πλήθος των οποίων εξαρτάται από το n. Για $n = 1$, η εξίσωση $x^2 \equiv a \pmod{p}$ όταν $p = 2$ έχει μία λύση, τη μονάδα. Όταν $p|a$, δηλαδή $p = 5$, κάθε $x = p\,b$, $b \in \mathbb{Z}$ είναι λύση. Για υψηλότερους εκθέτες όταν $p = 2$ οι λύσεις της $x^2 \equiv 25 \pmod{2^n}$ για $n \geq 3$ είναι οι ακόλουθες τέσσερις: ± 5 και $\pm 5 + 2^{n-1}$. Τέλος, μπορούμε να βρούμε πολλές λύσεις της (1.1) και όταν $p = 5$. Ένα απλό παράδειγμα είναι η $x^2 \equiv 25 \pmod{5^3}$, που έχει, μεταξύ άλλων, λύσεις τις $x = \pm 5,\ \pm 20,\ \pm 30,\ \pm 45,\ \pm 55,\ \pm 70$.

Ας επιστρέψουμε τώρα στο αρχικό πρόβλημα και ας προσπαθήσουμε να κατανοήσουμε λίγο παραπάνω τις λύσεις της εξίσωσης (1.1), και να τις συσχετίσουμε με την p-αδική θεωρία. Ας διαλέξουμε ένα συγκεκριμένο πρώτο, έστω $p = 3$. Όπως είπαμε η εξίσωση έχει δύο λύσεις. Θα βρούμε για καθεμία τον ισοϋπόλοιπο ακέραιο modulo 3^n που ανήκει στο σύνολο $\{0,\ 1,\ \ldots,\ 3^n - 1\}$. Δηλαδή:

$$x \equiv 5 \equiv 2 \pmod{3}$$
$$x \equiv 5 \equiv 2 + 3 \pmod{3^2}$$
$$x \equiv 5 \equiv 2 + 3 \pmod{3^3}$$

κ.ο.κ

Αυτό παραμένει το ίδιο όσο αυξάνει το n. Μπορούμε να δούμε το αποτέλεσμα ως ένα 3-αδικό ανάπτυγμα:

$$x = 2 + 1 \times 3.$$

Με ανάλογο τρόπο, ξεκινώντας από τη δεύτερη λύση παίρνουμε κάτι πιο ενδιαφέρον:

$$x \equiv -5 \equiv 1 \pmod 3$$
$$x \equiv -5 \equiv 4 \equiv 1 + 3 \pmod{3^2}$$
$$x \equiv -5 \equiv 22 \equiv 1 + 3 + 2 \times 9 \pmod{3^3}$$
$$x \equiv -5 \equiv 76 \equiv 1 + 3 + 2 \times 9 + 2 \times 27 \pmod{3^4}$$
κ.ο.κ

όπου και πάλι μπορούμε να δούμε το αποτέλεσμα ως ένα άπειρο 3-αδικό ανάπτυγμα:

$$x = -5 = 1 + 1 \times 3 + 2 \times 3^2 + 2 \times 3^3 + 2 \times 3^4 + \cdots$$

Παρατηρούμε πως η p-αδική έκφραση που προκύπτει από την επίλυση εξισώσεων ισοτιμίας modulo p^n για κάθε n σχετίζονται μεταξύ τους. Συγκεκριμένα, αν 'κόψουμε' τα παραπάνω αναπτύγματα στον όρο 3^i θα πάρουμε μία λύση της εξίσωσης $x^2 \equiv 25 \pmod{3^{i+1}}$.

Μάλιστα, τα αναπτύγματα που βρήκαμε με αυτή τη διαδικασία δεν είναι παρά οι 3-αδικές λύσεις της εξίσωσης $x^2 = 25$. Αυτό επαληθεύεται εύκολα εκτελώντας τις πράξεις όπως τις ορίσαμε προηγουμένως.

2. Μία εξίσωση που δεν έχει λύσεις στο $\mathbb{Q}$

Τα πράγματα γίνονται πολύ πιο ενδιαφέροντα αν η εξίσωσή μας δεν έχει ρίζες στους ρητούς, όπως για παράδειγμα η εξίσωση:

$$x^2 \equiv 2 \pmod{7^n}.$$

Για $n = 1$ οι ρίζες είναι οι $x \equiv 3 \pmod 7$ και $x \equiv 4 \equiv -3 \pmod 7$. Για $n = 2$ πρέπει να σκεφτούμε ότι παρμένες modulo 7 θα πρέπει να είναι ρίζες και για $n = 1$. Δηλαδή, αν θέσουμε $x = 3 + 7k$ και λύσουμε ως προς k έχουμε:

$$(3+7k)^2 \equiv 2 \pmod{7^2}$$
$$9+42k \equiv 2 \pmod{7^2}$$
$$7+42k \equiv 0 \pmod{7^2}$$
$$1+6k \equiv 0 \pmod{7}$$
$$k \equiv 1 \pmod{7}$$

και αντικαθιστώντας μας δίνει τη μία λύση, $x \equiv 10 \pmod{7^2}$. Ομοίως, τη δεύτερη λύση την παίρνουμε ξεκινώντας από τη δεύτερη λύση modulo 7, την $x = 4$. Αυτή είναι $x \equiv 39 \equiv -10 \pmod{7^2}$.

Συνεχίζοντας την ίδια διαδικασία βρίσκουμε λύσεις x_{1i}, x_{2j} που συνεχίζονται επ' άπειρον:

$x_1 = (x_{1_1}, x_{1_2}, x_{1_3}, \ldots) = (3, 10, 108, \ldots)$ και

$x_2 = (x_{2_1}, x_{2_2}, x_{2_3}, \ldots) = (4, 39, 235, \ldots) \equiv (-3, -10, -108, \ldots) = -x_1$.

Όπως και στο προηγούμενο παράδειγμα, μπορούμε να εκφράσουμε τα προηγούμενα ως p-αδικά αναπτύγματα:

$$x_1 = (3, 10, 108, \ldots)$$
$$3 = 3$$
$$10 = 3 + 1 \times 7$$
$$108 = 3 + 1 \times 7 + 2 \times 7^2$$
$$\ldots$$

και έτσι παίρνουμε την 7-δική έκφραση:

$$x_1 = 3 + 1 \times 7 + 2 \times 7^2 + 6 \times 7^3 + \cdots.$$

Παρόμοια βρίσκουμε την αντίστοιχη έκφραση για το x_2:

$$x_2 = 4 + 5 \times 7 + 4 \times 7^2 + 0 \times 7^3 + \cdots.$$

Παρατήρηση 1 Στα παραπάνω δεδομένα αξίζει να παρατηρήσουμε μια λεπτομέρεια που θα αναλύσουμε αργότερα: για κάθε λύση x_{1_n} με $x_{1_n}^2 \equiv 2 \pmod{7^n}$ έχουμε ότι $x_{1_n} \equiv x_{1_{n-1}} \pmod{7^n}$.
Δηλαδή:

$$10 \equiv 3 \pmod 7$$

$$108 \equiv 10 \pmod{7^2}$$

$$2166 \equiv 108 \pmod{7^3}$$

κ.ο.κ

Παρατήρηση 2 Στο σώμα $\mathbb{Q}_7$ η εξίσωση $x^2 = 2$ έχει λύσεις, τις x_1, x_2. Συμπεραίνουμε έτσι ότι το $\mathbb{Q}_7$ είναι γνήσια μεγαλύτερο από το $\mathbb{Q}$.

Με τα παραπάνω παραδείγματα προσπαθούμε να δώσουμε έμφαση στο γεγονός ότι το να λύνει κανείς εξισώσεις modulo όλο και υψηλότερες δυνάμεις ενός πρώτου p είναι πολύ κοντά στο να λύνει την ανάλογη εξίσωση στο $\mathbb{Q}_p$. Είναι μάλιστα από τους πιο σημαντικούς λόγους για τη χρήση p-αδικών μεθόδων στη Θεωρία Αριθμών.

Μελέτη της εξίσωσης $x = 1 + 3x$

Η παραπάνω εξίσωση επιλύεται εύκολα και βρίσκουμε ότι η λύση της είναι $x = -1/2$. Αν όμως τη δούμε ως ένα πρόβλημα σταθερού σημείου, δηλαδή ως ένα πρόβλημα εύρεσης λύσης μιας εξίσωσης $f(x) = x$ για τη συνάρτηση $f(x) = 1 + 3x$, θα δούμε κάποια πολύ ενδιαφέροντα πράγματα. Τέτοια προβλήματα επιλύονται τις περισσότερες φορές με κάποια επαναληπτική μέθοδο: ξεκινάμε από μία αρχική προσέγγιση x_0 και υπολογίζουμε την τιμή της $f(x)$ στο x_0. Αυτή την τιμή χρησιμοποιούμε ως δεύτερη προσέγγιση $x_1 = f(x_0)$ και υπολογίζουμε την $f(x_1)$. Συνεχίζουμε με αυτόν τον τρόπο και παράγουμε μια ακολουθία $(x_i)_i$, η οποία ελπίζουμε ότι θα συγκλίνει στη λύση της αρχικής μας εξίσωσης.

Αν εφαρμόσουμε αυτή τη διαδικασία στη δική μας περίπτωση, ξεκινώντας από την αρχική προσέγγιση $x_0 = 1$, θα πάρουμε τα παρακάτω:

$$x_0 = 1$$

$$x_1 = 1 + 3x_0 = 1 + 3$$

$$x_2 = 1 + 3x_1 = 1 + 3 + 3^2$$

$$\dots$$

$$x_n = 1 + 3 + 3^2 + \cdots + 3^n$$

Στους πραγματικούς αριθμούς με τη συνήθη νόρμα αυτή είναι μια αποκλίνουσα ακολουθία. Είναι μία γεωμετρική πρόοδος με λόγο 3, της οποίας οι όροι γίνονται όλο και μεγαλύτεροι. Αν μπορούσαμε να αμελήσουμε το γεγονός ότι ο λόγος της προόδου είναι 3, δηλαδή το πρόβλημα ότι $|3| > 1$, και χρησιμοποιούσαμε τον τύπο για άπειρο άθροισμα γεωμετρικής προόδου, τότε θα παίρναμε:

$$1 + 3 + 3^2 + 3^3 + \cdots = \frac{1}{1-3} = -\frac{1}{2},$$

που είναι και η σωστή λύση.

Αν και στο $\mathbb{R}$ η ακολουθία που σχηματίσαμε είναι αποκλίνουσα, δεν υπάρχει κάτι που να μας εμποδίζει να τη δούμε ως ακολουθία στο $\mathbb{Q}_3$, με τους όρους της να ανήκουν στο $\mathbb{Q}$. Προφανώς στο $\mathbb{Q}_3$ η ακολουθία (x_n) *συγκλίνει* στον 3-αδικό αριθμό

$$1 + 3 + 3^2 + 3^3 + \cdots.$$

Αυτό δεν είναι παρά το 3-αδικό ανάπτυγμα του $-1/2$.

Το ενδιαφέρον στην περίπτωση αυτή είναι ότι κάτι το 'απαγορευμένο' στο $\mathbb{R}$ φαίνεται να λειτουργεί καλά όταν το δούμε από p-αδική άποψη. *Εισάγοντας τα σώματα των p-αδικών αριθμών διευρύνουμε την προοπτική μας και πλέον μας επιτρέπονται επιχειρήματα που προηγουμένως ήταν αδύνατο να επικαλεστούμε.*

1.3 Διοφαντικές Εξισώσεις

Στο δεύτερο Διεθνές Συνέδριο των Μαθηματικών το 1900, ο Hilbert παρουσίασε μία λίστα από 23 άλυτα ως τότε προβλήματα, διαφορετικού χαρακτήρα το καθένα. Το μόναδικό πρόβλημα απόφασης από αυτά ήταν το δέκατο στη λίστα, και αφορούσε τις Διοφαντικές εξισώσεις. Μία Διοφαντική εξίσωση είναι μία πολυωνυμική εξίσωση $f(x_1, x_2, \ldots, x_n) = 0$ με ρητούς ή ακέραιους συντελεστές, στην οποία οι απροσδιόριστες μπορούν να πάρουν ρητές ή ακέραιες τιμές. Το δέκατο πρόβλημα του Hilbert διατυπώνεται ως εξής:

> *Δοθείσης μία Διοφαντικής εξίσωσης, υπάρχει πεπερασμένη διαδικασία η οποία να αποφαίνεται για το αν η εξίσωση έχει λύσεις; Δηλαδή, υπάρχει αποδοτικός αλγόριθμος που να αποφασίζει αν μία Διοφαντική εξίσωση είναι επιλύσιμη;*

Το ερώτημα απαντήθηκε το 1970, οπότε και αποδείχθηκε ότι δεν μπορεί να υπάρξει τέτοιος αλγόριθμος. Η απόδειξη βασίστηκε στη Μαθηματική Λογική και τη Θεωρία της Υπολογισιμότητας. Πιο συγκεκριμένα, ορίζουμε ως *Διοφαντικό Σύνολο* σχετικό με κάποια Διοφαντική εξίσωση f, το σύνολο:

$$\{(x_1, \ldots, x_n) \in \mathbb{N}^n | \exists\, y_1, \ldots, y_m \in \mathbb{N}\, [f(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}\,.$$

Ακόμα, ένα *αναδρομικά αριθμήσιμο σύνολο A (recursively enumerable set)* είναι εκείνο για το οποίο υπάρχει αλγόριθμος που, για τυχαίο στοιχείο ως είσοδο, σταματά σε κατάσταση αποδοχής αν και μόνο αν το στοιχείο αυτό ανήκει στο A. Τέλος, ένα *υπολογιστό σύνολο B (computable, recursive set)* είναι εκείνο το σύνολο για το οποίο υπάρχει αλγόριθμος που τερματίζει έπειτα από πεπεραμένο χρόνο και αποφαίνεται εάν ένα στοιχείο x ανήκει ή όχι στο B. Η απάντηση στο δέκατο πρόβλημα του Hilbert είναι άμεση συνέπεια του ακόλουθου αποτελέσματος των Yuri Matiyasevich, Julia Robinson, Martin Davis και Hilary Putnam, γνωστό και ως Θεώρημα MRDP:

Κάθε αναδρομικά αριθμήσιμο σύνολο είναι Διοφαντικό.

Επειδή υπάρχει αναδρομικά αριθμήσιμο σύνολο, το οποίο όμως δεν είναι υπολογιστό το συμπέρασμα έπεται άμεσα. Για περισσότερες λεπτομέρειες παραπέμπουμε στα [6], [2] και [19].

Κεφάλαιο 2

Μη αρχιμήδειες νόρμες πάνω σε σώμα $\mathbb{K}$

Σε αυτή την ενότητα θα θεμελιώσουμε τη θεωρία που διαισθητικά αναπτύξαμε στην Εισαγωγή. Θα μελετήσουμε τις μη αρχιμήδειες νόρμες πάνω σε ένα τυχαίο σώμα $\mathbb{K}$ και τελικά θα εισάγουμε μία τέτοια νόρμα στο σώμα των ρητών αριθμών $\mathbb{Q}$.

Οι μη αρχιμήδειες νόρμες έχουν πολύ διαφορετικές ιδιότητες, σε σχέση τουλάχιστον με αυτό που έχουμε συνηθήσει ως τώρα. Εισάγουν μια διαφορετική έννοια της απόστασης και του μεγέθους των πραγμάτων με συνέπειες μία τελείως διαφορετική τοπολογία και ανάλυση. Αλλά ας δούμε αναλυτικά αυτή τη διαφορετική προσέγγιση.

2.1 Νόρμες πάνω σε σώμα $\mathbb{K}$

Ορισμός 1 Έστω $\mathbb{K}$ σώμα. Μία απεικόνιση $\|\cdot\| : \mathbb{K} \longrightarrow \mathbb{R}^+$ λέγεται *νόρμα* αν ικανοποιεί τις ακόλουθες ιδιότητες:

(i) $\|x\| = 0 \Leftrightarrow x = 0$

(ii) $\|xy\| = \|x\|\|y\|$ για κάθε $x,\ y \in \mathbb{K}$

(iii) $\|x + y\| \leq \|x\| + \|y\|$ για κάθε $x,\ y \in \mathbb{K}$

Μία νόρμα πάνω στο $\mathbb{K}$ λέγεται *μη αρχιμήδεια* αν επιπλέον ικανοποιεί τη συνθήκη:

(iv) $\|x+y\| \leq \max\{\|x\|, \|y\|\}$ για κάθε $x,\ y \in \mathbb{K}$.

Διαφορετικά θα λέγεται *αρχιμήδεια*.

Κάθε μη αρχιμήδεια νόρμα συνδέεται με μία 'εκτίμηση' και αντιστρόφως.

Ορισμός 2 Μία *εκτίμηση* (valuation) πάνω σε σώμα $\mathbb{K}$ είναι μια συνάρτηση

$$\upsilon : \mathbb{K} \to \mathbb{R},$$

τέτοια ώστε για κάθε $x, y \in \mathbb{K}$ να ισχύουν:

(i) $\upsilon(0) = +\infty$, εξ' ορισμού

(ii) $\upsilon(xy) = \upsilon(x) + \upsilon(y)$

(iii) $\upsilon(x+y) \geq \min\{\upsilon(x), \upsilon(y)\}$.

Συγκρίνοντας τις ιδιότητες (ii) και (iii) του ορισμού της εκτίμησης με τις ιδιότητες (ii) (iv) του ορισμού της μη αρχιμήδειας νόρμας βλέπουμε ότι είναι αρκετά παρόμοιες. Οι διαφορές τους είναι ότι το γινόμενο της πρώτης είναι άθροισμα στη δεύτερη και ότι έχουν αντίστροφη φορά ανισότητας. Μπορούμε να αντιστρέψουμε τη φορά της ανισότητας αλλάζοντας το πρόσημο, και να μετατρέψουμε το άθροισμα σε γινόμενο κάνοντάς το εκθετικό. Έτσι περνάμε από μία εκτίμηση σε μία μη αρχιμήδεια νόρμα και αντιστρόφως.

Γενικότερα, εκτίμηση και μη αρχιμήδεια νόρμα μπορούν ισοδύναμα να αποτελέσουν την αφετηρία μας για τη θεωρία που θα αναπτύξουμε. Θα προτιμήσουμε την έννοια της νόρμας, αν και ειδικά για την p-αδική θεωρία η p-αδικη εκτίμηση είναι ιδιαίτερα σημαντική.

Θα παραθέσουμε ακόμα μερικές από τις πιο σημαντικές ιδιότητες μίας νόρμας, αρχιμήδειας ή όχι.

Λήμμα 1 *Για κάθε νόρμα $\|\cdot\|$ πάνω σε σώμα $\mathbb{K}$ έχουμε:*

(i) $\|1\| = 1$

(ii) *Αν* $x \in \mathbb{K}$ *και* $\|x^n\| = 1$ *για κάποιο* $n \in \mathbb{Z}$, *τότε* $\|x\| = 1$.

(iii) $\|-1\| = 1$

(iv) *Για κάθε* $x \in \mathbb{K}$, $\|-x\| = \|x\|$

(v) *Αν το* $\mathbb{K}$ *είναι πεπερασμένο σώμα, τότε η* $\|\cdot\|$ *είναι η τετριμμένη νόρμα.*

Απόδειξη:

(i) Αν σκεφτούμε ότι το πεδίο τιμών της νόρμας είναι οι θετικοί πραγματικοί αριθμοί και ότι η μονάδα είναι το μοναδικό στοιχείο για το οποίο $1^2 = 1$ τότε έχουμε:

$\|1\| = \|1^2\| = \|1\|^2 \Rightarrow \|1\| = 1.$

(ii) Αποδεικνύεται από τη δεύτερη ιδιότητα της νόρμας και από το (i).

(iii) Αρκεί να σκεφτούμε ότι

$1 = \|1\| = \|(-1)(-1)\| = \|-1\|\,\|-1\|,$

και με το ίδιο σκεπτικό όπως στο (i) έχουμε το ζητούμενο.

(iv) Προφανές, εφ' όσον με χρήση του (iii) έχουμε:

$\|-x\| = \|(-1)\cdot x\| = \|-1\|\,\|x\| = \|x\|.$

(v) Αρκεί να θυμηθούμε ότι σε ένα πεπερασμένο σώμα κάθε αντιστρέψιμο στοιχείο $k_i \in \mathbb{K}$ μαζί με την πράξη του πολλαπλασιασμού παράγει κυκλική υποομάδα τάξης $n \leq |\mathbb{K}|$. Οπότε, σε συνδυασμό με το (i) παίρνουμε το ζητούμενο:

$1 = \|1\| = \|k_i^n\| = \|k_i\|^n$

$\Rightarrow \|k_i\| = 1$ για κάθε στοιχείο $k_i \in \mathbb{K}$.

□

Μάλιστα, για τις μη αρχιμήδειες νόρμες ισχύει κάτι πολύ ενδιαφέρον, που σχετίζεται με την ιδιότητα (iv) του ορισμού για τις μη αρχιμήδειες νόρμες:

Πρόταση 1 *Έστω $\mathbb{K}$ σώμα και $\|\cdot\|$ μια μη αρχιμήδεια νόρμα στο $\mathbb{K}$. Αν $x, y \in \mathbb{K}$ με $\|x\| \neq \|y\|$, τότε*

$$\|x+y\| = \max\{\|x\|, \|y\|\}.$$

Απόδειξη: Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $\|x\| > \|y\|$. Τότε, από την ιδιότητα (iv) για μη αρχιμήδειες νόρμες έχουμε ότι:

$$\|x+y\| \leq \|x\| = \max\{\|x\|, \|y\|\}. \tag{2.1}$$

Ακόμα επειδή $x = (x+y) - y$, παίρνουμε:

$$\|x\| = \|(x+y) - y\| \leq \max\{\|x+y\|, \|y\|\}.$$

Όμως, έχουμε υποθέσει ότι $\|x\| > \|y\|$, οπότε η παραπάνω ανισότητα μπορεί να ισχύει μόνο αν

$$\max\{\|x+y\|, \|y\|\} = \|x+y\|.$$

Δηλαδή παίρνουμε ότι $\|x\| \leq \|x+y\|$ και σε συνδυασμό με την (2.1) μπορούμε να συμπεράνουμε ότι:

$$\|x\| = \|x+y\|.$$

□

Θα παρουσιάσουμε τώρα από μία άλλη οπτική γωνία το διαχωρισμό αρχιμήδειας και μη αρχιμήδειας νόρμας. Θυμόμαστε ότι για κάθε σώμα $\mathbb{K}$ υπάρχει μια αντιστοίχιση $h : \mathbb{Z} \to \mathbb{K}$ που ορίζεται ως:

$$n \mapsto \begin{cases} \underbrace{1+1+\cdots+1}_{n}, & \text{αν } n > 0 \\ 0, & \text{αν } n = 0 \\ -\underbrace{(1+1+\cdots+1)}_{-n}, & \text{αν } n < 0. \end{cases}$$

Για παράδειγμα, αν έχουμε $\mathbb{Q} \subset \mathbb{K}$, τότε η h δεν είναι παρά η συνήθης απεικόνιση του $\mathbb{Z}$ στο $\mathbb{Q}$. Αν το $\mathbb{K}$ είναι πεπερασμένο, τότε η εικόνα της h είναι ένα υπόσωμα του $\mathbb{K}$, με πληθικότητα έναν πρώτο αριθμό.

Θεώρημα 1 *Έστω $h(\mathbb{Z}) \subset \mathbb{K}$ η εικόνα του $\mathbb{Z}$ σε σώμα $\mathbb{K}$. Μία νόρμα $\|\cdot\|$ στο $\mathbb{K}$ είναι μη αρχιμήδεια αν και μόνο αν $\|a\| \leq 1$ για κάθε $a \in h(\mathbb{Z})$. Συγκεκριμένα, μια νόρμα στο $\mathbb{Q}$ είναι μη αρχιμήδεια αν και μόνο αν $\|n\| \leq 1$ για κάθε $n \in \mathbb{Z}$.*

Απόδειξη: Το ευθύ αποδεικνύεται εύκολα με επαγωγή:

$$\|\pm 1\| = 1$$

και από την ιδιότητα (iv) για μη αρχιμήδειες νόρμες έχουμε ότι: για $k \in \mathbb{Z}$

$$\|k \pm 1\| \leq \max\{\|k\|, 1\}.$$

Άρα, αν η υπόθεση ισχύει για k, δηλαδή $\|k\| \leq 1$, τότε ισχύει και για $k+1$ και το ζητούμενο απεδείχθη.

Για το αντίστροφο θα χρησιμοποιήσουμε το ανάπτυγμα του Νεύτωνα. Θέλουμε να δείξουμε ότι αν $\|a\| \leq 1$ για κάθε στοιχείο του $h(\mathbb{Z})$, τότε για οποιαδήποτε δύο στοιχεία του $x, y \in \mathbb{K}$ θα έχουμε $\|x+y\| \leq \max\{\|x\|, \|y\|\}$. Αν κάποιο από τα δύο στοιχεία είναι μηδέν τότε η ανισότητα προκύπτει αμέσως. Αν όχι, τότε μπορούμε να διαιρέσουμε με $\|y\|$, οπότε παίρνουμε την ισοδύναμη:

$$\left\|\frac{x}{y} + 1\right\| \leq \max\left\{\left\|\frac{x}{y}\right\|, 1\right\}.$$

Δηλαδή, αρκεί να δείξουμε την ιδιότητα (iv) του ορισμού της μη αρχιμήδειας νόρμας, με το ένα από τα δύο στοιχεία να είναι η μονάδα.

Έστω λοιπόν ότι και τα δύο στοιχεία είναι μη μηδενικά, $y = 1$ και έστω m οποιοσδήποτε θετικός ακέραιος. Τότε έχουμε:

$$\begin{aligned}
\|x+1\|^m &= \left\|\textstyle\sum_k \binom{m}{k} x^k\right\| \\
&\leq \textstyle\sum_k \left\|\binom{m}{k}\right\| \|x^k\| \\
&\leq \textstyle\sum_k \|x\|^k \qquad\qquad (\text{από υπόθεση, αφού} \textstyle\binom{m}{n} \in \mathbb{Z}) \\
&\leq (m+1)\max\{\|x\|^m, 1\}
\end{aligned}$$

Παίρνοντας την m-οστή ρίζα και στα δύο μέλη παίρνουμε:

$$\|x+1\| \leq \sqrt[m]{m+1}\max\{1,\,\|x\|\},$$

ανισότητα που ισχύει για κάθε θετικό ακέραιο m. Όμως γνωρίζουμε ότι

$$\lim_{m\to\infty}\sqrt[m]{m+1}=1,$$

οπότε αν αφήσουμε το m να τρέξει στο άπειρο έχουμε το ζητούμενο:

$\|x+1\| \leq \max\{\|x\|,\,1\}$. □

Εκφράζοντας το παραπάνω θεώρημα λίγο διαφορετικά, αυτό που μας λέει είναι το ακόλουθο:

Πόρισμα 1 *Μία νόρμα $\|\cdot\|$ είναι μη αρχιμήδεια αν και μόνο αν*

$$\sup\{\|n\| :\, n\in\mathbb{Z}\}=1.$$

Για να ολοκληρώσουμε τη σύγκριση μεταξύ μιας αρχιμήδειας και μιας μη αρχιμήδειας νόρμας θα χαρακτηρίσουμε τις αρχιμήδειες νόρμες ως αυτές που έχουν την ακόλουθη ιδιότητα:

Αρχιμήδεια ιδιότητα: Δοθέντων $x,\,y\in\mathbb{K}$, $x\neq 0$, υπάρχει θετικός ακέραιος n τέτοιος ώστε $\|nx\|>\|y\|$.

Ουσιαστικά, η παραπάνω ιδιότητα μας λέει ότι μετρώντας το μέγεθος των ακεραίων με μια αρχιμήδεια νόρμα, μπορούμε να πάρουμε αυθαίρετα 'μεγάλους' ακέραιους. Με άλλα λόγια αν η $\|\cdot\|$ είναι αρχιμήδεια τότε:

$$\sup\{\|n\| :\, n\in\mathbb{Z}\}=+\infty.$$

Τέλος, αξίζει να αναφέρουμε ότι αυτές οι δύο περιπτώσεις είναι και οι μοναδικές δυνατές. Πράγματι, λόγω της πολλαπλασιαστικής ιδιότητας της νόρμας, εάν υπάρχει κάποιος ακέραιος k με νόρμα μεγαλύτερη του ένα, τότε

$$\lim_{n\to\infty}\|k^n\|=\lim_{n\to\infty}\|k\|^n=+\infty,$$

και άρα:

$$\sup\{\|n\| :\, n\in\mathbb{Z}\}=+\infty.$$

Αν δεν υπάρχει τέτοιο k τότε, εφ' όσον $\|1\|=1$, θα έχουμε

$$\sup\{\|n\| :\, n\in\mathbb{Z}\}=1.$$

2.2 Ένα παράδειγμα: η p-αδική νόρμα στο $\mathbb{Q}$

Θα ξεκινήσουμε από την p-αδική εκτίμηση στο $\mathbb{Q}$ για να καταλήξουμε στην p-αδική νόρμα στο $\mathbb{Q}$, ως ένα παράδειγμα μίας μη αρχιμήδειας νόρμας πάνω σε σώμα. Αυτό θα είναι που θα μας απασχολήσει σε αυτή την εργασία.

Ορισμός 3 Έστω ένας πρώτος $p \in \mathbb{Z}$. Η *p-αδική εκτίμηση στο $\mathbb{Z}$* ορίζεται ως η συνάρτηση

$$\upsilon_p : \mathbb{Z} \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

τέτοια ώστε: για κάθε μη μηδενικό $n \in \mathbb{Z}$, η $\upsilon_p(n)$ είναι η μέγιστη δύναμη του p που τον διαιρεί, δηλαδή ο μοναδικός μη αρνητικός ακέραιος που ικανοποιεί τη σχέση:

$$n = p^{\upsilon_p(n)} n', \text{ με } p \nmid n'.$$

Μπορούμε να επεκτείνουμε την εκτίμηση στο σώμα των ρητών ως ακολούθως:

Ορισμός 4 Η *p-αδική εκτίμηση στο $\mathbb{Q}$* είναι η επέκταση της υ_p που ορίζεται ως εξής:

$$\upsilon_p : \mathbb{Q} \setminus \{0\} \to \mathbb{R},$$

τέτοια ώστε αν $x = a/b \in \mathbb{Q} \setminus \{0\}$ με $a, b \in \mathbb{Z},\ b \neq 0$, η p-αδική εκτίμηση του x δίνεται από τη σχέση:

$$\upsilon_p(x) = \upsilon_p(a) - \upsilon_p(b).$$

Για το 0 ορίζουμε $\upsilon_p(0) = +\infty$.

Σε αντιστοιχία με τον Ορισμό 3 μπορούμε να δούμε ότι για την p-αδική εκτίμηση ενός ρητού αριθμού x ισχύει:

$$x = p^{\upsilon_p(x)} \frac{a}{b}, \qquad p \nmid ab.$$

Θεώρημα 2 *Η p-αδική εκτίμηση είναι εκτίμηση, όπως αυτή ορίστηκε στον Ορισμό 2.*

Απόδειξη: Το μόνο που χρειάζεται να κάνουμε είναι να επαληθεύσουμε τις ιδιότητες της συνάρτησης εκτίμησης. Εξ' ορισμού έχουμε ότι $\upsilon_p(0) = +\infty$. Για τις ιδιότητες (ii) και (iii) έχουμε ότι αν $x = a/b,\ y = c/d \in \mathbb{Q}$ τότε:

$$\begin{aligned}\upsilon_p(xy) &= \upsilon_p(\frac{a}{b}\frac{c}{d}) = \upsilon_p(\frac{ac}{bd}) = \upsilon_p(ac) - \upsilon_p(bd) = \\ &= \upsilon_p(a) + \upsilon_p(c) - \upsilon_p(b) - \upsilon_p(d) = \\ &= \upsilon_p(x) + \upsilon_p(y).\end{aligned}$$

Επιπλέον, με $\upsilon_p(x) = n,\ \upsilon_p(y) = m$ έχουμε:

$$\upsilon_p(x+y) = \upsilon_p(p^n\frac{a'}{b'} + p^m\frac{c'}{d'}) = \upsilon_p(p^{\min\{n,\,m\}}x') \geq \min\{n,\ m\},$$

αφού ο ρητός x' μπορεί να διαιρείται ή όχι από τον p. □

Ορισμός 5 Για κάθε $x \in \mathbb{Q}$ ορίζουμε την *p-αδική νόρμα* του x ως:

$$|\,x|_p = p^{-\upsilon_p(x)}$$

αν $x \neq 0$, και $|0|_p = 0$.

Παρατήρηση 3 Ο ορισμός για τη νόρμα του μηδενός είναι απολύτως συμβατός με τον ορισμό για την εκτίμηση στο μηδέν.

Παρατήρηση 4 Αξίζει να προσέξουμε ότι το πεδίο τιμών της p-αδικής νόρμας είναι το σύνολο $\{p^n :\ n \in \mathbb{Z}\}$. Δηλαδή, έχουμε διακριτό και αριθμήσιμο πεδίο τιμών.

Μένει να δείξουμε ότι αυτό που ορίσαμε ως p-αδική νόρμα είναι πράγματι μια νόρμα.

Θεώρημα 3 *Η συνάρτηση $|\cdot|_p$ είναι μία μη αρχιμήδεια νόρμα στο $\mathbb{Q}$.*

Απόδειξη: Οι ιδιότητες της νόρμας προκύπτουν άμεσα, εφαρμόζοντας το Λήμμα 1 για την p-αδική εκτίμηση. □

Ως παράδειγμα, ας υπολογίσουμε τα ακόλουθα: $\upsilon_7(902)$, $\upsilon_7(902/35)$, $\upsilon_5(400)$ και τις αντίστοιχες p-αδικές νόρμες.

$$\left.\begin{array}{l} 902 = 2 \cdot 11 \cdot 41 \Rightarrow \upsilon_7(902) = 0 \\ 35 = 5 \cdot 7 \Rightarrow \upsilon_7(35) = 1 \end{array}\right\} \Rightarrow \upsilon_7(902/35) = \upsilon_7(902) - \upsilon_7(35) = -1$$

$$400 = 5^2 \cdot 2^4 \Rightarrow \upsilon_5(400) = 2$$

και για τις νόρμες των παραπάνω στοιχείων έχουμε:

$|902|_7 = 7^{-\upsilon_7(902)} = 7^0 = 1$
$\left|\frac{902}{35}\right|_7 = 7^{-\upsilon_7(902/35)} 7^{-(-1)} = 7$
$|400|_5 = 5^{-\upsilon_5(400)} = 5^{-2}$

2.3 Οι διαφορετικές νόρμες στο $\mathbb{Q}$

Ας δούμε τι ακριβώς κάνει η p-αδική νόρμα: όσο πιο 'πολυ' ένας αριθμός x διαιρείται από τον πρώτο p που έχουμε επιλέξει, τόσο πιο μεγάλη είναι η εκτίμησή του $\upsilon_p(x)$ και τόσο μικρότερη η p-αδική του νόρμα $|x|_p$. Η p-αδική νόρμα έχει έναν τελείως διαφορετικό τρόπο μέτρησης του μεγέθους ενός αριθμού σε σχέση με τη συνήθη νόρμα στο $\mathbb{Q}$. Η πρώτη μας λέει ότι ένας αριθμός είναι 'μικρός' όταν διαιρείται πολύ με τον p, ενώ η δεύτερη ότι είναι 'μικρός' όταν είναι κοντά στο μηδέν.

Θα κλείσουμε αυτή την ενότητα αναφέροντας ότι οι δύο αυτοί τύποι νορμών είναι οι μοναδικές, ως προς ισοδυναμία, μη τετριμμένες νόρμες που μπορούν να οριστούν στο $\mathbb{Q}$.

Συμβολίζουμε τη συνήθη απόλυτη τιμή $|\cdot|$ στο $\mathbb{Q}$ ως $|\cdot|_\infty$. Είναι βολικό να σκεφτόμαστε το σύμβολο ∞ σαν έναν πρώτο αριθμό στο $\mathbb{Z}$ και να αναφερόμαστε σε αυτόν ως ''ο άπειρος πρώτος'', κυρίως διότι μπορούμε έτσι να υιοθετήσουμε το συμβολισμό $|\cdot|_p$ για κάθε $p \leq \infty$.

Μάλιστα, είναι πολύ ενδιαφέρον το ακόλουθο:

Θεώρημα 4 *Για κάθε $x \in \mathbb{Q} \setminus \{0\}$, έχουμε ότι:*

$$\prod_{p \leq \infty} |x|_p = 1.$$

Απόδειξη: Αρκεί να δείξουμε το ζητούμενο για έναν θετικό ακέραιο, καθώς τα υπόλοιπα έπονται εύκολα από αυτό. Γνωρίζουμε από το Θεμελιώδες Θεώρημα της Αριθμητικής ότι ένας θετικός ακέραιος x γράφεται μοναδικά ως γινόμενο δυνάμεων πρώτων:

$$x = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}.$$

Τότε για την p-αδική νόρμα του x έχουμε ότι:

$$|x|_p = \begin{cases} 1, & \text{αν} p \neq p_i \text{ για κάθε } i \\ p_i^{-a_i}, & \text{αν } p = p_i \text{ για κάποιο } i = 1, 2, \dots, k \\ x = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, & \text{αν } p = \infty \end{cases}$$

Το ότι το γινόμενο όλων των p-αδικών νορμών του x έιναι ίσο με τη μονάδα προκύπτει άμεσα. □

Δεδομένου ότι, ορίζοντας μια νόρμα πάνω σε ένα σώμα $\mathbb{K}$, ταυτόχρονα επάγεται και μια τοπολογία σε αυτό, θα ορίσουμε πότε δύο νόρμες είναι ισοδύναμες ως ακολούθως:

Ορισμός 6 Δύο νόρμες $\|\cdot\|_1$ και $\|\cdot\|_2$ πάνω σε σώμα $\mathbb{K}$ είναι *ισοδύναμες* αν ορίζουν την ίδια τοπολογία στο $\mathbb{K}$, δηλαδή εάν κάθε σύνολο που είναι ανοικτό ως προς τη μία νόρμα είναι ανοικτό και ως προς την άλλη.

Περνάμε έτσι στο Θεώρημα Ostrowski, που μας λέει ότι έχουμε βρει όλες τις νόρμες πάνω στο $\mathbb{Q}$, το οποίο παραθέτουμε χωρίς απόδειξη.

Θεώρημα 5 (Ostrowski) *Κάθε μη τετριμμένη νόρμα στο $\mathbb{Q}$ είναι ισοδύναμη με κάποια από τις νόρμες $|\cdot|_p$, όπου ο p είναι είτε ένας πρώτος αριθμός ή $p = \infty$.*

2.4 Τοπολογία σε σώμα με μη αρχιμήδεια νόρμα

Κάθε νόρμα περικλείει μία έννοια 'μεγέθους' των στοιχείων στα οποία εφαρμόζεται. Επίσης επάγει μια *μετρική* στο σώμα μας, δηλαδή μπορούμε να μετρήσουμε αποστάσεις μεταξύ των στοιχείων του. Έχοντας τη μετρική μπορούμε

να ορίσουμε ανοικτά και κλειστά σύνολα, να μελετήσουμε τη συνεκτικότητα του σώματος, και γενικότερα να ερευνήσουμε την *τοπολογία* που ορίζεται σε αυτό. Όταν η νόρμα μας έχει ιδιαίτερες ιδιότητες, τότε και η μετρική που επάγεται δίνει στο χώρο ιδιαίτερη τοπολογία. Αυτή την ιδιαίτερη τοπολογία των μη αρχιμήδειων νορμών θα μελετήσουμε σε αυτή την ενότητα.

Ορισμός 7 Έστω $\mathbb{K}$ σώμα και $\|\cdot\|$ οποιαδήποτε νόρμα στο $\mathbb{K}$. Ορίζουμε ως *απόσταση* $d(x,\, y)$ μεταξύ δύο στοιχείων $x,\, y \in \mathbb{K}$ ως:

$$d(x,\, y) = \|x - y\|\,.$$

Η συνάρτηση $d(x,\, y)$ καλείται *μετρική* που επάγεται από τη νόρμα. Μία μετρική ικανοποιεί τις ακόλουθες ιδιότητες:

(i) για κάθε $x,\, y \in \mathbb{K}$ ισχύει: $d(x,\, y) \geq 0$ και $d(x,\, y) = 0 \Leftrightarrow x = y$

(ii) για κάθε $x,\, y \in \mathbb{K}$ ισχύει: $d(x,\, y) = d(y,\, x)$

(iii) για κάθε $x,\, y \in \mathbb{K}$ ισχύει: $d(x,\, z) \leq d(x,\, y) + d(x,\, z)$.

Η τελευταία ιδιότητα καλείται και τριγωνική ανισότητα, καθώς εκφράζει το γεγονός ότι το άθροισμα δύο πλευρών ενός τριγώνου είναι πάντα μεγαλύτερο ή ίσο από την τρίτη πλευρά.

Ένας χώρος πάνω στον οποίο είναι ορισμένη μία μετρική καλείται *μετρικός χώρος*. Η παραπάνω πρόταση μας λέει ότι οποιοδήποτε σώμα πάνω στο οποίο έχει οριστεί μία νόρμα μετατρέπεται σε μετρικό χώρο αν ορίσουμε τη μετρική $d(x,\, y)$ όπως παραπάνω. Μάλιστα αυτή η μετρική συμπεριφέρεται καλά ως προς τις πράξεις του σώματος. Συγκεκριμένα, η πρόσθεση, ο πολλαπλασιασμός και το αντίστροφο στοιχείο είναι ως προς τη $d(x,\, y)$ συνεχείς συναρτήσεις, και το σώμα λέγεται *τοπολογικό σώμα*.

Πρόταση 2 *Η μετρική $d(x,\, y) = \|x - y\|$ που επάγεται από τη νόρμα $\|\cdot\|$ στο σώμα $\mathbb{K}$ κάνει το $\mathbb{K}$* τοπολογικό σώμα.

Απόδειξη: Θα δειξουμε ότι η πρόσθεση, ο πολλαπλασιασμός και το αντίστροφο στοιχείο είναι συνεχείς συναρτήσεις.

Η συνάρτηση της πρόσθεσης $+ : I\!K \times I\!K \to I\!K$ είναι συνεχής στο (x_0, y_0) αν και μόνο αν για κάθε $\epsilon > 0$ υπάρχει $\delta > 0$, τέτοιο ώστε οποτεδήποτε $d(x, x_0) < \delta$ και $d(y, y_0) < \delta$ τότε $d(x + y, x_0 + y_0) < \epsilon$.

Πράγματι, για κάθε $\epsilon > 0$ μπορούμε να επιλέξουμε $\delta = \epsilon/2 > 0$ και έχουμε:

$$\begin{aligned} d(x+y, x_0+y_0) &= \|(x+y)-(x_0+y_0)\| = \|(x-x_0)+(y-y_0)\| \\ &\leq \|x-x_0\| + \|y-y_0\| = \delta + \delta = \epsilon \end{aligned}$$

Παρατηρούμε κάτι που θα χρησιμοποιήσουμε παρακάτω: για κάθε δ ώστε $d(x, x_0) = \|x - x_0\| < \delta$ ισχύει:

$$|\|x\| - \|x_0\|| \leq \|x - x_0\| < \delta$$

$$\Leftrightarrow -\delta < \|x\| - \|x_0\| < \delta$$

$$\Leftrightarrow \|x_0\| - \delta < \|x\| < \|x_0\| + \delta.$$

Η συνάρτηση του πολλαπλασιασμού $\cdot : I\!K \times I\!K \to I\!K$ είναι συνεχής στο (x_0, y_0) αν και μόνο αν για κάθε $\epsilon > 0$ υπάρχει $\delta > 0$ τέτοιο ώστε οποτεδήποτε $d(x, x_0) < \delta$ και $d(y, y_0) < \delta$ τότε $d(xy, x_0y_0) < \epsilon$.
Για κάθε ϵ μπορώ να επιλέξω $\delta = -a + \sqrt{a^2 + \epsilon'} > 0$, όπου $a = \max\{\|x_0\|, |y_0\|\}$ και ϵ' λίγο μικρότερο του ϵ. Έτσι προκύπτει:

$$\begin{aligned} d(xy,\, x_0y_0) &= \|xy - x_0y_0\| = \|xy - xy_0 + xy_0 - x_0y_0\| \\ &\leq \|x\|\,\|y - y_0\| + \|y_0\|\,\|x - x_0\| \\ &= \|x\|\,\delta + \|y_0\|\,\delta \\ &\leq (\delta + \|x_0\|)\delta + \|y_0\|\,\delta \\ &= (-a + \sqrt{a^2+\epsilon'} + a)(-a + \sqrt{a^2+\epsilon'}) + \|y_0\| - a + \sqrt{a^2+\epsilon'} \\ &= \sqrt{a^2+\epsilon'}\,(\|y_0\| - a) + a(\|y_0\| - a) + \epsilon' \\ &\approx (a + a')(\|y_0\| - a) + a(\|y_0\| - a) + \epsilon', \quad \text{με } a' < \epsilon' \\ &= a'(\|y_0\| - a) + \epsilon' \leq \epsilon' < \epsilon. \end{aligned}$$

Η συνάρτηση του αντιστρόφου $h : I\!K \to I\!K$ είναι συνεχής στο x_0 αν και μόνο αν για κάθε $\epsilon > 0$ υπάρχει $\delta > 0$, τέτοιο ώστε οποτεδήποτε $d(x, x_0) < \delta$ τότε $d(1/x,\, 1/x_0) < \epsilon$.

Για κάθε ϵ μπορούμε να επιλέξουμε $\delta = \frac{\epsilon'\|x_0\|^2}{1 - \epsilon'\|x_0\|}$, όπου ϵ' λίγο μικρότερο του ϵ, και έτσι έχουμε:

$$\begin{aligned} d(\tfrac{1}{x},\, \tfrac{1}{x_0}) &= \left\| \tfrac{1}{x} - \tfrac{1}{x_0} \right\| = \left\| \tfrac{x_0 - x}{x_0 x} \right\| = \tfrac{d(x,x_0)}{\|x\|\|x_0\|} \\ &< \tfrac{\delta}{\|x\|\|x_0\|} < \tfrac{\delta}{(\|x_0\| - \delta)\|x_0\|} \\ &= \tfrac{\epsilon' \|x_0\|^2}{(1-\epsilon'\|x_0\|)\|x_0\|^2 - \epsilon'\|x_0\|^2\|x_0\|} \\ &= \epsilon' < \epsilon. \end{aligned}$$

□

Πρόταση 3 *Μία νόρμα $\|\cdot\|$ πάνω σε σώμα $\mathbb{K}$ είναι μη αρχιμήδεια αν και μόνο αν για τη μετρική που αυτή επάγει στο σώμα ισχύει:*

$$d(x,z) \leq \max\{d(x,y),\, d(y,z)\} \qquad \textit{για κάθε } \; x,y,z \in \mathbb{K}.$$

Απόδειξη: Για το ευθύ, απλώς εφαρμόζουμε τη μη αρχιμήδεια ιδιότητα (βλ. Ορισμό 1 (iv)) στην ισότητα:

$$(x - z) = (x - y) + (y - z).$$

Για το αντίστροφο, επιλέγουμε $y = -y_1$ και $z = 0$ και τα αντικαθιστούμε στην ανισότητα, οπότε έχουμε:

$$d(x,y) \leq \max\{d(x,z),\, d(z,y)\} \Rightarrow d(x,\, -y_1) \leq \max\{d(x,0),\, d(0,-y_1)\}$$

δηλαδή:

$$\|x + y_1\| \leq \max\{\|x\|,\, \|y_1\|\}$$

για κάθε $x, y_1 \in \mathbb{K}$. □

Η ανισότητα στην πρόταση είναι γνωστή ως *ουλτραμετρική ανισότητα* και ένας μετρικός χώρος στον οποίο αυτή επαληθεύεται λέγεται *ουλτραμετρικός*.

Πρόταση 4 *Σε έναν ουλτραμετρικό χώρο $\mathbb{K}$ όλα τα 'τρίγωνα' είναι ισοσκελή.*

Απόδειξη: Έστω $x,\, y,\, z \in \mathbb{K}$. Μπορούμε να δούμε τις μεταξύ τους αποστάσεις ως τα μήκη των πλευρών ενός τριγώνου:

$$d(x,y) = \|x - y\|$$

$$d(y,z) = \|y - z\|$$

$$d(x,z) = \|x - z\| .$$

Θυμόμαστε την Πρόταση 1 που μας λέει ότι για μια μη αρχιμήδεια νόρμα ισχύει:

$$\text{για } x,\, y \in I\!K \text{ αν } \|x\| \neq \|y\| \text{ τότε } \|x - y\| = \max\{\|x\|, \|y\|\} .$$

Στη δική μας περίπτωση έχουμε ότι:

$$(x - y) + (y - z) = (x - z) \Leftrightarrow (x - z) - (y - z) = (x - y) ,$$

για κάθε $x,\, y,\, z \in I\!K$.

Επομένως, αν δύο πλευρές είναι άνισες, έστω $d(x,z) \neq d(y,z)$, τότε η τρίτη πλευρά, η $d(x,y)$, είναι ίση με τη μεγαλύτερη από τις δύο. Σε κάθε περίπτωση, αφού τα $x,\, y,\, z$ μπορούν να εναλλάσσονται στην παραπάνω ισότητα, δύο από τις τρεις πλευρές είναι ίσες, δηλαδή, κάθε τρία σημεία σχηματίζουν ισοσκελές τρίγωνο. □

Μια σημαντική έννοια στους μετρικούς χώρους είναι αυτή της μπάλας. Σε έναν ουλτραμετρικό χώρο οι μπάλες που ορίζονται έχουν ιδιότητες που θα μας φανούν ασυνήθιστες. Έστω $a \in I\!K$ και $r \in I\!R_+$. Συμβολίζουμε με $B(a,r)$ την *ανοικτή μπάλα* με κέντρο το a και ακτίνα r, ενώ συμβολίζουμε με $\overline{B}(a,r)$ την *κλειστή μπάλα* με κέντρο το a και ακτίνα r.

Πρόταση 5 *Έστω $(I\!K, \|\cdot\|)$ τοπολογικό σώμα με μη αρχιμήδεια νόρμα. Τότε ισχύουν:*

(i) Για κάθε $b \in B(a,\, r)$ ισχύει $B(a,\, r) = B(b,\, r)$. Δηλαδή κάθε σημείο μιας ανοικτής μπάλας είναι κέντρο της μπάλας.

(ii) Για κάθε $b \in \overline{B}(a,r)$ ισχύει $\overline{B}(a,r) = \overline{B}(b,r)$. Δηλαδή κάθε σημείο μιας κλειστής μπάλας είναι κέντρο της μπάλας.

(iii) Το σύνολο $B(a,r)$ είναι ανοικτό και κλειστό σύνολο.

(iv) Αν $r \neq 0$, το σύνολο $\overline{B}(a,r)$ είναι ανοικτό και κλειστό σύνολο.

(v) Έστω $a,\, b \in I\!K$ και $r,\, s$ μη μηδενικοί θετικοί αριθμοί. Ισχύει $B(a,\, r) \cap B(b,\, s) \neq 0$ αν και μόνο αν $B(a,\, r) \subset B(b,\, s)$ ή $B(a,\, r) \supset B(b,\, s)$. Δηλαδή κάθε δύο ανοικτές μπάλες είτε θα είναι ξένες μεταξύ τους ή η μία θα περιέχεται στην άλλη.

(vi) *Έστω* $a,\, b \in \mathbb{K}$ *και* $r,\, s$ *μη μηδενικοί θετικοί αριθμοί. Ισχύει* $\overline{B}(a,\, r) \cap \overline{B}(b,\, s) \neq 0$ *αν και μόνο αν* $\overline{B}(a,\, r) \subset \overline{B}(b,\, s)$ *ή* $\overline{B}(a,\, r) \supset \overline{B}(b,\, s)$. *Δηλαδη κάθε δύο κλειστές μπάλες είτε θα είναι ξένες μεταξύ τους ή η μία θα περιέχεται στην άλλη.*

Απόδειξη:

(i) Εξ' ορισμού έχουμε: $b \in B(a,\, r) \Leftrightarrow \|b - a\| < r$. Αν τώρα πάρουμε οποιοδήποτε $x \in B(a,\, r)$, από τη μη αρχιμήδεια ιδιότητα παίρνουμε:

$$\|x - b\| = \|x - a + a - b\| \leq \max\{\|x - a\|\,,\, \|b - a\|\} < r,$$

δηλαδή $x \in B(b, r)$ και άρα $B(a,\, r) \subset B(b, r)$. Για να δείξουμε ότι και $B(a,\, r) \supset B(b, r)$, αρκεί να αλλάξουμε τα a και b στην παραπάνω ανάλυση. Έτσι οι δύο μπάλες είναι ίσες.

(ii) Ακριβώς τα ίδια βήματα με το (i), μόνο που αντί για "$<$" βάζουμε "$\leq$".

(iii) Κάθε ανοικτή μπάλα σε μετρικό χώρο είναι ανοικτό σύνολο. Αυτό που θέλουμε να δείξουμε είναι ότι στη μη αρχιμήδεια περίπτωση είναι επίσης κλειστό. Πράγματι, έστω x οριακό σημείο της $B(a,\, r)$. Δηλαδή ισχύει ότι για κάθε $\epsilon > 0$, $B(x,\, \epsilon) \neq \emptyset$. Ακόμα, έστω $s \leq r$ και έστω η αντίστοιχη μπάλα με κέντρο x και ακτίνα s, $B(x,\, s)$. Αφού το x είναι οριακό σημείο, τότε:

$$B(a,\, r) \cap B(x,\, s) \neq \emptyset \;\Leftrightarrow\; \exists\, y \in B(a,\, r) \cap B(x,\, s)$$

$$\Leftrightarrow \|y - a\| < r \text{ και } \|y - x\| < s \leq r.$$

Εφαρμόζοντας τη μη αρχιμήδεια ιδιότητα παίρνουμε:

$$\|x - a\| \leq \max\{\|x - y\|\,,\, \|y - a\|\} < \max\{s,\, r\} = r,$$

δηλαδή $x \in B(a,\, r)$. Δηλαδή έχουμε ότι κάθε οριακό σημείο της $B(a,\, r)$ ανήκει στην $B(a,\, r)$, και άρα η $B(a,\, r)$ είναι ένα κλειστό σύνολο.

(iv) Η απόδειξη ότι η μπάλα $\overline{B}(a,r)$ είναι κλειστή είναι ακριβώς όπως του (iii). Θα δείξουμε ότι είναι και ανοικτή. Έστω $x \in \overline{B}(a,r)$ και έστω $s = \|x-a\| \leq r$. Θέτουμε $r' = r - s \leq r$. Τότε, $B(x,r') \subset \overline{B}(a,r)$. Πράγματι, έστω $y \in B(x,r')$. Τότε έχουμε:

$$\|y-a\| = \|y-x+x-a\| \leq \max\{\|y-x\|, \|x-a\|\} \leq r,$$

και άρα $y \in \overline{B}(a,r)$.

Προσέχουμε τη λεπτομέρεια $r \neq 0$. Αν $r = 0$ τότε η κλειστή μπάλα με κέντρο x και ακτίνα 0 είναι το μονοσύνολο $\{x\}$, το οποίο είναι κλειστό αλλά όχι ανοικτό, αφού δεν υπάρχει μη κενή ανοικτή μπάλα με κέντρο το x που να περιέχεται γνήσια στο $\{x\}$.

(v) Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $s \leq r$. Αν οι δύο μπάλες δεν είναι ξένες, τότε υπάρχει κάποιο $c \in B(a,\, r) \cap B(b,\, s)$. Τότε, γνωρίζουμε από το (i), ότι $B(a,\, r) = B(c,\, r)$ και $B(b,\, s) = B(c,\, s)$. Δηλαδή:

$$B(b,\, s) = B(c,\, s) \subset B(c,\, r) = B(a,\, r),$$

και το ζητούμενο απεδείχθη.

(vi) Ακριβώς όπως το (iv) με χρήση του (ii). □

Πόρισμα 2 *Η σφαίρα* $S(a,\, r) = \{x \in I\!K : |x-a| = r\}$ *είναι ανοικτό και κλειστό σύνολο.*

Απόδειξη: Ειναι ανοικτό διότι, αν πάρουμε τυχαίο σημείο $x \in S(a,\, r)$ και $0 \geq \epsilon < r$, τότε η $B(x,\, \epsilon) \subset S(a,\, r)$, αφού για κάθε $y \in B(x,\, \epsilon)$ έχουμε από Πρόταση (1):

$$\|y-a\| = \|y-x+x-a\| = \max\{\|y-x\|, \|x-a\|\} = r,$$

αφού $\|y-x\| \neq \|x-a\|$.

Είναι κλειστό, διότι είναι η τομή δύο κλειστών συνόλων, των $\overline{B}(a,\, r)$ και $I\!K \backslash B(a,\, r)$. □

Το γεγονός ότι υπάρχουν τόσα πολλά ανοικτά-κλειστά σύνολα σε έναν ουλτραμετρικό χώρο (κάθε μπάλα που μπορεί να οριστεί είναι ανοικτή-κλειστή) μας λέει πολλά πράγματα για την τοπολογία του. Κλείνοντας αυτή την παράγραφο θα μελετήσουμε τη συνεκτικότητα σε έναν τέτοιο χώρο, χρησιμοποιώντας πολλά από τα αποτελέσματα της προηγούμενης ανάλυσης.

Ορισμός 8 Ένα σύνολο S καλείται *μη συνεκτικό* αν μπορούν να βρεθούν δύο ανοικτά σύνολα $S_1,\ S_2$, τέτοια ώστε:

(i) $S_1 \cap S_2 = \emptyset$,

(ii) $S = (S \cap S_1) \cup (S \cap S_2)$,

(iii) τα $S_1,\ S_2$ είναι μη κενά.

Πρόταση 6 *Σε σώμα $\mathbb{K}$ με μη αρχιμήδεια νόρμα $\|\cdot\|$ κάθε κλειστή μπάλα ακτίνας $r > 0$ είναι μη συνεκτική. Ομοίως και για τις ανοικτές μπάλες.*

Απόδειξη: Για κάθε κλειστή μπάλα $\overline{B}(a,\, r)$ ισχύει ότι μπορεί να γραφεί ως ένωση δύο ανοικτών, μη κενών και ξένων μεταξύ τους συνόλων ως εξής:

$$\overline{B}(a,\, r) = B(a,\, r) \cup \{x \in \mathbb{K} : \|x - a\| = r\}\,.$$

Για κάθε μη κενή ανοικτή μπάλα $B(a,\, r)$ μπορούμε να επιλέξουμε $s < r$ και να σχηματίσουμε τα εξής ανοικτά μη κενά σύνολα:

$$\overline{B}(a,\, s) \text{ και } B(a,\, r) \backslash \overline{B}(a,\, s).$$

Το πρώτο σύνολο είναι ανοικτό επειδή είναι μπάλα. Το δεύτερο ως συμπλήρωμα ενός κλειστού συνόλου σε ανοικτό σύνολο. Μπορούμε να επιλέξουμε το s ώστε και τα δύο σύνολα να είναι μη κενά. Προφανώς τα δύο σύνολα είναι ξένα μεταξύ τους και η ένωσή τους μας δίνει όλη την ανοικτή μπάλα. Συνεπώς κάθε ανοικτή μπάλα είναι μη συνεκτικό σύνολο. □

Ορισμός 9 Έστω $x \in \mathbb{K}$. Ορίζουμε ως *συνεκτική συνιστώσα* του x να είναι η ένωση όλων των συνεκτικών συνόλων που περιέχουν το x. Ισοδύναμα είναι το μεγαλύτερο συνεκτικό σύνολο που περιέχει το x.

Πρόταση 7 *Σε σώμα $\mathbb{K}$ με μη αρχιμήδεια νόρμα $\|\cdot\|$ η συνεκτική συνιστώσα κάθε σημείου $x \in \mathbb{K}$ είναι το μονοσύνολο $\{x\}$. Δηλαδή το $\mathbb{K}$ είναι ολικά μη συνεκτικό τοπολογικό σώμα.*

Απόδειξη: Έστω ότι η συνεκτική συνιστώσα S του x περιέχει κάποιο $y \neq x$ και έστω $r = \|x - y\|$ η απόσταση των δύο στοιχείων. Τότε οι δύο μπάλες $B(x,\, r/2)$και $\overline{B}(y,\, r/2)$ είναι δύο σύνολα που πληρούν τις ιδιότητες του ορισμού της μη συνεκτικότητας.

Έχουμε: $S \supset \{x,\, y\} = (S \cap \overline{B}(y,\, r/2)) \cup (S \cap B(x,\, r/2))$.

Επιπλέον έναι ξένες μεταξύ τους, αφού εάν είχαν κάποιο κοινό στοιχείο, τότε από την Πρόταση 5 η μία θα περιείχετο στην άλλη. Τότε όμως $\|x - y\| \leq r/2$, το οποίο είναι άτοπο, αφού $\|x - y\| = r > r/2$. Τέλος είναι ανοικτά σύνολα, ως μπάλες, και μη κενές, αφού περιέχουν τα στοιχεία x και y αντίστοιχα.

Συνεπώς κάθε σύνολο μεγαλύτερο από το μονοσύνολο παύει να είναι συνεκτικό. □

2.5 Τοπολογία στο $\mathbb{Q}$ με την p-αδική νόρμα

Είδαμε πώς όλα τα τρίγωνα είναι ισοσκελή σε σώμα $\mathbb{K}$ με μία μη αρχιμήδεια νόρμα. Ας δούμε τώρα πώς φαίνεται η ιδιότητα αυτή στο $\mathbb{Q}$ με την p-αδική νόρμα. Θα πάρουμε τρεις ακεραίους $x,\, y,\, z$ και τις μεταξύ τους αποστάσεις:

$$\alpha = x - y, \qquad \beta = y - z \qquad \text{και} \qquad \gamma = x - z.$$

Θα δείξουμε ότι πάντα δύο από αυτές θα είναι ίσες. Προφανώς $\alpha,\ \beta,\ \gamma \in \mathbb{Z}$ και ισχύει $\gamma = \alpha + \beta$. Για τις νόρμες τους έχουμε:

$$|\,\alpha|_p = p^{-v_p(\alpha)} = p^{-n}, \qquad |\,\beta|_p = p^{-v_p(\beta)} = p^{-m} \quad \text{και} \quad |\,\gamma|_p = p^{-v_p(\gamma)} = p^{-k},$$

όπου $v_p(\alpha) = n,\ v_p(\beta) = m,\ v_p(\gamma) = k$. Ισοδύναμα, μπορούμε να γράψουμε τους $\alpha,\ \beta,\ \gamma$ ως:

$$\alpha = p^n\alpha', \qquad \beta = p^m\beta', \qquad \gamma = p^k\gamma', \quad \text{με} \quad p \nmid \alpha'\beta'\gamma'.$$

Έστω $|\,\alpha|_p > |\,\beta|_p$. Τότε $n < m$ και έστω $m = n + \epsilon$. Για το γ έχουμε:

$$\gamma = \alpha + \beta = p^n\alpha' + p^m\beta' = p^n(\alpha' + p^\epsilon\beta').$$

Αφού $p \nmid \alpha'$, τότε $p \nmid (\alpha' + p^\epsilon\beta')$. Άρα $k = \upsilon_p(\gamma) = n$ και

$$|\,\gamma|_p = p^{-n} = |\,\alpha|_p\,,$$

που είναι και το ζητούμενο της πρότασης.

Ας υποθέσουμε τώρα ότι $|\,\alpha|_p = |\,\beta|_p$, δηλαδή $n = m$, οπότε παίρνουμε:

$$\gamma = \alpha + \beta = p^n(\alpha' + \beta'), \quad \text{με} \quad p \nmid \alpha'\beta'.$$

Όμως, μπορεί κάλλιστα να ισχύει ότι $p|(\alpha' + \beta')$. Σε κάθε περίπτωση μπορούμε να πούμε $\upsilon_p(\gamma) \geq \min\{\upsilon_p(\alpha),\ \upsilon_p(\beta)\}$, που μεταφράζεται στο:

$$|\,\gamma|_p = |\alpha + \beta|_p \leq \max\left\{|\,\alpha|_p\,,\ |\,\beta|_p\right\} = |\,\alpha|_p = |\,\beta|_p\,.$$

Έχουμε δηλαδή και πάλι δύο από τις τρεις νόρμες $|\,\alpha|_p\,,\ |\,\beta|_p\,,$ και $|\,\gamma|_p$ να είναι ίσες. Μάλιστα, και στις δύο περιπτώσεις, αυτές που είναι ίσες είναι αυτές που έχουν τη μεγαλύτερη τιμή.

Οι μπάλες στο $\mathbb{Q}$ με την p-αδική νόρμα έχουν μεγάλο ενδιαφέρον. Λόγω της φύσης της p-αδικής νόρμας, η περίπτωση των ανοικτών μπαλών με κέντρο κάποιον ρητό και ακτίνα $r \in \mathbb{R}^+$ ανάγεται στην περίπτωση των κλειστών μπαλών. Το πεδίο τιμών της p-αδικής νόρμας είναι το $\{p^n :\ n \in \mathbb{Z}\}$. Από την άλλη, λόγω της αρχιμήδειας ιδιότητας και της καλής διάταξης του $\mathbb{R}$, για κάθε $r \in \mathbb{R}^+$ υπάρχει $n \in \mathbb{Z}$ ώστε $1/p^n \leq r < 1/p^{n+1}$. *Δηλαδή έχουμε $x \in B(a,\, r)$ τότε και μόνο τότε όταν $x \in \overline{B}(a,\, 1/p^n)$.*

Πρόταση 8 *Κάθε κλειστή μπάλα $\overline{B}(a,\, 1/p^n)$, άρα και κάθε ανοικτή, μπορεί να γραφεί ως ένωση ανοικτών και ξένων μεταξύ τους μπαλών.*

Απόδειξη: Επειδή για κάθε ρητό αριθμό a ισχύει:

$$\overline{B}(a,\, 1/p^n) = a + \overline{B}(0,\, 1/p^n) = a + \left(B(0,\, 1/p^n) \cup \left\{y \in \mathbb{Q}:\ |\,y|_p = 1/p^n\right\}\right),$$

αρκεί να δείξουμε το ζητούμενο για το σύνολο $\left\{y \in \mathbb{Q}:\ |\,y|_p = 1/p^n\right\}$.

Έστω ένας ρητός $x = a/b$. Τότε:

$$\left|\frac{a}{b}\right|_p = \frac{1}{p^n} \Leftrightarrow p^n \mid a, \text{ αν } n > 0, \text{ ή } p^{-n} \mid b, \text{ αν } n < 0.$$

Προφανώς ο $p^{|n|+1}$ δεν διαιρεί ούτε τον a ούτε τον b, μιας και τότε η νόρμα του x θα ήταν διαφορετική του $1/p^n$. Σημειώνουμε ότι οι $a,\ b$ μπορούν να έχουν μόνο μη αρνητική πολλαπλότητα του p στην παραγοντοποίησή τους. Επομένως, ο n είναι θετικός όταν ο p διαρεί τον a ενώ είναι αρνητικός όταν ο p διαιρεί τον b.

Επειδή $p^{|n|+1} \nmid b$ μπορεί να οριστεί μία ένα προς ένα και επί απεικόνιση, τέτοια ώστε για κάθε $i \in \mathbb{F}_{p^{|n|+1}}$ να υπάρχει μοναδικό $j \in \mathbb{F}_{p^{|n|+1}}$ τέτοιο ώστε $ib \equiv j \pmod{p^{|n|+1}}$. Είναι ένα προς ένα διότι αν υποθέσουμε ότι υπάρχει και κάποιο $k \in \mathbb{F}_{p^{|n|+1}}$ τέτοιο ώστε $ib \equiv k \pmod{p^{|n|+1}}$, τότε $k \equiv j \pmod{p^{|n|+1}}$, και άρα $j = k$. Ειναι επί, διότι τα σύνολα $\left\{ib :\ i \in \mathbb{F}_{p^{|n|+1}}\right\}$ και $\mathbb{F}_{p^{|n|+1}}$ έχουν πεπερασμένο πλήθος στοιχείων. Ακόμα, $p^{|n|+1} \nmid a$, δηλαδή $a \equiv j \pmod{p^{|n|+1}}$ για κάποιο $j \in \mathbb{F}_{p^{|n|+1}}$.

Συνοψίζοντας έχουμε ότι για τον ρητό $x = a/b$ υπάρχουν μοναδικά $i,\ j \in \mathbb{F}_{p^{|n|+1}}$ ώστε όταν $a \equiv j \pmod{p^{|n|+1}}$ να υπάρχει i με $ib \equiv j \pmod{p^{|n|+1}}$.

Με τη βοήθεια των παραπάνω θα δείξουμε ότι κάθε ρητός $x = a/b \in \left\{y \in \mathbb{Q} :\ |y|_p = 1/p^n\right\}$ ανήκει σε μοναδική ανοικτή μπάλα, συγκεκριμένα την $B(i,\, 1/p^n)$, με $i \in \mathbb{F}_{p^{|n|+1}}$. Πράγματι, επιλέγουμε τα μοναδικά εκείνα $i,\ j$ ώστε $a \equiv j \pmod{p^{|n|+1}}$ και $ib \equiv j \pmod{p^{|n|+1}}$. Τότε έχουμε:

$$\left|\frac{a}{b} - i\right|_p = \left|\frac{a - ib}{b}\right|_p = \frac{|a - ib|_p}{|b|_p}.$$

Αλλά

$$|b|_p = \begin{cases} 1, & \text{αν } p^{-n} \nmid b \Leftrightarrow n > 0 \\ \frac{1}{p^{|n|}}, & \text{αν } p^{-n} \mid b \Leftrightarrow n < 0 \end{cases}$$

και

$$|a - ib|_p = \frac{1}{p^k} \quad \text{με} \quad k > |n|\,.$$

Συνεπώς, ανάλογα με τη νόρμα του b, δηλαδή ανάλογα με το αν n θετικός ή αρνητικός, έχουμε:

$$\left|\frac{a}{b} - i\right|_p = \frac{1}{p^k} < \frac{1}{p^n}, \quad \text{όταν } |b|_p = 1 \Leftrightarrow n > 0$$

και

$$\left|\frac{a}{b}-i\right|_p=\frac{1/p^k}{1/p^{-n}}=\frac{p^{-n}}{p^k}=\frac{1}{p^{n+k}}<\frac{1}{p^n},\quad \text{όταν } |b|_p=\tfrac{1}{p^{-n}}\Leftrightarrow n<0\ .$$

Ουσιαστικά έχουμε δείξει ότι:

$$\left\{y\in\mathbb{Q}\colon\ |\,y|_p=1/p^n\right\}=B(1,\,1/p^n)\cup B(2,\,1/p^n)\cup\ldots\cup B(p^{n+1}-1,\,1/p^n).$$

Άρα

$$\overline{B}(a,\,1/p^n)=B(0+a,\,1/p^n)\cup\ldots\cup B(p^{n+1}-1+a,\,1/p^n).$$

□

Παρατήρηση 5 Αξίζει να δούμε την πρόταση αυτή ως έναν άλλον τρόπο να αποδείξουμε ότι η κλειστή μπάλα $\overline{B}(a,\,1/p^n)$ είναι και ανοικτό σύνολο, αφού είναι πεπερασμένη ένωση ανοικτών συνόλων.

Παρατήρηση 6 Από την παραπάνω πρόταση φαίνεται και η μη συνεκτικότητα κάθε μπάλας. Τα ανοικτά, μη κενά και ξένα μεταξύ τους σύνολα που θέλουμε να βρούμε για την επαλήθευση του ορισμού της μη συνεκτικότητας προσδιορίζονται εύκολα. Απλά παίρνουμε δύο ξένα μεταξύ τους υποσύνολα I_1 και I_2 ώστε $I_1\cup I_2=\{0,\,1,\ldots,\,p^{n+1}-1\}$ και τέτοια ώστε για τουλάχιστον ένα $i\in I_1$ και τουλάχιστον ενα $j\in I_2$ οι μπάλες $B(i,\,1/p^n)$ και $B(j,\ 1/p^n)$ είναι μη κενές. Τα $S_1,\ S_2$ του ορισμού είναι τότε τα $S_1=\cup_{i\in I_1}B(i,\,1/p^n)$ και $S_2=\cup_{j\in I_1}B(j,\,1/p^n)$.

Ας δούμε κάποια παραδείγματα των παραπάνω, που θα βοηθήσουν τη διαίσθησή μας για το πώς δρα η p-αδική νόρμα στο σώμα των ρητών.
1) Θα περιγράψουμε με την p-αδική νόρμα την κλειστή μπάλα στο $\mathbb{Q}$ με κέντρο το $x=0$ και ακτίνα 1:

$$\begin{aligned}\overline{B}(0,\,1)\ &=\left\{x\in\mathbb{Q}\colon|\,x|_p\le 1\right\}=\left\{a/b\in\mathbb{Q}\colon a,\,b\in\mathbb{Z},\ |a/b|_p\le 1\right\}\\&=\{a/b\in\mathbb{Q}\colon a,\,b\in\mathbb{Z},\ \upsilon_p(a/b)\ge 0\}\\&=\{a/b\in\mathbb{Q}\colon a,\,b\in\mathbb{Z},\ p\nmid b\}\,.\end{aligned}$$

Άρα η κλειστή μπάλα με κέντρο το 0 και ακτίνα 1 είναι όλοι εκείνοι οι ρητοί με τον παρονομαστή τους να μη διαιρείται από τον p.

2) Θα περιγράψουμε επίσης την ανοικτή μπάλα με κέντρο το $x = 3$ και ακτίνα 1 :

$$\begin{aligned} B(3,\,1) &= \left\{x \in \mathbb{Q} \colon |x-3|_p < 1\right\} = \left\{a/b \in \mathbb{Q} \colon a,\, b \in \mathbb{Z},\ |a/b-3|_p < 1\right\} \\ &= \left\{a/b \in \mathbb{Q} \colon a,\, b \in \mathbb{Z},\ |(a-3)/b|_p < 1\right\} \\ &= \{a/b \in \mathbb{Q} \colon a,\, b \in \mathbb{Z},\ v_p((a-3)/b) \geq 1\} \\ &= \{a/b \in \mathbb{Q} \colon a,\, b \in \mathbb{Z},\ p \nmid b \text{ και } p \mid (a-3)\}\,. \end{aligned}$$

Παρατηρούμε ότι σε αυτή τη μπάλα ανήκουν και όλοι εκείνοι οι ακέραιοι $a \in \mathbb{Z}$ τέτοιοι ώστε $a \equiv 3 \pmod{p}$. Γενικότερα η μπάλα $B(i,\,1)$ περιέχει όλους εκείνους τους ρητούς a/b, με $p \nmid b$ και $a \equiv i \pmod{p}$.

3) Με αυτό το παράδειγμα θα δούμε μια απλή περίπτωση της Πρότασης 8. Η κλειστή μπάλα $\overline{B}(0,\,1)$ μπορεί να γραφεί ως ένωση ξένων μεταξύ τους ανοικτών μπαλών:

$$\overline{B}(0,\,1) = B(0,\,1) \cup B(1,\,1) \cup B(2,\,1) \cup \ldots \cup B(p-1,\,1).$$

Ελέγχουμε πρώτα ότι οι ανοικτές μπάλες είναι πράγματι ξένες μεταξύ τους. Πράγματι έστω ότι κάποιες από αυτές δεν είναι ξένες μεταξύ τους, δηλαδή ότι για κάποια $i \neq j$ έχουμε $B(i,\,1) \cap B(j,\,1) \neq \emptyset$. Τότε ισοδύναμα:

$$\text{υπάρχει ρητός } \ y = \frac{a}{b} \in B(i,\,1) \cap B(j,\,1)$$

$$\Leftrightarrow p \nmid b \text{ και } p \mid (a-i) \text{ και } p \mid (a-j).$$

Όμως, τα παραπάνω μας λένε ότι ο a πρέπει να είναι ισοϋπόλοιπος με δύο διαφορετικούς ακεραίους, οι οποίοι ανήκουν σε διαφορετικές κλάσεις modulo p, άτοπο.

Θα δείξουμε τώρα και την ισότητα, ισοδύναμα ότι:

$$\overline{B}(0,\,1) \supset B(0,\,1) \cup B(1,\,1) \cup B(2,\,1) \cup \ldots \cup B(p-1,\,1),$$

και

$$\overline{B}(0,\,1) \subset B(0,\,1) \cup B(1,\,1) \cup B(2,\,1) \cup \ldots \cup B(p-1,\,1).$$

Για την πρώτη σχέση, έστω $x = a/b \in B(i,\,1)$ για κάποιο $i \in \{0,\,1 \ldots p-1\}$. Θα δείξουμε ότι τότε και $x \in \overline{B}(0,1)$. Κατ' αρχήν ισχύει:

$$x \in B(i,\,1) \Leftrightarrow |x-i|_p < 1,$$

Ακόμα παρατηρούμε ότι, για κάθε $i \in \{0,\,1\,\ldots p-1\}$ ισχύει $|i|_p = 1$, αν $i \neq 0$ και $|i|_p = 0$, αν $i = 0$.
Οπότε για τη νόρμα του x έχουμε:

$$|\,x|_p = |x-i+i|_p \leq \max\left\{|x-i|_p\,,\,|i|_p\right\} \leq 1$$

$$\Rightarrow x \in \overline{B}(0,\,1).$$

Θα αποδείξουμε τώρα και τη δεύτερη σχέση, ότι δηλαδή αν $x =\in \overline{B}(0,\,1)$ τότε υπάρχει κάποιο $i \in \{0,\,1\,\ldots p-1\}$ ώστε $x \in B(i,\,1)$. Ουσιαστικά μας ενδιαφέρει η περίπτωση $x \in \overline{B}(0,\,1)$ και $|\,x|_p = 1$, εφ' όσον, αν είναι μικρότερη, τότε το x θα ανήκει στην ανοικτή μπάλα $B(0,\,1)$.

Έστω λοιπόν $x = a/b$ τέτοιο ώστε $|\,x|_p = 1$. Τότε έχουμε:

$$|\,x|_p = 1 \Leftrightarrow \left|\frac{a}{b}\right|_p = 1 \Leftrightarrow \upsilon_p(a/b) = 0 \Leftrightarrow p \nmid a \text{ και } p \nmid b.$$

Αφού $p \nmid a$, τότε $a \equiv i \pmod{p}$ για κάποιο $i \in \{1,\,2,\,3\ldots,\,p-1\}$. Ακόμα $p \nmid b$, συνεπώς, σύμφωνα με το προηγούμενο παράδειγμα, $x = a/b \in B(i,\,1)$ και το ζητούμενο απεδείχθη.

2.6 Άλγεβρα σε σώμα με μη αρχιμήδεια νόρμα

Στην τελευταία ενότητα αυτού του κεφαλαίου θα ρίξουμε μια αλγεβρική ματιά στα μη αρχιμήδεια τοπολογικά σώματα. Μάλιστα θα δούμε ότι η αλγεβρική δομή του τοπολογικού σώματος συνδέεται άμεσα με τη νόρμα που έχουμε ορίσει πάνω στο σώμα μας. Τοπολογικές και αλγεβρικές ιδιότητες συμπληρώνουν η μία την άλλη, και μας δίνουν μια ολοκληρωμένη εικόνα για τους ουλτραμετρικούς χώρους.

Κάθε μη αρχιμήδεια νόρμα μπορεί να ορίσει έναν υποδακτύλιο πάνω στο σώμα που μας ενδιαφέρει, ο οποίος έχει πολύ ενδιαφέρουσες ιδιότητες.

Πρόταση 9 *Έστω $\mathbb{K}$ σώμα και $\|\cdot\|$ μια μη αρχιμήδεια νόρμα. Το σύνολο:*

$$\mathcal{O} = \overline{B}(0,\,1) = \{x \in \mathbb{K} :\ \|x\| \leq 1\}$$

είναι υποδακτύλιος του $\mathbb{K}$. Το υποσύνολό του:

$$\mathcal{B} = B(0,\,1) = \{x \in \mathbb{K} :\ \|x\| < 1\}$$

είναι ιδεώδες του $\mathcal{O}$. Επιπλέον, το $\mathcal{B}$ είναι μέγιστο ιδεώδες του $\mathcal{O}$ και κάθε στοιχείο του $\mathcal{O}\setminus\mathcal{B}$ είναι αντιστρέψιμο στο $\mathcal{O}$.

Απόδειξη: Δεδομένου ότι το $\mathbb{K}$ είναι σώμα, εξασφαλίζουμε την αντιμεταθετικότητα της πρόσθεσης, την προσεταιριστικότητα του πολλαπλασιασμού και τους επιμεριστικούς νόμους στο υποσύνολό του $\mathcal{O}$. Ακόμα, το προσθετικό ουδέτερο του $\mathbb{K}$ θα είναι και το προσθετικό ουδέτερο για τον $\mathcal{O}$, ο οποίος επιπλέον θα είναι δακτύλιος με μοναδιαίο στοιχείο τη μονάδα του σώματος, αφού $\|1\| = 1$.

Μένει μόνο να δείξουμε την κλειστότητα της πρόσθεσης και του πολλαπλασιασμού. Έστω $x,\ y \in \mathcal{O}$. Τότε:

$$\|x+y\| \leq \max\{\|x\|,\,\|y\|\} \leq 1,\ \text{άρα}\ \ (x+y) \in \mathcal{O},$$

$$\|xy\| = \|x\|\,\|y\| \leq 1,\ \text{άρα}\ \ (xy) \in \mathcal{O}.$$

Δείξαμε ότι ο $\mathcal{O}$ είναι πράγματι υποδακτύλιος.

Ότι το $\mathcal{B}$ είναι ιδεώδες του $\mathcal{O}$ προκύπτει εύκολα: για κάθε $x \in \mathcal{O},\ y \in \mathcal{B}$ ισχύει:

$$\|xy\| = \|x\|\,\|y\| < 1 \Rightarrow (xy) \in \mathcal{B}.$$

Για το τελευταίο παρατηρούμε ότι αν δείξουμε ότι κάθε στοιχείο του $\mathcal{O}\setminus\mathcal{B}$ είναι αντιστρέψιμο στο $\mathcal{O}$, τότε αμέσως προκύπτει ότι το $\mathcal{B}$ είναι μέγιστο. Δεν θα μπορούσε να περιέχει κανένα άλλο στοιχείο του δακτυλίου και να μην ταυτιστεί με αυτόν. Επειδή το $\mathbb{K}$ είναι σώμα, κάθε στοιχείο έχει αντίστροφο στο $\mathbb{K}$. Έστω $x \in \mathcal{O}$. Έστω $x \in \mathcal{O}\setminus\mathcal{B}$. Τότε $\|x\| = 1$ και για τον αντίστροφό του, x^{-1}, έχουμε:

$$1 = \|1\| = \left\|xx^{-1}\right\| = \|x\| \left\|x^{-1}\right\|$$

$$\Rightarrow \left\|x^{-1}\right\| = 1/\|x\| = 1.$$

$$\Rightarrow x^{-1} \in \mathcal{O}\backslash\mathcal{B}.$$

Γενικά για κάθε $x \in \mathcal{O}$ θα είναι $x^{-1} \in \mathcal{O}$ αν και μόνο αν $\|x\| = 1$. Δηλαδή τα αντιστρέψιμα στοιχεία του $\mathcal{O}$ είναι ακριβώς εκείνα με νόρμα ίση με ένα.

□

Παρατήρηση 7 Το ιδεώδες $\mathcal{B}$ είναι το μοναδικό μέγιστο ιδεώδες που μπορεί να οριστεί στο δακτύλιο $\mathcal{O}$, αφού περιέχει όλα τα δυνατά στοιχεία που θα μπορούσε να περιέχει ένα ιδεώδες. Κάθε άλλο ιδεώδες διαφορετικό του $\mathcal{B}$ ή θα είχε λιγότερα στοιχεία ή δεν θα ήταν γνήσιο ιδεώδες του $\mathcal{O}$.

Παρατήρηση 8 Έχουμε ένα δακτύλιο και ένα ιδεώδες του. Μπορούμε λοιπόν να ορίσουμε το δακτύλιο πηλίκο του $\mathcal{O}$ ως προς το $\mathcal{B}$, το οποίο μάλιστα θα είναι σώμα, αφού το $\mathcal{B}$ είναι μέγιστο ιδεώδες.

Ορισμός 10 Καλούμε *τοπικό δακτύλιο* κάθε δακτύλιο που περιέχει μοναδικό μέγιστο ιδεώδες του οποίου το συμπλήρωμα αποτελείται από αντιστρέψιμα στοιχεία.

Ορισμός 11 Έστω σώμα $\mathbb{K}$ με μία μη αρχιμήδεια νόρμα $\|\cdot\|$.
Ονομάζουμε *δακτύλιο εκτίμησης* της $\|\cdot\|$ στο $\mathbb{K}$ τον υποδακτύλιο:

$$\mathcal{O} = \overline{B}(0,\,1) = \{x \in \mathbb{K} :\ \|x\| \leq 1\},$$

που ορίσαμε παραπάνω.
Ονομάζουμε *ιδεώδες εκτίμησης* της $\|\cdot\|$ στο $\mathbb{K}$ το ιδεώδες:

$$\mathcal{B} = B(0,\,1) = \{x \in \mathbb{K} :\ \|x\| < 1\},$$

που ορίσαμε παραπάνω.
Τέλος, ονομάζουμε *σώμα πηλίκο* της $\|\cdot\|$ στο $\mathbb{K}$ τον δακτύλιο-πηλίκο $k = \mathcal{O}/\mathcal{B}$.

2.7 Άλγεβρα στο $\mathbb{Q}$ με την p-αδική νόρμα

Πρόταση 10 *Στο σώμα $\mathbb{Q}$ των ρητών αριθμών με την p-αδική νόρμα ο δακτύλιος εκτίμησης είναι το σύνολο:*

$$\mathcal{O} = \mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : \ p \nmid b\}.$$

Το ιδεώδες εκτίμησης είναι το σύνολο:

$$\mathcal{B} = p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : \ p \nmid b \text{ και } p \mid a.\}$$

Τέλος το σώμα πηλίκο είναι το $k = \mathbb{F}_p$.

Απόδειξη: Τα πρώτα αποδεικνύονται εύκολα, τα έχουμε αναλύσει εξ' άλλου και στην προηγούμενη ενότητα με τις μπάλες. Θα σταθούμε στο τελευταίο ζήτημα, θα δείξουμε δηλαδή ότι $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Θα βρούμε έναν ισομορφισμό μεταξύ των δύο σωμάτων, και επειδή το $\mathbb{F}_p$ είναι πεπερασμένο οι δομές θα ταυτίζονται. Ορίζουμε την ακόλουθη απεικόνιση: $h : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$:

$$h(n) + p\mathbb{Z} = n + p\mathbb{Z}_{(p)},$$

πάει δηλαδή κάθε ακέραιο n στο σύμπλοκό του στον δακτύλιο πηλίκο k.

Η απεικόνιση αυτή είναι ένας ομομορφισμός:

$$h(x+y) = (x+y) + p\mathbb{Z}_{(p)} = x + p\mathbb{Z}_{(p)} + y + p\mathbb{Z}_{(p)} = h(x) + h(y),$$

$$h(xy) = (xy) + p\mathbb{Z}_{(p)} = (x + p\mathbb{Z}_{(p)})(y + p\mathbb{Z}_{(p)}) = h(x) \cdot h(y),$$

από τις πράξεις μεταξύ συμπλόκων ενός δακτυλίου πηλίκου.

Επίσης, η h είναι ένα προς ένα:

$$ker(h) = \left\{n \in \mathbb{Z}/p\mathbb{Z} : \ h(n) = p\mathbb{Z}_{(p)}\right\} = \left\{n \in \mathbb{Z}/p\mathbb{Z} : \ n \in p\mathbb{Z}_{(p)}\right\} = p\mathbb{Z}.$$

Τέλος είναι επί: για κάθε $x + p\mathbb{Z}_{(p)}$, $x = a/b \in \mathbb{Z}_{(p)}$, μπορώ να βρω $n \in \mathbb{Z}/p\mathbb{Z}$ ώστε $h(n) = x + p\mathbb{Z}_{(p)}$:

$$h(n) = x + p\mathbb{Z}_{(p)} \Leftrightarrow n + p\mathbb{Z}_{(p)} = x + p\mathbb{Z}_{(p)}$$

$$\Leftrightarrow (x-n) \in p\mathbb{Z}_{(p)} \Leftrightarrow (x-n) = \frac{c}{d} \text{ με } p \nmid d \text{ και } p \mid c$$

$$\Leftrightarrow \frac{a-bn}{b} = \frac{c}{d} \text{ με } p \nmid d \text{ και } p \mid c \Leftrightarrow p \mid (a-bn)$$
$$\Leftrightarrow bn \equiv a \pmod{p} \Leftrightarrow n \equiv b^{-1}a \pmod{p},$$

αφού στο $\mathbb{F}_p$ όλα τα στοιχεία είναι αντιστρέψιμα και άρα ορίζεται ο αντίστροφος του b. Συνεπώς το n που θα επαληθεύει την παραπάνω σχέση θα έχει εικόνα του το σύμπλοκο $x + p\mathbb{Z}_{(p)}$. □

Παρατήρηση 9 Η ανοικτή μπάλα $B(a, 1)$ στο $\mathbb{Q}$ μπορεί να περιγραφεί τώρα και με αλγεβρικούς όρους. Βλέπουμε ότι είναι το σύμπλοκο του ιδεώδους εκτίμησης $a + p\mathbb{Z}_{(p)} = a + B(0, 1)$.

Πρόταση 11 *Στο $\mathbb{Q}$ με την p-αδική νόρμα, το ιδεώδες εκτίμησης είναι κύριο ιδεώδες, αποτελείται δηλαδή από όλα τα πολλαπλάσια κάποιου πρωταρχικού στοιχείου.*

Απόδειξη: Στο ιδεώδες εκτίμησης ανήκουν όλοι οι ρητοί a/b τέτοιοι ώστε $p \nmid b$ και $p \mid a$. Δηλαδή μπορούμε να γράψουμε τον a/b ως:

$$\frac{a}{b} = p^n \frac{a'}{b'}, \quad \text{με} \quad p \nmid a'b', \ n > 0.$$

$$\Leftrightarrow \frac{a}{b} = p^n x, \ |x|_p \leq 1, \ \text{ή } x \in \mathbb{Z}_{(p)}.$$

Το n δεν είναι απαραίτητο να είναι και η εκτίμηση του a, μπορεί να είναι κάποιος μικρότερος φυσικός αριθμός, γι' αυτό και η νόρμα του x είναι μικρότερη ή ίση του ένα.

Έχουμε έτσι ότι κάθε ρητός στο ιδεώδες εκτίμησης γράφεται ως κάποιο πολλαπλάσιο του πρώτου p επί κάποιο στοιχείο του δαχτυλίου, δηλαδή ότι είναι ένα πρωταρχικό ιδεώδες που παράγεται από τον πρώτο p. □

Κεφάλαιο 3

Το σώμα των p-αδικών αριθμών

Σε αυτό το κεφάλαιο θα αναπτύξουμε φορμαλιστικά όσα αναφέραμε στο εισαγωγικό κεφάλαιο. Θα κατασκευάσουμε τα σώματα των p-αδικών αριθμών τα οποία θα συμβολίζουμε με $\mathbb{Q}_p$. Αρχικά θα εφαρμόσουμε τη θεωρία που αναπτύξαμε στο δεύτερο κεφάλαιο, πάνω στο σώμα $\mathbb{Q}$ με την p-αδική νόρμα, και θα κατασκευάσουμε τα $\mathbb{Q}_p$ χρησιμοποιώντας Ανάλυση. Κατόπιν θα ακολουθήσουμε διαφορετική προσέγγιση και θα κατασκευάσουμε τα σώματα $\mathbb{Q}_p$ αλγεβρικά. Τέλος θα δούμε τις κυριότερες από τις ιδιότητες των νέων αυτών σωμάτων. Σημειώνουμε ότι οι μέθοδοι κατασκευής των σωμάτων αυτών δεν είναι τόσο σημαντικές όσο οι ιδιότητες που προκύπτουν σε αυτά. Είναι όμως μη παραλείψιμη, καθώς κατοχυρώνει την ύπαρξή τους.

3.1 Η αναλυτική κατασκευή του $\mathbb{Q}_p$

Ορισμός 12 Έστω σώμα $\mathbb{K}$ και έστω νόρμα $\|\cdot\|$ πάνω στο $\mathbb{K}$.

(i) Μία ακολουθία $(x_n)_n$ με $x_n \in \mathbb{K}$ λέγεται *Cauchy* αν και μόνο αν για κάθε $\epsilon > 0$ υπάρχει n_0 τέτοιο ώστε $\|x_n - x_m\| < \epsilon$ για όλα τα $n,\ m > n_0$.

(ii) Το σώμα $\mathbb{K}$ λέγεται πλήρες ως προς τη νόρμα $\|\cdot\|$ αν και μόνο αν κάθε ακολουθία Cauchy στοιχείων του $\mathbb{K}$ έχει όριο στο $\mathbb{K}$.

(iii) Ένα υποσύνολο S του $\mathbb{K}$ λέγεται πυκνό στο $\mathbb{K}$ αν και μόνο αν κάθε ανοικτή μπάλα με κέντρο κάποιο στοιχείο του $\mathbb{K}$ περιέχει κάποιο στοιχείο του S. Δηλαδή όταν για κάθε $x \in \mathbb{K}$ και κάθε ϵ ισχύει:

$$B(x, \epsilon) \cap S \neq \emptyset.$$

Οι ακολουθίες Cauchy χαρακτηρίζονται πολύ εύκολα σε ένα χώρο με μη αρχιμήδεια νόρμα. Συγκεκριμένα ισχύει το ακόλουθο:

Λήμμα 2 *Μία ακολουθία (x_n) στοιχείων ενός σώματος $\mathbb{K}$ είναι Cauchy ως προς τη μη αρχιμήδεια νόρμα $\|\cdot\|$ αν και μόνο αν:*

$$\lim_{n\to\infty} \|x_{n+1} - x_n\| = 0.$$

Απόδειξη: Έστω $m = n + r > n$. Τότε:

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

Το λήμμα προκύπτει αμέσα. □

Παρατήρηση 10 Σημειώνουμε ότι σε αρχιμήδειες νόρμες η παραπάνω συνθήκη είναι ασθενέστερη της συνθήκης Cauchy. Για παράδειγμα ας πάρουμε ως σώμα το $\mathbb{R}$ με τη συνήθη νόρμα. Τότε η ακολουθία $x_n = \sum_{k=1}^{n} 1/k$ επαληθεύει την $\lim_{n\to\infty} |x_{n+1} - x_n| = \lim_{n\to\infty} 1/(n+1) = 0$, αλλά δεν είναι συγκλίνουσα, και συνεπώς ούτε Cauchy, αφού το $\mathbb{R}$ είναι πλήρες.

Στο Κεφάλαιο 2 αναφέραμε ότι οι μοναδικές, ως προς ισοδυναμία, μη τετριμμένες νόρμες που ορίζονται στο $\mathbb{Q}$ είναι οι διαφορετικές p-αδικές και η συνήθης νόρμα. Η τελευταία είναι και η μόνη αρχιμήδεια νόρμα. Γνωρίζουμε ότι μπορούμε να επεκτείνουμε το $\mathbb{Q}$ με τη συνήθη νόρμα, ώστε να περιλάβουμε τα όρια των ακολουθιών Cauchy . Ως αποτέλεσμα θα πάρουμε το σώμα των πραγματικών αριθμών $\mathbb{R}$ με τη συνήθη νόρμα, όπως αυτή επεκτείνεται στο $\mathbb{R}$, και με το $\mathbb{Q}$ να είναι πυκνό στο $\mathbb{R}$ ως προς την επέκταση της νόρμας. Επιπλέον το σώμα $\mathbb{R}$ θα είναι ένα πλήρες σώμα. Δηλαδή το σώμα των πραγματικών

αριθμών $\mathbb{R}$ είναι η *πλήρωση* του σώματος $\mathbb{Q}$ των ρητών αριθμών ως προς τη συνήθη νόρμα.

Σημειώνουμε ότι το $\mathbb{R}$ είναι το ελάχιστο σώμα με την παραπάνω ιδιότητα. Κάθε πλήρωση του $\mathbb{Q}$ διαφορετική του $\mathbb{R}$ θα περιείχε το όριο κάθε ακολουθίας Cauchy στοιχείων του $\mathbb{Q}$, και εφόσον το $\mathbb{Q}$ είναι πυκνό στο $\mathbb{R}$, κάθε στοιχείο του $\mathbb{R}$ είναι όριο μιας τέτοιας ακολουθίας.

Παρόμοια, για κάθε μία από τις p-αδικές νόρμες, μπορούμε να κατασκευάσουμε μιά πλήρωση ανάλογη του $\mathbb{R}$. Παρακάτω θα δείξουμε ότι για κάθε πρώτο p υπάρχει κάποιο σώμα στο οποίο μπορούμε να επεκτείνουμε την p-αδική νόρμα, το οποίο θα είναι πλήρες ως προς την επέκταση αυτή, και στο οποίο το $\mathbb{Q}$ είναι πυκνό. Πρώτα όμως ας δείξουμε ότι το $\mathbb{Q}$ από μόνο του δεν είναι πλήρες ως προς καμιά από τις p-αδικές νόρμες.

Λήμμα 3 *Το σώμα $\mathbb{Q}$ των ρητών αριθμών δεν είναι πλήρες για καμμία από τις μη τετριμμένες νόρμες που μπορούν να οριστούν σε αυτό.*

Απόδειξη: Από το Θεώρημα Ostrowski (Θεώρημα 5) και από τα παραπάνω για να αποδείξουμε το θεώρημα αρκεί να το αποδείξουμε για κάποια τυχαία p-αδική νόρμα.

Έστω πρώτος $p \neq 2$ και $|\cdot|_p$ η αντίστοιχη p-αδκική νόρμα. Θα κατασκευάσουμε μια ακολουθία Cauchy στο $\mathbb{Q}$ η οποία δεν έχει όριο στο $\mathbb{Q}$.

Μπορούμε να διαλέξουμε έναν ακέραιο $a \in \mathbb{Z}$ τέτοιο ώστε:

- ο p δε διαιρεί τον a,
- ο a δεν είναι τετράγωνο στο $\mathbb{Q}$,
- ο a είναι τετραγωνικό υπόλοιπο modulo p, δηλαδή η εξίσωση $x^2 \equiv a \pmod{p}$ να έχει λύση στο $\mathbb{Q}$.

Ένα παράδειγμα που είδαμε στην αρχή ήταν η εξίσωση $x^2 \equiv 2 \pmod{7}$.

Θα κατασκευάσουμε τώρα την ακολουθία Cauchy:

Επιλέγουμε μία λύση x_0 της εξίσωσης $x^2 \equiv a \pmod{p}$.

Κατόπιν μπορούμε να επιλέξουμε x_1 τέτοιο ώστε $x_1 \equiv x_0 \pmod{p}$ και $x_1^2 \equiv a \pmod{p^2}$.

Στο πρώτο κεφάλαιο είχαμε αναφέρει ότι οι εξισώσεις $x^2 \equiv a \pmod{p^n}$ όταν $p \neq 2$ και $p \nmid a$ έχουν είτε δύο είτε καμμία λύσεις. Επιπλέον όσες λύσεις υπάρχουν modulo p τόσες θα υπάρχουν και modulo p^n. Συνεπώς, αφού υπάρχει το x_0, υπάρχει και x_1 τέτοιο ώστε $x_1^2 \equiv a \pmod{p^2}$. Από τη συνθήκη αυτή προκύπτει ότι:

$$x_1^2 \equiv a \pmod{p} \Leftrightarrow x_1^2 \equiv x_0^2 \pmod{p} \Leftrightarrow x_1^2 - x_0^2 \equiv 0 \pmod{p}$$

$$\Leftrightarrow (x_1 - x_0)(x_1 + x_0) \equiv 0 \pmod{p} \Leftrightarrow p|(x_1 - x_0) \text{ ή } p|(x_1 + x_0)$$

$$\Leftrightarrow x_1 \equiv x_0 \pmod{p} \text{ ή } x_1 \equiv (-x_0) \pmod{p}.$$

Εμείς επιλέγουμε εκείνο το x_1 με $x_1 \equiv x_0 \pmod{p}$.

Γενικότερα μπορούμε να επιλέξουμε x_n τέτοια ώστε $x_n \equiv x_{n-1} \pmod{p^n}$ και $x_n^2 \equiv a \pmod{p^{n+1}}$. Έτσι σχηματίζουμε μία ακολουθία στοιχείων (x_n) με $x_n \in \mathbb{Q}$.

Τώρα, η ακολουθία μας είναι ακολουθία Cauchy, γεγονός που είναι άμεσο από την κατασκευή της. Πράγματι:

$$|x_{n+1} - x_n|_p = \left|\kappa p^{n+1}\right|_p \leq p^{-(n+1)} \longrightarrow 0,$$

και άρα, από Λήμμα 2, η ακολουθία (x_n) είναι Cauchy.
Όμως, πάλι από κατασκευή, η ακολουθία δεν έχει όριο στο $\mathbb{Q}$, αφού:

$$\left|x_n^2 - a\right| = \left|\mu p^{n+1}\right| \leq p^{-n+1} \longrightarrow 0,$$

δηλαδή το όριό της είναι η τετραγωνική ρίζα του a, η οποία όμως δεν ανήκει στο $\mathbb{Q}$.

Άρα το $\mathbb{Q}$ δεν είναι πλήρες ως προς τις p-αδικές νόρμες για $p \neq 2$.

Όσο για την περίπτωση $p = 2$ μπορεί να θεωρήσει κανείς την ακολουθία που προκύπτει από την επίλυση της $x_n^3 \equiv 3 \pmod{2^{n+1}}$. □

Αφού λοιπόν το $\mathbb{Q}$ δεν είναι πλήρες ως προς την p-αδική νόρμα, μπορούμε να κατασκευάσουμε την πλήρωσή του. Θέλουμε να προσθέσουμε τα όρια των ακολουθιών Cauchy, τα οποία όμως δεν ακήκουν στο $\mathbb{Q}$. Θα αντικαταστήσουμε τα όρια, που δεν έχουμε, με τις ακολουθίες που τείνουν σε αυτά, τις οποίες έχουμε. Θεωρούμε ως ισοδύναμες αυτές που έχουν το ίδιο όριο, κατασκευάζοντας έτσι κλάσεις ισοδυναμίας.

Ορισμός 13 Συμβολίζουμε με $\mathcal{C}$ το σύνολο όλων των ακολουθιών Cauchy στο $\mathcal{Q}$ ως προς την p-αδική νόρμα, δηλαδή:

$$\mathcal{C} = \left\{ (x_n) : \ (x_n) \text{ είναι ακολουθία Cauchy ως προς την } |\cdot|_p \right\}.$$

Πρόταση 12 *Ορίζοντας τις ακόλουθες πράξεις πάνω στο $\mathcal{C}$:*

$$(x_n) + (y_n) = (x_n + y_n)$$

$$(x_n) \cdot (y_n) = (x_n y_n)$$

τότε το $\mathcal{C}$ είναι αντιμεταθετικός δακτύλιος με μονάδα.

Απόδειξη: Η πρόταση αποδεικνύεται εύκολα. Θα σταθούμε σε κάποια ενδεικτικά σημεία, στην κλειστότητα των πράξεων, στο προσθετικό και πολλαπλασιαστικό ουδέτερο.
Για τις ακολουθίες (x_n), (y_n) έχουμε:

$$(x_n) \in \mathcal{C} \Leftrightarrow \forall \epsilon \ \exists n_0 \ : \ \forall \ n, m > n_0 \quad |x_n - x_m|_p < \epsilon$$

$$(y_n) \in \mathcal{C} \Leftrightarrow \forall \epsilon \ \exists m_0 \ : \ \forall \ n, m > m_0 \quad |y_n - y_m|_p < \epsilon.$$

Θέτοντας $N = \max\{n_0, m_0\}$ ισχύει:

$$\forall \ n, m > N \text{ τοτε } \ |x_n - x_m|_p < \epsilon \text{ και } \quad |y_n - y_m|_p < \epsilon.$$

Τότε η $(x_n + y_n)$ είναι Cauchy, αφού για όλα τα n, $m > N$ ισχύει:

$$\begin{aligned} |(x_n + y_n) - (x_m + y_m)|_p &= |(x_n - x_m) + (y_n - y_m)|_p \\ &\leq \max\left\{ |(x_n - x_m)|_p \, , \, |(y_n - y_m)|_p \right\} < \epsilon. \end{aligned}$$

Παρόμοια αποδεικνύεται και η κλειστότητα για τον πολλαπλασιασμό. Το προσθετικό ουδέτερο στοιχείο είναι η μηδενική ακολουθία, η οποία είναι Cauchy ως προς την p-αδική νόρμα, και το πολλαπλασιαστοκό ουδέτερο η $(1, 1 \ldots, 1, \ldots)$.
□

Παρατήρηση 11 Σημειώνουμε ότι τα αντιστρέψιμα στοιχεία του δακτυλίου είναι εκείνες οι ακολουθίες που δεν έχουν μηδενικό όρο σε καμία θέση. Συνεπώς το $\mathcal{C}$ δεν είναι σώμα. Επιπλέον, παρατηρούμε ότι όλες οι σταθερές ακολουθίες $(x) = (x, x, \ldots)$, $x \in \mathcal{Q}$ ανήκουν στο $\mathcal{C}$. Θα τις συμβολίζουμε με (x).

Λήμμα 4 *Η απεικόνιση $h : x \to (x)$ δίνει έναν εγκλεισμό του $\mathcal{Q}$ στο $\mathcal{C}$.*

Απόδειξη: Η απόδειξη του λήμματος προκύπτει εύκολα από τα παραπάνω. □

Παρατήρηση 12 Το γεγονός ότι το $\mathcal{Q}$ περιέχεται στο $\mathcal{C}$ μας δείχνει ότι έχουμε πάρει κάτι μεγαλύτερο, χωρίς να χάσουμε το αρχικό μας σώμα. Παρ' όλα αυτά δεν έχουμε καταφέρει ακόμα να ολοκληρώσουμε τη διαδικασία προσθήκης των ορίων των ακολουθιών, με την έννοια ότι δύο ακολουθίες με το ίδιο όριο είναι διαφορετικά στοιχεία στο $\mathcal{C}$. Για να πετύχουμε την ταύτιση όλων αυτών των στοιχείων θα πρέπει να περάσουμε σε έναν δακτύλιο-πηλίκο.

Ορισμός 14 Ορίζουμε ως $\mathcal{N} \subset \mathcal{C}$ να είναι το ιδεώδες:

$$\mathcal{N} = \{(x_n) : x_n \to 0\} = \left\{(x_n) : \lim_{n\to\infty} |x_n|_p = 0\right\}.$$

Λήμμα 5 *Το $\mathcal{N}$ είναι μέγιστο ιδεώδες του $\mathcal{C}$.*

Απόδειξη: Θα δείξουμε ότι αν υπήρχε ιδεώδες που να περιείχε το $\mathcal{N}$ και επιπλέον περιείχε κάποια μη μηδενική ακολουθία του $\mathcal{C}$, τότε αυτό θα περιείχε και το μοναδιαίο στοιχείο. Άρα θα ταυτιζόταν με το $\mathcal{C}$.

Έστω $(x_n) \in \mathcal{C}$ μία ακολουθία $\mathcal{C}$ που όμως δεν είναι μηδενική, και έστω I το ιδεώδες που παράγεται από την (x_n) και το $\mathcal{N}$, δηλαδή:

$$I = \langle (x_n) \cup \mathcal{N} \rangle = (x_n)(y_n) + (x_n)(z_n), \text{ με } (y_n) \in \mathcal{C} \text{ και } (z_n) \in \mathcal{N}.$$

Εφ' όσον η (x_n) δεν τείνει στο μηδέν, θα πρέπει να υπάρχει κάποιος θετικός αριθμός $c > 0$ και κάποιος ακέραιος N, ώστε για κάθε $n > N$ να ισχύει $|x_n|_p \geq c > 0$. Δηλαδή, για $n > N$ θα έχουμε $x_n \neq 0$, οπότε και μπορούμε να ορίσουμε μια νέα ακολουθία (y_n) ως εξής:

$$y_n = 0, \text{ για κάθε } n < N, \text{ και } y_n = \frac{1}{x_n}, \text{ για } n \geq N.$$

Η ακολουθία που κατασκευάσαμε ανήκει στο $\mathcal{C}$, αφού για κάθε $n > N$ έχουμε:

$$|y_{n+1} - y_n|_p = \left|\frac{1}{x_{n+1}} - \frac{1}{x_n}\right|_p = \frac{|x_{n+1} - x_n|_p}{|x_{n+1}x_n|_p} \leq \frac{|x_{n+1} - x_n|_p}{c} \to 0.$$

Ακόμα παρατηρούμε το ακόλουθο:

$$x_n y_n = \begin{cases} 0, & \text{αν } n < N \\ 1, & \text{αν } n \geq N, \end{cases}$$

είναι δηλαδή μία ακολουθία της μορφής: $(0, 0, \ldots, 0, 1, 1, \ldots, 1, \ldots)$. Συγκεκριμένα αν την αφαιρέσουμε από το 1 θα πάρουμε μία ακολουθία που τείνει στο μηδέν. Τότε όμως:

$$1 - (x_n)(y_n) \in \mathcal{N} \Leftrightarrow 1 - (x_n)(y_n) = (z_n),\ (z_n) \in \mathcal{N}$$

$$\Leftrightarrow 1 = (x_n)(y_n) + (z_n) \Leftrightarrow 1 \in I.$$

Άρα κάθε άλλο ιδεώδες μεγαλύτερο του $\mathcal{N}$ θα ταυτίζεται με όλο το δακτύλιο, συνεπώς το $\mathcal{N}$ είναι μέγιστο. □

Θέλουμε να ταυτίσουμε τις ακολουθίες που διαφέρουν κατά στοιχεία του $\mathcal{N}$, με την έννοια ότι τότε θα έχουν το ίδιο όριο. Για να το επιτύχουμε αυτό παίρνουμε το δακτύλιο-πηλίκο του δακτυλίου $\mathcal{C}$ προς το ιδεώδες $\mathcal{N}$. Μάλιστα, παίρνοντας το $\mathcal{N}$ που είναι μέγιστο ιδεώδες, ο δακτύλιος-πηλίκο που προκύπτει είναι σώμα.

Ορισμός 15 Ορίζουμε ως *σώμα των p-αδικών αριθμών* $\mathbb{Q}_p$ να είναι ο δακτύλιος-πηλίκο του δακτυλίου $\mathcal{C}$ προς το μέγιστο ιδεώδες του $\mathcal{N}$:

$$\mathbb{Q}_p = \frac{\mathcal{C}}{\mathcal{N}}.$$

Σημειώνουμε ότι εξακολουθούμε να έχουμε εγκλεισμό του $\mathbb{Q}$ στο $\mathbb{Q}_p$. Μόνο η μηδενική ακολουθία ανήκει στο ιδεώδες, αφού κάθε άλλη σταθερή έχει όριο διαφορετικό του μηδενός. Επομένως, κάθε δύο διαφορετικές σταθερές ακολουθίες ανήκουν σε διαφορετικό σύμπλοκο:

$$(x) \neq (y) \ \text{ όπου } \ x, y \in \mathbb{Q} \Leftrightarrow (x) - (y) \neq (0) \Leftrightarrow$$

$$(x) - (y) = (x - y) \notin \mathcal{N} \ \Leftrightarrow (x) + \mathcal{N} \ \neq (y) + \mathcal{N}\ .$$

Έχουμε αποκτήσει ένα σώμα που περιέχει γνήσια το $\mathbb{Q}$. Θα δείξουμε επιπλέον ότι αυτό είναι μια πλήρωσή του. Κατ' αρχάς θα επεκτείνουμε την p-αδική νόρμα του $\mathbb{Q}$ στο $\mathbb{Q}_p$.

Λήμμα 6 *Έστω* $(x_n) \in \mathcal{C}$, $(x_n) \notin \mathcal{N}$. *Τότε η ακολουθία των πραγματικών αριθμών* $|x_n|_p$ *είναι τελικά σταθερή, δηλαδή υπάρχει ακέραιος* n_0*, τέτοιος ώστε για κάθε* n, $m > n_0$ *έχουμε* $|x_n|_p = |x_m|_p$.

Απόδειξη: Η ακολουθία (x_n) δεν ανήκει στο $\mathcal{N}$, δηλαδή δεν τείνει στο μηδέν. Επομένως, υπάρχουν θετικοί αριθμοί $N_1,\ c$, τέτοιοι ώστε:

$$n \geq N_1 \Rightarrow |x_n|_p \geq c > 0.$$

Επιπλέον η είναι ακολουθία Cauchy, άρα υπάρχει $N_2 \in \mathbb{N}$ ώστε για $\epsilon = c$ έχουμε:

$$n,\, m > N_2 \Rightarrow |x_n - x_m|_p < c.$$

Θέτουμε $N = \max\{N_1,\, N_2\}$. Τότε ισχύει:

$$n,\, m > N \Rightarrow |x_n - x_m|_p < c \leq \max\left\{|x_n|_p\,,\, |x_m|_p\right\},$$

άρα, από την ιδιότητα των μη αρχιμήδειων χώρων ότι ‘‘όλα τα τρίγωνα είναι ισοσκελή’’, $|x_n|_p = |x_m|_p$. □

Έχοντας το παραπάνω λήμμα έχει νόημα να επεκτείνουμε την p-αδική νόρμα πάνω στο $\mathbb{Q}_p$.

Ορισμός 16 Έστω $\lambda \in \mathbb{Q}_p$ στοιχείο του $\mathbb{Q}_p$ και (x_n) ακολουθία Cauchy ρητών αριθμών που ανήκει στο σύμπλοκο του λ. Ορίζουμε ως p-αδική νόρμα του λ το θετικό αριθμό $|\lambda|_p$, τέτοιο ώστε:

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p\,.$$

Παρατήρηση 13 Η p-αδική νόρμα πάνω στο $\mathbb{Q}_p$ είναι καλά ορισμένη. Πράγματι, για κάθε στοιχείο του $\mathbb{Q}_p$ ορίζεται η p-αδική του νόρμα, διότι το όριο των νορμών της ακολουθίας-εκπροσώπου πάντα υπάρχει, αφού η ακολουθία των νορμών ακολουθιών Cauchy είναι τελικά σταθερή ή μηδενική. Επιπλέον, η νόρμα κάθε p-αδικού είναι ανεξάρτητη από την ακολουθία-εκπρόσωπο που επιλέγουμε.

Παρατήρηση 14 Το σύνολο τιμών της p-αδικής νόρμας πάνω στο $\mathbb{Q}_p$ είναι το ίδιο με αυτό της p-αδικής νόρμας στο $\mathbb{Q}$. Δηλαδή η εικόνα του $\mathbb{Q}_p$ μέσω της $|\cdot|_p$ είναι η ίδια με την εικόνα του $\mathbb{Q}$ μέσω της $|\cdot|_p$.

Πρόταση 13 *Η p-αδική νόρμα πάνω στο $\mathbb{Q}_p$ είναι μη αρχιμήδεια νόρμα.*

Απόδειξη: Η απόδειξη είναι προφανής από το γεγονός ότι τελικά η νόρμα ενός p-αδικού αριθμού είναι ίση με αυτή ενός ρητού, και η p-αδική νόρμα στο $\mathbb{Q}$ είναι μη αρχιμήδεια. □

Παρατήρηση 15 Η p-αδική εκτίμηση επίσης επεκτείνεται στο $\mathbb{Q}_p$. Για κάθε p-αδικό αριθμό $x \in \mathbb{Q}_p,\ x \neq 0$, υπάρχει ακέραιος $\upsilon_p(x)$, τέτοιος ώστε $|x|_p = p^{-\upsilon_p(x)}$.

Στη συνέχεια έχουμε το εξής:

Πρόταση 14 *Η εικόνα του $\mathbb{Q}$ μέσω της συνάρτησης εγκλεισμού του στο $\mathbb{Q}_p$, $h(x) = (x)$, είναι πυκνό υποσύνολο του $\mathbb{Q}_p$.*

Απόδειξη: Θα δείξουμε ότι κάθε ανοικτή μπάλα γύρω από κάποιον p-αδικό αριθμό λ περιέχει μία σταθερή ακολουθία, δηλαδή ένα στοιχείο της εικόνας του $\mathbb{Q}$.

Έστω λοιπόν $\epsilon > 0$ και έστω η μπάλα $B(\lambda, \epsilon)$ με κέντρο το λ και ακτίνα ϵ. Επιπλέον, έστω (x_n) ακολουθία Cauchy που ανήκει στο σύμπλοκο του λ και έστω $\epsilon' < \epsilon$. Επειδή η (x_n) είναι Cauchy, τότε υπάρχει αριθμός N, τέτοιος ώστε:

$$\text{για κάθε } n,\ m > N \text{ ισχύει } |x_n - x_m|_p < \epsilon'.$$

Θέτουμε $y = x_N$, και θεωρούμε τη σταθερή ακολουθία (y). Θα δείξουμε ότι αυτή η ακολουθία, που είναι ένα στοιχείο της εικόνας του $\mathbb{Q}$, ανήκει στη μπάλα $B(\lambda, \epsilon)$.

Σύμφωνα με τον ορισμό της p-αδικής νόρμας, για το στοιχείο $\lambda - y \in \mathbb{Q}_p$ ισχύει:

$$|\lambda - y|_p = \lim_{n\to\infty} |(x_n - y)|_p \,,$$

και για την p-αδική νόρμα της ακολουθίας $(x_n - y)$ έχουμε:

$$|(x_n - y)|_p = \lim_{n\to\infty} |x_n - x_N|_p \leq \epsilon' < \epsilon \quad \text{για κάθε } n > N.$$

Συνεπώς, παίρνοντας τα όρια έχουμε:

$$|\lambda - y|_p \leq \epsilon' < \epsilon \Leftrightarrow (y) \in B(\lambda, \epsilon).$$

□

Για να ολοκληρώσουμε την απόδειξη ότι το $\mathbb{Q}_p$ είναι η πλήρωση του $\mathbb{Q}$ μένει να δείξουμε ότι το $\mathbb{Q}_p$ είναι πλήρες με την p-αδική νόρμα, ότι δηλαδή κάθε ακολουθία στοιχείων του $\mathbb{Q}_p$ συγκλίνει σε κάποιο στοιχείο του $\mathbb{Q}_p$.

Πρόταση 15 *Το σώμα $\mathbb{Q}_p$ των p-αδικών αριθμών είναι πλήρες ως προς την p-αδική νόρμα.*

Απόδειξη: Έστω $\lambda_1, \lambda_2, \ldots$ ακολουθία Cauchy p-αδικών αριθμών. Είναι εύκολο να βρούμε ακολουθία ρητών αριθμών $y_1,\ y_2, \ldots$, τέτοια ώστε:

$$\lim_{n\to\infty} |\lambda_n - (y_n)|_p = 0,$$

όπου (y_n) η εικόνα του ρητού y_n στο $\mathbb{Q}_p$, δηλαδή η σταθερή ακολουθία $y_n,\ y_n, \ldots$. Μπορούμε να σκεφτόμαστε τα λ_n ως ακολουθίες Cauchy ρητών αριθμών. Τα y_n προκύπτουν από την πυκνότητα των ρητών αριθμών στο σώμα των p-αδικών αριθμών.

Ισχυριζόμαστε ότι η ακολουθία $y_1,\ y_2, \ldots$ είναι ακολουθία Cauchy στο $\mathbb{Q}$. Κατ' αρχάς θα δείξουμε ότι η ακολουθία $(y_1), (y_2), \ldots$ είναι ακολουθία Cauchy στο $\mathbb{Q}_p$, οπότε ο ισχυρισμός μας έπεται φυσιολογικά, περνώντας από τη σταθερή ακολουθία $(y_n) \in \mathbb{Q}_p$ στο ρητό $y_n \in \mathbb{Q}$.

Έστω $\epsilon > 0$. Έχουμε επιλεξει τα y_n ώστε:

$$\lim_{n\to\infty} |\lambda_n - (y_n)| = 0$$

και άρα υπάρχει $N_1 > 0$, τέτοιο ώστε για κάθε $n > N_1$ να ισχύει:

$$|\lambda_n - (y_n)| < \epsilon.$$

Επιπλέον, η ακολουθία $\lambda_1, \lambda_2, \ldots, \lambda_n, \ldots$ είναι ακολουθία Cauchy, οπότε υπάρχει $N_2 > 0$, τέτοιο ώστε για κάθε $n, m > N_2$:

$$|\lambda_n - \lambda_m| < \epsilon.$$

Έστω $N = \max\{N_1, N_2\}$. Τότε, για $n, m > N$ έχουμε:

$$\begin{aligned} |(y_n) - (y_m)|_p &= |((y_n) - \lambda_n) + (\lambda_n - \lambda_m) + (\lambda_m - (y_m))|_p \\ &\leq \max\{|(y_n) - \lambda_n|, |\lambda_n - \lambda_m|, |\lambda_n - (y_m)|\} < \epsilon, \end{aligned}$$

δηλαδή η ακολουθία $y_1, y_2, \ldots, y_n, \ldots$ είναι Cauchy στο $\mathbb{Q}_p$, και άρα και στο $\mathbb{Q}$.

Έστω $\lambda = [(y_n)] \in \mathbb{Q}_p$ ο p-αδικός αριθμός στον οποίο συγκλίνει η ακολουθία (y_n). Θα δείξουμε ότι ο p-αδικός αριθμός λ είναι το όριο της ακολουθίας $\lambda_1, \lambda_2, \ldots, \lambda_n, \ldots$.

Έστω $\epsilon > 0$. Αφού η ακολουθία (y_n) έχει όριο το λ, ισχύει ότι:

$$\text{υπάρχει } n_0 \text{ ώστε για κάθε } n > n_0 \text{ ισχύει } \quad |y_n - \lambda|_p < \epsilon.$$

Επιπλέον, από τον τρόπο που έχουμε επιλέξει τα y_n, υπάρχει κάποιο n_0', τέτοιο ώστε για κάθε $n > n_0$ έχουμε:

$$|\lambda_n - (y_n)| < \epsilon.$$

Έτσι παίρνουμε:

$$|\lambda_n - \lambda|_p = |\lambda_n - (y_n) + (y_n) - \lambda|_p \leq \max\left\{|\lambda_n - (y_n)|_p, |(y_n) - \lambda|_p\right\} < \epsilon,$$

για κάθε $n > \max\{n_0, n_0'\}$. Ισοδύναμα:

$$\lim_{n\to\infty} \lambda_n = \lambda.$$

Συνοψίζοντας, έχουμε βρει ότι η τυχαία ακολουθία Cauchy p-αδικών αριθμών έχει όριο έναν p-αδικό αριθμό, ότι δηλαδή το $\mathbb{Q}_p$ είναι πλήρες ως προς την p-αδική νόρμα. □

Από το Λήμμα 6 και τον ορισμό της p-αδικής νόρμας στο $\mathbb{Q}_p$ και από τις Προτάσεις 14 και 15, έπεται το ακόλουθο θεώρημα ύπαρξης και μοναδικότητας του $\mathbb{Q}_p$.

Θεώρημα 6 *Για κάθε πρώτο αριθμό p υπάρχει ένα σώμα $\mathbb{Q}_p$ με μία μη αρχιμήδεια νόρμα $|\cdot|_p$, τέτοιο ώστε:*

(i) υπάρχει εγκλεισμός $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, και η νόρμα $|\cdot|_p$ είναι επέκταση της p-αδικής νόρμας στο $\mathbb{Q}$,

(ii) *η εικόνα του $\mathbb{Q}$ μέσω του εγκλεισμού αυτού είναι πυκνή στο $\mathbb{Q}_p$,*

(iii) *το $\mathbb{Q}_p$ είναι πλήρες ως προς τη νόρμα $|\cdot|_p$.*

Το σώμα $\mathbb{Q}_p$ που ικανοποιεί και τις τρεις παραπάνω ιδιότητες είναι μοναδικό ως προς μοναδικό ισομορφισμό που διατηρεί τις νόρμες.

Απόδειξη: Έχουμε αποδείξει τις τρεις ιδιότητες. Μένει να δείξουμε τον ισχυρισμό για τη μοναδικότητα του ισομορφισμού που διατηρεί τις νόρμες. Έστω κάποιο άλλο σώμα $\mathbb{K}$ που ικανοποιεί τις ιδιότητες (i), (ii) και (iii). Τότε μπορούμε να σκεφτόμαστε τον εγκλεισμό $\mathbb{Q} \hookrightarrow \mathbb{K}$ ως μία συνάρτηση με πεδίο ορισμού ένα πυκνό υποσύνολο του $\mathbb{Q}_p$.

Ο εγκλεισμός αυτός είναι μία συνάρτηση που πρέπει να διατηρεί τις νόρμες των στοιχείων του $\mathbb{Q}$, το οποίο έχει πυκνή εικόνα στο $\mathbb{K}$. Άρα είναι μία συνεχής συνάρτηση.

Γνωρίζουμε ότι μία συνεχής συνάρτηση ορισμένη πάνω σε πυκνό υποσύνολο, επεκτείνεται μοναδικά σε ολόκληρο το σώμα. Συνεπώς μπορούμε να πάρουμε μία συνάρτηση από το $\mathbb{Q}_p$ στο $\mathbb{K}$, η οποία είναι η μοναδική εκείνη επέκταση της συνάρτησης εγκλεισμού του $\mathbb{Q}$ στο $\mathbb{K}$.

Είναι εύκολο να δείξει κανείς ότι αυτή η συνάρτηση είναι ισομορφισμός που διατηρεί τις νόρμες και η μοναδικότητά του είναι προφανής από κατασκευή. □

Η μοναδικότητα του παραπάνω ισομορφισμού είναι πολύ σημαντική. Μας λέει ότι μπορούμε να 'ξεχάσουμε' την κατασκευή του $\mathbb{Q}_p$ και να δουλέυουμε με τις ιδιότητες που το χαρακτηρίζουν. Ότι δηλαδή είναι η πλήρωση του $\mathbb{Q}$ ως προς την p-αδική νόρμα.

3.2 Ο δακτύλιος εκτίμησης του $\mathbb{Q}_p$

Έχοντας στα χέρια μας το σώμα των p-αδικών αριθμών συνοδευόμενο από τη μη αρχιμήδεια p-αδική μετρική, μπορούμε να μελετήσουμε την τοπολογία του. Προτρέχοντας της ενότητας **''Ανάλυση στο $\mathbb{Q}_p$''**, θα δούμε εδώ τον δακτύλιο εκτίμησης του $\mathbb{Q}_p$, καθώς και μερικές ιδιότητές του, χρήσιμες για την αμέσως επόμενη ενότητα.

Ορισμός 17 Ο δακτύλιος εκτίμησης του $\mathbb{Q}_p$ ως προς την p-αδική νόρμα είναι το σύνολο:

$$\mathcal{O}_p = \left\{ x \in \mathbb{Q}_p : \ |x|_p \leq 1 \right\}.$$

Πρόταση 16 *Ο δακτύλιος $\mathcal{O}_p$ είναι τοπικός δακτύλιος με μέγιστο ιδεώδες το κύριο ιδεώδες $p\mathcal{O}_p = \left\{ x \in \mathbb{Q}_p : \ |x|_p < 1 \right\}$. Επιπλέον,*

(i) $\mathbb{Q} \cap \mathcal{O}_p = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : \ p \nmid b \right\}$.

(ii) Η εικόνα του $\mathbb{Z}$ είναι πυκνή στο $\mathcal{O}_p$. Πιο συγκεκριμένα, δοθέντος $x \in \mathcal{O}_p$ και δοθέντος $n \geq 1$, υπάρχει μοναδικός $a \in \mathbb{Z}$, με $0 \leq a \leq p^{n-1}$, τέτοιος ώστε $|x - a|_p \leq p^{-n}$.

(iii) Για κάθε $x \in \mathcal{O}_p$ υπάρχει μοναδική ακολουθία Cauchy (a_n) που να συγκλίνει στο x, με τις εξής ιδιότητες:

$$a_n \in \mathbb{Z} \quad \text{και} \quad 0 \leq a_n \leq p^{n-1}$$

και

$$a_{n+1} \equiv a_n \pmod{p^n} \quad \text{για κάθε } n.$$

Απόδειξη: Αποδεικνύουμε μία μία τις ιδιότητες της πρότασης. Κατ' αρχήν, ο $\mathcal{O}_p$ ορίστηκε να είναι ο δακτύλιος εκτίμησης της, μη αρχιμήδειας, p-αδικής νόρμας πάνω στο $\mathbb{Q}_p$, συνεπώς είναι ένας τοπικός δακτύλιος.

Θα δείξουμε ότι το ιδεώδες εκτίμησης του $\mathcal{O}_p$ είναι κύριο, και ότι το πρωταρχικό στοιχείο από το οποίο παράγεται είναι το p. Αρκεί να δείξουμε ότι το ιδεώδες εκτίμησης περιέχεται στο $p\mathcal{O}_p$, διότι ξέρουμε ότι το ιδεώδες εκτίμησης είναι μέγιστο και προφανώς $p\mathcal{O}_p \neq \mathcal{O}_p$.

Θα δείξουμε ότι αν $x \in \left\{ y \in \mathbb{Q}_p : \ |y|_p < 1 \right\}$, τότε $x \in p\mathcal{O}_p = \{ p\,a : \ a \in \mathcal{O}_p \}$:

$$|x|_p < 1 \Rightarrow |x|_p \leq \frac{1}{p} \Rightarrow \left| \frac{x}{p} \right|_p \leq 1 \Rightarrow \frac{x}{p} \in \mathcal{O}_p \Rightarrow x \in p\mathcal{O}_p.$$

Δηλαδή $\left\{ y \in \mathbb{Q}_p : \ |y|_p < 1 \right\} \subset p\mathcal{O}_p$.

(i) Η ιδιότητα αυτή έπεται φυσιολογικά από το γεγονός ότι $\mathbb{Z}_{(p)}$ είναι ο δακτύλιος εκτίμησης του $\mathbb{Q}$ με την p-αδική νόρμα:

$$x \in \mathbb{Q} \cap \mathcal{O}_p \Rightarrow x \in \mathbb{Q} \ \text{ και } \ |x|_p < 1 \Rightarrow x \in \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \colon \ p \nmid b \right\}.$$

(ii) Θα δείξουμε ότι οι ακέραιοι αριθμοί είναι πυκνοί στο $\mathcal{O}_p$. Έστω $x \in \mathcal{O}_p$ και $n \geq 1$. Αφού το $\mathbb{Q}$ είναι πυκνό στο $\mathbb{Q}_p$ και $\mathcal{O}_p \subset \mathbb{Q}_p$, μπορούμε να βρούμε έναν ρητό αριθμό $a/b \in \mathbb{Q}$, τέτοιο ώστε:

$$\left| x - \frac{a}{b} \right|_p \leq p^{-n} < 1.$$

Θα δείξουμε ότι ο x μπορεί να προσεγγιστεί και από έναν ακέραιο. Παρατηρούμε τα εξής:

$$y \in \mathbb{Z} \Rightarrow |y|_p \leq 1 \ \text{ και } \ |y|_p = 1 \Leftrightarrow p \nmid y.$$

Ακόμα,

$$\left| \frac{a}{b} \right|_p = \left| \frac{a}{b} - x + x \right|_p \leq \max \left\{ |x|_p, \left| x - \frac{a}{b} \right| \right\} \leq 1,$$

δηλαδή $a/b \in \mathcal{O}_p$ και άρα $p \nmid b$. Όμως $p \nmid b$ σημαίνει ότι το b είναι αντιστρέψιμο στοιχείο στο $\mathbb{Z}/p\mathbb{Z}$, ισοδύναμα υπάρχει $b' \in \mathbb{Z}$, τέτοιος ώστε:

$$bb' \equiv 1 \pmod{p^n} \Leftrightarrow 1 - bb' = kp^n.$$

Τότε όμως, για το στοιχείο $ab' \in \mathbb{Z}$ και για τον ρητό a/b ισχύει:

$$\left| \frac{a}{b} - ab' \right|_p = |a|_p \left| \frac{1 - bb'}{b} \right|_p \leq \frac{|\kappa p^n|_p}{|b|_p} = p^{-n}.$$

Τέλος, προκύπτει εύκολα από τη σχέση μεταξύ p-αδικής νόρμας και εξισώσεων ισοτιμίας ότι μπορούμε να βρούμε ακέραιο $\alpha \in \{0, 1, \ldots, p^n - 1\}$ που να επάληθεύει την ανισότητα $|x - \alpha|_p \leq p^{-n}$. Πράγματι, έστω $\alpha \in \mathbb{Z}$ ο μοναδικός εκείνος ακέραιος, τέτοιος ώστε:

$$0 \leq \alpha \leq p^n - 1 \quad \text{και} \quad \alpha \equiv ab' \pmod{p^n}.$$

Τότε έχουμε:

$$\begin{aligned} |x-\alpha|_p &= \left|x - \tfrac{a}{b} + \tfrac{a}{b} - ab' + ab' - \alpha\right|_p \\ &\leq \max\left\{\left|x-\tfrac{a}{b}\right|_p, \left|\tfrac{a}{b} - ab'\right|_p, |ab'-\alpha|_p\right\} \\ &\leq p^{-n}. \end{aligned}$$

(iii) Από το (ii) για κάθε n μπορούμε να πάρουμε μοναδική ακολουθία (a_n) για $x \in \mathcal{O}_p$, με τις εξής ιδιότητες:

$$a_n \in \mathbb{Z} \quad \text{και} \quad 0 \leq a_n \leq p^{n-1}.$$

Η ακολουθία αυτή είναι Cauchy. Έστω $\epsilon > 0$. Τότε, για n_0 τέτοιο ώστε $1/p^{n_0} < \epsilon \leq 1/p^{n_0+1}$ ισχύει:

$$\begin{aligned} |a_n - a_m|_p &= |a_n - x + x - a_m|_p \\ &\leq \max\left\{|x-a_m|_p, |a_n - x|_p\right\} \\ &\leq p^{-n} < \epsilon \quad \text{για κάθε } n, m > n_0. \end{aligned}$$

Επιπλέον, η (a_n) συγκλινει στο x:

$$\lim_{n\to\infty} |a_n - x|_p = \lim_{n\to\infty} p^{-n} \to 0.$$

Τέλος για τη συνέπεια της ακολουθίας (a_n), έχουμε:

$$|x - a_n|_p \leq p^{-n} \Leftrightarrow p^n \mid x - a_n \quad \text{για κάθε } n \in \mathbb{N}.$$

Οπότε, για τα n, $n+1$ έχουμε:

$$x - a_n = \kappa p^n \quad \text{και} \quad x - a_{n+1} = \lambda p^{n+1},$$

και αφαιρώντας κατά μέλη παίρνουμε:

$$a_{n+1} - a_n = \lambda p^n - \kappa p^{n+1} = p^n(\lambda - \kappa p) \Leftrightarrow$$

$$p^n \mid a_{n+1} - a_n \quad \Leftrightarrow \quad a_{n+1} \equiv a_n \pmod{p^n}.$$

□

Η προηγούμενη πρόταση επισημαίνει πολλά ενδιαφέροντα πράγματα για το $\mathcal{O}_p$, όπως για παράδειγμα ότι το $\mathcal{O}_p$ είναι η πλήρωση του $\mathbb{Z}$ ως προς την p-αδική νόρμα. Ο δακτύλιος εκτίμησης είναι ένα πολύ σημαντικό υποσύνολο των p-αδικών αριθμών, όπως θα φανεί και στη συνέχεια.

Την τελευταία ιδιότητα που χαρακτηρίζει τα στοιχεία του p-αδικού δακτυλίου εκτίμησης είχαμε συναντήσει και στο εισαγωγικό κεφάλαιο. Επειδή θα μας απασχολήσει αρκετά, δίνουμε ένα ονομα στις ακολουθίες που ικανοποιούν την ιδιότητα αυτή:

Ορισμός 18 Ακολουθίες (a_n), τέτοιες ώστε για κάθε όρο a_n ισχύει $a_n \equiv a_{n-1} \pmod{p^{n-1}}$, λέγονται *συνεπείς (coherent).*

3.3 Η αλγεβρική κατασκευή του $\mathbb{Q}_p$

Μπορούμε να φτάσουμε στο σώμα $\mathbb{Q}_p$ και με διαφορετικό τρόπο από την διαδικασία πλήρωσης του $\mathbb{Q}$ ως προς την p-αδική νόρμα. Θα χρησιμοποιήσουμε τις αλγεβρικές έννοιες των αντιστρόφων συστημάτων και θα κατασκευάσουμε το δακτύλιο των p-αδικών ακεραίων. Το σώμα των p-αδικών αριθμών θα προκύψει τότε ως το σώμα όλων των πολυωνύμων μεταβλητής $\frac{1}{p}$, με τους συντελεστές p-αδικούς ακεραίους.

3.3.1 Αντίστροφα συστήματα και αντίστροφα όρια

Ορισμός 19 Ένα *αντίστροφο σύστημα (inverse system)* (X_i, ϕ_j^i) τοπολογικών χώρων πάνω σε ένα καλά διατεταγμένο σύνολο δεικτών I, αποτελείται από μία οικογένεια τοπολογικών χώρων $(X_i : \ i \in I)$ και μία οικογένεια συνεχών απεικονίσεων $(\phi_j^i : X_i \to X_j, \ \ i, j \in I, \ \ i \geq j)$, τέτοιες ώστε:

$$\phi_i^i = id_{X_i} \quad \text{και} \quad \phi_k^j \circ \phi_j^i = \phi_k^i \ \ \text{οποτεδήποτε} \ \ i \geq j \geq k.$$

Στην περίπτωση που τα X_i είναι τοπολογικές ομάδες τότε οι συνεχείς απεικονίσεις ϕ_j^i απαιτείται να είναι επιπλέον ομομορφισμοί. Αντίστροφα συστήματα τοπολογικών δακτυλίων, τοπολογικών διανυσματικών χώρων κ.ο.κ. ορίζονται ανάλογα.

Ορισμός 20 Το *αντίστροφο όριο (inverse limit)* $\lim_{\leftarrow} X_i$ του αντιστρόφου συστήματος $(X_i,\, \phi^i_j)$ ορίζεται ως το ακόλουθο υποσύνολο του καρτεσιανού γινομένου $\prod X_i$:

$$\lim_{\longleftarrow} X_i := \left\{ z \in \prod X_i : \quad (\phi^i_j \circ \varpi_i)(z) = \varpi_j(z) \;\; \text{οποτεδήποτε} \;\; j \geq i \right\},$$

όπου με ϖ_i συμβολίζουμε την προβολή του $\prod X_i$ στο X_i.

Το $\lim_{\leftarrow} X_i$ είναι μοναδικά ορισμένο και κληρονομεί την επαγόμενη τοπολογία του τοπολογικού χώρου $\prod X_i$, δηλαδή την τοπολογία του καρτεσιανού γινομένου. Εύκολα επαληθεύεται η κλειστότητα του $\lim_{\leftarrow} X_i$ στο $\prod X_i$. Ακόμα, το $\lim_{\leftarrow} X_i$ είναι μη κενό όταν κάθε X_i είναι ένας μη κενός συμπαγής τοπολογικός χώρος Hausdorff.

Αν τα X_i είναι τοπολογικές ομάδες, τότε το $\lim_{\leftarrow} X_i$ είναι επίσης τοπολογική ομάδα με πράξη αυτήν που επάγεται φυσιολογικά στο $\prod X_i$ από τις πράξεις των τοπολογικών ομάδων X_i. Σε αυτή την περίπτωση το $\lim_{\leftarrow} X_i$ είναι πάντα μη κενό. Παρόμοια αποτελέσματα ισχύουν για τοπολογικούς δακτυλίους, τοπολογικούς διανυσματικούς χώρους κ.ο.κ. Τέλος σημειώνουμε ότι αν $X_i = X$ για όλα τα i και ϕ^i_j είναι η ταυτοτική συνάρτηση για όλα τα i, j, τότε το $\lim_{\leftarrow} X_i = \lim_{\leftarrow} X$ μπορεί να ταυτιστεί φυσιολογικά με το X. Απλά αντιστοιχίζουμε σε κάθε σταθερή ακολουθία $(x,\, x, \ldots)$ το $x \in X$.

Ορισμός 21 Ένας *μορφισμός* μεταξύ δύο αντιστρόφων συστημάτων $(X_i,\, \phi^i_j)$ και $(Y_i,\, \psi^i_j)$, ορισμένων στο ίδιο σύνολο δεικτών I, είναι μία συλλογή συνεχών απεικονίσεων με την ακόλουθη ιδιότητα:

$$(\rho_i : \; X_i \longrightarrow Y_i, \; i \in I) \;\; \text{ώστε} \;\; \psi^i_j \circ \rho_i = \rho_j \circ \phi^i_j \;\; \text{για κάθε} \;\; i \in I.$$

Εάν επιπλέον τα αντίστροφα συστήματα είναι τοπολογικές ομάδες, τότε οι απεικονίσεις ρ_i πρέπει να είναι και ομομορφισμοί ομάδων. Ανάλογα ορίζονται οι μορφισμοί όταν έχουμε τοπολογικούς δακτυλίους, τοπολογικούς διανυσματικούς χώρους, κ.τ.λ.

Παρακάτω παραθέτουμε τις πιο σημαντικές ιδιότητες των αντίστροφων ορίων παραλείποντας τις αποδείξεις.

Ένας μορφισμός $(\rho_i : i \in I)$ από το αντίστροφο σύστημα (X_i, ϕ^i_j) στο αντίστροφο σύστημα (Y_i, ψ^i_j) επάγει έναν μορφισμό μεταξύ των αντιστρόφων ορίων τους:

$$\varprojlim \rho_i : \varprojlim X_i \longrightarrow \varprojlim Y_i$$

θέτοντας

$$\varprojlim \rho_i((x_i)) := (\rho_i(x_i)).$$

Αν έχουμε εγκλεισμούς ι_i από τους X_i στους Y_i, τότε αυτοί επάγουν έναν εγκλεισμό μεταξύ των αντίστροφων ορίων τους:

$$\varprojlim \iota_i : \varprojlim X_i \longrightarrow \varprojlim Y_i.$$

Επιπλέον, αν η ακολουθία

$$0 \longrightarrow X_i \xrightarrow{\iota_i} Y_i \xrightarrow{\varphi_i} Z_i \longrightarrow 0$$

είναι ακριβής για κάθε i, τότε και η ακολουθία

$$0 \longrightarrow \varprojlim X_i \xrightarrow{\varprojlim \iota_i} \varprojlim Y_i \xrightarrow{\varprojlim \varphi_i} \varprojlim Z_i$$

είναι ακριβής.

Ακόμα, για οποιοδήποτε υποσύνολο J του συνόλου δεικτών I, τέτοιο ώστε για κάθε $i \in I$ υπάρχει $j \in J$ με $j \leq i$ ισχύει:

$$\varprojlim_{i \in I} X_i \cong \varprojlim_{j \in J} X_j.$$

Για παράδειγμα, αν παρατηρήσουμε ότι το σύνολο των διαγωνίων στοιχείων του $I \times I$ είναι ένα τέτοιο υποσύνολο, μπορούμε να συμπεράνουμε το ακόλουθο αποτέλεσμα:

$$X \times Y \cong \varprojlim_{(i,i)} (X_i \times Y_i) \cong \varprojlim_{(i,j) \in I \times I} (X_i \times Y_j),$$

όπου X, Y να είναι αντίστοιχα τα αντίστροφα όρια των αντιστρόφων συστημάτων (X_i, ϕ^i_j) και (Y_j, ψ^j_m) με $i, j \in I$.

Η ένα προς ένα και επί συνάρτηση μεταξύ των $X \times Y$ και $\varprojlim_{(i,i)} (X_i \times Y_i)$ απεικονίζει ζευγάρια ακολουθιών $((x_i), (y_i)) \in X \times Y$ στην ακολουθία $(x_i, y_i) \in \varprojlim_{(i,i)} (X_i \times Y_i)$. Είναι μάλιστα ισομορφισμός όταν τα X_i, Y_i είναι ομάδες, δακτύλιοι, κ.τ.λ. Τα παραπάνω γενικεύονται για οποιοδήποτε πεπερασμένο καρτεσιανό γινόμενο αντίστροφων ορίων.

3.3.2 Η κατασκευή των p-αδικών ακεραίων $\mathbb{Z}_p$

Για κάθε $n \geq 1$ θέτουμε A_n να είναι ο δακτύλιος των κλάσεων ισοδυναμίας των ακεραίων modulo p^n, δηλαδή $A_n = \mathbb{Z}/p^n\mathbb{Z}$.

Μπορούμε εύκολα να περάσουμε από ένα στοιχείο του A_n σε ένα στοιχείο του A_m, όπου $0 \leq m \leq n$. Παίρνουμε έτσι έναν επιμορφισμό

$$\theta_m^n : A_n \to A_m,$$

με πυρήνα $p^{n-m}A_1$.

Για να γίνουν τα παραπάνω πιο ξεκάθαρα, μπορούμε να σκεφτόμαστε κάθε ακέραιο a γραμμένο σε βάση p, δηλαδή τη μοναδική του αναπαράσταση ως $a = a_0 + a_1p + \cdots + a_rp^r$, με τους συντελεστές a_i να ανήκουν στο $A_1 = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ και $r \in \mathbb{N}$. Τότε, θεωρώντας τον επιμορφισμό $\rho_n : \mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, που στέλνει κάθε ακέραιο στον ισοϋπόλοιπο ακέραιο modulo p^n, έχουμε ότι κάθε στοιχείο του A_n μπορεί να γραφεί ως εξής:

$$\rho_n(a) = \begin{cases} a_0 + a_1p + \cdots + a_rp^r + p^n\mathbb{Z}, & r < n \\ a_0 + a_1p + \cdots + a_{n-1}p^{n-1} + p^n\mathbb{Z}, & r \geq n. \end{cases}$$

Οπότε για τους επιμορφισμούς θ_m^n έχουμε $\theta_m^n(\rho_n(x)) = \rho_m(x)$. Δηλαδή:

$$\theta_m^n(x_0 + x_1p + \cdots + x_{n-1}p^{n-1} + p^n\mathbb{Z}) = x_0 + x_1p + \cdots + x_{m-1}p^{m-1} + p^m\mathbb{Z}.$$

Η ακολουθία

$$\ldots \to A_n \to A_{n+1} \to \ldots \to A_2 \to A_1$$

μαζί με τους επιμορφισμούς θ_m^n αποτελούν ένα αντίστροφο σύστημα τοπολογικών δακτυλίων, με σύνολο δεικτών το σύνολο των φυσικών αριθμών $\mathbb{N}$.

Ορισμός 22 Το αντίστροφο όριο του συστήματος (A_n, θ_m^n), με τα A_n και θ_m^n όπως ορίστηκαν παραπάνω, είναι ο δακτύλιος των *p-αδικών ακεραίων* $\mathbb{Z}_p$.

Από τον ορισμό, ένα στοιχείο του $\mathbb{Z}_p = \lim_{\leftarrow}(A_n, \theta_m^n)$ είναι μία ακολουθία $a = (a_1, \ldots, a_n, \ldots,)$, με $a_n \in A_n$ και με $\theta_{n-1}^n(a_n) = a_{n-1}$ για κάθε $n \geq 2$. Δηλαδή, το $\mathbb{Z}_p$ είναι το σύνολο των ακολουθιών:

$$\mathbb{Z}_p = \{(a_n) : \ a_n \in \mathbb{Z}, \ a_{n+1} \equiv a_n \pmod{p^n}\}.$$

Γενικότερα, τα στοιχεία του $\mathbb{Z}_p$ συμβολίζονται ως:

$$a_{\leftarrow} := (a_1,\, a_2,\, a_3, \ldots) \in \mathbb{Z}_p.$$

Το $\mathbb{Z}_p$, ως αντίστροφο όριο, κληρονομεί τις πράξεις της πρόσθεσης και του πολλαπλασιασμού από τον δακτύλιο $\prod_{n\geq 1} A_n$, δηλαδή συντεταγμένη προς συντεταγμένη. Μάλιστα, αποτελεί υποδακτύλιο του $\prod_{n\geq 1} A_n$. Εφοδιάζοντας τα A_n με τη διακριτή τοπολογία, και το $\prod A_n$ με την τοπολογία του καρτεσιανού γινομένου, ο δακτύλιος $\mathbb{Z}_p$ κληρονομεί τοπολογία, τέτοια ώστε να είναι συμπαγής μετρικός χώρος. Τη συμπάγεια του $\mathbb{Z}_p$ θα την μελετήσουμε σε επόμενη ενότητα.

Πρόταση 17 *Η ακολουθία* $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varpi_n} A_n \to 0$ *είναι ακριβής. Με* p^n *συμβολίζουμε τον πολλαπλασιασμό κάθε στοιχείου με* p^n*, όπου* $n \in \mathbb{N}$*, και με* ϖ_n *συμβολίζουμε τη συνάρτηση προβολή του* p*-αδικού ακεραίου* x *στο* n*-οστό του όρο* x_n*.*

Απόδειξη: Για να είναι η ακολουθία ακριβής πρέπει κατ' αρχάς να δείξουμε ότι $Im(0) = Ker(p^n)$ για κάθε n. Αρκεί να το δείξουμε για $n = 1$ και τότε ο ισχυρισμός 'για κάθε n' προκύπτει άμεσα.

Ας προσδιορίσουμε τον πυρήνα της συνάρτησης $x \to p\,x$. Ο πολλαπλασιασμός με το p είναι συνάρτηση ένα προς ένα στο $\mathbb{Z}_p$. Αν για κάποιο p-αδικό ακέραιο $x = (x_k)$ έχουμε $p\,x = 0$, τότε $p\,x_{k+1} = 0 \pmod{p^{k+1}}$ για κάθε $k \in \mathbb{N}$, και άρα $x_{k+1} = 0 \pmod{p^k}$ για κάθε $k \in \mathbb{N}$.

Παρατηρούμε ότι κάτι τέτοιο δεν μπορούμε να ισχυριστούμε για την περίπτωση $k = 0$, διότι από την ισοδυναμία $px_0 \equiv 0 \pmod{p}$ δεν μπορούμε να συμπεράνουμε ότι $x_0 \equiv 0 \pmod{p}$. Όμως, από τη συνθήκη της συνέπειας έχουμε ότι αν $x_{k+1} \equiv 0 \pmod{p}^k$, τότε:

$$0 \equiv x_{k+1} \equiv x_k \pmod{p^k} \Rightarrow x_k \equiv 0 \pmod{p^k}.$$

Άρα, η απαίτηση $p\,x = 0$ συνεπάγεται $x_k = 0$ για κάθε μη αρνητικό ακέραιο k, δηλαδή $Im(0) = Ker(p)$, επομένως η συνάρτηση p είναι ένα προς ένα.

Επιπλέον, πρέπει να δείξουμε ότι $Im(p^n) = ker(\varpi_n)$. Δηλαδή ότι η εικόνα κάθε p-αδικού ακεραίου μέσω της p^n, είναι ένα στοιχείο $x' \in \mathbb{Z}_p$, τέτοιο ώστε

$\varpi_n(x') = 0 \Leftrightarrow x'_n \equiv 0 \pmod{p^n}$, και αντιστρόφως, ότι κάθε στοιχείο του πυρήνα της ϖ_n είναι της μορφής $p^n\, y$, όπου $y \in \mathbb{Z}_p$.

Ο πρώτος ισχυρισμός προκύπτει άμεσα, αφού:

$$x' = p^n\, x \Rightarrow x'_n = p^n\, x_n \Rightarrow \varpi_n(x') = x'_n \equiv 0 \pmod{p^n} \rightarrow x' \in kern(\varpi_n).$$

Ο δεύτερος ισχυρισμός προκύπτει από την ιδιότητα της συνέπειας της ακολουθίας $x = (x_n)$ ως ακολούθως:

$$x \in ker(\varpi_n) \Leftrightarrow x_n \equiv 0 \pmod{p^n} \Leftrightarrow x_n = ap^n,\ a \in A_n.$$

Έστω $m \leq n$. Αν έχουμε ότι για κάποιον όρο x_m ισχύει $x_m \equiv 0 \pmod{p^n}$, που είναι και η δική μας περίπτωση, τότε:

$$x_{m-1} \equiv x_m \equiv ap^n \equiv 0 \pmod{p^{m-1}}.$$

Δηλαδή, όλοι οι προηγούμενοι όροι είναι μηδέν modulo p υψωμένο σε δύναμη ίση με το δείκτη του όρου.
Έστω τώρα $m > n$. Και πάλι, αν έχουμε ότι για κάποιον όρο x_m ισχύει $x_m \equiv 0 \pmod{p^n}$, τότε:

$$x_{m+1} \equiv x_m \equiv ap^n \equiv 0 \pmod{p^n} \Leftrightarrow p^n \mid x_{m+1}.$$

Επομένως μπορούμε να βγάλουμε κοινό παράγοντα το p^n από όλους τους όρους της ακολουθίας. Δηλαδή, $x = p^n y$, όπου το y είναι ένα στοιχείο του $\mathbb{Z}_p$. Πράγματι, για $m > n$, έχουμε:

$$y_{m+1} \equiv \frac{x_{m+1}}{p^n} \equiv \frac{x_m}{p^n} \pmod{p^m},$$

δηλαδή η ακολουθία (y_n) είναι συνεπής, και άρα το $y \in \mathbb{Z}_p$. □

Πρόταση 18 *Ο δακτύλιος εκτίμησης του $\mathbb{Q}_p$ ως προς την p-αδική νόρμα είναι το σύνολο των p-αδικών ακεραίων, δηλαδή*

$$\mathcal{O}_p = \mathbb{Z}_p.$$

Απόδειξη: Το ότι $\mathcal{O}_p \subset \mathbb{Z}_p$ προκύπτει άμεσα από την Πρόταση 16. Για το αντίστροφο έχουμε τα εξής:

- Κάθε $x \in \mathbb{Z}_p$ ανήκει και στο $\mathbb{Q}_p$, αφού είναι μια ακολουθία Cauchy ρητών αριθμών.
- Για κάθε $x \in \mathbb{Z}_p$ ισχύει ότι $|x|_p \leq 1$. Πράγματι, η νόρμα του p-αδικού αριθμού x είναι ίση με το όριο των νορμών των όρων x_n. Όμως, από το Λήμμα 6, η ακολουθία των νορμών των όρων x_n είναι σταθερή και ίση με τη νόρμα ενός ακεραίου, για την οποία γνωρίζουμε ότι είναι μικρότερη ή ίση του ένα.

□

Λήμμα 7 *Η συνάρτηση $h : \mathbb{Q}_p \to \mathbb{Q}_p$ με $h(x) = p\,x$ είναι ομοιομορφισμός.*

Απόδειξη: Η h είναι προφανώς ένα προς ένα και επί. Επιπλέον, η h όπως και η h^{-1} είναι συνεχείς, αφού οι πράξεις του πολλαπλασιασμού στο σώμα $\mathbb{Q}_p$ είναι συνεχείς συναρτήσεις ως προς την p-αδική μετρική. □

Πρόταση 19 *Το σώμα των p-αδικών αριθμών $\mathbb{Q}_p$ είναι το σώμα $\mathbb{Z}_p[1/p]$.*

Απόδειξη: Έστω $x \in \mathbb{Z}_p[1/p]$. Τότε:

$$\begin{aligned} & x = x_0 + x_1\tfrac{1}{p} + \cdots + x_n\tfrac{1}{p^n}, \quad x_i \in \mathbb{Z}_p,\ n \geq 0 \Leftrightarrow \\ & x = p^{-n}(x_0 p^n + x_1 p^{n+1} + \cdots + x_n) \Leftrightarrow \\ & x = p^{-n}\alpha,\ \alpha \in \mathbb{Z}_p \Rightarrow \\ & x \in \mathbb{Q}_p, \end{aligned}$$

από Λήμμα 7 και Πρόταση 17.

Έστω $x \in \mathbb{Q}_p$. Τότε $|x|_p = p^{\upsilon_p(x)}$. Αν $\upsilon_p(x) > 0$, τότε $x \in \mathbb{Z}_p$ και άρα $x \in \mathbb{Z}_p[1/p]$. Έστω λοιπόν $\upsilon_p(x) < 0$. Τότε $p^{-\upsilon_p(x)}x \in \mathbb{Z}_p$, αφού $\left|p^{-\upsilon_p(x)}x\right|_p = 0$. Δηλαδή έχουμε:

$$p^{-\upsilon_p(x)}x = \alpha,\ \alpha \in \mathbb{Z}_p \Leftrightarrow x = p^{\upsilon_p(x)}\alpha \in \mathbb{Z}_p[1/p].$$

□

Πόρισμα 3 *Κάθε p-αδικός αριθμός x μπορεί να γραφεί ως:*

$$x = p^{\upsilon_p(x)}\alpha,\ \alpha \in \mathbb{Z}_p.$$

Επιπλέον, ισχύει ότι $p \nmid \alpha$.

Απόδειξη: Το ζητούμενο προκύπτει από το δεύτερο κομμάτι της προηγούμενης απόδειξης. Όσο για τον τελευταίο ισχυρισμό για το α, αυτός προκύπτει άμεσα από τον ορισμό της p-αδικής εκτίμησης. □

3.4 Ο δακτύλιος $\mathbb{Z}_p$

Στην προηγούμενη ενότητα κατασκευάσαμε τους p-αδικούς ακεραίους για να πάρουμε το σώμα των p-αδικών αριθμών. Μάλιστα, ο δακτύλιος αυτός ταυτίστηκε με το δακτύλιο εκτίμησης του $\mathbb{Q}_p$. Το πρώτο πράγμα που θα δούμε σε αυτή την ενότητα είναι το πώς μπορούμε να απεικονίσουμε τα στοιχεία του $\mathbb{Z}_p$. Στη συνέχεια, θα δούμε σημαντικές ιδιότητές του, εφοδιασμένοι πια με την p-αδική μετρική.

Επιστρέφουμε στην Πρόταση 16 για να δούμε πώς μπορούμε να σκεφτόμαστε τα στοιχεία του $\mathbb{Z}_p$. Έχουμε αποδείξει ότι για κάθε x p-αδικό ακέραιο μπορούμε να βρούμε ακολουθία Cauchy ακεραίων (a_n) που συγκλίνει στο x, τέτοια ώστε:

- $a_n \equiv x \pmod{p^n}$
- $a_{n+1} \equiv a_n \pmod{p^n}$
- $0 \leq a_n \leq p^n - 1$.

Οι όροι a_n ως ακέραιοι αριθμοί, μπορούν να γραφούν ως πεπερασμένα αθροίσματα της μορφής:

$$a_n = b_0 + b_1 p + \cdots + b_{n-1} p^{n-1},$$

όπου οι συντελεστές b_i ανήκουν στο σύνολο $\{0, 1, \ldots, p-1\}$. Επιτυγχάνουμε έτσι να απλοποιήσουμε την πράξη modulo p^n, που ισοδυναμεί έτσι με την αποκοπή όλων των όρων, εκτός των n πρώτων. Από αυτή την οπτική, η συνθήκη της συνέπειας της ακολουθίας (a_n) λέει απλώς ότι οι $n+1$ πρώτοι όροι των αναπτυγμάτων των δύο διαδοχικών αριθμών a_n, a_{n+1} είναι οι ίδιοι:

$$
\begin{array}{ll}
a_0 = b_0 & 0 \leq b_0 \leq p-1 \\
a_1 = b_0 + b_1 p & 0 \leq b_1 \leq p-1 \\
a_2 = b_0 + b_1 p + b_2 p^2 & 0 \leq b_2 \leq p-1 \\
a_3 = b_0 + b_1 p + b_2 p^2 + b_3 p^3 & 0 \leq b_3 \leq p-1 \\
\text{κ.ο.κ.} &
\end{array}
$$

Παίρνουμε έτσι ένα άπειρο p-αδικό ανάπτυγμα για το x,

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots .$$

Λήμμα 8 *Για κάθε $x \in \mathbb{Z}_p$, η σειρά $x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$, όπως αποκτήθηκε παραπάνω, συγκλίνει στο x.*

Απόδειξη: Μία σειρά συγκλίνει αν και μόνο αν η ακολουθία των μερικών αθροισμάτων συγκλίνει. Όμως, τα μερικά αθροίσματα στην προκειμένη περίπτωση είναι τα a_n, τα οποία ξέρουμε ότι συγκλίνουν στο x. □

Πόρισμα 4 *Κάθε $x \in \mathbb{Z}_p$ μπορεί να αναπαρασταθεί ως:*

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots ,$$

με $0 \leq b_i \leq p-1$, και η αναπαράσταση αυτή είναι μοναδική.

Απόδειξη: Έχουμε αποδείξει τα πάντα εκτός από τη μοναδικότητα των b_i, η οποία όμως προκύπτει άμεσα από τη μοναδικότητα των a_i. □
Επομένως, μια διαφορετική απεικόνιση του $\mathbb{Z}_p$ είναι το σύνολο των δυναμοσειρών:

$$\mathbb{Z}_p = \left\{ \sum_{n=0}^{\infty} b_n p^n : \ b_n \in \{0, 1, \ldots, p-1\} \right\}.$$

Ορισμός 23 Οι *p-αδικές μονάδες* $\mathbb{Z}_p^{\times}$ είναι το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_p$.

Πρόταση 20 *(i) Ένα στοιχείο του $\mathbb{Z}_p$ είναι αντιστρέψιμο αν και μόνο αν δεν διαιρείται από τον p.*

(ii) Έστω $\mathbb{Z}_p^\times$ η ομάδα των αντιστρέψιμων στοιχείων του $\mathbb{Z}_p$. Τότε, κάθε μη μηδενικό στοιχείο του $\mathbb{Z}_p$ μπορεί να γραφεί μοναδικά ως $p^n u$, όπου $u \in U$ και $n \geq 0$.

Απόδειξη:

(i) Αρκεί να αποδείξουμε ότι τα αντιστρέψιμα στοιχεία των A_n είναι αυτά που δεν διαιρούνται με το p, και ο ισχυρισμός έπεται για το $\mathbb{Z}_p$. Όμως, για να έχει λύση η εξίσωση $ax \equiv 1 \pmod{p^n}$ πρέπει $\gcd(a, p^n) \mid 1$, δηλαδή οι a, p^n να είναι πρώτοι μεταξύ τους, ισοδύναμα $p \nmid a$.

(ii) Έστω $x = (x_n) \in \mathbb{Z}_p$ μη μηδενικό. Τότε, υπάρχει μέγιστος ακέραιος n, τέτοιος ώστε $x_n \equiv 0 \pmod{p^n}$, από όπου προκύπτει ότι $x_m \equiv 0 \pmod{p^m}$ για κάθε $m \leq n$ (βλ. Πρόταση 17). Έτσι $x = p^n \alpha$ με $p \nmid \alpha$, δηλαδή $\alpha \in \mathbb{Z}_p^\times$.

□

Πρόταση 21 *Οι p-αδικές μονάδες είναι το σύνολο:*

$$\mathbb{Z}_p^\times = \left\{ x \in \mathbb{Q}_p : \ |x|_p = 1 \right\}.$$

Επιπλέον,

$$\mathbb{Z}_p^\times \cap \mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{Q} : \ p \nmid ab \right\}.$$

Απόδειξη: Έχουμε:

$$x \in \mathbb{Z}_p \Rightarrow |x|_p \leq 1$$

και

$$x^{-1} \in \mathbb{Z}_p \Rightarrow \left|x^{-1}\right|_p = |x|_p^{-1} \leq 1.$$

Οπότε το $x \in \mathbb{Z}_p$ είναι αντιστρέψιμο στο $\mathbb{Z}_p$ αν και μόνο αν $|x|_p = |x^{-1}|_p = 1$.

Το δεύτερο κομμάτι προκύπτει εύκολα, αφού $\mathbb{Z}_p \cap \mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{Q} : \ p \nmid b \right\}$. □

Όπως σε κάθε δακτύλιο, το σύνολο των p-αδικών μονάδων αποτελέι πολλαπλασιαστική ομάδα. Μάλιστα, αποτελείται από πάρα πολλά στοιχεία. Όπως φαίνεται και από το δεύτερο κομμάτι της πρότασης όλοι οι ρητοί με μηδενική p-αδική εκτίμηση ανήκουν στο $\mathbb{Z}_p^\times$.

Πρόταση 22 *Έστω $x \in \mathbb{Z}_p$. Τότε το x είναι μονάδα αν και μόνο αν έχει μη μηδενικό σταθερό όρο.*

Απόδειξη: Έστω το p-αδικό ανάπτυγμα του x:

$$x = b_0 + b_1 p + \cdots + b_n p^n + \cdots.$$

Προφανώς, αν το x είναι μονάδα, τότε:

$$1 = |x|_p \Leftrightarrow 1 = |b_0 + b_1 p + \cdots|_p \leq \max\left\{|b_0|_p, |b_1 p|_p, \ldots\right\}.$$

Όμως, τα $b_i p^i$ είναι ακέραιοι αριθμοί και συνεπώς έχουν νόρμα μικρότερη ή ίση του ένα. Επιπλέον οι $b_1 p$, $b_2 p^2, \ldots$, προφανώς διαιρούνται με τον p, και άρα η νόρμα τους είναι μικρότερη της μονάδας, δηλαδή $|b_0|_p = \max\left\{|b_0|_p, |b_1 p|_p, \ldots\right\}$. Έτσι:

$$1 = |x|_p = |b_0|_p \Leftrightarrow p \nmid b_0.$$

Αντίστροφα, αν $b_0 = 0$, τότε μπορούμε να βγάλουμε κοινό παράγοντα τουλάχιστον p από όλους τους υπόλοιπους όρους, και άρα η p-αδική νόρμα είναι μικρότερη του 1. □

3.5 Ανάλυση στο $\mathbb{Z}_p$

Κατ' αρχάς, θα δείξουμε ένα σημαντικό αποτέλεσμα για τις άπειρες ακολουθίες p-αδικών ακεραίων και έπειτα θα μελετήσουμε τη συμπάγεια του $\mathbb{Z}_p$.

Πρόταση 23 *Κάθε άπειρη ακολουθία p-αδικών ακεραίων έχει συγκλίνουσα υπακολουθία.*

Απόδειξη: Έστω (x_n) άπειρη ακολουθία στο $\mathbb{Z}_p$. Μπορούμε να γράψουμε κάθε όρο x_i ως p-αδικό ανάπτυγμα, δηλαδή ως:

$$x_i = x_{i0} + x_{i1} p + x_{i2} p^2 + \cdots, \quad x_{ij} \in \{0, 1, \ldots, p-1\}.$$

Κατασκευάζουμε τη ζητούμενη υπακολουθία ως εξής: εφόσον η ακολουθία (x_n) είναι άπειρη και το πλήθος των δυνατών συντελεστών x_{ij} πεπερασμένο, θα υπάρχουν άπειροι το πλήθος όροι που θα έχουν ως πρώτο συντελεστή x_{i0} κάποιον $b_0 \in \{0, 1, \ldots, p-1\}$. Συμβολίζουμε τους όρους αυτούς ως $X_{01}, X_{02}, \ldots$. Η ακολουθία (X_{0n}) είναι μια άπειρη υπακολουθία της (x_n).

Μπορούμε να κάνουμε την ίδια σκέψη για την ακολουθία X_{0n} και το δεύτερο συντελεστή κάθε όρου. Υπάρχουν άπειροι όροι της ακολουθίας με δεύτερο συντελεστή κάποιον $b_1 \in \{0, 1, \ldots, p-1\}$. Συμβολίζουμε με X_{1n} την άπειρη υπακολουθία της X_{0n}, με όρους της μορφής:

$$X_{1j} = b_0 + b_1 p + x_{1j2} p^2 + \cdots.$$

Συνεχίζοντας τη διαδικασία αυτή παίρνουμε μία ακολουθία άπειρων υπακολουθιών της x_n:

$$\begin{aligned}(X_{0n}) &= X_{01}, X_{02}, \ldots, X_{0n}, \ldots \\ (X_{1n}) &= X_{11}, X_{12}, \ldots, X_{1n}, \ldots \\ (X_{2n}) &= X_{21}, X_{22}, \ldots, X_{2n}, \ldots \\ &\vdots\end{aligned}$$

για την οποία ισχύουν ότι κάθε ακολουθία (X_{ij}) είναι υπακολουθία της προηγούμενής της $(X_{(i-1)j})$, και σε κάθε υπακολουθία (X_{ij}) οι πρώτοι i συντελεστές είναι οι $b_0, b_1, \ldots, b_i$.

Αν θεωρήσουμε την ακολουθία $(X_n) = (X_{nn})$, τότε αυτή προφανώς είναι υπακολουθία της (x_n) και επιπλέον είναι Cauchy ως προς την p-αδική νόρμα, άρα συγκλίνουσα (Λήμμα 9). □

Ορισμός 24 Ένα σύνολο X λέγεται *συμπαγές*, όταν οποιοδήποτε κάλυμμα του X έχει πεπερασμένο υποκάλυμμα. Ένας μετρικός χώρος λέγεται *τοπικά συμπαγής*, όταν κάθε κάθε σημείο του χώρου έχει γειτονιά που είναι συμπαγές σύνολο.

Πρόταση 24 *Ο δακτύλιος $\mathbb{Z}_p$ είναι συμπαγής.*

Απόδειξη: Θα δείξουμε ότι το $\mathbb{Z}_p$ είναι πλήρες και ολικά φραγμένο. Είναι πλήρες διότι είναι κλειστό υποσύνολο του πλήρους μετρικού χώρου $\mathbb{Q}_p$ (εξ' άλλου είναι η πλήρωση του $\mathbb{Z}$ ως προς την p-αδική μετρική).

Μένει να δείξουμε ότι είναι ολικά φραγμένος, ότι δηλαδή για κάθε $\epsilon > 0$ το $\mathbb{Z}_p$ μπορεί να καλυφθεί από πεπερασμένες το πλήθος μπάλες ακτίνας ϵ. Αρκεί να πάρουμε $\epsilon_n = p^{-n}$, $n \geq 0$.

Τότε έχουμε ότι:

$$\mathbb{Z}_p \subset \cup_{a\in\mathbb{F}_{p^n}} a + p^n\mathbb{Z}_p.$$

Πράγματι, έχουμε ότι το $\mathbb{Z}$ είναι πυκνό στο $\mathbb{Z}_p$ και άρα οι μπάλες $a+p^n\mathbb{Z}_p$, $a \in \mathbb{Z}$ καλύπτουν το $\mathbb{Z}_p$. Όμως, για δύο ακεραίους που ανήκουν στην ίδια κλάση ισοδυναμίας modulo p^n, δηλαδή $a_1 \equiv a_2 \pmod{p^n}$, έχουμε:

$$|a_1 - a_2|_p \leq p^{-n}, \quad \text{αφού τουλάχιστον το } p^n \text{ διαιρεί το } a_1 - a_2.$$

Αν $x \in a_1 + p^n\mathbb{Z}_p$ τότε $|x - a_1|_p \leq p^{-n}$ και

$$|x - a_2|_p \leq \max\left\{|x - a_1|_p\,,\, |a_1 - a_2|_p\right\} = p^{-n},$$

δηλαδή $x \in a_2 + p^n\mathbb{Z}_p$.

Εναλλάσσοντας τα a_1, a_2 παίρνουμε ότι και $a_1+p^n\mathbb{Z}_p \supset a_2+p^n\mathbb{Z}_p$. Καταλήγουμε στο ότι για δύο ισοϋπόλοιπους modulo p^n ακεραίους έχουμε:

$$a_1 + p^n\mathbb{Z}_p = a_2 + p^n\mathbb{Z}_p,$$

και άρα το $\mathbb{Z}_p$ μπορεί να καλυφθεί από πεπερασμένες το πλήθος μπάλες ακτίνας p^{-n}. Μάλιστα, το πλήθος των μπαλών είναι p^n, όσα δηλαδή και τα διαφορετικά υπόλοιπα modulo p^n, γεγονός αναμενόμενο αν σκεφτούμε ότι $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Γνωρίζουμε όμως, ότι κάθε πλήρες και ολικά φραγμένο υποσύνολο ενός μετρικού χώρου είναι συμπαγές (βλ. για παράδειγμα [1]), άρα το ζητούμενο απεδείχθη. □

Ορισμός 25 Ένα *θεμελιώδες σύνολο γειτονιών* X_i, $i \in I$, είναι ένα σύνολο γειτονιών, τέτοιο ώστε για κάθε άλλη γειτονιά A να ισχύει $X_i \subset A$ για κάποιο $i \in I$.

Ορισμός 26 Μιά συλλογή συνόλων *καλύπτει* ένα σύνολο X αν η ένωση όλων των συνόλων που ανήκουν σε αυτήν περιέχει το σύνολο X.

Πόρισμα 5 *Τα σύνολα* $p^n\mathbb{Z}_p$, $n \in \mathbb{Z}$ *αποτελούν ένα θεμελιώδες σύστημα γειτονιών του μηδενός στο* $\mathbb{Q}_p$, *που καλύπτει το* $\mathbb{Q}_p$.

Απόδειξη: Κατ' αρχάς τα σύνολα $p^n\mathbb{Z}_p,\ n \in \mathbb{Z}$ αποτελούν ένα σύστημα γειτονιών του μηδενός στο $\mathbb{Q}_p$, δηλαδή κάθε $p^n\mathbb{Z}_p$ περιέχει μία ανοικτή μπάλα με κέντρο το μηδέν.

Θυμόμαστε ότι η ανοικτή μπάλα $B(0,\, p^{-(n-1)})$ ταυτίζεται με την κλειστή μπάλα $\overline{B}(0,\, p^{-n}),$ η οποία ταυτίζεται με το $p^n\mathbb{Z}_p$. Πράγματι, $\overline{B}(0,\, p^{-n}) \subset B(0,\, p^{-(n-1)})$. Θα δείξουμε και το αντίστροφο:

$$x \in B(0, p^{-(n-1)}) \Leftrightarrow |\, x|_p < p^{-(n-1)} = \left|p^{n-1}\right|_p \Leftrightarrow \left|\frac{x}{p^{n-1}}\right|_p < 1.$$

Τότε όμως

$$\left|\frac{x}{p^{n-1}}\right|_p \leq \frac{1}{p} \Leftrightarrow |\, x|_p \leq \frac{p^{-(n-1)}}{p} = p^{-n}.$$

Για το δεύτερο κομμάτι του ισχυρισμού έχουμε:

$$x \in \overline{B}(0, p^n) \Leftrightarrow |\, x|_p \leq p^n \Leftrightarrow |xp^n|_p \leq 1 \Leftrightarrow xp^n \in \mathbb{Z}_p \Leftrightarrow x \in p^{-n}\mathbb{Z}_p.$$

Άρα κάθε $p^n\mathbb{Z}_p$ είναι μια γειτονιά του μηδενός.

Θα δείξουμε ότι το σύστημα αυτό είναι ένα θεμελιώδες σύστημα γειτονιών. Έστω Γ μια γειτονιά του $0 \in \mathbb{Q}_p$. Τότε περιέχει μια ανοικτή μπάλα γύρω από το μηδέν, δηλαδή κάποια $B(0, \epsilon)$ για $\epsilon > 0$. Ισοδύναμα θα περιέχει κάποια κλειστή μπάλα $\overline{B}(0, p^n),\ n \in \mathbb{Z}$, οπότε και το $p^{-n}\mathbb{Z}_p$.

Τέλος, το σύστημα αυτό καλύπτει το $\mathbb{Q}_p$, δηλαδή:

$$\mathbb{Q}_p \ \subset \bigcup_{n\in\mathbb{Z}} p^n\mathbb{Z}_p \Rightarrow x \in \overline{B}(0,\, p^{-n}).$$

Αυτό προκύπτει από την Πρόταση 19, αφού για κάθε p-αδικό αριθμό x έχουμε $x = p^{v_p(x)}\alpha$, όπου $\alpha \in \mathbb{Z}_p$. Άρα $x \in p^{v_p(x)}\mathbb{Z}_p$.

□

Ένα πολύ σημαντικό συμπέρασμα όσων αναφέραμε μέχρι τώρα είναι το πόσο στενά συνδεδεμένες είναι η τοπολογία και η αλγεβρική δομή του $\mathbb{Q}_p$. Για παράδειγμα, έχουμε ότι για οποιαδήποτε $x,\, y \in \mathbb{Q}_p$ ισχύει:

$$|x - y|_p \leq p^{-n} \quad \text{αν και μόνο αν} \quad x - y \in p^n\mathbb{Z}_p \Leftrightarrow x \equiv y \pmod{p^n\mathbb{Z}_p}.$$

Τα σύνολα $p^n\mathbb{Z}_p$ είναι ιδεώδη του $\mathbb{Z}_p$ και τα σύμπλοκά τους, $\alpha + p^n\mathbb{Z}_p$, όπου $\alpha \in \mathbb{Z}_p$, είναι μπάλες του $\mathbb{Q}_p$.

Επίσης, έχουμε το εξής πολύ σημαντικό αποτέλεσμα:

Πρόταση 25

$$\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}}.$$

Απόδειξη: Αν σκεφτούμε ότι κάθε στοιχείο στο $\mathbb{Z}_p$ είναι όριο ακολουθίας Cauchy ακεραίων (a_n), τότε η απεικόνιση:

$$\alpha + p^n\mathbb{Z}_p \longrightarrow n\text{-οστός όρος της ακολουθίας Cauchy}$$

είναι ο ζητούμενος ισομορφισμός. □

3.6 Απεικονίσεις των p-αδικών αριθμών

Σε προηγούμενη ενότητα είδαμε πώς οι p-αδικοί ακέραιοι μπορούν να αναπαρασταθούν ως αθροίσματα θετικών δυνάμεων του p. Ανάλογα, παίρνουμε την έκφραση ενός p-αδικού αριθμού ως άθροισμα δυνάμεων του p.

Πρόταση 26 *Κάθε $x \in \mathbb{Q}_p$ μπορεί να αναπαρασταθεί μοναδικά ως:*

$$\begin{aligned} x &= b_{-n_0}p^{-n_0} + \cdots + b_0 + b_1p + \cdots + b_np^n + \cdots \\ &= \textstyle\sum_{n\geq -n_0} b_np^n, \end{aligned}$$

όπου $0 \leq b_n \leq p-1$ και $-n_0 = v_p(x)$.

Απόδειξη: Η μορφή της αναπαράστασης και η μοναδικότητα προκύπτει από το γεγονός ότι κάθε p-αδικός αριθμός μπορεί να γραφεί ως $x = p^na$, όπου $n \in \mathbb{Z}$ και $a \in \mathbb{Z}_p$ (Πόρισμα 3), και από το ότι κάθε p-αδικός ακέραιος γράφεται μοναδικά ως άπειρο άθροισμα θετικών δυνάμεων του p (Πόρισμα 4).

Η p-αδική εκτίμηση του $x \in \mathbb{Q}_p$ είναι προφανώς ίση με το $-n_0$. Πράγματι, παρατηρούμε ότι ισχύουν:

- $b_{-n_0} \neq 0$,
- $p \nmid \sum_{n\geq 0} b_np^n \Leftrightarrow b_0 \neq 0 \Rightarrow \left|\sum_{n\geq 0} b_np^n\right|_p = 1$ και
- $$\begin{aligned} x &= \textstyle\sum_{n\geq -n_0} b_np^n = p^{-n_0}\sum_{n\geq -n_0} b_np^{n+n_0} \\ &= p^{-n_0}(b_{-n_0} + b_{-n_0+1}p + \cdots + b_0p^{n_0} + \cdots). \end{aligned}$$

Έτσι, αν πάρουμε p-αδικές νόρμες και στα δύο μέλη της τελευταίας ισότητας έχουμε:

$$p^{-\upsilon_p(x)} = |\,x|_p = \left|p^{-n_0}\right|_p \left|\sum_{n\geq -n_0} b_n p^{n+n_0}\right|_p = \left|p^{-n_0}\right|_p = p^{n_0}$$

$$\Rightarrow \upsilon_p(x) = -n_0.$$

□

Η παραπάνω πρόταση επιβεβαιώνει τη διαισθητική εικόνα που είχαμε για τους p-αδικούς ακεραίους ως άπειρα αναπτύγματα σε βάση p. Τα b_n δεν είναι απαραίτητο να ικανοποιούν τη συνθήκη $0 \leq b_n \leq p-1$. Μπορεί μάλιστα να μην είναι καν ακέραιοι αριθμοί. Είναι εκπρόσωποι των συμπλόκων $\mathbb{Z}_p/p\mathbb{Z}_p$, συνεπώς μπορούν να είναι οποιοδήποτε στοιχείο ανήκει στην εκάστοτε κλάση.

Πόρισμα 6 *Κάθε p-αδικός αριθμός x μπορεί να γραφεί ως:*

$$x = p^{\upsilon_p(x)}\alpha,\ \alpha \in \mathbb{Z}_p^*.$$

Απόδειξη: Προκύπτει άμεσα από την Πρόταση 26 και το Πόρισμα 3. □

Όταν μελετούμε έναν μετρικό χώρο είναι συχνά χρήσιμη η διαίσθηση που έχουμε για την έννοια της απόστασης. Στο $\mathbb{Z}$, στο $\mathbb{Q}$ και στο $\mathbb{R}$ με την απόλυτη τιμή τοποθετούμε τα στοιχεία πάνω σε μία ευθεία, και οι μπάλες είναι ευθύγραμμα τμήματα της ευθείας αυτής. Στο $\mathbb{Z}\times\mathbb{Z}$, στο $\mathbb{Q}\times\mathbb{Q}$, στο $\mathbb{R}\times\mathbb{R}$ ή στο $\mathbb{C}$ με την ευκλείδεια νόρμα χρησιμοποιούμε το καρτεσιανό επίπεδο. Μία μπάλα είναι ένας κύκλος γύρω από το σημείο-κέντρο της μπάλας.

Σε έναν ουλτραμετρικό χώρο, δηλαδή σε έναν χώρο όπου η μετρική ικανοποιεί τη μη αρχιμήδεια ιδιότητα:

$$d(x,z) \leq \max\{d(x,y), d(y,z)\}$$

η ευθεία ή το καρτεσιανό επίπεδο δεν ανταποκρίνονται καθόλου στις ιδαιτερότητες που παρατηρήσαμε στο προηγούμενο κεφάλαιο. Το πιο κατάλληλο μοντέλο για την απεικόνιση των p-αδικών αριθμών φαίνεται να είναι αυτό του δέντρου.

Σημειώνουμε ότι ένα δέντρο χαρακτηρίζεται από ιεραρχική διάταξη: κάθε κόμβος βρίσκεται σε υψηλότερο επίπεδο από ότι τα ''παιδιά'' του.

Ας δούμε μέσα από ένα παράδειγμα πώς η δομή του δέντρου περιγράφει καλύτερα τους ουλτραμετρικούς χώρους. Για τους 3-αδικούς ακέραιους και τις μεταξύ τους αποστάσεις θα είχαμε κάτι σαν το Σχήμα 3.1. Κάθε ιεραρχικό επίπεδο κόμβων του δέντρου αντιστοιχεί σε ένα 'επίπεδο 3-αδικής απόστασης' και κάθε κόμβος έχει ακριβώς τρία κλαδιά. Θα μπορούσαμε να βλέπουμε κάθε επίπεδο απόστασης ως τη νόρμα ενός 3-αδικού ακεραίου.

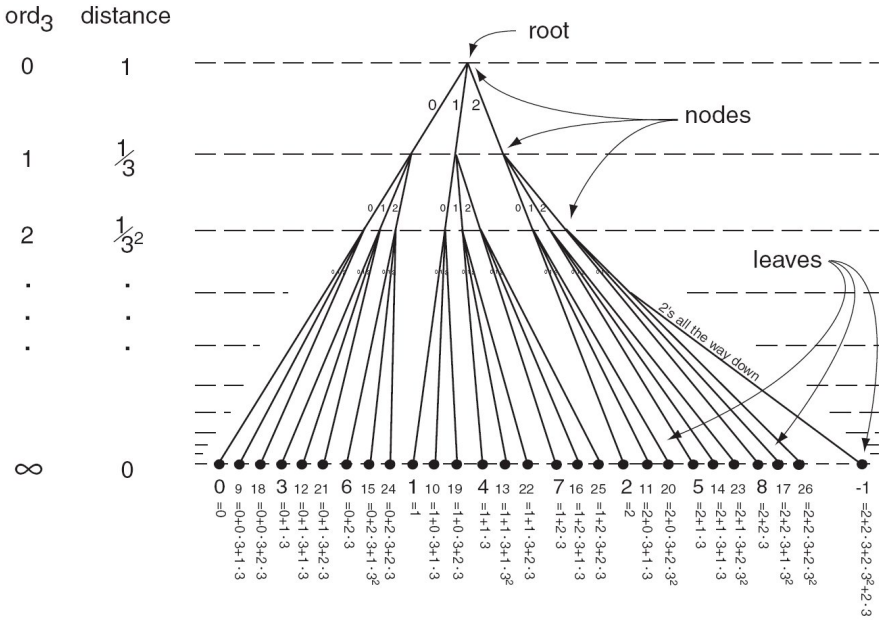
Τα κλαδιά ενός κόμβου στο επίπεδο όπου $ord_3 = i$ σχετίζονται με το ψηφίο a_i του αναπτύγματος του 3-αδικού ακεραίου, $\sum a_i p^i$. Ξεκινώντας από τη ρίζα και κάνοντας συγκεκριμένες επιλογές για τους συντελεστές a_i, καταλήγουμε σε κάποιον 3-αδικό ακέραιο (για ευκολία στο Σχήμα 3.1 απεικονίζονται μόνο ακέραιοι αριθμοί).

Η απόσταση μεταξύ δύο p-αδικών αριθμών είναι ίση με την τιμή της απόστασης στο επίπεδο εκείνο, από το οποίο και έπειτα οι δύο αριθμοί ακολουθούν διαφορετική πορεία στο δέντρο. Για παράδειγμα, οι $x = 2 + 1 \cdot 3 + 1 \cdot 3^2$ και $y = 2 + 2 \cdot 3^2$ ξεκινούν να διαφέρουν στο δεύτερο ψηφίο, συνεπώς η αποστασή τους είναι ίση με αυτή του δευτέρου επιπέδου, δηλαδή $1/3$. Πράγματι, $|x - y|_3 = |3 - 3^2|_3 = 1/3$. Χάρην απλότητος θα ταυτίζουμε το επίπεδο με την τιμή της απόστασης που αντιστοιχεί σε αυτό. Αν ξεκινήσουμε από τα φύλλα του δέντρου, η απόσταση δύο αριθμών x, y δίνεται από το επίπεδο στο οποίο συναντιούνται για πρώτη φορά τα ''μονοπάτια'' των συντελεστών τους.

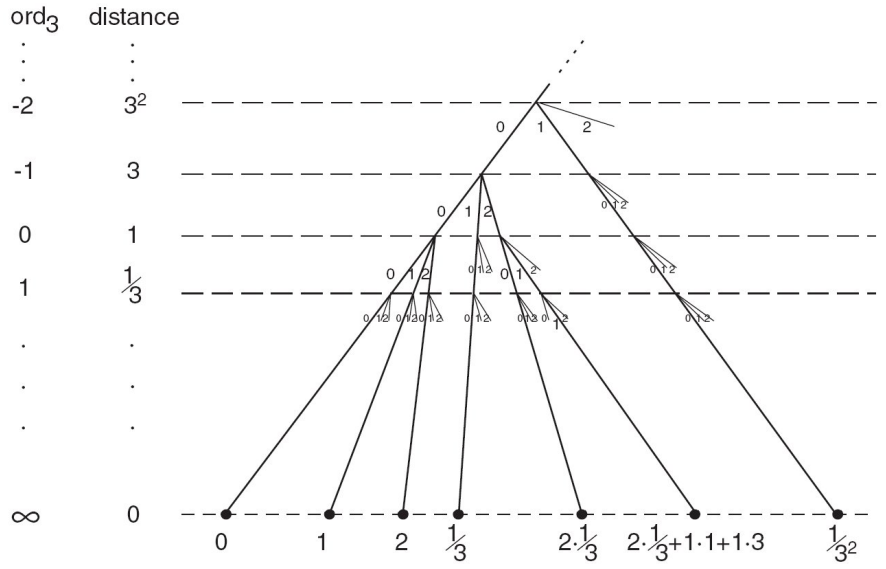
Παρατηρούμε ότι υπάρχουν άπειρα δυνατά επίπεδα απόστασης στο δέντρο του σχήματος και ότι υπάρχουν άπειροι ακέραιοι σε ολόκληρο το δέντρο. Ακόμα, το δέντρο είναι μοναδικό, αν εξαιρέσουμε τις αναδιατάξεις των κλαδιών.

Για να αποκτήσουμε την εικόνα των p-αδικών αριθμών πρέπει να επεκτείνουμε το δέντρο προς τα πάνω, ώστε να έχουμε επίπεδα και για τις θετικές δυνάμεις του p. Έτσι, το δέντρο για τους p-αδικούς αριθμούς δεν έχει ρίζα, όπως το δέντρο για τους p-αδικούς ακεραίους, αλλά είναι άπειρο και προς τα πάνω και προς τα κάτω. Στο σχήμα 3.2 φαίνεται ένα δέντρο για τους 3-αδικούς αριθμούς.

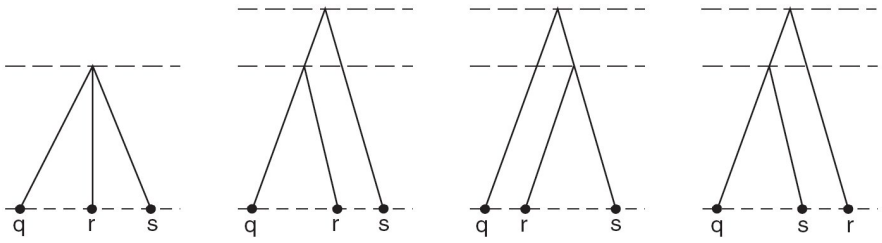
Μπορούμε να δούμε γιατί αυτή η δομή παράγματι ανταποκρίνεται στη γεωμετρία και την τοπολογία ενός ουλτραμετρικού χώρου με δύο απλά παραδείγαμτα. Κατ' αρχάς, θα δούμε πώς επαληθεύεται το ότι όλα τα τρίγωνα είναι ισοσκελή.



Σχήμα 3.1: Οι 3-αδικοί ακέραιοι

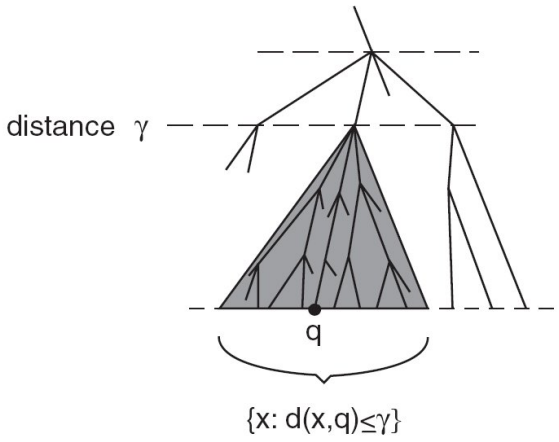


Σχήμα 3.2: Οι 3-αδικοί αριθμοί



Σχήμα 3.3: p-αδικά τρίγωνα

Στο Σχήμα 3.3 βλέπουμε τις δυνατές περιπτώσεις που μπορεί να έχουμε για τρία στοιχεία πάνω στο p-αδικό δέντρο. Όταν δύο στοιχεία q, r έχουν απόσταση a, συναντιούνται δηλαδή στο επίπεδο a (βλ. δεύτερη περίπτωση του Σχήματος 3.3), τότε ακολουθούν κοινή πορεία σε όλα τα επόμενα επίπεδα, εώς ότου συναντηθούν με το τρίτο στοιχείο s σε κάποιο ανώτερο επίπεδο b (ή και στο ίδιο, όπως φαίνεται στην πρώτη περίπτωση του Σχήματος 3.3). Έτσι, $d(r,s) = d(q,s) = b \geq a$, δηλαδή και τα δύο απέχουν το ίδιο από το s, και μάλιστα αυτή η απόσταση είναι η μέγιστη από τις $d(q,r)$, $d(q,s)$, $d(r,s)$.



Σχήμα 3.4: p-αδικές μπάλες

Τέλος, μπορούμε να δούμε τις ιδιότητες της Πρόταση 5, που αφορά στις μπάλες σε ουλτραμετρικούς χώρους. Η εικόνα μιας κλειστής μπάλας με κέντρο το σημείο q και ακτίνα γ είναι εκείνο ακριβώς το υποδένδρο που ξεκινάει από το επίπεδο γ και περιέχει το σημείο q σε κάποιο από τα φύλλα του (βλ. Σχήμα 3.4). Εύκολα παρατηρεί κανείς ότι οποιοδήπτε άλλο στοιχείο που ανήκει στη

μπάλα θα είναι και κέντρο της μπάλας, εφόσον το υποδέντρο, και άρα η μπάλα, δεν αλλάζει αν αλλάξουμε το κέντρο της, δηλαδή το στοιχείο από τα φύλλα του που επιλέγουμε. Είναι επίσης προφανές ότι δύο υποδέντρα ή θα περιέχονται το ένα στο άλλο, ή δεν θα έχουν κανέναν κοινό κόμβο, δηλαδή δύο μπάλες ή θα περιέχονται η μία στην άλλη, ή θα είναι ξένες μεταξύ τους.

3.7 Ανάλυση στο $\mathbb{Q}_p$

Περνάμε τώρα στις τοπολογικές ιδιότητες του $\mathbb{Q}_p$, καθώς και σε άλλα αποτελέσματα που αφορούν ακολουθίες και σειρές p-αδικών αριθμών.

Πρόταση 27 *Ο $\mathbb{Q}_p$ είναι ολικά μη συνεκτικός τοπολογικός χώρος Hausdorff.*

Απόδειξη: Ο $\mathbb{Q}_p$ είναι ολικά μη συνεκτικός χώρος τοπολογικός χώρος Hausdorff ως μετρικός χώρος με μη αρχιμήδεια νόρμα (βλ. Ενότητα 2, Πρόταση 2.4). □

Πρόταση 28 *Ο $\mathbb{Q}_p$ είναι τοπικά συμπαγής.*

Απόδειξη: Ένας χώρος είναι τοπικά συμπαγής αν και μόνο αν υπάρχει γειτονιά του μηδενός που να είναι συμπαγής. Οι p-αδικοί ακέραιοι $\mathbb{Z}_p$ είναι γειτονιά του μηδενός, αφού περιέχουν την ανοικτή μοναδιαία μπάλα με κέντρο το μηδέν (είναι η μοναδιαία μπάλα με κέντρο το μηδέν). Επιπλέον είναι συμπαγές σύνολο, όπως είδαμε στην προηγούμενη παράγραφο. Άρα ο $\mathbb{Q}_p$ είναι τοπικά συμπαγής. □

Θα συνεχίσουμε μελετώντας τις βασικές ιδιότητες σύγκλισης ακολουθιών και σειρών στο $\mathbb{Q}_p$. Έχουμε ήδη ότι ο $\mathbb{Q}_p$ είναι πλήρης μετρικός χώρος, επομένως κάθε ακολουθία Cauchy συγκλίνει σε στοιχείο του $\mathbb{Q}_p$. Επιπλέον, όλα τα αξιώματα που ισχύουν για τη συνήθη μετρική στο $\mathbb{R}$ εξακολουθούν να ισχύουν για την p-αδική μετρική στο $\mathbb{Q}_p$, αφού η μη αρχιμήδεια ιδιότητα είναι επιπλέον των ιδιοτήτων της νόρμας. Συνεπώς, τα περισσότερα από τα βασικά θεωρήματα της πραγματικής ανάλυσης εξακολουθούν να ισχύουν στην p-αδική θεωρία, μάλιστα με τις ίδιες αποδείξεις.

Παρ' όλα αυτά μια μη αρχιμήδεια μετρική επιφέρει και πολλές διαφορές. Η πιο σημαντική από αυτές είναι ότι ο έλεγχος για το πότε μία ακολουθία είναι Cauchy είναι πολύ απλούστερος:

Λήμμα 9 *Μία ακολουθία* (a_n), $a_n \in \mathbb{Q}_p$ *είναι Cauchy αν και μόνο αν οι όροι της ικανοποιούν την:*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

Απόδειξη: Σε προηγούμενη ενότητα έχουμε αποδείξει αυτό το λήμμα για ακολουθίες με όρους $a_n \in \mathbb{K}$, όπου $\mathbb{K}$ οποιοδήποτε σώμα με μη αρχιμήδεια νόρμα. Επομένως ισχύει και για το σώμα $\mathbb{Q}_p$ με την (μη αρχιμήδεια) p-αδική νόρμα. □

Όπως με τις ακολουθίες, έτσι και με τις σειρές, ισχύει η κλασσική θεωρία. Για παράδειγμα, η απόλυτη σύγκλιση μίας σειράς συνεπάγεται και σύγκλισή της, δηλαδή:

Πρόταση 29

Αν η $\sum |a_n|_p$ *συγκλίνει στο* $\mathbb{R}$*, τότε η* $\sum a_n$ *συγκλίνει στο* $\mathbb{Q}_p$*.*

Όμως, στην p-αδική περίπτωση, με το Λήμμα 9 στη διάθεσή μας, παίρνουμε κάτι καλύτερο.

Πρόταση 30 *Μία άπειρη σειρά* $\sum_{n=0}^{\infty} a_n$ *με* $a_n \in \mathbb{Q}_p$ *συγκλίνει αν και μόνο αν*

$$\lim_{n\to\infty} a_n = 0 \Leftrightarrow \lim_{n\to\infty} |a_n|_p = 0,$$

και σε αυτή την περίπτωση έχουμε

$$\left|\sum_{n=0}^{\infty} a_n\right|_p \leq \max_n \left\{|a_n|_p\right\} \qquad (*)$$

Απόδειξη: Μία σειρά συγκλίνει όταν και μόνο όταν η ακολουθία των μερικών αθροισμάτων $S_n = \sum_{i=1}^{n} a_n$ συγκλίνει. Όμως, $a_n = S_n - S_{n-1}$. Επομένως, η ακολουθία των μερικών αθροισμάτων είναι Cauchy, και άρα συγκλίνουσα (Λήμμα 9), αν και μόνο αν $(a_n) \to 0$.

Η ανισότητα προκύπτει άμεσα από τη μη αρχιμήδεια ιδιότητα της νόρμας με επαγωγή. □

Με την παραπάνω πρόταση βλέπουμε ότι στην p-αδική περίπτωση μπορούμε να χειριστούμε πολύ εύκολα τη σύγκλιση άπειρων σειρών. Στο $\mathbb{R}$ έχουμε περιπτώσεις, για παράδειγμα τη σειρά $\sum \frac{1}{n}$, όπου το αντίστροφο δεν ισχύει, δηλαδή: αν και ο γενικός όρος της σειράς τείνει στο μηδέν η σειρά δεν συγκλίνει.

Ορισμός 27 Μία σειρά $\sum_{n=0}^{\infty} a_n$ συγκλίνει *αυστηρά (unconditionally)*, εάν για κάθε αναδιάταξη των όρων $a_n \to b_n$, η σειρά $\sum_{n=0}^{\infty} b_n$ συγκλίνει.

Ειναι προφανές ότι η αυστηρή σύγκλιση συνεπάγεται την απλή σύγκλιση. Στο $\mathbb{Q}_p$ ισχύει και το αντίστροφο. Αντίθετα, κάτι τέτοιο δεν ισχύει στο $\mathbb{R}$. Πιο συγκεκριμένα, στο $\mathbb{R}$ έχουμε ότι μόνον όταν η σειρά συγκλίνει απολύτως, οποιαδήποτε αναδιάταξη των όρων της δεν επηρεάζει τη σύγκλισή της. Μάλιστα, ισχύει το Θεώρημα Riemann: Αν η σειρά $\sum_{n=0}^{\infty} a_n$ συγκλίνει, αλλά δεν συγκλίνει απολύτως, τότε μπορούμε με κατάλληλη αναδιάταξη να πάρουμε μία σειρά, τέτοια ώστε είτε να συγκλίνει σ' έναν προκαθορισμένο αριθμό λ, ή να ταλαντεύεται, ή να συγκλίνει στο $+\infty$ ή $-\infty$.

Θεώρημα 7 *Εάν η σειρά $\sum_{n=0}^{\infty} a_n$ συγκλίνει στο $\mathbb{Q}_p$, τότε συγκλίνει αυστηρά, και το άθροισμα είναι ανεξάρτητο της αναδιάταξης που επιβάλλεται.*

Απόδειξη: Έστω (b_n) η ακολουθία που προκύπτει μετά από αναδιάταξη των όρων της (a_n).

Κατ' αρχάς θα δείξουμε ότι η σειρά $\sum_{n=0}^{\infty} b_n$ είναι συγκλίνουσα. Από υπόθεση, η σειρά $\sum_{n=0}^{\infty} a_n$ συγκλίνει, άρα η ακολουθία (a_n) συγκλίνει στο μηδέν (Πρόταση 30). Τότε όμως, κάθε αναδιάταξη των όρων της (b_n) θα συγκλίνει επίσης στο μηδέν. Πράγματι, εφόσον η (a_n) συγκλίνει στο μηδέν, τότε για κάθε $\epsilon > 0$, υπάρχει φυσικός αριθμός $n_0(\epsilon)$, τέτοιος ώστε για κάθε $n > n_0$, να ισχύει $|a_n|_p < \epsilon$. Εφόσον η ακολουθία (b_n) είναι αναδιάταξη των όρων της (a_n), υπάρχει αριθμός $k_0 \in \mathbb{N}$, τέτοιος ώστε:

$$\{a_1, a_2, \ldots, a_{n_0}\} \subset \{b_1, b_2, \ldots b_{k_0}\}\,.$$

Τότε όμως, για κάθε $n > k_0$ θα ισχύει ότι $|b_n|_p < \epsilon$, δηλαδή $\lim_{n\to\infty} b_n = 0$. Άρα, η σειρά $\sum_{n=0}^{\infty} b_n$ επίσης συγκλίνει.

Θα δείξουμε τώρα ότι οι δύο σειρές έχουν το ίδιο όριο. Θεωρούμε την ακολουθία $A_M = \sum_{n=0}^{\infty} a_n - \sum_{n=0}^{M} a_n = \sum_{n=M+1}^{\infty} a_n$. Η (A_M) συγκλίνει στο μηδέν. Πράγματι, χρησιμοποιώντας την $(*)$ έχουμε:

$$\lim_{M\to\infty} |A_M|_p = \lim_{M\to\infty} \left| \sum_{n=M+1}^{\infty} a_n \right|_p \leq \lim_{M\to\infty} \left(\max_{M+1\leq n\leq\infty} \{|a_n|_p\} \right) = 0,$$

εφόσον $|a_n|_p \longrightarrow 0$.

Έστω $\epsilon > 0$. Τότε, υπάρχει N ακέραιος αριθμός, τέτοιος ώστε για κάθε $n \geq N$ να ισχύουν:

$$|\,a_n|_p < \epsilon, \quad |\,b_n|_p < \epsilon \;\; \text{και} \quad |A_n|_p = \left| \sum_{m=0}^{\infty} a_m - \sum_{m=0}^{n} a_m \right|_p < \epsilon.$$

Θέτουμε $S = \sum_{m=0}^{N} a_m$ και $S' = \sum_{m=0}^{N} b_m$ και συμβολίζουμε με S_1 και S_1' τα αθροίσματα εκείνων των όρων του S, αντίστοιχα του S', για τους οποίους ισχύει $|a_m|_p \geq \epsilon$, αντίστοιχα $|b_m|_p \geq \epsilon$.

Λόγω της επιλογής του N, τα S_1, S_1' περιέχουν τους ίδιους όρους, δηλαδή $S_1 = S_1'$. Το S διαφέρει από το S_1 στους όρους εκείνους με $|a_m|_p < \epsilon$. Όμοια το S' διαφέρει από το S_1' στους όρους με $|b_m|_p < \epsilon$. Επομένως, εφαρμόζοντας την ουλτραμετρική ιδιότητα της νόρμας, έχουμε:

$$|S - S_1|_p < \epsilon \quad \text{και} \quad |S' - S_1|_p < \epsilon \Rightarrow$$
$$|S - S'|_p \leq \max\{|S - S_1|_p,\ |S_1 - S'|_p\} < \epsilon.$$

Έτσι, παίρνουμε:

$$\left| \sum_{m=0}^{\infty} a_m - \sum_{m=0}^{N} b_m \right|_p \leq \max\left\{ \left| \sum_{m=0}^{\infty} a_m - \sum_{m=0}^{N} a_m \right|_p, \left| \sum_{m=0}^{N} a_m - \sum_{m=0}^{N} b_m \right|_p \right\}$$

$$= \max\{A_N,\ S - S'\} < \epsilon.$$

Παίρνοντας το όριο του N στο άπειρο προκύπτει το ζητούμενο, ότι δηλαδή

$$\sum_{m=0}^{\infty} a_m = \sum_{m=0}^{\infty} b_m.$$

□

Σημειώνουμε ότι η απόλυτη σύγκλιση είναι πιο ισχυρή έννοια από την απλή σύγκλιση. Για παράδειγμα, η σειρά $\sum_{n=0}^{\infty}(-1)^{n+1}\frac{1}{n+1}$ συγκλίνει στο $\mathbb{R}$, εφόσον η σειρά των μερικών αθροισμάτων συγκλίνει. Παρ' όλα αυτά δεν είναι απολύτως συγκλίνουσα, εφόσον η σειρά των απολύτων τιμών της είναι η αρμονική σειρά, η οποία αποκλίνει. Το ίδιο ισχύει και στο $\mathbb{Q}_p$, ότι δηλαδή η απόλυτη σύγκλιση είναι πιο ισχυρή εννοια, όπως φαίνεται και στο παρακάτω θεώρημα.

Θεώρημα 8 *Υπάρχει σειρά $\sum_{n=0}^{\infty}a_n$ στο $\mathbb{Q}_p$, η οποία συγκλίνει, αλλά δεν συγκλίνει απολύτως.*

Απόδειξη: Ας θεωρήσουμε την ακόλουθη σειρά:

$$1+\underbrace{p+p+\cdots+p}_{p\text{ φορές}}+\underbrace{p^2+p^2+\cdots+p^2}_{p^2\text{ φορές}}+\cdots+\underbrace{p^i+p^i+\cdots+p^i}_{p^i\text{ φορές}}+\cdots.$$

Η σειρά αυτή συγκλίνει, εφόσον οι όροι της τείνουν στο μηδέν. Όμως, δεν συγκλίνει απολύτως:

$$\sum_{n=0}^{\infty}|a_n|_p = 1+p\cdot p^{-1}+p^2\cdot p^{-2}+\cdots = \infty.$$

□

Η επόμενη πρόταση απλουστεύει πολύ τις περιπτώσεις προβλημάτων όπου απαιτούνται διπλές σειρές και όπου είναι συχνή η εναλλαγή των αθροισμάτων.

Πρόταση 31 *Έστω $b_{ij}\in\mathbb{Q}_p$ και έστω ότι για κάθε $\epsilon>0$ υπάρχει ένας ακέραιος $N=N(\epsilon)$, τέτοιος ώστε:*

$$\max(i,j)\geq N \Rightarrow |b_{ij}|_p<\epsilon. \tag{3.1}$$

Τότε οι δύο σειρές

$$\sum_i\sum_j b_{ij} \qquad \text{και} \qquad \sum_j\sum_i b_{ij}$$

συγκλίνουν και έχουν τα ίδια αθροίσματα.

Απόδειξη: Κατ' αρχάς, είναι εύκολο να δει κανείς ότι τα αθροίσματα $\sum_j b_{ij}$ και $\sum_i b_{ij}$ συγκλίνουν. Πράγματι, αν θεωρήσουμε το i ή το j αντίστοιχα σταθερό, η υπόθεση (3.1) εξασφαλίζει ότι $\lim_{j\to\infty} b_{ij} = 0$ και $\lim_{i\to\infty} b_{ij} = 0$.

Επιπλέον, οι διπλές σειρές συγκλίνουν. Πράγματι, πάλι από την υπόθεση (3.1), για κάθε $i \geq N$ και για κάθε $j \geq N$ έχουμε αντίστοιχα:

$$\left|\sum_j b_{ij}\right|_p \leq \max_j \{|b_{ij}|_p\} < \epsilon \quad \text{και} \quad \left|\sum_i b_{ij}\right|_p \leq \max_i \{|b_{ij}|_p\} < \epsilon.$$

Άρα, από Πρόταση 30, θα συγκλίνουν και οι διπλές σεορές.

Μένει να δείξουμε ότι τα δύο αθροίσματα είναι ίσα. Για το λόγο αυτό παρατηρούμε ότι:

$$\left|\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} b_{ij} - \sum_{i=0}^{N}\sum_{j=0}^{N} b_{ij}\right|_p = \left|\sum_{i=0}^{N}\sum_{j=N+1}^{\infty} b_{ij} + \sum_{i=N+1}^{\infty}\sum_{j=0}^{\infty} b_{ij}\right|_p$$

$$\leq \max\left\{\left|\sum_{i=0}^{N}\sum_{j=N+1}^{\infty} b_{ij}\right|_p, \left|\sum_{i=N+1}^{\infty}\sum_{j=0}^{\infty} b_{ij}\right|_p\right\}$$

$$\leq \max\left\{\max_{0\leq i\leq N}\left\{\left|\sum_{j=N+1}^{\infty} b_{ij}\right|_p\right\}, \max_{i\geq N}\left\{\left|\sum_{j}^{\infty} b_{ij}\right|_p\right\}\right\} < \epsilon,$$

που αποδεικνύει το ζητούμενο. □

p-αδικές δυναμοσειρές

Μία σειρά της μορφής

$$\sum_{n=0}^{\infty} a_n (X-\xi)^n \in \mathbb{F}[[X]],$$

όπου $\mathbb{F}$ σώμα και X είναι μία απροσδιόριστη, ονομάζεται *δυναμοσειρά* με *κέντρο* ξ και *συντελεστές* $a_n \in \mathbb{F}$. Επειδή κάθε σειρά με την παραπάνω μορφή μπορεί να αναχθεί, με την αντικατάσταση $t = X - \xi$, σε μία σειρά με κέντρο το μηδέν:

$$\sum_{n=0}^{\infty} a_n t^n, \qquad (*)$$

από εδώ και στο εξής θα χρησιμοποιούμε αυτό το συμβολισμό.

Μας ενδιαφέρουν οι δυναμοσειρές στο σώμα των p-αδικών αριθμών, δηλαδή οι σειρές της μορφής $(*)$ με τους συντελεστές a_n να ανήκουν στο $\mathbb{Q}_p$. Μπορούμε να θεωρήσουμε κάθε p-αδική δυναμοσειρά ως μία συνάρτηση

$$f(X) = \sum_{n=0}^{\infty} a_n X^n.$$

Όταν η απροσδιόριστη X πάρει τιμές στο $\mathbb{Q}_p$ μπορούμε να μελετήσουμε τη συμπεριφορά της δυναμοσειράς, δηλαδή για ποια $x \in \mathbb{Q}_p$ η σειρά συγκλίνει. Όπως και στην κλασσική περίπτωση, το σύνολο όλων αυτών των x καλείται *διάστημα σύγκλισης* και είναι μία μπάλα του $\mathbb{Q}_p$.

Γνωρίζουμε ήδη ότι για $x \in \mathbb{Q}_p$ η σειρά $f(x)$ συγκλίνει αν και μόνο αν $|a_n x^n|_p \longrightarrow 0$. Για τον προσδιορισμό του διαστήματος σύγκλισης έχουμε την ακόλουθη πρόταση:

Πρόταση 32 *Έστω $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$. Ορίζουμε την ποσότητα $0 \leq \rho \leq \infty$:*

$$\rho = \frac{1}{\limsup \sqrt[n]{|a_n|_p}},$$

η οποία καλείται ακτίνα σύγκλισης. *Τότε, ισχύουν τα ακόλουθα:*

(i) Εάν $\rho = 0$, τότε η $f(x)$ συγκλίνει μόνον όταν $x = 0$.

(ii) Εάν $\rho = \infty$, τότε η $f(x)$ συγκλίνει για κάθε $x \in \mathbb{Q}_p$.

(iii) Εάν $0 < \rho < \infty$ και $\lim_{n\to\infty} |a_n|_p \rho^n = 0$, τότε η $f(x)$ συγκλίνει αν και μόνο αν $|x|_p \leq \rho$.

(iv) Εάν $0 < \rho < \infty$ και $\lim_{n\to\infty} |a_n|_p \rho^n \neq 0$, τότε η $f(x)$ συγκλίνει αν και μόνο αν $|x|_p < \rho$.

Απόδειξη: Κατ' αρχάς, είναι προφανές ότι το $f(0)$ συγκλίνει στο a_0. Παρατηρούμε ότι η σειρά $\sum_{n=0}^{\infty} |a_n|_p \, |x|_p^n$ είναι μια δυναμοσειρά στο $\mathbb{R}$, για την οποία θα ισχύει η κλασσική θεωρία. Επομένως, λόγω των Προτάσεων 29 και 30, προκύπτουν άμεσα οι ισχυρισμοί (i)-(iv).

Πιο συγκεκριμένα, για τους δύο τελευταίους έχουμε τα ακόλουθα: εάν $|x|_p < \rho < \infty$, τότε η σειρά:

$$\sum_{n=0}^{\infty} |a_n|_p \, |x|_p^n \in \mathbb{R}[[x]],$$

συγκλίνει στο $\mathbb{R}$. Πράγματι, το διάστημα σύγκλισης της σειράς είναι το $(-\rho', +\rho')$, όπου

$$\rho' = 1/\limsup \sqrt[n]{||a_n|_p|} = 1/\limsup \sqrt[n]{|a_n|_p} = \rho$$

και $||x|_p| = |x|_p \in (-\rho', +\rho')$. Δηλαδή, η σειρά $\sum_{n=0}^{\infty} a_n x^n$ συγκλίνει απολύτως, άρα συγκλίνει και στο $\mathbb{Q}_p$ (Πρόταση 29).

Αν, τώρα, $|x|_p > \rho$, μπορεί να δει κανείς ότι η ποσότητα $|a_n x^n|_p$ δεν μπορεί να τείνει στο μηδέν καθώς το n τείνει στο άπειρο. Πράγματι, εφόσον $\lim |a_n|_p \to 1/\rho^n$, και $|x|_p > \rho$, η ποσότητα $|a_n x^n|_p = (|x|_p/\rho)^n$ τείνει στο άπειρο καθώς αυξάνει το n. Άρα, από την Πρόταση 30, η $f(x)$ δεν συγκλίνει.

Τέλος, πάλι από την Πρόταση 30, συμπεραίνουμε ότι όταν $|x|_p = \rho$ (δηλαδή στα άκρα του διαστήματος σύγκλισης), η $f(x)$ θα συγκλίνει αν και μονον αν $\lim_{n\to\infty} |a_n|_p |x|_p^n = \lim_{n\to\infty} |a_n|_p \rho^n = 0$. □

Παρατήρηση 16 Στην p-αδική περίπτωση, η συμπεριφορά της σειράς στο όριο του διαστήματος σύγκλισης είναι πολύ απλή: *είτε θα συγκλίνει σε όλα τα σημεία που ανήκουν στο όριο, ή σε κανένα από αυτά*. Αυτό συμβαίνει διότι η σύγκλιση εξαρτάται από τη νόρμα του x, και όχι από το ίδιο το x.

Αντίθετα, στο $\mathbb{R}$, μία σειρά μπορεί να συγκλίνει στο ένα άκρο του διαστήματος και να αποκλίνει στο άλλο. Για παράδειγμα, η σειρά $\sum (-1)\frac{(x-2)^n}{n}$, με ακτίνα σύγκλισης $\rho = 1$ και διάστημα σύγκλισης το $(2-1, 2+1) = (1, 3)$, συγκλίνει για $x = 1$, ενώ αποκλίνει για $x = 3$.

Παράδειγμα 1 Θα προσδιορίσουμε το διάστημα σύγκλισης της p-αδικής δυναμοσειράς $\sum p^n X^n$. Κατ' αρχάς, υπολογίζουμε την ποσότητα ρ:

$$\limsup \sqrt[n]{|a_n|_p} = \limsup \sqrt[n]{p^{-n}} = \limsup p^{-1} = p^{-1}$$

$$\Rightarrow \rho = p.$$

Επιπλέον, έχουμε ότι $\lim_{n\to\infty} |a_n|_p \rho^n = \lim_{n\to\infty} 1 = 1 \neq 0$. Επομένως, από την Πρόταση 32, η σειρά συγκλίνει για κάθε $x \in \mathbb{Q}_p$, με $|\, x|_p < p$.

Μπορούμε να καταλήξουμε στο παραπάνω αποτέλεσμα ακολουθώντας την πορεία της απόδειξης της Πρόταση 32. Η σειρά $\sum p^n x^n$ συγκλίνει για κάθε $x \in \mathbb{Q}_p$ με $|p^n x^n|_p \to 0$. Ας δούμε για ποια x ισχύει η προηγούμενη σχέση. Έχουμε:

$$|p^n x^n|_p = p^{-n} p^{-\upsilon_p(x)n} = p^{-n(1+\upsilon_p(x))} \to 0 \quad \Leftrightarrow \quad n(1+\upsilon_p(x)) \to +\infty.$$

Επομένως, θα πρέπει

$$(1+\upsilon_p(x)) > 0 \Leftrightarrow \upsilon_p(x) > -1 \Leftrightarrow$$

$$|\, x|_p = p^{-\upsilon_p(x)} < p.$$

■

Όπως και στην κλασσική περίπτωση, οι συναρτήσεις που ορίζονται με τη βοήθεια p-αδικών δυναμοσειρών είναι συνεχείς στο διάστημα σύγκλισής τους:

Πρόταση 33 *Έστω $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$ και έστω $D \subset \mathbb{Q}_p$ το διάστημα σύγκλισης της $f(X)$. Τότε, η συνάρτηση*

$$f : D \longrightarrow \mathbb{Q}_p$$

είναι συνεχής στο D.

Απόδειξη: Έστω $x \in D$, και έστω (x_n) ακολουθία στοιχείων του D που συγκλίνει στο x. Θα αποδείξουμε ότι τότε η ακολουθία $f(x_n)$ θα συγκλίνει στο $f(x)$. Έχουμε ότι:

$$f(x_n) - f(x) = a_1(x_n - x) + a_2(x_n^2 - x^2) + \cdots = \sum_{i=1}^{\infty} a_i(x_n^i - x^i).$$

Η παραπάνω σειρά συγκλίνει στο $\mathbb{Q}_p$, εφόσον οι όροι της τείνουν στο μηδέν. Πράγματι,

$$\left|a_i(x_n^i - x^i)\right|_p = |a_i|_p \, |(x_n - x)|_p \left|x_n^{i-1} + x_n^{i-2}x + \cdots + x^{i-1}\right|_p$$

$$\leq |a_i|_p \, |(x_n - x)|_p \max_j \left\{ \left|x_n^{i-j}x^{j-1}\right|_p \right\}.$$

Διακρίνουμε δύο περιπτώσεις (ουσιαστικά χρησιμοποιούμε το ότι όλα τα τρίγωνα στο $\mathbb{Q}_p$ είναι ισοσκελή):

- $|x_n - x|_p < |\,x|_p = |x_n|_p$ και
- $|x_n - x| = \max\left\{|\,x|_p\,, |x_n|_p\right\} \geq \min\left\{|\,x|_p\,, |x_n|_p\right\}$.

Για την πρώτη περίπτωση έχουμε:

$$|a_i|_p \, |(x_n - x)|_p \max_j \left\{ \left|x_n^{i-j}x^{j-1}\right|_p \right\} = |a_i|_p |x_n - x|_p \, |\,x|_p^{i-1} < |a_i|_p \, |\,x|_p^i \,,$$

το οποίο τείνει στο μηδέν, εφόσον το x ανήκει στο διάστημα σύγκλισης της σειράς $f(X)$.
Για τη δεύτερη περίπτωση, μπορούμε χωρίς βλάβη της γενικότητας, να υποθέσουμε ότι $\max\left\{|\,x|_p\,, |x_n|_p\right\} = |x_n|_p$. Τότε παίρνουμε:

$$|a_i|_p \, |(x_n - x)|_p \max_j \left\{ \left|x_n^{i-j}x^{j-1}\right|_p \right\} = |a_i|_p |x_n|_p |x_n|_p^{i-1} = |a_i|_p |x_n|_p^i,$$

το οποίο τείνει στο μηδέν, εφόσον οι σειρές $f(x_n)$ συγκλίνουν. Αντίστοιχα αποτελέσματα θα παίρναμε αν είχαμε υποθέσει ότι $\max\left\{|\,x|_p\,, |x_n|_p\right\} = |\,x|_p$.

Άρα έχουμε ότι για κάθε n η σειρά $f(x_n) - f(x)$ συγκλίνει. Θα δείξουμε ότι για $n \to \infty$, η ακολουθία $f(x_n) - f(x)$ συγκλίνει στο μηδέν:

$$\lim_{n\to\infty} |f(x_n) - f(x)|_p \leq \lim_{n\to\infty} \max_i \left\{ \left|a_i(x_n^i - x^i)\right|_p \right\} \longrightarrow 0.$$

εφόσον $x_n \to x$. Επομένως, η $f(x_n)$ συγκλίνει στην $f(x)$, και άρα, από την αρχή της μεταφοράς, η f είναι συνεχής στο διάστημα σύγκλισής της. □

Παραθέτουμε χωρίς απόδειξη ένα πολύ ενδιαφέρον αποτέλεσμα για τις p-αδικές δυναμοσειρές. Αντίθετα με την περίπτωση των πραγματικών δυναμοσειρών, όπου η αντικατάσταση του κέντρου με οποιοδήποτε σημείο του διαστήματος σύγκλισης μπορεί να επιφέρει αλλαγή στο διάστημα σύγκλισης, στην p-αδική περίπτωση, αν αντικαταστήσουμε το κέντρο μιας δυναμοσειράς, θα καταλήξουμε στο ίδιο ακριβώς διάστημα σύγκλισης.

Πρόταση 34 *Έστω $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$ δυναμοσειρά στο $\mathbb{Q}_p$, και έστω $\xi \in \mathbb{Q}_p$, τέτοιο ώστε το $f(\xi)$ να συγκλίνει. Για κάθε $m \geq 0$ ορίζουμε την ποσότητα*

$$b_m = \sum_{n \geq m} \binom{n}{m} a_n \xi^{n-m},$$

και θεωρούμε τη δυναμοσειρά

$$g(X) = \sum_{m=0}^{\infty} b_m (X - \xi)^m.$$

Τότε, ισχύουν τα ακόλουθα:

(i) Οι σειρές που ορίζουν τα b_m συγκλίνουν για κάθε m, δηλαδή τα b_m είναι καλά ορισμένα.

(ii) Οι δυναμοσειρές $f(X)$ και $g(X)$ έχουν το ίδιο διάστημα σύγκλισης, δηλαδή, για $\lambda \in \mathbb{Q}_p$, ισχύει ότι το $f(\lambda)$ συγκλίνει αν και μόνο αν συγκλίνει το $g(\lambda)$.

(iii) Για κάθε λ που ανήκει στο διάστημα σύγκλισης, ισχύει $f(\lambda) = g(\lambda)$.

Η παραπάνω πρόταση δείχνει ότι στους p-αδικούς αριθμούς δεν μπορούμε να έχουμε *αναλυτική συνέχεια*, επέκταση, δηλαδή, μιας *αναλυτικής* συνάρτησης f σε μία f', η οποία είναι αναλυτική σε διάστημα μεγαλύτερο από αυτό της f.

Θυμίζουμε ότι μία συνάρτηση καλείται αναλυτική στο ανοικτό σύνολο D, εάν μπορεί να γραφεί ως δυναμοσειρά με κέντρο x_0, για κάθε $x_0 \in D$. Ισοδύναμα, μία αναλυτική συνάρτηση είναι μία απείρως παραγωγίσιμη συνάρτηση, και άρα έχει ανάπτυγμα Taylor.

Για μία πραγματική δυναμοσειρά, η οποία είναι αναλυτική στο διάστημα σύγκλισής της, μπορούμε να πάρουμε αναλυτικές συνέχειες, αλλάζοντας το κέντρο της με οποιοδήποτε σημείο του διαστήματος σύγκλισης. Με κάθε αλλαγή του κέντρου λαμβάνουμε και διαφορετικά διαστήματα σύγκλισης. Επαναλαμβάνοντας τη διαδικασία για κάθε νέα σειρα μπορούμε να πάρουμε αναλυτικές συνέχειες της αρχικής δυναμοσειράς. Φαίνεται άμεσα από την Πρόταση 34, ότι δεν μπορούμε να εφαρμόσουμε μία τέτοια διαδικασία σε μία p-αδική δυναμοσειρά.

Το επόμενο θεώρημα αναφέρεται στις ρίζες p-αδικών συναρτήσεων $f : \mathbb{Z}_p \to \mathbb{Q}_p$, που ορίζονται από δυναμοσειρές.

Θεώρημα 9 (Strassman) *Έστω μία μη μηδενική σειρά* $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$, *και έστω ότι* $\lim_{n\to\infty} a_n = 0$, *έτσι ώστε η* $f(x)$ *να συγκλίνει για κάθε* $x \in \mathbb{Z}_p$. *Θέτουμε* $N \in \mathbb{N}$ *να είναι ο αριθμός εκείνος, για τον οποίο ικανοποιούνται οι ακόλουθες συνθήκες:*

$$|a_N|_p = \max_n |a_n|_p \qquad \textit{και} \qquad |a_n|_p < |a_N|_p \quad \textit{για κάθε} \quad n > N.$$

Τότε, η συνάρτηση $f : \mathbb{Z}_p \to \mathbb{Q}_p$ *έχει το πολύ* N *ρίζες.*

Απόδειξη: Κατ' αρχάς, η ύπαρξη του N εξασφαλίζεται από το γεγονός ότι οι συντελεστές a_n τείνουν στο μηδέν. Άρα, υπάρχει μέγιστη τιμή μεταξύ των νορμών τους, και ο N είναι ο δείκτης του τελευταίου συντελεστή, με νόρμα ίση με αυτήν την τιμή.

Αποδεικνύουμε το Θεώρημα με επαγωγή στο N.

Επαγωγική Βάση: Εάν $N = 0$, τότε θα έχουμε ότι $|a_0|_p > |a_n|_p$ για κάθε $n \geq 1$. Θα δείξουμε ότι στην περίπτωση αυτή η f δεν έχει καμία ρίζα, ότι δηλαδή $f(x) \neq 0$ για κάθε $x \in \mathbb{Z}_p$.

Πράγματι, αν είχαμε $f(x) = 0$ για κάποιο $x \in \mathbb{Z}_p$, τότε:

$$0 = f(x) = a_0 + a_1 x + a_2 x^2 + \cdots \Rightarrow$$

$$\begin{aligned} |\, a_0|_p &= |\, a_1 x + a_2 x^2 + \cdots|_p \\ &\leq \max\left\{|a_n x^n|_p\right\} \\ &\leq \max\left\{|a_n|_p\right\}. \end{aligned}$$

Αυτό όμως αντιτίθεται στην υπόθεση ότι $|a_0|_p > |a_n|_p$ για κάθε $n \geq 1$.

Επαγωγικό Βήμα: Έστω ότι για κάθε δυναμοσειρά στην οποία ο αριθμός του Θεωρήματος Strassman N' είναι ίσος με $N-1<N$, ισχύει η υπόθεση του Θεωρήματος, ότι δηλαδή τότε θα έχει το πολύ N' p-αδικές ακέραιες ρίζες. Θα δείξουμε ότι τότε, η $f(x)$ έχει το πολύ N ρίζες, όπου N όπως ορίστηκε παραπάνω.

Εάν η f δεν έχει ρίζες, τότε το Θεώρημα ισχύει τετριμμένα. Έστω λοιπόν $f(x_0)=0$ για κάποιο $x_0\in\mathbb{Z}_p$. Τότε, για κάθε $x\in\mathbb{Z}_p$ θα έχουμε:

$$f(x)=f(x)-f(x_0)=\sum_{n=1}^{\infty}a_n(x^n-x_0^n)=(x-x_0)\sum_{n=1}^{\infty}\sum_{j=0}^{n-1}a_nx^jx_0^{n-1-j}.$$

Ορίζοντας $k=n-j-1$ και εναλλάσοντας τα δύο αθροισμάτα από την Πρόταση 31, έχουμε:

$$f(x)=(x-x_0)\sum_{j=0}^{\infty}b_jx^j=(x-x_0)g(x),$$

όπου τα $b_j=\sum_{k=0}^{\infty}a_{j+1+k}x_0^k$ είναι δυναμοσειρές που συγκλίνουν στο $\mathbb{Q}_p$.

Για τις νόρμες των b_j έχουμε ότι για κάθε j ισχύει:

$$|b_j|_p\leq\max_{k\geq0}\left\{|a_{j+1+k}|_p\right\}\leq|a_N|_p\,,$$

εφόσον $|x_0|_p\leq1$ και $|a_n|_p\leq|a_N|_p$ για κάθε n.
Επιπλέον,

$$|b_{N-1}|_p=\left|a_N+a_{N+1}x_0+a_{N+2}x_0^2+\cdots\right|_p=|a_N|_p\,,$$

από Πρόταση 1, εφόσον $\left|a_jx_0^j\right|_p<|a_N|_p$ για κάθε $j>N$.
Τέλος, αν $j\geq N$, ισχύει:

$$|b_j|_p\leq\max_{k\geq0}\left\{|a_{j+1+k}|_p\right\}\leq\max_{i\geq N+1}|a_i|_p<|a_N|_p\,.$$

Δηλαδή, το b_{N-1} έχει τη μέγιστη νόρμα που ικανοποιεί τις συνθήκες του Θεωρήματος Strassman για την $g(x)$. Επομένως, από την επαγωγική υπόθεση, η $g(x)$ έχει το πολύ $N-1$ ρίζες στο $\mathbb{Z}_p$. Άρα, η $f(x)$ έχει το πολύ N ρίζες στο $\mathbb{Z}_p$ (αυτές της g και την x_0). □

Από το Θεώρημα του Strassman προκύπτουν αρκετά ενδιαφέροντα πορίσματα, τα οποία παραθέτουμε, σκιαγραφώντας τις αποδείξεις τους.

Πόρισμα 7 *Έστω* $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$ *δυναμοσειρά με διάστημα σύγκλισης το* $p^m\mathbb{Z}_p$ *για κάποιο* $m \in \mathbb{Z}$. *Τότε, η* $f(X)$ *έχει πεπερασμένο αριθμό ριζών στο* $p^m\mathbb{Z}_p$, *το πολύ* N *το πλήθος, όπου το* N *ικανοποιεί τα ακόλουθα:*

$$\left|p^{mN}a_N\right|_p = \max_n \left\{|p^{mn}a_n|_p\right\} \quad \textit{και} \quad |p^{mn}a_n|_p < \left|p^{mN}a_N\right|_p \quad \textit{για κάθε} \quad n > N.$$

Απόδειξη: Η συνάρτηση $g(X) = f(p^m X) = \sum a_n p^{mn} X^n$ συγκλίνει στο $\mathbb{Z}_p$, εφόσον η f συγκλίνει στο $p^m/\mathbb{Z}_p$. Το ζητούμενο προκύπτει άμεσα από το Θεώρημα Strassman. □

Πόρισμα 8 *Έστω δύο* p*-αδικές δυναμοσειρές* $f(X) = \sum_{n=0}^{\infty} a_n X^n$ *και* $g(X) = \sum_{n=0}^{\infty} b_n X^n$, *οι οποίες συγκλίνουν σε κάποιο* $p^m\mathbb{Z}_p$. *Εάν υπάρχουν άπειροι το πλήθος αριθμοί* $\alpha \in p^m/\mathbb{Z}_p$, *τέτοιοι ώστε* $f(\alpha) = g(\alpha)$, *τότε* $a_n = b_n$ *για κάθε* $n \geq 0$.

Απόδειξη: Εφαρμόζουμε το Πόρισμα 7 στη συνάρτηση $f(X) - g(X)$. Εφόσον έχει άπειρες ρίζες στο $p^m\mathbb{Z}_p$, θα πρόκειται για τη μηδενική δυναμοσειρά, δηλαδή θα έχει μηδενικούς συντελεστές. Επομένως, $a_n = b_n$ για κάθε n. □

Πόρισμα 9 *Έστω* $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$, *που συγκλίνει σε κάποιο* $p^m\mathbb{Z}_p$. *Εάν η συνάρτηση* $f(X) : p^m\mathbb{Z}_p \to \mathbb{Q}_p$ *είναι περιοδική, δηλαδή εάν υπάρχει* $\pi \in p^m\mathbb{Z}_p$ *τέτοιο ώστε* $f(x + \pi) = f(x)$ *για κάθε* $x \in p^m\mathbb{Z}_p$, *τότε η* $f(X)$ *είναι σταθερή.*

Απόδειξη: Ευκολα βλέπει κανείς ότι η συνάρτηση $f(X) - f(0)$ έχει ρίζες στο $n\pi$ για κάθε $n \in \mathbb{Z}$. Εφόσον το $p^m\mathbb{Z}_p$ είναι ιδεώδες του $\mathbb{Z}_p$ [1], τότε $n\pi \in p^m\mathbb{Z}_p$ για κάθε $n \in \mathbb{Z}$. Δηλαδή, η $f(X) - f(0)$ έχει άπειρες το πλήθος ρίζες στο $p^m\mathbb{Z}_p$, και άρα θα είναι η μηδενική δυναμοσειρά. Συνεπώς, η $f(X)$ θα είναι ίση με μία σταθερά. □

Από το πόρισμα φαίνεται ότι συναρτήσεις *ολόμορφες παντού*, που μπορούν να εκφραστούν ως δυναμοσειρές που συγκλίνουν σε όλο το $\mathbb{Q}_p$ (entire), δεν

[1] Πράγματι, $\pi \in p^m\mathbb{Z}_p \Leftrightarrow |\pi|_p \leq p^{-m}$, και για $x \in \mathbb{Z}_p \Leftrightarrow |x|_p \leq 1$, θα ισχύει $|\pi x|_p = |\pi|_p\,|x|_p \leq p^{-m} \Leftrightarrow \pi x \in p^m\mathbb{Z}_p$. Υπενθυμίζουμε ότι όλοι οι ακέραιοι ανήκουν στο $\mathbb{Z}_p$.

μπορούν να είναι περιοδικές. Όλα τα πολλαπλάσια της περιόδου βρίσκονται στο ίδιο φραγμένο διάστημα. Αντίθετα, αντιπροσωπευτικά παραδείγματα πραγματικών συναρτήσεων, ολόμορφων παντού και περιοδικών, αποτελούν οι $\sin(X)$ και $\cos(X)$.

p-αδική λογαριθμική και p-αδική εκθετική συνάρτηση

Θα χρησιμοποιήσουμε δυναμοσειρές για να ορίσουμε τις p-αδικές συναρτήσεις τις ανάλογες με τη λογαριθμική και την εκθετική όπως τις ξέρουμε ως τώρα.

Για την κλασσική λογαριθμική συνάρτηση γνωρίζουμε ότι προέρχεται από τη δυναμοσειρά:

$$\log(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} \in \mathbb{Q}[[X]].$$

Εφόσον οι συντελεστές της σειράς είναι ρητοί, μπορούμε να τη σκεφτόμαστε και ως p-αδική δυναμοσειρά. Για την ακτίνα σύγκλισης έχουμε:

$$|a_n|_p = \left|\frac{1}{n}\right|_p = p^{v_p(n)} \Rightarrow \sqrt[n]{|a_n|_p} = p^{v_p(n)/n}.$$

Η ποσότητα αυτή τείνει στο 1 καθώς το n τείνει στο άπειρο. Πράγματι, η p-αδική εκτίμηση του n ορίζεται ως ο μεγαλύτερος ακέραιος m, τέτοιος ώστε το n να διαιρείται από το p^m. Στη συγκεκριμένη περίπτωση έχουμε ότι ο n ανήκει στους φυσικούς, και άρα θα ισχύει ότι $v_p(n) \geq 0$. Έτσι, έχουμε:

$$n = p^{v_p(n)} n' \Leftrightarrow v_p(n) = \log_p \frac{n}{n'} = \frac{\log(n/n')}{\log p} \leq \frac{\log n}{\log p},$$

εφόσον η συνάρτηση του λογαρίθμου είναι αύξουσα συνάρτηση. Άρα,

$$\frac{v_p(n)}{n} \leq \frac{\log(n)}{n \log p} \to 0,$$

από το οποίο έπεται ότι $p^{v_p(n)/n} \to 1$. Έτσι, η ακτίνα σύγκλισης ρ είναι ίση με τη μονάδα.

Θα δούμε τώρα εάν το διάστημα σύγκλισης είναι η ανοικτή ή η κλειστή μοναδιαία μπάλα. Πρέπει να ελέγξουμε τι γίνεται με τη νόρμα στο σύνορο:

$$|a_n \rho^n|_p = |a_n|_p = \left|\frac{1}{n}\right|_p = p^{v_p(n)} \not\to 0,$$

Άρα η σειρά συγκλίνει για κάθε x με $|x|_p < 1$, δηλαδή η $f(X)$ ορίζει μια συνάρτηση στην ανοικτή μπάλα $B(0,\,1)$.

Ορισμός 28 Έστω $B = B(1,1) = \left\{x \in \mathbb{Z}_p : |x-1|_p < 1\right\} = 1 + p\mathbb{Z}_p$. Ορίζουμε ως *p-αδικό λογάριθμο* του $x \in B$ την ποσότητα:

$$\log_p(x) = \log(1 + (x-1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}$$

Ορίζοντας έτσι τον p-αδικό λογάριθμο, εξασφαλίζεται η θεμελιώδης ιδιότητα του λογαρίθμου

$$\log_p(x) + \log_p(y) = \log_p(xy).$$

εφόσον:

$$\log(1+X) + \log(1+Y) = \log(1+X+Y+XY).$$

Για την εκθετική συνάρτηση, γνωρίζουμε ότι στην κλασσική περίπτωση η σειρά:

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$$

συγκλίνει παντού στο $\mathbb{R}$, καθώς η ποσότητα $1/n!$ τείνει πολύ γρήγορα στο μηδέν. Βέβαια, στην p-αδική περίπτωση κάτι τέτοιο δεν ισχύει, καθώς, p-αδικά, το $1/n!$ γίνεται παρα πολύ μεγάλο. Την ίδια σειρά μελετούμε και στο $\mathbb{Q}_p$.

Η ακτίνα σύγκλισης της p-αδικής αυτής δυναμοσειράς αποδεικνύεται ότι είναι ίση με $p^{\frac{-1}{p-1}}$. Για την απόδειξη χρησιμοποιείται η σχέση

$$v_p(n!) = \frac{n - s_n}{p-1},$$

όπου s_n είναι το άθροισμα των n πρώτων ψηφίων της p-αδικής αναπαράστασης του n. Επιπλέον, αποδεικνύεται ότι στο σύνορο η σειρά αποκλίνει, άρα η σειρά συγκλίνει στην ανοικτή μπάλα $B(0, p^{-1/(p-1)})$

Παρατήρηση 17 Υπάρχει κάτι που αξίζει να προσέξουμε σχετικά με την ακτίνα σύγκλισης. Για $p \neq 2$ η εκτίμηση ενός στοιχείου δεν παίρνει τιμές μεταξύ των $-1/(p-1)$ και 1. Επομένως,

$$|x|_p < p^{-1/(p-1)} \Leftrightarrow |x|_p \leq p^{-1} \Leftrightarrow x \in p\mathbb{Z}_p \Leftrightarrow |x|_p < 1.$$

Όμως, σε οποιοδήποτε σώμα που περιέχει το $\mathbb{Q}_p$ και στο οποίο είναι δυνατή η επέκταση της p-αδικής νόρμας, είναι δυνατόν να υπάρχουν στοιχεία με $p^{-1/(p-1)} \leq |x|_p < 1$.
Συνοψίζοντας, έχουμε ότι:

- Αν $p \neq 2$, τότε η σειρά $\exp(x)$ συγκλίνει αν και μόνο αν $x \in p\mathbb{Z}_p$.
- Αν $p = 2$, τότε η σειρά $\exp(x)$ συγκλίνει αν και μόνο αν $x \in 4\mathbb{Z}_2$.

Ορισμός 29 Έστω $D = B(0, p^{-1/(p-1)}) = \left\{x \in \mathbb{Z}_p : |x|_p < p^{-1/(p-1)}\right\}$. Η *$p$-αδική εκθετική συνάρτηση* είναι η συνάρτηση $\exp_p(x) : D \to \mathbb{Q}_p$, που ορίζεται ως:

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Όπως και στην περίπτωση του p-αδικού λογαρίθμου, ισχύει η ιδιότητα της εκθετικής συνάρτησης

$$\exp_p(x+y) = \exp_p(x)\exp_p(y),$$

για κάθε $x, y \in D$. Παρατηρούμε ότι, αν $x, y \in D$, τότε θα έχουμε και $x + y \in D$, επομένως δεν έχουμε πρόβλημα σύγκλισης για την ποσότητα $\exp_p(x+y)$.

Ακόμα, μια σημαντική σχέση που ισχύει μεταξύ των κλασσικών συναρτήσεων του λογαρίθμου και της εκθετικής, ισχύει και στην p-αδική περίπτωση.

Πρόταση 35 *Έστω $x \in D$, όπου D όπως ορίστηκε παραπάνω. Τότε, έχουμε ότι:*

$$\left|\exp_p(x)\right|_p < 1,$$

δηλαδή το $\exp_p(x)$ ανήκει στο πεδίο ορισμού της $\log_p$, και

$$\log_p(\exp_p(x)) = x.$$

Αντίστροφα, αν $x \in D$*, έχουμε ότι:*

$$\left|\log_p(1+x)\right|_p < p^{-1/(p-1)},$$

άρα το $\log_p(1+x)$ *ανήκει στο πεδίο ορισμού της* $\exp_p$*, και*

$$\exp_p(\log_p(1+x)) = 1+x.$$

Παραλείπουμε την απόδειξη της πρότασης, καθώς προκύπτει από τη θεωρία των τυπικών δυναμοσειρών, και τις ιδιότητες της σύνθεσής δύο δυναμοσειρών. Η απόδειξη των $\exp_p(x) \in p\mathbb{Z}_p$ και $\log_p \in D$ για κάθε $x \in D$, προκύπτει από τις εκτιμήσεις που έχουμε κάνει για τις ποσότητες $\upsilon_p(n!)$ και $\upsilon_p(n)$.

Τονίζουμε όμως, ότι οι υποθέσεις του θεωρήματος για το x είναι πολύ σημαντικές. Για παράδειγμα, για $p = 2$ και $x = -2$, έχουμε:

$$|x|_2 = \frac{1}{2} = 2^{\frac{-1}{2-1}} < 1,$$

δηλαδή $x \notin D$ αλλά $x \in B(0,1)$, και

$$0 = \log_p(1) = \log_p\left((-1)(-1)\right) = 2\log_p(-1) \Rightarrow \log_p(-1) = 0 \in D.$$

Όμως,

$$\exp_p\left(\log_p(-1)\right) = 1 \neq -1.$$

Όπως ορίσαμε την p-αδική λογαριθμική και εκθετική συνάρτηση, μπορούμε να ορίσουμε τη συνάρτηση του p-αδικού ημιτόνου και συνημιτόνου:

$$\sin_p(X) = \sum_{n=0}^{\infty} (-1)^n \frac{X^{2n+1}}{(2n+1)!}$$

$$\cos_p(X) = \sum_{n=0}^{\infty} (-1)^n \frac{X^{2n}}{(2n)!}$$

Οι ακτίνες σύγκλισης των παραπάνω σειρών είναι ίδιες με αυτές της p-αδικής εκθετικής συνάρτησης, εφόσον εμπλέκεται κι εδώ η νόρμα ενός παραγοντικού. Επομένως, το διάστημα σύγκλισης θα είναι και εδώ το D.

Πρόταση 36 *Εάν* $p \equiv 1 \pmod 4$, *τότε υπάρχει* $i \in \mathbb{Q}_p$, *τέτοιο ώστε* $i^2 = -1$, *και ισχύει η σχέση:*

$$\exp_p(ix) = \cos_p(x) + i \sin_p(x)$$

Απόδειξη: Θα εφαρμόσουμε το Λήμμα του Hensel (πρβλ. Ενότητα 4.1, Θεώρημα 11) στη συνάρτηση $f(x) = x^2 + 1$. Αρκέι να βρούμε i_0, τέτοιο ώστε $f(i_0) \equiv 0 \pmod p$, και να επιβεβαιώσουμε ότι $f'(i_0) = 2i_0 \not\equiv 0 \pmod p$.

Μάλιστα, η συνθήκη για την παράγωγο εξασφαλίζεται άμεσα, εφόσον $p = 2 \Rightarrow p \not\equiv 1 \pmod 4$. Έτσι, $f'(i_0) \equiv 0 \pmod p \Leftrightarrow i_0 \equiv 0 \pmod p$. Όμως τότε, $f(i_0) = (\lambda p)^2 + 1 \not\equiv 0 \pmod p$. Επομένως, αρκεί να δείξουμε ότι $f(i_0) \equiv 0 \pmod p$ για κάποιο $i_0 \in \mathbb{F}_p$.

Θα δείξουμε ότι το (-1) είναι τετραγωνικό υπόλοιπο modulo p, όταν $p \equiv 1 \pmod 4$. Από το κριτήριο του *Euler* [2], για $p \neq 2$, έχουμε ότι: ένας αριθμός α, με $\gcd(\alpha, p) = 1$, είναι τετραγωνικό υπόλοιπο modulo p, αν και μόνο αν ισχύει η σχέση:

$$1 \equiv \alpha^{\frac{p-1}{2}} \pmod p.$$

Για $\alpha = (-1)$, έχουμε ότι:

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4\kappa+1-1}{2}} = (-1)^{2\kappa} = 1,$$

Επομένως, υπάρχει i_0 τέτοιο ώστε $f(i_0) \equiv 0 \pmod p$. Από το Λήμμα του Hensel έπεται ότι υπάρχει $i \in \mathbb{Q}_p$, τέτοιο ώστε $f(i) = 0 \Leftrightarrow i^2 = -1$.

Η ισότητα μεταξύ των δυναμοσειρών προκύπτει άμεσα, εφόσον:

$$\exp_p(ix) = \sum_{n=0}^{\infty} \frac{(ix)^n}{n!} = \sum_{n=0}^{\infty} i^n \frac{(x)^n}{n!} = \sum_{k=0}^{\infty} (i)^{2k} \frac{(x)^{2k}}{(2k+1)!} + \sum_{k=0}^{\infty} i^{2k+1} \frac{(x)^{2k+1}}{(2k)!}$$

$$= \sum_{k=0}^{\infty} (-1)^k \frac{(x)^{2k}}{(2k+1)!} + i \sum_{k=0}^{\infty} (-1)^k \frac{(x)^{2k+1}}{(2k)!} = \cos_p(x) + i \sin_p(x).$$

□

[2] βλ. για παράδειγμα [17]

3.8 Σύνοψη και συγκρίσεις

Το σώμα των p-αδικών αριθμών $\mathbb{Q}_p$, για κάθε διαφορετικό πρώτο p, είναι ένα σώμα με αρκετές ομοιότητες με το σώμα των πραγματικών αριθμών $\mathbb{R}$. Είναι σώμα με νόρμα και είναι πλήρες ως προς τη μετρική που επάγει η νόρμα αυτή. Επίσης, αμφότερα είναι πληρώσεις του $\mathbb{Q}$ ως προς τις νόρμες που τα συνοδεύουν, είναι τοπικά συμπαγή, ενώ δεν είναι αλγεβρικά κλειστά.

Όλες αυτές οι ομοιότητες συνεπάγονται και ομοιότητες στα βασικά θεωρήματα, δεδομένου ότι κάθε p-αδική νόρμα κατ' αρχάς είναι νόρμα και έπειτα μη αρχιμήδεια. Συνεπώς, όλη η Ανάλυση που γνωρίζουμε ως τώρα, και που αφορά χώρους με νόρμες, εξακολουθεί να ισχύει.

Όμως, είναι η ιδιότητα της μη αρχιμηδειότητας αυτή που επιφέρει και τις πολλές διαφορές μεταξύ των $\mathbb{Q}_p$ και $\mathbb{R}$. Κατ' αρχάς, το σώμα των πραγματικών αριθμών είναι ένα καλά διατεταγμένο σώμα. Υπάρχει μία καλά ορισμένη έννοια "μεγαλύτερου από" για κάθε δύο στοιχεία του σώματος, η οποία είναι συμβατή με τις πράξεις που ορίζονται σε αυτό. Αντίθετα, κάτι τέτοιο δεν ισχύει για το σώμα των p-αδικών αριθμών, εφόσον, για παράδειγμα, υπάρχουν πολλά διαφορετικά στοιχεία του $\mathbb{Q}_p$ με την ίδια νόρμα.

Επιπλέον, η νόρμα στο $\mathbb{R}$ είναι αρχιμήδεια, ενώ όλες οι p-αδικές νόρμες είναι μη αρχιμήδειες. Αυτό συνεπάγεται ότι το $\mathbb{R}$ είναι συνεκτικό, ενώ το $\mathbb{Q}_p$ είναι ολικά μη συνεκτικό. Έτσι, στα $\mathbb{Q}_p$ δεν υπάρχει ξεκάθαρη η έννοια του διαστήματος και συνεπώς ούτε κάτι ανάλογο της καμπύλης. Είναι αυτές οι αντιθέσεις που επιφέρουν και τις περισσότερες διαφορές μεταξύ της πραγματικής και της p-αδικής αναλυσης.

Συνοψίζουμε τα σημαντικότερα από τα αποτελέσματα που είδαμε ως τώρα:

- Οι μοναδικές, ως προς ισοδυναμία, νόρμες που ορίζονται στο $\mathbb{Q}$ είναι οι διάφορετικές p-αδικές και η συνήθης απόλυτη τιμή, και το $\mathbb{Q}$ δεν είναι πλήρες ως προς καμία από αυτές. Όλες οι p-αδικές νόρμες είναι μη αρχιμήδειες, ενώ η απόλυτη τιμή είναι μία αρχιμήδεια νόρμα.

- Το $\mathbb{Q}_p$ είναι η *πλήρωση* του $\mathbb{Q}$ και το $\mathbb{Z}_p$ είναι η *πλήρωση* του $\mathbb{Z}$ ως προς την p-αδική νόρμα.

- Το $\mathbb{Z}_p$ είναι *συμπαγές*, ενώ το $\mathbb{Q}_p$ είναι *τοπικά συμπαγές*. Επίσης, το $\mathbb{Q}_p$ δεν είναι διατεταγμένο σώμα.

- Το $\mathbb{Q}_p$ είναι ένας ολικά μη συνεκτικός τοπολογικός χώρος Hausdorff.

Όπως σε κάθε σώμα πάνω στο οποίο ορίζεται μία μη αρχιμήδεια νόρμα, στο $\mathbb{Q}_p$ με την p-αδική νόρμα ισχύουν τα ακόλουθα:

- *Όλα τα τρίγωνα είναι ισοσκελή.*

- Κάθε σημείο που περιέχεται σε μια μπάλα είναι και κέντρο της μπάλας.

  Κάθε μπάλα, εκτός της $\overline{B}(x,0) = \{x\}$, είναι *κλειστό-ανοικτό* σύνολο.

  Δύο μπάλες είναι είτε *ξένες ή η μία περιέχει την άλλη.*

Τέλος, ξεχωρίζουμε τις ακόλουθες προτάσεις για την απλότητά τους και τη διαφοροποίησή τους από την κλασσική περίπτωση:

- *Μία ακολουθία* $(a_n)\,,\ a_n \in \mathbb{Q}_p$ *είναι Cauchy ως προς την* p*-αδική νόρμα* $|\cdot|_p$ *αν και μόνο αν:*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

- *Μία άπειρη σειρά* $\sum_{n=0}^{\infty} a_n$ *με* $a_n \in \mathbb{Q}_p$ *συγκλίνει αν και μόνο αν*

$$\lim_{n\to\infty} a_n = 0 \Leftrightarrow \lim_{n\to\infty} |a_n|_p = 0,$$

  και σε αυτή την περίπτωση έχουμε

$$\left|\sum_{n=0}^{\infty} a_n\right|_p \leq \max_n \left\{|a_n|_p\right\}$$

Κεφάλαιο 4

Το Λήμμα του Hensel και μία εφαρμογή στις Διοφαντικές εξισώσεις

Το πρώτο παράδειγμα που μπορεί να μας δείξει τη χρησιμότητα των p-αδικών αριθμών είναι η συμβολή τους στη μελέτη των Διοφαντικών εξισώσεων. Μία Διοφαντική εξίσωση είναι μία πολυωνυμική εξίσωση $f(x_1, x_2, \ldots, x_n) = 0$ με ρητούς ή ακέραιους συντελεστές, στην οποία οι απροσδιόριστες μπορούν να πάρουν ρητές ή ακέραιες τιμές. Η εύρεση ακεραίων λύσεων μιας Διοφαντικής εξίσωσης είναι από τα βασικά προβλήματα της Θεωρίας Αριθμών και μάλιστα από τα δυσκολότερα, αν σκεφτεί κανεις το Τελευταίο Θεώρημα Fermat και το χρόνο που απαίτησε η απόδειξή του.

Μία μέθοδος για τον προσδιορισμό των ακεραίων λύσεων μίας πολυωνυμικής εξίσωσης είναι η διερεύνηση του προβλήματος modulo m, για διαφορετικούς ακεραίους m, δεδομένου ότι: αν υπάρχει ακέραια λύση α, τότε αυτή είναι και λύση modulo m. Όμως, η πολυωνυμική εξίσωση modulo m θα είχε πεπερασμένο αριθμό πιθανών λύσεων. Έτσι, το πρόβλημα εύρεσης ακεραίων λύσεων μιας Διοφαντικής εξίσωσης, μεταξύ άπειρων δυνατών, θα μπορούσε να αναχθεί στο πρόβλημα εύρεσης λύσεων modulo m για κάθε m, που είναι πεπερασμένο για κάθε επιλογή του m.

Στην παραπάνω μέθοδο μπορούμε να εφαρμόσουμε το Κινέζικο Θεώρημα Υπολοίπων, που μας λέει ότι ένα σύστημα εξισώσεων ισοτιμίας modulo ακερ-

αίους a_i, πρώτους προς αλλήλους, είναι ισοδύναμο με μοναδική εξίσωση ισοτιμίας modulo το γινόμενο των a_i. Έτσι, κάθε ακέραιος m της μεθόδου μπορεί να αντικατασταθεί από τις δυνάμεις των πρώτων αριθμών που εμφανίζονται στην παραγοντοποίησή του. Κι επειδή μας ενδιαφέρουν οι λύσεις modulo m για κάθε $m \in \mathbb{Z}$ μελετούμε ισοδύναμα τις λύσεις modulo δυνάμεις οποιουδήποτε πρώτου αριθμού.

Ποιό είναι το όφελος από όλη αυτή τη διαδικασία, σκέφτεται κανείς, αφού έχουμε αντικαταστήσει μία μοναδική εξίσωση από άπειρες άλλες; Η απάντηση βρίσκεται στο ότι για την επίλυση της πρώτης δεν μπορούμε να εφαρμόσουμε κάποιον αλγόριθμο που θα μας δώσει τις λύσεις της Διοφαντικής. Αντίθετα, για την επίλυση των πολλών έχουμε πεπερασμένο αριθμό πιθανών λύσεων για κάθε πρώτο αριθμό, συνεπώς υπάρχει ο εξαντλητικός αλγόριθμος που απλά δοκιμάζει όλες τις πιθανές λύσεις.

Σίγουρα, η διερεύνηση modulo m μας βοηθάει να δώσουμε αρνητικές απαντήσεις για το πρόβλημα, αφού κάθε ακέραια λύση επαληθεύει την εξίσωση και modulo m για κάθε m. Συνεπώς, αν δεν υπάρχει λύση για κάποιο m, τότε δεν μπορεί να υπάρξει ούτε λύση στο $\mathbb{Q}$. Από την p-αδική σκοπιά, το $\mathbb{Q}$ περιέχεται σε κάθε $\mathbb{Q}_p$, άρα αν μία Διοφαντική εξίσωση δεν έχει λύση σε κάποιο από τα $\mathbb{Q}_p$, δεν θα έχει ούτε στο $\mathbb{Q}$.

Θα μπορούσαμε όμως να χρησιμοποιήσουμε τα αποτελέσματα modulo p και modulo δυνάμεις του p για να απαντήσουμε καταφατικά στο ερώτημα της ύπαρξης λύσης; Η ερώτηση αυτή σχετίζεται με το Λήμμα του Hensel και με την Τοπική-Ολική Αρχη, όπως θα δούμε εκτενώς παρακάτω.

4.1 Το Λήμμα του Hensel

Δεδομένου ότι η p-αδική ανάλυση είναι συχνά απλούστερη της πραγματικής, το πρώτο βήμα για την εύρεση ρητών λύσεων μίας εξίσωσης είναι το πέρασμα από την ύπαρξη λύσεων modulo δυνάμεις του p στην ύπαρξη p-αδικών λύσεων. Σε αυτή την καταύθυνση έχουμε το παρακάτω:

Θεώρημα 10 *Ένα πολυώνυμο $F(x) \in \mathbb{Z}[x]$ έχει p-αδική ακέραια ρίζα $a \in \mathbb{Z}_p$ αν και μόνο αν έχει μία ακέραια ρίζα modulo p^n για κάθε $n \geq 1$.*

Απόδειξη: Έστω το πολυώνυμο $F(x) \in \mathbb{Z}[x]$ και $a \in \mathbb{Z}_p$ μια ρίζα του, δηλαδή

$$F(a) = 0.$$

Από την Πρόταση 16 υπάρχει ακολουθία ακεραίων (a_i), τέτοια ώστε:

$$a \equiv a_n \pmod{p^n}.$$

Ισοδύναμα έπεται ότι:

$$F(a) \equiv F(a_n) \pmod{p^n} \Leftrightarrow 0 \equiv F(a_n) \pmod{p^n}.$$

Αντίστροφα, έστω ότι η εξίσωση $F(x) \equiv 0 \pmod{p^n}$ έχει μία ακέραια λύση a_n για κάθε $n \geq 1$. Σύμφωνα με την Πρόταση 23, η ακολουθία (a_n) περιέχει Cauchy υπακολουθία (a_{n_i}). Έστω $a \in \mathbb{Z}_p$ το όριο της (a_{n_i}), το οποίο υπάρχει λόγω πληρότητας του $\mathbb{Z}_p$.

Εφόσον ένα πολυώνυμο είναι συνεχής συνάρτηση, θα έχουμε:

$$F(a) = F(\lim_{i\to\infty} a_{n_i}) = \lim_{i\to\infty} F(a_{n_i}).$$

Δοθέντος ότι $F(a_{k_i}) \equiv 0 \pmod{p^{k_i}}$, για το όριο $\lim_{i\to\infty} F(a_{n_i})$ παίρνουμε:

$$|F(a_{n_i}) - F(a_{n_i-1})|_p = |\kappa p^{n_i} - \lambda p^{n_i-1}|_p \leq \frac{1}{p^{n_i-1}} \longrightarrow_{i\to\infty} 0.$$

Συνεπώς, $F(a) = 0$. □

Παρατήρηση 18 Η ακολουθία (a_n), τα στοιχεία της οποίας είναι ρίζες modulo p^n, είναι ουσιαστικά μια ακολουθία προσεγγίσεων της p-αδικής ρίζας του $F(x)$ ως προς την p-αδική νόρμα.

Το θεώρημα που ειναι γνωστό ως *Λήμμα του Hensel* αφορά πλήρεις αντιμεταθετικούς δακτυλίους (τα p-αδικά σώματα είναι τέτοιοι δακτύλιοι) και είναι ίσως η πιο σημαντική αλγεβρική ιδιότητα των p-αδικών αριθμών. Είναι ένας απλός έλεγχος για το πότε ένα πολυώνυμο έχει ρίζα στους p-αδικούς ακεραίους, που έγκειται στην εύρεση μιας λύσης modulo p, δηλαδή μιας πρώτης

προσέγγισης της ρίζας του πολυωνύμου, και στην επιβεβαίωση μίας συνθήκης για την παράγωγό του στην προσέγγιση αυτή.

Στην απόδειξη του Λήμματος του Hensel κατασκευάζεται μία ακολουθία ριζών modulo p^n, άρα μια ακολουθία προσεγγίσεων της p-αδικής ρίζας του πολυωνύμου.

Θεώρημα 11 (Λήμμα του Hensel) *Έστω $F(x) \in \mathbb{Z}_p[x]$, με $F(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, και έστω ότι υπάρχει $\beta \in \mathbb{Z}_p$ τέτοιο ώστε:*

$$F(\beta) \equiv 0 \pmod{p\mathbb{Z}_p}$$

και

$$F'(\beta) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

όπου με $F'(x)$ συμβολίζουμε την τυπική παράγωγο του πολυωνύμου $F(x)$. Τότε, υπάρχει p-αδικός ακέραιος $\alpha \in \mathbb{Z}_p$, τέτοιος ώστε $\alpha \equiv \beta \pmod{p\mathbb{Z}_p}$ και $F(\alpha) = 0$.

Απόδειξη: Θα δείξουμε ότι η ρίζα α υπάρχει, κατασκευάζοντας ακολουθία Cauchy που να συγκλίνει σε αυτήν. Οι όροι της ακολουθίας μπορεί να είναι στο $\mathbb{Z}$ είτε στο $\mathbb{Z}_p$. Σε κάθε περίπτωση, η ακολουθία θα συγκλίνει σε έναν p-αδικό ακέραιο, εφόσον το $\mathbb{Z}_p$ είναι η πλήρωση του $\mathbb{Z}$ (Πρόταση 16). Εμείς θα κατασκευάσουμε ακολουθία ακεραίων, αν και τα δύο είναι ισοδύναμα, καθώς έχουν να κάνουν με τις κλάσεις ισοδυναμίας που ορίζονται στο $\mathbb{Z}_p/p\mathbb{Z}_p$, το οποίο είναι ισόμορφο με το $\mathbb{Z}/p\mathbb{Z}$.

Ισχυριζόμαστε ότι δοθέντων των υποθέσεων του λήμματος, υπάρχει ακολουθία ακεραίων $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$, τέτοια ώστε:

(i) $F(\alpha_n) \equiv 0 \pmod{p^n}$

(ii) $\alpha_n \equiv \alpha_{n-1} \pmod{p^n}$.

Μάλιστα, η ακολουθία θα είναι μοναδική, αν επιπλέον απαιτήσουμε την παρακάτω συνθήκη για τα α_n:

$$0 \leq \alpha_n < p^{n+1}.$$

Θα κατασκευάσουμε την ακολουθία με επαγωγή στο n.

Παίρνουμε ως α_1 το μοναδικό εκείνο ακέραιο, για τον οποίο ισχύει $\alpha_1 \equiv \beta \pmod{p}$. Για τον α_1 εξακολουθεί να ισχύει ότι $F(\alpha_1) \equiv 0 \pmod{p}$ και $F'(\alpha_1) \not\equiv 0 \pmod{p}$. Θα βρούμε ακέραιο α_2, τέτοιο ώστε να επαληθεύει τις συνθήκες (i) και (ii).

Η συνθήκη (ii) απαιτεί για το α_2 να είναι της μορφής:

$$\alpha_2 = \alpha_1 + b_1 p, \quad \text{όπου } b_1 \in \mathbb{Z}.$$

Αντικαθιστώντας στο πολυώνυμο $F(x)$ το α_2 και αναλύοντας το ανάπτυγμα έχουμε:

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1 p) = \textstyle\sum_{i=0}^{n} a_i(\alpha_1 + b_1 p)^i \\ &= \textstyle\sum_{i=0}^{n} a_i \alpha_1^i + i a_i \alpha_1^{i-1} p + \text{όροι τάξης μεγαλύτερης του } p \\ &= F(\alpha_1) + F'(\alpha_1) b_1 p + \text{όροι τάξης μεγαλύτερης του } p \\ &\equiv F(\alpha_1) + F'(\alpha_1) b_1 p \pmod{p^2}. \end{aligned}$$

Θα προσδιορίσουμε το α_2, δηλαδή ουσιαστικά το b_1, απαιτώντας να ισχύει και η συνθήκη (i). Όμως:

$$F(\alpha_1) \equiv 0 \pmod{p} \Leftrightarrow F(\alpha_1) = \kappa p, \ \kappa \in \mathbb{Z}$$

και

$$F'(\alpha_1) \not\equiv 0 \pmod{p} \Leftrightarrow F'(\alpha_1) \text{ αντιστρέψιμο στο } \mathbb{Z}/p\mathbb{Z},$$

άρα έχουμε:

$$F(\alpha_2) \equiv F(\alpha_1) + F'(\alpha_1) b_1 p \equiv 0 \pmod{p^2} \Leftrightarrow$$

$$\kappa p + F'(\alpha_1) b_1 p \equiv 0 \pmod{p^2} \Leftrightarrow$$

$$\kappa + F'(\alpha_1) b_1 \equiv 0 \pmod{p} \Leftrightarrow$$

$$b_1 \equiv -\kappa (F'(\alpha_1))^{-1} \pmod{p}.$$

Είναι προφανές ότι το b_1 είναι μοναδικό και ότι μπορούμε να το επιλέξουμε έτσι ώστε $0 \leq b_1 \leq p-1$. Έτσι, δοθέντος του α_1 υπάρχει μοναδικό α_2 που να ικανοποιεί τις συνθήκες (i) και (ii).

Θα δείξουμε τώρα και το επαγωγικό βήμα, ότι δηλαδή δοθέντος του α_k μπορούμε να βρούμε μοναδικό α_{k+1} που να ικανοποιεί τις παραπάνω συνθήκες.

Ακολουθώντας τις ίδιες ακριβώς σκέψεις, ο όρος α_{k+1} θα είναι της μορφής:

$$\alpha_{k+1} = \alpha_k + b_k p^k, \text{ με } b_k \in \mathbb{Z}.$$

Αντικαθιστούμε στο πολυώνυμο το α_{k+1} και κάνουμε το ανάπτυγμα, οπότε παίρνουμε:

$$\begin{aligned} F(\alpha_{k+1}) &= F(\alpha_k + b_k p^k) = \textstyle\sum_{i=0}^{n} a_i(\alpha_k + b_k p^k)^i \\ &= \textstyle\sum_{i=0}^{n} a_i \alpha_k^i + i a_i \alpha_k^{i-1} + \text{όροι τάξης μεγαλύτερης του } p^k \\ &= F(\alpha_k) + F'(\alpha_k) b_k p^k + \text{όροι τάξης μεγαλύτερης του } p^k \\ &\equiv F(\alpha_k) + F'(\alpha_k) b_k p^k \pmod{p^{k+1}}. \end{aligned}$$

Θα απαιτήσουμε την ισχύ της πρώτης συνθήκης για το α_{k+1}, έχοντας τα εξής:

$$\begin{aligned} &\alpha_k \equiv \alpha_{k-1} \pmod{p^{k-1}} \\ &\alpha_{k-1} \equiv \alpha_{k-2} \pmod{p^{k-2}} \\ &\vdots \\ &\alpha_2 \equiv \alpha_1 \pmod{p} \end{aligned}$$

$$\Rightarrow F'(\alpha_k) \equiv F'(\alpha_1) \not\equiv 0 \pmod{p},$$

δηλαδή το $F'(\alpha_k)$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}/p\mathbb{Z}$. Ακόμα, $F(\alpha_k) \equiv 0 \pmod{p^k} \Leftrightarrow F(\alpha_k) = \kappa' p^k$.

Επομένως, $\alpha_{k+1} = \alpha_k + b_k p^k$, όπου το b_k προκύπτει από το:

$$F(\alpha_k) + F'(\alpha_k) b_k p^k \equiv 0 \pmod{p^{k+1}} \Rightarrow$$

$$\kappa' p^k + F'(\alpha_k) b_k p^k \equiv 0 \pmod{p^{k+1}} \Rightarrow$$

$$\kappa' + F'(\alpha_k)b_k \equiv 0 \pmod{p} \Rightarrow$$

$$b_k \equiv -\kappa'(F'(\alpha_k))^{-1} \pmod{p}.$$

Δηλαδή, ο $(k+1)$-οστός όρος της ακολουθίας έχει τη μορφή:

$$\begin{aligned}\alpha_{k+1} &= \alpha_k - \kappa'(F'(\alpha_k))^{-1}p^k \\ &= \alpha_k - \tfrac{F(\alpha_k)}{p^k}(F'(\alpha_k))^{-1}p^k \\ &= \alpha_k - F(\alpha_k)(F'(\alpha_k))^{-1}.\end{aligned}$$

Έτσι, κατασκευάσαμε μια συνεπή ακολουθία ακεραίων αριθμών, άρα Cauchy ως προς την p-αδική νόρμα, της οποίας το όριο α θα ικανοποιεί ότι $F(\alpha) = 0$ λόγω συνέχειας, και $\alpha \equiv \beta \pmod{p}$ από κατασκευή. □

Παρατήρηση 19 Αξίζει να αναλύσουμε λίγο περισσότερο τη σημασία των δύο συνθηκών που απαιτούνται στο λήμμα. Η πρώτη συνθήκη μας εξασφαλίζει μία p-αδική ρίζα modulo p του πολυωνύμου F, δηλαδή μία πρώτη προσέγγιση β της ρίζας που στέλνει την τιμή $F(\beta)$ στη μπάλα με κέντρο το μηδέν και ακτίνα $1/p$. Πράγματι, το $F(\beta)$ ανήκει στο $\mathbb{Z}_p$, λόγω της κλειστότητας της πρόσθεσης και του πολλαπλασιασμού στον δακτύλιο $\mathbb{Z}_p$, και $p \mid F(\beta)$, δηλαδή:

$$F(\beta) \in \mathbb{Z}_p \quad \text{και} \quad |F(\beta)|_p \leq \frac{1}{p}. \tag{4.1}$$

Η δεύτερη συνθήκη μας λέει ότι η προσέγγιση β είναι απλή ρίζα modulo p, δηλαδή $F(x) \equiv (x-\beta)G(x) \pmod{p}$ και το β δεν είναι ρίζα του $G(x)$. Πράγματι, αν η προσέγγιση β ήταν διπλή ρίζα modulo p, δηλαδή $F(x) \equiv (x-\beta)^2 H(x) \pmod{p}$, τότε, μετά από τις απαραίτητες πράξεις, προκύπτει ότι $F'(\beta) = G(\beta) \equiv 0 \pmod{p}$, και άρα το $F'(\beta)$ δεν θα ήταν αντιστρέψιμο στοιχείο στο $\mathbb{Z}_p$.

Το $F'(\beta)$ ανήκει επίσης στο $\mathbb{Z}_p$ και η δεύτερη συνθήκη απαιτεί ότι:

$$p \nmid F'(\beta) = G(\beta) \Leftrightarrow |F'(\beta)|_p = |G(\beta)|_p = 1,$$

και άρα

$$p^2 \nmid F(\beta) \Leftrightarrow |F(\beta)|_p > \frac{1}{p^2}. \tag{4.2}$$

Από τις εξισώσεις (4.1) και (4.2) προκύπτει ότι $|F(\beta)|_p = 1/p$.

Το Λήμμα του Hensel καλείται και p-αδική μέθοδος Newton, καθώς η τεχνική προσέγγισης της ρίζας που χρησιμοποιείται στην απόδειξη είναι ουσιαστικά ίδια με την αριθμητική μέθοδο Newton-Raphson.

Ας θυμίσουμε όμως τη μέθοδο αυτή της Αριθμητικής Ανάλυσης, ώστε να κάνουμε τελικά και τη σύγκριση μεταξύ των δύο. Η μέθοδος Newton-Raphson είναι μια επαναληπτική μέθοδος, ειδική περίπτωση της μεθόδου σταθερού σημείου, και είναι μία από τις πιο δυνατές και γνωστές μεθόδους για την προσέγγιση μίας πραγματικής ρίζας ξ μίας εξίσωσης $f(x) = 0$. Δοθέντος ενός αρχικού σημείου ξ_0, αυτό παράγει μία ακολουθία προσεγγίσεων της ρίζας ξ, τέτοια ώστε κάθε επόμενη προσέγγιση να δίνεται από τον τύπο:

$$\xi_{n+1} = \xi_n - \frac{f(\xi_n)}{f'(\xi_n)}.$$

Η κατασκευή της γίνεται είτε γεωμετρικά ή με το ανάπτυγμα Taylor. Όσον αφορά τη σύγκλιση της μεθόδου έχουμε το ακόλουθο θεώρημα:

Θεώρημα 12 *Υποθέτουμε ότι $f \in C^2[a,b]$. Αν $\xi \in [a,b]$ με $f(\xi) = 0$ και $f'(\xi) \neq 0$, δηλαδή αν το ξ είναι μία απλή ρίζα, τότε υπάρχει θετικός πραγματικός αριθμός δ, τέτοιος ώστε η ακολουθία προσεγγίσεων (ξ_n) η οποία ορίζεται με τη μέθοδο Newton-Raphson, να συγκλίνει στη ρίζα ξ της εξίσωσης για κάθε αρχική προσέγγιση $\xi_0 \in [\xi - \delta, \xi + \delta]$.*

Στο Λήμμα του Hensel έχουμε ότι για να υπάρχει ρίζα του πολυωνύμου F στους p-αδικούς αριθμούς πρέπει να υπάρχει ρίζα modulo p, στην οποία επιπλέον να εξασφαλίζεται μία συνθήκη για την παράγωγο F'. Αντίστοιχα, στη Newton-Raphson η ύπαρξη ρίζας μιας συνάρτησης f ελέγχεται είτε γραφικά ή με το Θεώρημα Bolzano. Και σε αυτήν την περίπτωση ζητείται μια συνθήκη για την παράγωγο f', όμως αυτή τη φορά την παράγωγο στη ρίζα. Θα μπορούσαμε να πούμε ότι η ρίζα modulo p είναι το αντίστοιχο του ελέγχου των προσήμων της f στα άκρα του διαστήματος, του Θεωρήματος Bolzano. Η συνθήκη της παραγώγου μας λέει και στις δύο περιπτώσεις ότι πρόκειται για απλή ρίζα του πολυωνύμου.

Αφού εξασφαλιστεί η ύπαρξη ρίζας, η μέθοδος προσέγγισής της είναι και στα δύο ακριβώς η ίδια. Όμως, το μεν Λήμμα του Hensel εγγυάται ότι η ακολουθία προσεγγίσεων συγκλίνει σε αυτήν, η δε Newton-Raphson συγκλίνει στη ρίζα

εφόσον η αρχική προσέγγιση βρίσκεται αρκετά κοντά της, μεσα σε ένα διάστημα $(\xi \pm \delta)$. Γι' αυτό το λόγο, για να δοθεί κατάλληλο ξ_0, πρέπει να προηγηθεί είτε γραφικός εντοπισμός της ρίζας και επιλογή κάποιου ξ_0 κοντά της, ή κάποια άλλη αριθμητική μέθοδος, που ίσως είναι πιο αργή από τη Newton-Raphson, αλλά σίγουρα συγκλίνει στη ρίζα.

Σημειώνουμε ότι λόγω πληρότητας των $\mathbb{R}$ και $\mathbb{Z}_p$, οι ακολουθίες προσεγγίσεων θα συγκλίνουν σε κάποιο στοιχείο στους χώρους αυτούς.

4.1.1 Άλλες μορφές του Λήμματος του Hensel

Υπάρχει μια άλλη μορφή του Λήμματος του Hensel, πιο ισχυρή από αυτήν που μόλις παρουσιάσαμε. Την παραθέτουμε χωρίς απόδειξη.

Θεώρημα 13 (Λήμμα του Hensel-ισχυρή μορφή) *Έστω $F(x) \in \mathbb{Z}_p[x]$ και έστω ότι υπάρχει ένα στοιχείο $a_0 \in \mathbb{Z}_p$, τέτοιο ώστε:*

$$|F(a_0)|_p < |F'(a_0)|_p^2,$$

όπου με $F'(x)$ συμβολίζουμε την τυπική παράγωγο του πολυωνύμου $F(x)$. Τότε, υπάρχει μοναδικός p-αδικός ακέραιος $a \in \mathbb{Z}_p$, τέτοιος ώστε:

$$|a - a_0|_p \leq |F(a_0)|_p / |F'(a_0)|_p$$

και $F(a) = 0$.

Τέλος, παραθέτουμε μία μορφή του Λήμματος που περιλαμβάνει την έννοια του αναγώγου πολυωνύμου. Η ιδέα της είναι ότι αν ένα πολυώνυμο δεν είναι ανάγωγο modulo p και ένας από τους παράγοντες είναι την μορφής $(x - \alpha)$, δηλαδή

$$f(x) \equiv (x - \alpha) g(x) \pmod{p},$$

τότε υπάρχει παρόμοια παραγοντοποίηση στο $\mathbb{Z}_p[x]$.

Θα μπορούσαμε να εισάγουμε μία έννοια ''πρώτων μεταξύ τους'' παραγόντων ενός πολυωνύμου, καθώς η συνθήκη για την παράγωγο στο Λήμμα ουσιαστικά μας λέει ότι η ο δεύτερος παράγοντας $g(x)$ δεν διαιρείται από το $(x - a)$.

Ορισμός 30 *Έστω $g(x), h(x)$ πολυώνυμα του $\mathbb{Z}_p[x]$. Έστω $\overline{g}(x)$ και $\overline{h}(x)$ να είναι τα πολυώνυμα $g(x)$ και $h(x)$ με τους συντελεστές τους παρμένους modulo p, δηλαδή $\overline{g}(x), \overline{h}(x) \in \mathbb{Z}_p/p\mathbb{Z}_p[x] \cong \mathbb{Z}/p\mathbb{Z}[x]$. Λέμε ότι τα πολυώνυμα $g(x), h(x)$ είναι πρώτα μεταξύ τους* modulo p, *όταν* $\gcd(\overline{g}, \overline{h}) = 1$ *στο* $\mathbb{Z}/p\mathbb{Z}[x]$. *Ισοδύναμα, όταν υπάρχουν πολυώνυμα $a(x), b(x) \in \mathbb{Z}_p[x]$, τέτοια ώστε:*

$$a(x)g(x) + b(x)h(x) \equiv 1 \pmod{p},$$

όπου η ισοτιμία νοείται συντελεστή προς συντελεστή, δηλαδή λέμε ότι δύο πολυώνυμα είναι ισότιμα modulo p αν κάθε συντελεστής του ενός είναι ισότιμος modulo p με τον αντίστοιχο συντελεστή του δευτέρου.

Θεώρημα 14 (Λήμμα του Hensel, δεύτερη μορφή) *Έστω $f(x) \in \mathbb{Z}_p[x]$ πολυώνυμο με συντελεστές στο $\mathbb{Z}_p$. Υποθέτουμε ότι υπάρχουν πολυώνυμα $g_1(x)$ και $h_1(x)$ στο $\mathbb{Z}_p$, τέτοια ώστε:*

(i) *το $g_1(x)$ είναι μονικό,*

(ii) *τα $g_1(x)$ και $h_1(x)$ είναι πρώτα μεταξύ τους modulo p,*

(iii) $f(x) \equiv g_1(x)h_1(x) \pmod{p}$.

Τότε υπάρχουν πολυώνυμα $g(x), h(x) \in \mathbb{Z}_p[x]$, τέτοια ώστε:

(i) *το $g(x)$ είναι μονικό,*

(ii) $g(x) \equiv g_1(x) \pmod{p}$ *και* $h(x) \equiv h_1(x) \pmod{p}$, *και*

(iii) $f(x) = g(x)h(x)$.

4.1.2 Εφαρμογές του Λήμματος του Hensel

Θα δουμε τρεις απλές, αλλά πολύ ενδιαφέρουσες εφαρμογές του Λήμματος του Hensel.

Πρώτη Εφαρμογή: Οι ρίζες της μονάδας στο $\mathbb{Q}_p$

Θυμίζουμε ότι ένα στοιχείο ξ λέγεται m-οστή ρίζα της μονάδας αν $\xi^m = 1$. Αν επιπλέον το m είναι ο ελάχιστος τέτοιος αριθμός, δηλαδή $\xi^n \neq 1$ για $0 < n < m$, τότε η ξ καλείται πρωταρχική ρίζα της μονάδας.

Για να χρησιμοποιήσουμε το Λήμμα του Hensel χρειαζόμαστε ένα πολυώνυμο. Αφού ψάχνουμε για ρίζες της μονάδας, το κατάλληλο πολυώνυμο είναι το $F(x) = x^m - 1$ με $F'(x) = mx^{m-1}$. Θα αναζητήσουμε λύσεις διάφορες της τετριμμένης, δηλαδή διάφορες της μονάδας.

Θέλουμε να ισχύει η δεύτερη συνθήκη του λήμματος, δηλαδή $F'(x) \not\equiv 0 \pmod{p}$. Παρατηρούμε ότι αν $F'(\lambda) \equiv 0 \pmod{p}$ για κάποιο $\lambda \in \mathbb{Z}_p$, θα πρέπει είτε ο p να διαιρεί τον λ, που όμως τότε το λ δεν είναι ρίζα του πολυωνύμου $F(x)$ modulo p, ή πρέπει ο p να διαιρεί το m. Συνεπώς, η δεύτερη συνθήκη του λήμματος ισχύει όταν ο p δεν διαιρεί το m.

Για την πρώτη συνθήκη πρέπει να βρούμε μια αρχική προσέγγιση της ρίζας, δηλαδή έναν ακέραιο $\alpha_1 \not\equiv 1 \pmod{p}$ που να ικανοποιεί την $\alpha_1^m \equiv 1 \pmod{p}$. Κάτι τέτοιο όμως είναι άμεσο απο το γεγονός ότι η πολλαπλασιαστική ομάδα του σώματος $\mathbb{Z}/p\mathbb{Z}$ είναι κυκλική, τάξης $p-1$. Συνεπώς, για m διαιρέτη του $p-1$ υπάρχει υποομάδα τάξης m, και άρα στοιχείο α_1 που την παράγει, και αντιστρόφως (από το Θεώρημα Lagrange).

Συνοψίζοντας, για κάθε πρώτο αριθμό p και θετικό ακέραιο m, με $m \mid p-1$, μπορούμε να βρούμε α_1 ώστε $\alpha_1 \not\equiv 0, 1 \pmod{p}$ και $\alpha_1^m \equiv 1 \pmod{p}$. Αν $\gcd(m, p-1) = 1$, τότε δεν υπάρχει α_1 ώστε $\alpha_1^m \equiv 1 \pmod{p}$. Επομένως, εφαρμόζοντας το Λήμμα του Hensel παίρνουμε την ακόλουθη πρόταση.

Πρόταση 37 *Για κάθε πρώτο p και για κάθε θετικό ακέραιο m που δεν διαιρείται από τον p, υπάρχει πρωταρχική m-οστή ρίζα της μονάδας στο $\mathbb{Q}_p$ αν και μόνο αν το m διαιρεί τον $p-1$.*

Παρατήρηση 20 Το γεγονός ότι η ρίζα θα είναι πρωταρχική ρίζα της μονάδας προκύπτει άμεσα από τον ορισμό της τάξης ενός στοιχείου μιας ομάδας. Επιπλέον, η ρίζα θα ανήκει στο $\mathbb{Z}_p$, αφού:

$$\xi^m = 1 \Leftrightarrow |\xi^m|_p = 1 \Leftrightarrow |\xi|_p^m = 1 \Rightarrow |\xi|_p = 1.$$

Παρατήρηση 21 Τέλος, αξίζει να σημειώσουμε ότι αν $m \mid p-1$, τότε κάθε m-οστή ρίζα της μονάδας είναι επίσης και $(p-1)$-οστή ρίζα της μονάδας.

Συνεπώς, οι ρίζες τάξης m της μονάδας στο $\mathbb{Q}_p$, όπου m, p πρώτοι προς αλλήλους, είναι ακριβώς οι $(p-1)$-οστές ρίζες της μονάδας.

Με την προηγούμενη ανάλυση καταφέραμε να προσδιορίσουμε όλες τις ρίζες της μονάδας στο $\mathbb{Q}_p$, εκτός από αυτές με τάξη $m = p^n$, αφού για να εφαρμόσουμε το Λήμμα του Hensel απαιτήσαμε ο p να μη διαιρεί τον m. Επομένως, δεν μπορούμε να προσεγγίσουμε τις p^n-οστές ρίζες της μονάδας με αυτή τη μέθοδο. Όμως, αποδεικνύεται ότι αυτές δεν ανήκουν στο $\mathbb{Q}_p$, με εξαίρεση την περίπτωση όπου $p = 2$. Έτσι, έχουμε βρει όλες τις ρίζες της μονάδας που ανήκουν στο $\mathbb{Q}_p$, αν και αυτό δεν μπορούμε να το αποδείξουμε με τα τωρινά μας εφόδια.

Δεύτερη εφαρμογή: ο καθορισμός των τετραγώνων στο $\mathbb{Q}_p$

Ένα $b \in \mathbb{Q}_p$ είναι τετράγωνο αν υπάρχει $a \in \mathbb{Q}_p$, τέτοιο ώστε $a^2 = b$. Κατ' αρχάς θα εξετάσουμε την περίπτωση, πότε ένα στοιχείο του $\mathbb{Z}_p^*$, δηλαδή μία p-αδική μονάδα, είναι τετράγωνο:

Πρόταση 38 *Έστω $p \neq 2$ ένας πρώτος αριθμός και έστω $b \in \mathbb{Z}_p^*$ μία p-αδική μονάδα. Εάν υπάρχει $a_1 \in \mathbb{Z}_p^*$, τέτοιο ώστε $a_1^2 \equiv b \pmod{p\mathbb{Z}_p}$, τότε το b είναι το τετράγωνο κάποιου στοιχείου του $\mathbb{Z}_p$.*

Απόδειξη: Θα εφαρμόσουμε το Λήμμα του Hensel στο πολυώνυμο $F(x) = x^2 - b$. Από υπόθεση έχουμε ότι υπάρχει $a_1 \in \mathbb{Z}_p$, τέτοιο ώστε $a_1^2 \equiv b \pmod{p\mathbb{Z}_p}$, δηλαδή $F(a_1) \equiv 0 \pmod{p\mathbb{Z}_p}$.

Επιπλέον, $F'(a_1) = 2a_1 \not\equiv 0 \pmod{p\mathbb{Z}_p}$. Πράγματι, αν $F'(a_1) \equiv 0 \pmod{p\mathbb{Z}_p}$, τότε θα είχαμε είτε $p \mid 2$ ή $p \mid a_1$. Από υπόθεση $p \neq 2$, άρα θα πρέπει $p \mid a_1$. Τότε όμως ο p θα διαιρεί και το b, δηλαδή $b \notin \mathbb{Z}_p^*$ (Πρόταση 20), που είναι άτοπο αφού από υπόθεση $b \in \mathbb{Z}_p^*$.

Έτσι, από το Λήμμα του Hensel, έχουμε το ζητούμενο, ότι δηλαδή το πολυώνυμο $x^2 = b$ έχει ρίζα στο $\mathbb{Z}_p$, άρα ότι το b είναι τπο τετράγωνο κάποιου στοιχείου a του $\mathbb{Z}_p$. Το a θα είναι επίσης αντιστρέψιμο, εφόσον $a \equiv a_1 \pmod{p\mathbb{Z}_p}$. □

Μπορούμε να επεκτείνουμε τα παραπάνω σε ολόκληρο το $\mathbb{Q}_p$, αν θυμηθούμε ότι κάθε $x \in \mathbb{Q}_p$ γράφεται ως $x = p^{v_p(x)}x'$, όπου $x' \in \mathbb{Z}_p^*$ (Πόρισμα 6). Επιπλέον, θυμίζουμε ότι ένας αριθμός a καλείται *τετραγωνικό υπόλοιπο* modulo κάποιον πρώτο p, αν $p \nmid a$ και η εξίσωση $x^2 \equiv a \pmod{p}$ έχει λύση.

Πόρισμα 10 *(i) Έστω $p \neq 2$ πρώτος αριθμός. Ένα στοιχείο $x \in \mathbb{Q}_p$ είναι τετράγωνο κάποιου p-αδικού αριθμού, αν και μόνο αν μπορεί να γραφεί ως $x = p^{2n}y^2$, με $n \in \mathbb{Z}$ και $y \in \mathbb{Z}_p^\star$.*

(ii) Η ομάδα πηλίκο $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ έχει τάξη τέσσερα. Αν $c \in \mathbb{Z}_p^\star$ είναι οποιοδήποτε στοιχείο, που δεν είναι τετραγωνικό υπόλοιπο modulo p, τότε το σύνολο $\{1, p, c, cp\}$ είναι ένα πλήρες σύνολο εκπροσώπων των συμπλόκλων του $(\mathbb{Q}_p^\times)^2$ στο $\mathbb{Q}_p^\times$.

Απόδειξη:

(i) Προφανώς, αν $x = a^2$ με $x,\ a \in \mathbb{Q}_p$, και δεδομένου ότι $a = p^{v_p(a)}a',\ a' \in \mathbb{Z}_p^\star$, τότε $x = p^{2v_p(a)}a'^2$ με $v_p(a) \in \mathbb{Z}$ και $a' \in \mathbb{Z}_p^\star$.

Αντίστροφα, αν $x = p^{2n}y^2$, τότε $x = (p^n y)^2$ με $p^n y \in \mathbb{Q}_p$.

(ii) Για τον δεύτερο ισχυρισμό έχουμε ότι τα σύμπλοκα της ομάδας-πηλίκο $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ θα είναι της μορφής $x(\mathbb{Q}_p^\times)^2,\ x \in \mathbb{Q}_p$. Ένα $x \in \mathbb{Q}_p^\times$ είναι της μορφής $p^{v_p(x)}x',\ x' \in \mathbb{Z}_p^\star$. Τότε θα έχουμε τις εξής περιπτώσεις:

- $v_p(x)$ άρτιος και $x' = y^2,\ y \in \mathbb{Z}_p^\star$. Τότε, $x \in 1 \cdot (\mathbb{Q}_p^\times)^2$.
- $v_p(x)$ άρτιος και x' όχι τετράγωνο στο $\mathbb{Z}_p^\star$. Τότε, το $p^{v_p(x)}$ απορροφάται στο $(\mathbb{Q}_p^\times)^2$, ενώ το x' όχι. Έτσι, $x \in x' \cdot (\mathbb{Q}_p^\times)^2$.
- $v_p(x)$ περιττός και $x' = y^2,\ y \in \mathbb{Z}_p^\star$, δηλαδή $x = p^{2k+1}y^2 = pp^{2k}y^2$. Τότε, το $p^{2k}y^2$ απορροφάται στο $(\mathbb{Q}_p^\times)^2$ και άρα $x \in p \cdot (\mathbb{Q}_p^\times)^2$.
- $v_p(x)$ περιττός και x' όχι τετράγωνο στο $\mathbb{Z}_p^\star$, δηλαδή $x = pp^{2k}x'$. Τότε, $x \in p\,x'(\mathbb{Q}_p^\times)^2$.

Έτσι, καταλήξαμε σε τέσσερις διαφορετικές μορφές συμπλόκων. Το δεύτερο κομμάτι του ισχυρισμού φαίνεται ξεκάθαρα από τη μορφή των συμπλόκων. □

Το πιο ενδιαφέρον σε σχέση με το παραπάνω αποτέλεσμα είναι όταν κάνουμε τη σύγκριση με το ανάλογό του στο $\mathbb{R}$. Στο $\mathbb{R}$ έχουμε ότι ένας πραγματικός αριθμός είναι τέλειο τετράγωνο αν και μόνο αν είναι θετικός αριθμός. Η ομάδα-πηλίκο $\mathbb{R}^\times/(\mathbb{R}^\times)^2$ έχει τάξη δύο και σύνολο εκπροσώπων το $\{1, -1\}$. Το Πόρισμα 10 φαίνεται τώρα ως η p-αδική άποψη του ''κανόνα των προσήμων'' για τον πολλαπλασιασμό πραγματικών αριθμών.

Για να ολοκληρώσουμε το πόρισμα πρέπει να αναφέρουμε και την περίπτωση όπου $p = 2$. Γι' αυτό χρησιμοποιούμε την ισχυρότερη μορφή του Λήμματος του Hensel, εφόσον το $F'(a_1) = 2a_1$ πάντα θα διαιρείται από το δύο, και έτσι δεν θα εξασφαλίζεται η δεύτερη συνθήκη του Λήμματος όπως πριν.

Τρίτη εφαρμογή: Οι p-αδικές ρίζες μιας Τετραγωνικής Μορφής

Θυμίζουμε ότι μία τετραγωνική μορφή είναι ουσιαστικά ένα ομογενές πολυώνυμο δευτέρου βαθμού.

Ορισμός 31 Έστω V διανυσματικός χώρος διάστασης n ορισμένος πάνω σε ένα σώμα $\mathbb{K}$. Μια *τετραγωνική τορφή* είναι μία συνάρτηση $F : V \longrightarrow \mathbb{K}$ τέτοια ώστε:

$$F(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_{ii} x_i^2 + 2 \sum_{i<j} a_{ij} x_i x_j, \ a_{ij} \in \mathbb{K}.$$

Θυμίζουμε ακόμα ότι η τετραγωνική μορφή $F(x_1, \ldots, x_n)$ μπορεί μέσω ενός γραμμικού μετασχηματισμού να έρθει στην κανονική της μορφή

$$F(x_1, \ldots, x_n) = \sum_{i=1}^{n} c_{ii} x_i^2, \quad c_{ii} \in \mathbb{K}.$$

Τέλος, μπορούμε να υποθέσουμε ότι οι συντελεστές c_{ii} είναι ελεύθεροι τετραγώνων, δηλαδή δεν είναι της μορφής $c_{ii} = c'_{ii} s^2$, εφόσον οποιαδήποτε τετράγωνα στην ανάλυση των συντελεστών απορροφούνται στις μεταβλητές.

Άρα, στη δική μας περίπτωση, η γενική περίπτωση μιας τετραγωνικής μορφής είναι η:

$$F(x_1, \ldots, x_n, y_1, \ldots, y_m) = \sum_{j=1}^{n} a_j x_j^2 + \sum_{i=1}^{m} p\, b_i y_i^2, \quad a_j, b_i \in \mathbb{Z}_p^*$$

Θα μελετήσουμε διεξοδικά τη συνάρτηση $ax^2 + by^2 + cz^2$, όπου υποθέτουμε ότι a, b, $c \in \mathbb{Z}$, για να βρούμε όλες τις συνθήκες που απαιτούνται ώστε αυτή να έχει μη τετριμμένες p-αδικές ρίζες σε κάθε σώμα $\mathbb{Q}_p$, $p \leq \infty$.

Κατ' αρχάς, αν κάποιο από τα a, b, c είναι μηδέν, τότε βρίσκουμε εύκολα μία μη τετριμμένη λύση της εξίσωσης: Θέτουμε τις δύο μεταβλητές των μη

μηδενικών συντελεστών ίσες με το μηδέν, και δίνουμε στην τρίτη οποιαδήποτε μη μηδενική τιμή.

Επιπλέον, είναι προφανές ότι μπορούμε να απλοποιήσουμε τους όποιους παρονομαστές, άρα μπορούμε να υποθέσουμε ότι τα a, b, c είναι ακέραιοι. Μπορούμε επίσης να υποθέσουμε ότι είναι ελεύθεροι τετραγώνων. Τέλος, μπορούμε να υποθέσουμε ότι δεν έχουν κοινούς παράγοντες, ότι δηλαδή $\gcd(a,b,c)=1$, διότι τότε θα μπορούσαμε να τους διαγράψουμε.

Μάλιστα, μπορούμε να δούμε ότι τότε $\gcd(a,b)=\gcd(a,c)=\gcd(c,b)=1$, ότι δηλαδή ανά δύο δεν έχουν κοινούς παράγοντες. Ισοδύναμα, θα έχουμε ότι το γινόμενο abc είναι ελεύθερο τετραγώνων.

Θα δείξουμε ότι μία λύση (x,y,z) της εξίσωσης $ax^2+by^2+cz^2=0$ είναι και λύση μιας $dx^2+ey^2+fz^2=0$, η οποία ικανοποιεί την υπόθεση ότι το abc είναι ελεύθερο τετραγώνων. Πράγματι, έστω $k=\gcd(a,b)>1$, δηλαδή $a=a'k,\ b=b'k$, ενώ $\gcd(a,c)=\gcd(b,c)=1$. Το k είναι ελεύθερο τετραγώνων, λόγω της υπόθεσής μας ότι τα a, b είναι ελευθέρα τετραγώνων. Ακόμα, $\gcd(k,c)=1$. Αντικαθιστώντας τα a, b στην εξίσωση παίρνουμε:

$$a'kx^2+b'ky^2+cz^2=0 \Rightarrow k|cz^2 \overset{\gcd(k,c)=1}{\Longrightarrow} k|z^2.$$

Επειδή όμως το k είναι ελεύθερο τετραγώνων, και άρα δεν μπορεί να είναι τετράγωνο, έπεται ότι $k|z$. Αν αντικαταστήσουμε το z με kz' στην εξίσωση παίρνουμε:

$$a'kx^2+b'ky^2+c(kz')^2=0 \Rightarrow a'x^2+b'y^2+kcz'^2=0.$$

Δηλαδή, προκύπτει μία εξίσωση τριών μεταβλητών, x,y,z', ισοδύναμη με την αρχική, που ικανοποιεί ότι $\gcd(a',b')=\gcd(a',kc)=\gcd(kc,b')=1$.

Έχουμε λοιπόν την εξίσωση $ax^2+by^2+cz^2=0$, τέτοια ώστε τα a, b, c να είναι *ακέραιοι, ελεύθεροι τετραγώνων και ανά δύο πρώτοι μεταξύ τους.* Θα μελετήσουμε τη συμπεριφορά της εξίσωσης στα διαφορετικά $\mathbb{Q}_p$, δηλαδή πότε έχει λύσεις σε όλα τα $\mathbb{Q}_p$, $p\leq\infty$.

Με χρήση του Λήμματος του Hensel θα δείξουμε το παρακάτω Θεώρημα:

Θεώρημα 15 *Έστω ακέραιοι $a,b,c\in\mathbb{Z}$, ανά δύο πρώτοι μεταξύ τους και ελεύθεροι τετραγώνων. Η εξίσωση*

$$ax^2+by^2+cz^2=0$$

έχει μη τετριμμένες λύσεις σε κάθε $\mathbb{Q}_p$, $p \leq \infty$, αν και μόνο αν ικανοποιούνται οι ακόλουθες συνθήκες:

(i) *Τα a, b, c δεν είναι ομόσημα.*

(ii) *Για κάθε περιττό πρώτο p που διαιρεί έναν από τους συντελεστές, έστω τον a, τότε για τους άλλους δύο υπάρχει ακέραιος αριθμός r, τέτοιος ώστε $b + r^2 c \equiv 0 \pmod{p}$.*

(iii) *Αν τα a, b, c είναι όλοι περιττοί, τότε δύο από αυτους θα έχουν άθροισμα διαιρετό από το τέσσερα.*

(iv) *Αν κάποιος από τους a, b, c είναι άρτιος, τότε είτε το άθροισμα των υπόλοιπων δύο ή το άθροισμα και των τριών είναι διαιρετό από το οκτώ.*

Απόδειξη Θεωρήματος 15:

Ας εξετάσουμε πρώτα την περίπτωση $p = \infty$, δηλαδή στο $\mathbb{Q}_p = \mathbb{R}$, που είναι και η πιο απλη. Η εξίσωση δεν έχει μη τετριμμένες πραγματικές λύσεις ακριβώς όταν τα a, b, c είναι όλα θετικά ή όλα αρνητικά.

Έστω τώρα p πρώτος, που δεν διαιρεί κανέναν από τους συντελεστές a, b, c. Θα μελετήσουμε τη συμπεριφορά της εξίσωσης modulo p για να διεξάγουμε συμπεράσματα για τη συμπεριφορά της στο $\mathbb{Q}_p$, τα οποία παραθέτουμε υπό μορφή προτάσεων και λημμάτων. Ως προς το πρώτο σκέλος ισχύει το ακόλουθο αποτέλεσμα για $p \neq 2$. Στη συνέχεια θα εξετάσουμε και την περίπτωση $p = 2$.

Πρόταση 39 *Έστω p περιττός πρώτος και έστω a, b, c ακέραιοι, ανά δύο πρώτοι μεταξύ τους, τέτοιοι ώστε να μην διαιρούνται από τον p. Τότε, υπάρχουν ακέραιοι x_0, y_0, z_0, όχι όλοι μηδέν modulo p, τέτοιοι ώστε:*

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}.$$

Πριν αποδείξουμε την πρόταση, παραθέτουμε ένα λήμμα.

Λήμμα 10 *Για κάθε περιττό πρώτο p και κάθε ακέραιο n, τέτοιο ώστε $0 \leq n < p - 1$, ισχύει ότι:*

$$\sum_{x=0}^{p-1} x^n \equiv 0 \pmod{p}.$$

Απόδειξη: Για $n = 0$ παίρνουμε το άθροισμα p μονάδων, το οποίο προφανώς είναι ίσο με μηδέν modulo p.

Για $0 < n < p-1$ μπορούμε να επιλέξουμε έναν αριθμό a, $2 \leq a \leq p-1$, τέτοιον ώστε $a^n \not\equiv 1 \pmod{p}$. Η συνάρτηση $f(x) = ax$ είναι ένα προς ένα, άρα και επί αφού έχουμε πεπερασμένο πλήθος στοιχείων. Επομένως ισχύει ότι:

$$\sum_{x=0}^{p-1} x^n \equiv \sum_{x=0}^{p-1} (ax)^n \pmod{p}.$$

Ισοδύναμα, δοθέντος ότι $a^n \not\equiv 1 \pmod{p}$, θα έχουμε:

$$0 \equiv \sum_{x=0}^{p-1} x^n - \sum_{x=0}^{p-1} a^n x^n \equiv (1-a^n) \sum_{x=0}^{p-1} x^n \pmod{p} \Rightarrow \sum_{x=0}^{p-1} x^n \equiv 0 \pmod{p}.$$

□

Απόδειξη Πρότασης 39: Μας ενδιαφέρουν οι λύσεις modulo p, συνεπώς, τα x, y, z μπορούν να πάρουν όλες τις ακέραιες τιμές μεταξύ των 0 και $p-1$. Αυτό μας δίνει p^3 διαφορετικούς πιθανούς συνδυασμούς που μπορούν να αποτελέσουν λύσεις της εξίσωσης. Θα προσπαθήσουμε να μετρήσουμε πόσες από αυτές είναι λύσεις της $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}$.

Από το Μικρό Θεώρημα Fermat έχουμε:

$$(ax_0^2 + by_0^2 + cz_0^2)^{p-1} \equiv \begin{cases} 1 \pmod{p}, & \text{αν } (x_0, y_0, z_0) \text{ δεν είναι λύση} \\ 0 \pmod{p}, & \text{αν } (x_0, y_0, z_0) \text{ είναι λύση.} \end{cases}$$

Οπότε, εάν θέσουμε N να είναι ο συνολικός αριθμός των συνδυασμών που δεν είναι λύσεις, και S το πλήθος των συνδυασμών που είναι λύσεις, τότε:

$$N = p^3 - S \equiv \sum_{(x,y,z)} (ax^2 + by^2 + cz^2)^{p-1} \pmod{p},$$

με τα x, y, z να διατρέχουν τις ακέραιες τιμές από 0 εώς και $p-1$. Αναλύοντας τις δυνάμεις στο άθροισμα παίρνουμε μία εξίσωση για το N που θα είναι ένα άθροισμα αθροισμάτων της μορφής:

$$\sum_{(x,y,z)} \alpha x^{2i} y^{2j} z^{2k},$$

με $2i + 2j + 2k = 2(p-1)$ και $\alpha \in \mathbb{Z}$. Ισχυριζόμαστε ότι κάθε ένα από τα αθροίσματα αυτά είναι ίσο με μηδέν modulo p.

Πράγματι, παρατηρούμε ότι κάποιο από τα $2i, 2j, 2k$, έστω το $2i$, πρέπει να έιναι μικρότερο του $p-1$, διαφορετικά το άθροισμά των τριών θα ήταν μεγαλύτερο από $2(p-1)$. Έτσι, μπορούμε να γράψουμε το προηγούμενο άθροισμα ως:

$$\sum_{(y,z)} \alpha y^{2j} z^{2k} \sum_{x} x^{2i}.$$

Όμως, από το Λήμμα 10, φαίνεται ότι το άθροισμα αυτό είναι ίσο με μηδέν modulo p.

Από τον ισχυρισμό έπεται ότι $N \equiv 0 \pmod{p}$, δηλαδή, το πλήθος των τριάδων που δεν αποτελούν λύσεις διαιρείται από τον p. Τότε, και το πλήθος των λύσεων $S = p^3 - N$ επίσης θα διαιρείται από τον p. Όμως, ξέρουμε ότι υπάρχει ένας συνδυασμός, ο $(0,0,0)$, που είναι λύση, και άρα το S θα είναι μεγαλύτερο της μονάδας και διαιρετό από τον p. Αυτό σημαίνει ότι υπάρχουν τουλάχιστον p λύσεις , δηλαδή ότι υπάρχουν λύσεις διάφορες της τετριμμένης. □

Πόρισμα 11 *Έστω p περιττός πρώτος που δε διαιρεί το abc. Τότε, η εξίσωση $ax^2 + by^2 + cz^2 = 0$ έχει μη τετριμμένη λύση στο $\mathbb{Q}_p$.*

Απόδειξη: Από το προηγούμενο θεώρημα γνωρίζουμε ότι η εξίσωση $ax^2 + by^2 + cz^2 = 0$ έχει μη τετριμμένες λύσεις modulo p. Έστω (x_0, y_0, z_0) μία από αυτές και έστω $x_0 \not\equiv 0 \pmod{p}$.

Έστω το πολυώνυμο $f(x) = ax^2 + by_0^2 + cz_0^2$. Προφανώς η τιμή x_0 είναι ρίζα του πολυωνύμου modulo p, δηλαδή $f(x_0) = 0 \pmod{p}$. Επιπλέον, $f'(x_0) = 2ax_0 \not\equiv 0 \pmod{p}$, εφόσον $a \not\equiv 0 \pmod{p}$, $x_0 \not\equiv 0 \pmod{p}$ και $p \neq 2$. Τότε, από το Λήμμα του Hensel έχουμε ότι υπάρχει μη τετριμμένη p-αδική ρίζα ρ του πολυωνύμου f.

Είναι άμεσο ότι η (ρ, y_0, z_0) θα αποτελεί λύση της αρχικής εξίσωσης στο $\mathbb{Q}_p$, και το πόρισμα έχει δειχθεί. □

Στην προηγούμενη ανάλυση υποθέσαμε ότι ο p είναι περιττός πρώτος και δεν διαιρεί το abc. Θα δούμε υπό ποιές συνθήκες υπάρχει p-αδική λύση όταν ο p διαιρεί κάποιον από τους συντελεστές a, b, c. Έστω λοιπόν ότι $p|a$. Κατ'

αρχάς, αν $p|a$, τότε $p \nmid bc$, αφού έχουμε υποθέσει ότι το γινόμενο abc είναι ελεύθερο τετραγώνων. Ισχύει το ακόλουθο θεώρημα:

Πρόταση 40 *Έστω $p \neq 2$ και $a \equiv 0 \pmod{p}$. Η εξίσωση*

$$ax^2 + by^2 + cz^2 = 0$$

έχει μη τετριμμένη λύση στο $\mathbb{Q}_p$, αν και μόνο αν υπάρχει ακέραιος $r \in \mathbb{Z}$, τέτοιος ώστε:

$$b + r^2 c \equiv 0 \pmod{p}$$

Απόδειξη: Θα δείξουμε πρώτα το ευθύ. Αν (x_0, y_0, z_0) μία μη τετριμμένη λύση στο $\mathbb{Q}_p$, τότε αυτή θα είναι λύση και modulo p. Όμως, $a \equiv 0 \pmod{p}$, έτσι παίρνουμε:

$$ax_0^2 + by_0^2 + cz_0^2 \equiv by_0^2 + cz_0^2 \equiv 0 \pmod{p}.$$

Τα b, c είναι p-αδικές μονάδες, αφού δεν διαιρούνται από τον p, και άρα αντιστρέψιμα στοιχεία modulo p. Επομένως, παίρνουμε:

$$y_0^2 \equiv -(cb^{-1})z_0^2 \equiv \alpha z_0^2,$$

όπου $\alpha \equiv -(cb^{-1})$. Αφού έχουμε ισόδυναμία τετραγώνων, είτε θα πρέπει $y_0 \equiv z_0 \equiv 0 \pmod{p}$ ή θα πρέπει $y_0, z_0 \not\equiv 0 \pmod{p}$ και το α να είναι τετράγωνο κάποιου p-αδικού αριθμού. Η πρώτη περίπτωση δεν μας δίνει άλλη επιλογή για την x_0 εκτός από τη μηδενική, δηλαδή θα είχαμε ξεκινήσει από τετριμμένη λύση. Επομένως, θα πρέπει να ισχύει:

$$\alpha \equiv y_0^2 (z_0^2)^{-1} \equiv r^2 \equiv -(cb^{-1}) \pmod{p} \Leftrightarrow$$

$$b + r^2 c \equiv 0 \pmod{p}, \quad r \in \mathbb{Z}_p / p\mathbb{Z}_p.$$

Αν πάρουμε τον ισοϋπόλοιπο ακέραιο modulo p με το r, τότε έχουμε το ζητούμενο.

Το αντίστροφο προκύπτει άμεσα από το Λήμμα του Hensel. Έστω ότι ισχύει $b + r^2 c \equiv 0 \pmod{p}$ για τους συντελεστές b, c. Τότε, λύνοντας ως προς b έχουμε:

$$b \equiv -r^2 c \pmod{p}.$$

Θα μελετήσουμε τη συμπεριφορά της εξίσωσης modulo p, ώστε τελικά να εφαρμόσουμε το Λήμμα του Hensel. Αντικαθιστώντας την παραπάνω σχέση στην εξίσωση modulo p παίρνουμε:

$$ax^2 - r^2cy^2 + cz^2 \equiv -r^2cy^2 + cz^2 \pmod{p}.$$

Η εξίσωση $-r^2cy^2 + cz^2 \equiv 0 \pmod{p}$ έχει παντα λύση modulo p. Πράγματι, έστω $y_0 \not\equiv 0 \pmod{p}$. Τότε, η εξίσωση γίνεται:

$$-r^2cy^2 + cz_0^2 \equiv 0 \pmod{p} \Leftrightarrow z^2 \equiv r^2y_0^2 \equiv (ry_0)^2 \pmod{p},$$

επομένως, για $z_0 = ry_0$, η εξίσωση $ax^2 - r^2cy^2 + cz^2 = 0$ έχει μη τετριμμένη λύση modulo p, την (x_0, y_0, z_0), όπου x_0 οποιοσδήποτε p-αδικός ακέραιος.

Όμοια με την περίπτωση όπου $p \nmid abc$, θεωρούμε το πολυώνυμο $f(y) = ax_0^2 + by^2 + cz_0^2$. Προφανώς ισχύει $f(y_0) \equiv 0 \pmod{p}$ και $f'(y_0) = 2by_0 \not\equiv 0 \pmod{p}$, συνεπώς εφαρμόζοντας το Λήμμα του Hensel παίρνουμε μία μη τετριμμένη p-αδική ρίζα για το πολυώνυμο, άρα και μία p-αδική λύση της αρχικής εξίσωσης. □

Μένει τώρα να μελετήσουμε την περίπτωση που ο p είναι άρτιος, δηλαδή $p = 2$. Διακρίνουμε και πάλι δύο περιπτώσεις: τα a, b, c να είναι όλα περιττοί ή κάποιο από τα a, b, c να είναι άρτιος.

Πρόταση 41 *Έστω $p = 2$ και a, b, c περιττοί ακέραιοι. Η εξίσωση $ax^2 + by^2 + cz^2 = 0$ έχει μη τετριμμένη λύση στο $\mathbb{Q}_2$ αν και μόνο αν το άθροισμα δύο εκ των a, b, c διαιρείται από το 4.*

Απόδειξη: Έστω (x_0, y_0, z_0) μία μη τετριμμένη λύση της $ax^2+by^2+cz^2 = 0$. Μπορούμε να υποθέσουμε ότι τουλάχιστον ένα από τα x_0, y_0, z_0, έστω το x_0, είναι 2-αδική μονάδα, δηλαδή δεν διαιρείται από το 2. Αλλιώς, μπορούμε να πολλαπλασιάσουμε και τα τρία στοιχεία με κατάλληλη δύναμη του δύο.

Η λύση (x_0, y_0, z_0) θα είναι και λύση modulo 2^n για κάθε n θετικό ακέραιο, άρα και $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{2}$. Εφόσον τα a, b, c είναι όλα περιττοί

αριθμοί, και έχουμε υποθέσει $2 \nmid x_0$, θα πρέπει ακριβώς ένα από τα y_0, z_0 να είναι επίσης 2-αδική μονάδα, διότι διαφορετικά δεν θα είχαμε λύση modulo δύο. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι το y_0 είναι 2-αδική μονάδα.

Παρατηρούμε ότι, αν $a = 1 + a_1 2 + a_2 2^2 + \cdots,\ a_i \in \{0, 1\}$, μία 2αδική μονάδα, τότε για το τετράγωνό της ισχύει ότι $a^2 \in 1 + 8\mathbb{Z}_2$. Πράγματι, έχουμε:

$$\begin{aligned} a^2 &= (1 + a_1 2 + a_2 2^2 + \cdots)(1 + a_1 2 + a_2 2^2 + \cdots) \\ &= 1 + a_1 2 + a_2 2^2 + \cdots + a_1 2 + a_1^2 2^2 + \cdots + a_2 2^2 + \cdots \\ &= 1 + (a_1 + 1) a_1 2^2 + a_2 2^3 + \text{όροι τάξης} \geq 3 \\ &= 1 + \text{όροι τάξης} \geq 3. \end{aligned}$$

Αντίστοιχα βρίσκουμε ότι αν κάποιο στοιχείο $b = b_1 2 + b_2 2^2 + \cdots$ δεν είναι 2-αδική μονάδα, τότε το τετράγωνό του ανήκει στο $4\mathbb{Z}_2$.

Επομένως, έχοντας κάνει τις υποθέσεις ότι x_0, y_0 είναι 2-αδικές μονάδες, ενώ το z_0 όχι, για τα τετράγωνά τους παίρνουμε ότι $x_0^2, y_0^2 \in 1 + 8\mathbb{Z}_2$ (άρα και $x_0^2, y_0^2 \in 1 + 4\mathbb{Z}_2$) και $z_0^2 \in 4\mathbb{Z}_2$. Έτσι, μελετώντας την εξίσωση modulo 4, καταλήγουμε στο ζητούμενο:

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod 4 \Rightarrow$$

$$a + b \equiv 0 \pmod 4.$$

Εάν είχαμε υποθέσει διαφορετικά για το ποια στοιχεία από τα x_0, y_0, z_0 είναι οι 2-αδικές μονάδες, θα είχαμε καταλήξει στα αντίστοιχα αποτελέσματα για τους συντελεστές τους.

Για το αντίστροφο, υποθέτουμε χωρίς βλάβη της γενικότητας ότι για τους συντελεστές a, b ισχύει ότι $a + b \equiv 0 \pmod 4$. Διακρίνουμε δύο περιπτώσεις: $a + b \equiv 0 \pmod 8$ και $a + b \equiv 4 \pmod 8$.

Για την πρώτη περίπτωση μπορούμε να δούμε ότι η επιλογή $(x_0, y_0, z_0) = (1, 1, 0)$ είναι λύση της εξίσωσης modulo δύο. Θεωρώντας τώρα το πολυώνυμο $F(x) = ax^2 + by_0^2 + cz_0^2$, μπορούμε να εφαρμόσουμε την ισχυρή μορφή του Λήμματος του Hesnel:

$$|F(x_0)|_2 = |ax_0^2 + by_0^2|_2 = |8\lambda|_2 \leq \frac{1}{8}$$

και

$$|F'(x_0)|_2^2 = |2a|_2^2 = (\frac{1}{2})^2 = \frac{1}{4}, \quad \text{εφόσον } 2 \nmid a.$$

Έχουμε ότι $|F(x_0)|_2 < |F'(x_0)|_2^2$, άρα εξασφαλίζεται η συνθήκη της ισχυρής μορφής του Λήμματος του Hensel. Από το Λήμμα έπεται ότι υπάρχει μοναδική 2-αδική ακέραια ρίζα ρ, τέτοια ώστε $F(\rho) = 0$, δηλαδή $a\rho^2 + by_0^2 + cz_0^2 = 0$.

Για τη δεύτερη περίπτωση, ακολουθούμε ακριβώς τα ίδια βήματα, και βρίσκουμε ότι η $(x_0, y_0, z_0) = (1, 1, 2)$ είναι η κατάλληλη επιλογή, ώστε εφαρμόζοντας το Λήμμα του Hensel να πάρουμε λύση στο $\mathbb{Q}_2$. □

Πρόταση 42 *Έστω $p = 2$ και ένας από τους a, b, c είναι άρτιος. Η εξίσωση $ax^2 + by^2 + cz^2 = 0$ έχει μη τετριμμένη λύση στο $\mathbb{Q}_2$ αν και μόνο αν είτε το άθροισμα δύο εκ των a, b, c ή το άθροισμα και των τριών διαιρείται από το 8.*

Απόδειξη: Μπορούμε, χωρίς βλάβη της γενικότητας, να υποθέσουμε ότι $2|a$. Έστω (x_0, y_0, z_0) μία λύση της εξίσωσης στο $\mathbb{Q}_2$. Τότε αυτή είναι λύση της εξίσωσης modulo 2, δηλαδή $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod 2$.

Όπως και στην προηγούμενη απόδειξη, μπορούμε να συμπεράνουμε ότι τα y_0, z_0 θα πρέπει να είναι 2-αδικές μονάδες, ενώ το x_0 μπορεί να είναι οτιδήποτε.

Εάν υποθέσουμε ότι ο x_0 είναι άρτιος, τότε το x_0^2 είναι πολλαπλάσιο του τέσσερα, και άρα ο όρος ax_0^2 είναι πολλαπλάσιο του οκτώ. Σε συνδυασμό με το γεγονός ότι $y_0^2 \equiv z_0^2 \equiv 1 \pmod 8$, εφόσον είναι 2-αδικές μονάδες, παίρνουμε:

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod 8 \Rightarrow$$

$$b + c \equiv 0 \pmod 8.$$

Εάν υποθέσουμε ότι ο x_0 είναι περιττός, δηλαδή 2-αδική μονάδα, τότε έχουμε $ax_0^2 \equiv a \pmod 8$, και άρα:

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod 8 \Rightarrow$$

$$a + b + c \equiv 0 \pmod 8.$$

Δηλαδή, αν (x_0, y_0, z_0) μία μη τετριμμένη λύση της $ax^2 + by^2 + cz^2 = 0$ στο $\mathbb{Q}_2$, τότε είτε το άθροισμα και των τριών συντελεστών ή το άθροισμα δύο από αυτών είναι διαιρετό από το 8.

Το αντίστροφο αποδεικνύεται χρησιμοποιώντας το Λήμμα του Hensel ακριβώς όπως στην προηγούμενη απόδειξη, μονο που τώρα είναι απλούστερο, δεδομένου ότι γνωρίζουμε τι ισχύει για τους συντελεστές modulo 8. Επομένως, αν υποθέσουμε ότι $2|a$ και $a+b+c \equiv 0 \pmod 8$, τότε μπορούμε να επιλέξουμε την $(x_0, y_0, z_0) = (1, 1, 1)$ ως κατάλληλη λύση για να εφαρμόσουμε το Λήμμα. Διαφορετικά, αν έστω $b+c \equiv 0 \pmod 8$, τότε κατάλληλη λύση είναι η $(x_0, y_0, z_0) = (0, 1, 1)$. □

Συγκεντρώνοντας τις παραπάνω προτάσεις, έχει ολοκληρωθεί η απόδειξη του Θεωρήματος 15. □

Παρατήρηση 22 Στις αποδείξεις του Πορίσματος 11 και των Προτάσεων 40, 41, 42 το βασικό εργαλείο είναι το Λήμμα του Hensel. Παρότι το Λήμμα του Hensel αφορά πολυώνυμα μίας μεταβλητής, το εφαρμόσαμε στη Διοφαντική εξισώση $ax^2 + by^2 + cz^2$ ''παγώνοντας'' τις δύο από τις τρεις μεταβλητές. Το ίδιο τέχνασμα εφαρμόζουμε και στο παρακάτω θεώρημα, το οποίο γενικεύει το Θεώρημα 15.

Θεώρημα 16 *Έστω η τετραγωνική μορφή*

$$F(x_1, \ldots, x_n, y_1, \ldots, y_m) = \sum_{j=1}^{n} a_j x_j^2 + \sum_{i=1}^{m} p\, b_i y_i^2,\ a_j, b_i \in \mathbb{Z}_p^*,$$

δηλαδή τα a_j, b_i είναι p-αδικές μονάδες: $|a_j|_p = |b_i|_p = 1$, για κάθε i, j.

(i) Εάν $p \neq 2$, τότε ικανή και αναγκαία συνθήκη για την ύπαρξη $X_1, \ldots, X_n$, $Y_1, \ldots, Y_m \in \mathbb{Q}_p$, όχι όλων μηδέν, τέτοιων ώστε:

$$F(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = 0,$$

είναι η επαλήθευση μίας (τουλάχιστον) εκ των δύο ακόλουθων συνθηκών:

(α΄) Υπάρχουν $c_1, \ldots, c_n \in \mathbb{Z}$, όχι όλοι διαιρετοί από τον p, τέτοιοι ώστε:

$$\sum_{j=1}^{n} a_j c_j^2 \equiv 0 \pmod p.$$

(β′) *Υπάρχουν* $d_1, \ldots, d_m \in \mathbb{Z}$, *όχι όλοι διαιρετοί από τον* p, *τέτοιοι ώστε:*

$$\sum_{i=1}^{m} b_i d_i^2 \equiv 0 \pmod{p}.$$

(ii) *Εάν* $p = 2$, *τότε οι δύο προηγούμενες συνθήκες αντικαθίστανται από τις εξής δύο:*

(α′) *Υπάρχουν* $c_1, \ldots, c_n \in \mathbb{Z}$, *όχι όλοι άρτιοι, και* $d_1, \ldots, d_m \in \mathbb{Z}$, *τέτοιοι ώστε:*

$$\sum_{j=1}^{n} a_j c_j^2 + 2\sum_{i=1}^{m} b_i d_i^2 \equiv 0 \pmod{8}.$$

(β′) *Υπάρχουν* $d_1, \ldots, d_m \in \mathbb{Z}$, *όχι όλοι άρτιοι, και* $c_1, \ldots, c_n \in \mathbb{Z}$, *τέτοιοι ώστε:*

$$\sum_{i=1}^{m} b_i d_i^2 + 2\sum_{j=1}^{n} a_j c_j^2 \equiv 0 \pmod{8}.$$

Για λεπτομέρειες για την απόδειξη του Θεωρήματος παραπέμπουμε στο ενδέκατο κεφάλαιο του [3].

4.2 Τοπική και Ολική Αρχή

Το δεύτερο βήμα για την εύρεση ρητών λύσεων μιας εξίσωσης είναι το πέρασμα από την ύπαρξη p-αδικών λύσεων σε λύσεις στο $\mathbb{Q}$. *Θα μπορούσαμε, γνωρίζοντας τη συμπεριφορά μιας Διοφαντικής εξίσωσης σε κάθε* $\mathbb{Q}_p$, *να διεξάγουμε συμπεράσματα για τη συμπεριφορά της στο* $\mathbb{Q}$;

Προφανώς, αν μια Διοφαντική εξίσωση έχει μία ρητή ρίζα, τότε αυτή είναι και ρίζα σε κάθε $\mathbb{Q}_p$, εφόσον το $\mathbb{Q}$ εμπεριέχεται στο $\mathbb{Q}_p$ για κάθε $p \leq \infty$. Επομένως, αν δεν υπάρχουν ρίζες σε κάποιο $\mathbb{Q}_p$, $p \leq \infty$, μπορούμε σίγουρα να συμπεράνουμε ότι δεν υπάρχουν ρητές ρίζες.

Θα μας ενδιέφερε περισσότερο να ισχύει το αντίστροφο: η ύπαρξη ριζών σε κάθε $\mathbb{Q}_p$ να εγγυάται την ύπαρξη ρίζας στο $\mathbb{Q}$. Θα θέλαμε να μπορούμε να ''συρράψουμε'' τοπικές (local) λύσεις και να παράγουμε ολικές (global).

Η σκέψη αυτή πρωτοδιατυπώθηκε από τον Hasse, ο οποίος θεωρούσε ότι οι τοπικές λύσεις μπορούν να δώσουν ολικές, και εκφράζεται από την ακόλουθη αρχή:

Τοπική-Ολική Αρχή (Local-Global Principle): *Η ύπαρξη ή μη ύπαρξη λύσεων στο $\mathbb{Q}$ (ολικών λύσεων) μιας Διοφαντικής εξίσωσης μπορεί να ανιχνευθεί μελετώντας τις λύσεις της εξίσωσης στο $\mathbb{Q}_p$, για κάθε $p \leq \infty$ (τοπικές λύσεις).*

Η Τοπική-Ολική Αρχή έχει αποδειχθεί πολύτιμος οδηγός για τη μελέτη Διοφαντικών εξισώσεων, διότι, ουσιαστικά, προτείνει μία μεθοδολογία για τον προσδιορισμό των ρητών λύσεων μίας εξίσωσης: Πρώτα πρέπει να μελετήσει κανείς το πρόβλημα τοπικά και μετά να συνδέσει την τοπική πληροφορία για να αποκομίσει την ολική.

Δυστυχώς όμως, η Τοπική-Ολική Αρχή δεν ισχύει για όλες τις εξισώσεις. Ο ισχυρισμός ότι μία εξίσωση έχει λύσεις στο $\mathbb{Q}$ αν και μονο αν έχει σε κάθε $\mathbb{Q}_p$ δεν είναι αληθής. Θα δούμε μερικά παραδείγματα, στα οποία η αρχή επαληθεύεται και μερικά στα οποία αποτυγχάνει.

Πρόταση 43 *Ένας ρητός αριθμός $x \in \mathbb{Q}$ είναι τετράγωνο αν και μόνο αν είναι τετράγωνο σε κάθε $\mathbb{Q}_p$, $p \leq \infty$.*

Ισοδύναμα η πρόταση διατυπώνεται ως εξής: η εξίσωση $x^2 + \alpha,\ \alpha \in \mathbb{Q}$, έχει λύση στο $\mathbb{Q}$ αν και μόνο αν έχει λύση σε κάθε $\mathbb{Q}_p$.

Απόδειξη: Το ευθύ είναι προφανές. Για το αντίστροφο, έστω $x \in \mathbb{Q}$ και ο x είναι τετράγωνο σε κάθε $\mathbb{Q}_p$. Τότε, από Πόρισμα 10, για κάθε $p < \infty$ ο x γράφεται ως:

$$x = p_i^{v_{p_i}(x)} x'^2,\ v_{p_i}(x) = 2k_i,\ x' \in \mathbb{Z}_p^*,\quad k_i \in \mathbb{Z},\quad i \in \mathbb{N}.$$

Επιπλέον, ο x είναι τετράγωνο και για $p = \infty$, δηλαδή στο $\mathbb{R}$, άρα είναι θετικός αριθμός. Έτσι, από το Θεμελιώδες Θεώρημα της Αριθμητικής, πάιρνουμε:

$$x = \prod_{p_i < \infty} p_i^{v_{p_i}(x)} = p_1^{v_{p_1}(x)} p_2^{v_{p_2}(x)} \ldots = (p_1^{k_1} p_2^{k_2} \ldots)^2,$$

δηλαδή ο x είναι το τετράγωνο του ρητού αριθμού $\prod p_i^{k_i}$. □

Έστω τώρα η Διοφαντική εξίσωση $x^2 + y^2 + z^2 = 0$. Φαίνεται αμέσως ότι η μοναδική ρητή λύση της εξίσωσης αυτής είναι η τετριμμένη $x = y = z = 0$, εφόσον είναι και η μοναδική λύση στο $\mathbb{R}$ (δηλαδή το $\mathbb{Q}_\infty$), και οποιαδήποτε μη τετριμμένη ρητή λύση θα ήταν και λύση στο $\mathbb{R}$.

Παρόμοια, η Διοφαντική εξίσωση $x^2 + y^2 = z^2$ έχει μη τετριμμένες λύσεις στο $\mathbb{Q}$, και άρα σε κάθε $\mathbb{Q}_p$.

Τα προηγούμενα παραδείγματα επαληθεύουν όλα την Τοπική-Ολική Αρχή. Ας δούμε τώρα μία περίπτωση που η Αρχή διαψεύδεται. Θα δείξουμε ότι η εξίσωση $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$ έχει λύσεις σε κάθε $\mathbb{Q}_p$, $p \leq \infty$, αλλά, όπως είναι προφανές από τη μορφή της, δεν έχει λύση στο $\mathbb{Q}$.

Κατ' αρχάς, για κάθε $p \neq 2, 17$, αν οι $x^2 - 2,\ x^2 - 17$ δεν έχουν λύση στο $\mathbb{Q}_p$, τότε η $x^2 - 34$ έχει λύση. Πράγματι, έστω ότι τα 2, 17 δεν είναι τετράγωνα. Τότε δεν είναι ούτε τετραγωνικά υπόλοιπα modulo p (αν ήταν θα μπορούσαμε να εφαρμόσουμε το Λήμμα του Hensel). Δεδομένου ότι η ομάδα $\mathbb{Z}/p\mathbb{Z}$ είναι κυκλική, τα 2, 17 θα είναι κάποια περιττή δύναμη κάποιου γεννήτορά της, τον οποίο συμβολίζουμε με g. Επομένως, το γινόμενό τους θα είναι κάποια άρτια δύναμη του γεννήτορα, δηλαδή της μορφής g^{2k}, και άρα το τετράγωνο του στοιχείου g^k.

Για $p = 17$ έχουμε ότι $6^2 \equiv 2 \pmod{17}$ και επιπλέον $2 \cdot 6 = 12 \not\equiv 0 \pmod{17}$. Επομένως, ικανοποιούνται οι συνθήκες του Λήμματος του Hensel, το οποίο αποφαίνεται ότι το 2 είναι τετράγωνο στο $\mathbb{Q}_{17}$, και άρα η αρχική εξίσωση έχει λύση στο $\mathbb{Q}_{17}$.

Τέλος, για $p = 2$, ακολουθούμε μια διαφορετική σκέψη. Αν το 17 είναι το τετράγωνο κάποιου $a \in \mathbb{Q}_2$, τότε αυτό θα ανήκει στο $\mathbb{Z}_2$. Θα χρησιμοποιήσουμε τις απεικονίσεις των στοιχείων του $\mathbb{Z}_2$ ως αναπτύγματα με βάση το δύο για να προσδιορίσουμε το a. Έχουμε ότι, αν $a = a_0 + a_1 2 + a_2 2^2 + a_3 2^3 + \cdots$, $a_i \in \mathbb{Z}/2\mathbb{Z}$, τότε:

$$a^2 = a_0^2 + (a_0 a_1 + a_1 a_0)2 + (a_0 a_2 + a_1 a_1 + a_2 a_0)2^2 + \cdots = \sum_{i \geq 0} \alpha_i 2^i,$$

όπου $\alpha_n = \sum_{i+j=n} a_i a_j$. Επιπλέον, $17 = 2^0 + 2^4$. Εξισώνοντας το 17 με το a^2, ώστε να προσδιορίσουμε τους συντελεστές a_i, παίρνουμε μία σειρά ισοδυναμιών:

$$\alpha_0 = a_0^2 \equiv 1 \pmod 2$$
$$\alpha_1 = 2a_0a_1 \equiv 0 \pmod 2$$
$$\alpha_2 = a_1^2 + 2a_0a_2 \equiv a_1^2 \equiv 0 \pmod 2$$
$$\alpha_3 = 2a_0a_3 + 2a_1a_2 \equiv 0 \pmod 2$$
$$\alpha_4 = a_2^2 + 2a_0a_4 + 2a_1a_3 \equiv a_2^2 \equiv 1 \pmod 2$$

$$\alpha_n \equiv \sum_{i+j=n} a_ia_j \equiv 0 \pmod 2 \quad \text{για κάθε} \quad n > 4.$$

Παρατηρούμε ότι όλοι οι a_i, εμφανίζονται στο τετράγωνο σε κάποια από τις παραπάνω εξισώσεις, ενώ όλοι οι υπόλοιποι όροι της εξίσωσης είναι της μορφής $2a_ia_j$, δηλαδή μηδέν modulo 2. Έτσι, για $i = 0, 2$ οι a_0 και a_2 δίνονται από την εξίσωση $a_0^2 \equiv a_2^2 \equiv 1 \pmod 2$, ενώ για τους υπόλοιπους όρους ισχύει ότι $a_i^2 \equiv 0 \pmod 2$. Επειδή το τετράγωνο περιττού αριθμού ειναι περιττός και το τετράγωνο ενός άρτιου αριθμού είναι άρτιος συμπεραίνουμε ότι $a_0 = a_2 = 1$ και $a_1 = a_3 = a_4 = \ldots = 0$. Έτσι, ο δυαδικός ακέραιος $a = 2^0 + 2^2$ είναι η τετραγωνική ρίζα του 17 στο $\mathbb{Q}_2$.

Έχουμε δείξει ότι η εξίσωση έχει τουλάχιστον μια ρίζα σε κάθε $\mathbb{Q}_p$, $p \leq \infty$. Παρ' όλα αυτά δεν έχει ρίζες στο $\mathbb{Q}$, αφού κανένα από τα 2, 17, 34 δεν είναι το τετράγωνο κάποιου ρητού αριθμού. Άρα, η Τοπική-Ολική Αρχή δεν ισχύει.

4.3 Το Θεώρημα Hasse-Minkowski

Έχουμε όμως ένα πολύ σημαντικό παράδειγμα στο οποίο η Τοπική-Ολική Αρχή επαληθεύεται:

Θεώρημα 17 (Hasse-Minkowski) *Έστω μία τετραγωνική μορφή*

$$F(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n].$$

Η εξίσωση

$$F(x_1, \ldots, x_n) = 0$$

έχει μη τετριμμένες λύσεις στο $\mathbb{Q}$ αν και μόνο αν έχει μη τετριμμένες λύσεις σε κάθε $\mathbb{Q}_p$, $p \leq \infty$.

Αξίζει να τονίσουμε ότι με το Θεώρημα Hasse-Minkowski λύνουμε το πρόβλημα της ύπαρξης μη τετριμμένων ρητών λύσεων μίας τετραγωνικής μορφής, εφόσον το ''τοπικό πρόβλημα'' λύνεται εύκολα σε κάθε περίπτωση. Πιο συγκεκριμένα, όπως είδαμε στην προηγούμενη ενότητα για κάθε πρώτο p, η κατάλληλη μορφή του Λήμματος του Hensel αποφαίνεται, μετά από πεπερασμένη διαδικασία, για το αν η τετραγωνική μορφή έχει ή όχι λύσεις στο $\mathbb{Q}_p$.

Βέβαια, υπάρχουν άπειροι πρώτοι αριθμοί. Όμως, όπως είδαμε στο Θεώρημα 16, αυτοί χωρίζονται σε πεπερασμένες κατηγορίες, έτσι ώστε τελικά η διαδικασία εύρεσης τοπικών λύσεων για όλους τους πρώτους να είναι πεπερασμένη. Συνεπώς, δοθέντος του Θεωρήματος Hasse-Minkowski, έχουμε ανάγει το πρόβλημα ύπαρξης ρητής λύσης μίας τετραγωνικής μορφής σε μία πεπερασμένη διαδικασία.

Πρωτού περάσουμε στην απόδειξη του Θεωρήματος Hasse-Minkowski θα αναλύσουμε περαιτέρω το παράδειγμα της προηγούμενης ενότητας, που αφορά στην εξίσωση $ax^2 + by^2 + cz^2 = 0$ και θα αποδείξουμε το Θεώρημα Hasse-Minkowski για την παραπάνω εξίσωση.

Ο λόγος που ξεκινάμε από αυτή την ειδική περίπτωση είναι ότι-σε αντίθεση με τη γενική περίπτωση- μπορούμε να κάνουμε χρήση μιας μορφής του Θεωρήματος Κυρτού Σώματος του Minkowski (Minkowski's Convex Body Theorem), την οποία και παραθέτουμε χωρίς απόδειξη (Για την απόδειξη, βλ. για παράδειγμα [3]).

Θεώρημα 18 (Minkowski Κυρτού Σώματος) *Έστω H υποομάδα του $\mathbb{Z}^n$ με δείκτη m και έστω $C \subset \mathbb{R}^n$ συμμετρικό και κυρτό με όγκο*

$$V(C) > m2^n.$$

Τότε, υπάρχει μη μηδενικό στοιχείο c που ανήκει στο $H \cap C$.

Ειδική περίπτωση του παραπάνω θεωρήματος αποτελεί η περίπτωση όπου θεωρούμε ως υποομάδα του $\mathbb{Z}^n$ το ίδιο το $\mathbb{Z}^n$ με δείκτη $m = 1$. Τότε μπορούμε εύκολα να δούμε μία γεωμετρική ερμηνεία: Το C του θεωρήματος θα πρέπει να είναι συμμετρικό και κυρτό, και να έχει όγκο τουλάχιστον τόσο, όσο ο n-διάστατος κύβος που ορίζεται από τα μοναδιαία διανύσματα της βάσης του $\mathbb{Z}^n$ και τα αντίθετά τους.

Στη συνέχεια θα αποδείξουμε το ακόλουθο:

Θεώρημα 19 (Hasse-Minkowski για τρεις μεταβλητές) *Έστω η τετραγωνική μορφή $F(x,y,z) = ax^2 + by^2 + cz^2 \in \mathbb{Q}[x,y,z]$, και έστω ότι υπάρχει μη τετριμμένη λύση της $ax^2 + by^2 + cz^2 = 0$ στο $\mathbb{Q}_p$, για κάθε $p \leq \infty$. Τότε, η εξίσωση έχει μη τετριμμένη λύση στο $\mathbb{Q}$.*

Απόδειξη: Για τα a, b, c έχουμε υποθέσει ότι είναι ακέραιοι, ελεύθεροι τετραγώνων και ανά δύο πρώτοι μεταξύ τους. Υποθέτουμε ότι η τετραγωνική μορφή έχει ρίζες σε κάθε $\mathbb{Q}_p$. Τότε, από το Θεώρημα 15 θα ικανοποιούνται οι ακόλουθες συνθήκες:

(i) Τα a, b, c δεν είναι ομόσημα.

(ii) Για κάθε $p \neq 2$, αν $p \mid c$, τότε υπάρχει $r \in \mathbb{Z}$, τέτοιο ώστε $ar^2 + b \equiv 0 \pmod{p}$. Αντίστοιχες συνθήκες ισχύουν αν $p \mid a$ ή b.

(iii) Για $p = 2$, αν $2 \nmid abc$ τότε, για δύο εκ των a, b, c, έστω τα a, b, ισχύει ότι $a + b \equiv 0 \pmod{4}$,

(iv) Για $p = 2$, αν $2 \mid c$, υπάρχει $s \in \{0, 1\}$, τέτοιο ώστε $a + b + cs^2 \equiv 0 \pmod{8}$. Αντίστοιχες συνθήκες προκύπτουν αν $2 \mid a$ ή b.

Ορίζουμε τώρα ως H το σύνολο των τριάδων $(x, y, z) \in \mathbb{Z}^3$, οι οποίες για τις διάφορες τιμές των πρώτων αριθμών p, με $p \mid 2abc$, ικανοποιούν τις ακόλουθες ισοτιμίες:

(i) Αν $p \neq 2$ και ισχύει η (ii), τότε $x \equiv ry \pmod{p}$. (Παρόμοια αν $p \mid a$ ή b).

(ii) Αν $p = 2$ και ισχύει η (iii), τότε $z \equiv 0 \pmod{2}$.

(iii) Αν $p = 2$ και ισχύει η (iv), τότε $x \equiv y \pmod{4}$ και $z \equiv sy \pmod{2}$.

Για τη συνέχεια της απόδειξης θα χρειαστούμε τα παρακάτω λήμματα, στα οποία λαμβάνουμε ως $|\cdot|$ τη συνήθη απόλυτη τιμή.

Λήμμα 11 *H $(H, +)$ είναι υποομάδα του $\mathbb{Z}^3$ με δείκτη το πολύ $4|abc|$.*

Απόδειξη: Η προσεταιριστικότητα της πράξης κληρονομείται από το $\mathbb{Z}^3$. Η κλειστότητα προκύπτει άμεσα, εφόσον όλα τα στοιχεία της H ικανοποιούν τις συνθήκες (i)-(iii). Θα δείξουμε την κλειστότητα για τη συνθήκη (iii).

Έστω $(x_1, y_1, z_1),\ (x_2, y_2, z_2) \in H$. Τότε,

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2) = (x, y, z).$$

Για το (x, y, z) έχουμε:

$$x \equiv x_1 + x_2 \equiv y_1 + y_2 \pmod 4 \Leftrightarrow x \equiv y \pmod 4$$

και

$$z \equiv z_1 + z_2 \equiv sy_1 + sy_2 \pmod 2 \Leftrightarrow z \equiv sy \pmod 2.$$

Ουδέτερο στοιχείο της υποομάδας είναι το $(0, 0, 0) \in H$ και το αντίθετο κάθε στοιχείου (x, y, z) ορίζουμε να είναι το $(-x, -y, -z)$.

Το στοιχείο που ορίσαμε ως αντίθετο ανήκει στην H, εφόσον οι ισοδυναμίες (i)-(iii) μπορούν να πολλαπλασιαστούν επί (-1) και να μας δώσουν τις ζητούμενες σχέσεις για τα $-x, -y, -z$.

Τέλος, θα δείξουμε ότι ο δείκτης της H στο $\mathbb{Z}^3$ είναι το πολύ $4|abc|$. Δοθείσης της συνάρτησης $ax^2 + by^2 + cz^2$, η H θα περιέχει τα στοιχεία εκείνα που ικανοποιούν ορισμένες ισοδυναμίες.

Έστω $a = \pm p_1 p_2 \dots p_n,\ b = \pm q_1 q_2 \dots q_m$ και $c = \pm r_1 r_2 \dots r_k$, όπου p_i, q_j, r_k διαφορετικοί μεταξύ τους πρώτοι αριθμοί. Έστω ότι κάποιος από τους συντελεστές διαρείται από το δυο, για παράδειγμα, έστω $r_1 = 2$. Τότε, οι ισοδυναμίες που καθορίζουν τα στοιχεία της H είναι οι ακόλουθες:

$$\begin{array}{lll}
y \equiv r_{p_1} z \pmod{p_1} & x \equiv r_{q_1} z \pmod{q_1} & x \equiv r_{r_2} y \pmod{r_2} \\
y \equiv r_{p_2} z \pmod{p_2} & x \equiv r_{q_2} z \pmod{q_2} & x \equiv r_{r_3} y \pmod{r_3} \\
\vdots & \vdots & \vdots \\
y \equiv r_{p_n} z \pmod{p_n} & x \equiv r_{q_m} z \pmod{q_m} & x \equiv r_{r_l} y \pmod{r_l}
\end{array}$$

Επιπλέον, εφόσον $r_1 = 2|c$, τα στοιχεία της H ικανοποιούν τις:

$$x \equiv y \pmod 4 \quad \text{και} \quad z \equiv sy \pmod 2.$$

Προφανώς, κάθε στοιχείο $(i,j,k) \in \mathbb{Z}^3$, τέτοιο ώστε κάποια από τις παραπάνω ισοδυναμίες να μην επαληθεύεται, για παράδειγμα $i \equiv r_{p_1} z+1 \pmod{p_1}$, ανήκει και σε διαφορετικό σύμπλοκο της H.

Συνολικά μπορούμε να έχουμε $a = p_1 \cdot p_2 \cdots p_n$ διαφορετικές ισοδυναμίες που να συνδέουν δεύτερη και τρίτη συντεταγμένη, $b = q_1 q_2 \dots q_m$ διαφορετικές ισοδυναμίες που να συνδέουν πρώτη και τρίτη συντεταγμενη, $r_2 \dots r_l$ που να συνδέουν πρώτη και δέυτερη συντεταγμένη. Επιπλέον, έχουμε τέσσερις διαφορετικές ισοδυναμίες για την πρώτη και τη δεύτερη, και δύο για τη δεύτερη και την τρίτη.

Έτσι, ο αριθμός διαφορετικών τριάδων, ως προς τις σχέσεις μεταξύ των συντεταγμένων τους, άρα και των διαφορετικών συμπλόκων, θα δίνεται από το γινόμενο $4|abc|$.

Στα προηγούμενα υποθέσαμε ότι $2| c$. Εάν $2 \nmid abc$, τότε οι δύο τελευταίες ισοδυναμίες αντικαθίστανται από τις εξής δύο: την $x \equiv r_{r_1} y \pmod{r_1}$ και την $z \equiv 0 \pmod{2}$. Άρα ο συνολικός αριθμός συμπλόκων είναι $2|abc| < 4|abc|$. □

Λήμμα 12 *Για $(x,y,z) \in H$ ισχύει:*

$$F(x,y,z) \equiv 0 \pmod{4|abc|}.$$

Απόδειξη: Έστω ότι ισχύουν οι αναλύσεις των a, b, c της προηγούμενης απόδειξης. Τότε, η εξίσωση

$$F(x,y,z) \equiv 0 \pmod{4abc}$$

είναι ισοδύναμη με το σύστημα εξισώσεων:

$$\begin{aligned}
&F(x,y,z) \equiv 0 \pmod{p_i}, \quad \text{για κάθε} \quad i = 1,2,\dots,n \\
&F(x,y,z) \equiv 0 \pmod{q_j}, \quad \text{για κάθε} \quad j = 1,2,\dots,m \\
&F(x,y,z) \equiv 0 \pmod{r_k}, \quad \text{για κάθε} \quad k = 1,2,\dots,l \\
&F(x,y,z) \equiv 0 \pmod{4}
\end{aligned}$$

Θα δείξουμε ότι οι παραπάνω ισοτιμίες επαληθεύονται όλες όταν $(x,y,z) \in H$. Πράγματι, έστω κάποιο από τα p_i, q_j, r_k διάφορο του δύο, για παράδειγμα το p_1. Τότε, λόγω των (ii) και (i) έχουμε:

$$br_{p_1}^2 + c \equiv 0 \pmod{p_1}$$

και

$$y \equiv r_{p_1} z \pmod{p_1}.$$

Άρα, για την F έχουμε:

$$ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \equiv b(r_{p_1} z)^2 + cz^2 \equiv (c + br_{p_1}^2)z^2 \equiv 0 \pmod{p_1}.$$

Με όμοιο τρόπο πάιρνουμε τα αντίστοιχα αποτελέσματα για τους υπόλοιπους περιττούς πρώτους που εμφανίζονται στην παραγοντοποίηση των a, b, c.

Αν, τώρα, κάποιος από τους p_i, q_j, r_k είναι ίσος με δύο, τότε η εξίσωση $F(x, y, z) \equiv 0 \pmod 2$, θα έπεται από την $F(x, y, z) \equiv 0 \pmod 4$. Άρα, μένει να αναλύσουμε την περίπτωση της τελευταίας ισοτιμίας. Κατ' αρχάς, έστω $2 | abc$, για παράδειγμα έστω $r_1 = 2 | c$. Από τις συνθήκες (iv) και (iii) έχουμε:

$$a + b + cs^2 \equiv 0 \pmod 8 \Leftrightarrow a + b + cs^2 = 8\lambda$$

και

$$x \equiv y \pmod 4 \quad \text{και} \quad z \equiv sy \pmod 2 \Leftrightarrow 2z = 2sy \pmod 4.$$

Έτσι, για την F παίρνουμε:

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv ay^2 + by^2 + c'2zz \equiv ay^2 + by^2 + c'2syz \\ &\equiv ay^2 + by^2 + c'2s^2y^2 \equiv (a + b + cs^2)y^2 \\ &\equiv 8\lambda y^2 \equiv 0 \pmod 4. \end{aligned}$$

Έστω τέλος $2 \nmid abc$. Τότε, από τις συνθήκες (iii), (ii) έχουμε:

$$a + b \equiv 0 \pmod 4, \text{ με } a, b \not\equiv 2 \pmod 4 \quad \text{και}$$

$$z \equiv 0 \pmod 2 \Leftrightarrow z^2 \equiv 0 \pmod 4.$$

Επιπλέον, η F έχει ρίζα στο $\mathbb{Q}_2$, επομένως θα έχει και modulo 2. Παίρνουμε έτσι:

$$ax^2 + by^2 + cz^2 \equiv ax^2 + by^2 \equiv x^2 + y^2 \equiv 0 \pmod 2 \Leftrightarrow x \equiv y \pmod 2.$$

Έτσι, για την F έχουμε:

$$ax^2 + by^2 + cz^2 \equiv ax^2 + by^2 \equiv 0 \pmod 4.$$

□

Συνέχεια της Απόδειξης του Θεωρήματος 19

Έχοντας αποδείξει τα προηγούμενα λήμματα, εφαρμόζουμε το Θεώρημα Minkowski για κυρτά σώματα στο σύνολο C που ορίζεται από τη σχέση:

$$C : |a|x^2 + |b|y^2 + |c|z^2 < 4|abc|.$$

Το C είναι κυρτό και συμμετρικό (τμήμα ελλειψοειδούς) και έχει όγκο

$$V(C) = \frac{\pi}{3} 2^3 4|abc| > 2^3.$$

Επομένως, υπάρχει ένα μη μηδενικό $\mathbf{c} = (c_1, c_2, c_3) \in H \cap C$, δηλαδή τέτοιο ώστε:

$$F(c_1, c_2, c_3) = ac_1^2 + bc_2^2 + cc_3^2 \equiv 0 \pmod{4|abc|} \Leftrightarrow F(c_1, c_2, c_3) = \lambda \cdot 4|abc|$$

και

$$\left|ac_1^2 + bc_2^2 + cc_3^2\right| \leq |\,a|c_1^2 + |\,b|c_2^2 + |\,c|c_3^2 < 4|abc| \Leftrightarrow$$

$$-4|abc| < ac_1^2 + bc_2^2 + cc_3^2 < 4|abc|.$$

Επομένως, $F(c_1, c_2, c_3) = 0$, δηλαδή η τετραγωνική μορφή $F(x, y, z)$ έχει λύση στο $\mathbb{Z}^3$, άρα και στο $\mathbb{Q}^3$.

□

Απόδειξη Θεωρήματος 17 (Hasse-Minkowski)

Θα ολοκληρώσουμε αυτή την ενότητα με την απόδειξη της γενικής περίπτωσης του Θεωρήματος Hasse-Minkowski. Θα χρειαστούμε κάποιες έννοιες από τη θεωρία των τετραγωνικών μορφών, καθώς και κάποια θεωρήματα και προτάσεις, των οποίων τις αποδείξεις είτε θα παραλείψουμε ή θα σκιαγραφήσουμε.

Ορισμός 32 Έστω $a, b \in \mathbb{Q}_p^\star$, $p \leq \infty$. Ορίζουμε το *σύμβολο Hilbert* $(a,b)_p$ των a, b ως προς τον πρώτο p ως ακολούθως:

$$(a,b)_p = \begin{cases} 1, & \text{αν η } z^2 - ax^2 - by^2 = 0 \text{ έχει μη τετριμμένη λύση στο } \mathbb{Q}_p^3 \\ -1, & \text{διαφορετικά.} \end{cases}$$

Είναι προφανές ότι το σύμβολο Hilbert $(a,b)_p$ δεν αλλάζει τιμή όταν τα a και b πολλαπλασιαστούν με κάποιο τετράγωνο. Επομένως, μέσω του συμβόλου Hilbert, ορίζεται μια συνάρτηση από το $\mathbb{Q}_p^\star/(\mathbb{Q}_p^\star)^2 \times \mathbb{Q}_p^\star/(\mathbb{Q}_p^\star)^2$ στο $\{\pm 1\}$.

Αποδεικνύεται ότι το σύμβολο Hilbert είναι διγραμμικό ως προς τον πολλαπλασιασμό, ότι δηλαδή:

$$(aa', b)_p = (a,b)_p (a',b)_p.$$

Η Πρόταση 15 εκφράζεται στη γλώσσα του συμβόλου Hilbert ως ακολούθως:

Πρόταση 44 *Έστω $a,\ b \in \mathbb{Q}_p^\star$ και έστω $\mathbb{Q}_{pb} = \mathbb{Q}_p(\sqrt{b})$. Το σύμβολο Hilbert $(a,b)_p$ ισούται με ένα, εάν και μόνο αν το a ανήκει στην ομάδα των νορμών $N\mathbb{Q}_{pb}^\star$[1] των στοιχείων του $\mathbb{Q}_{pb}^\star$.*

Απόδειξη: Εάν το b είναι το τετράγωνο κάποιου στοιχείου $c \in \mathbb{Q}_p^\star$, τότε η εξίσωση

$$z^2 - ax^2 - by^2 = 0$$

έχει την $(c,\ 0,\ 1)$ για λύση, και άρα $(a,b)_p = 1$. Η πρόταση είναι προφανής σε αυτήν την περίπτωση, εφόσον $\mathbb{Q}_{pb} = \mathbb{Q}_p$ και $N\mathbb{Q}_{pb}^\star = \mathbb{Q}_p^\star$.

Διαφορετικά, η επέκταση $\mathbb{Q}_{pb}$ είναι βαθμού δύο πάνω από το $\mathbb{Q}_p$ και κάθε στοιχείο γράφεται ως $z + \beta y$, όπου $\beta = \sqrt{b}$ και $z,\ y \in \mathbb{Q}_p$. Εάν έχουμε $a \in N\mathbb{Q}_{pb}^\star$, τότε υπάρχουν $z_0,\ y_0 \in \mathbb{Q}_p$, τέτοια ώστε $a = z_0^2 - by_0^2$, και άρα, η τετραγωνική μορφή $z^2 - ax^2 - by^2$ έχει ρίζα την $(z_0,\ 1,\ y_0)$, και έτσι $(a,b)_p = 1$.

[1] Ένα στοιχείο $a = \kappa + \lambda\sqrt{b} \in \mathbb{Q}_p(\sqrt{b})$ έχει νόρμα $N(a) = \kappa^2 - \lambda^2 b \in N\mathbb{Q}_{pb}^\star$.

Αντίστροφα, εάν $(a,b)_p = 1$, τότε η τετραγωνική μορφή έχει μη τετριμμένη ρίζα (z_0, x_0, y_0). Εάν το b είναι τετράγωνο, τότε προφανώς, το a θα ανήκει στο σύνολο των νορμών, εφόσον $N\mathbb{Q}_{pb}^* = \mathbb{Q}_p^*$.

Αν, τώρα, το b δεν είναι τετράγωνο, θα ισχύει ότι $x \neq 0$. Επομένως, βλέπουμε ότι το a ειναι η νόρμα του στοιχείου $z_0/x_0 + \beta y_0/x_0$. □

Για $a, a', b \in \mathbb{Q}_p$, αποδεικνύονται εύκολα τα ακόλουθα:

(i) $(a,b)_p = (b,a)_p$ και $(a,c^2)_p = 1$,

(ii) $(a,-a)_p = 1$ και $(a,1-a)_p = 1$,

(iii) $(a,b)_p = 1 \Rightarrow (aa',b)_p = (a',b)_p$,

(iv) $(a,b)_p = (a,-ab)_p = (a,a(1-a)b)_p$.

Η Πρόταση 44 μας δίνει έναν κλειστό τύπο για τον υπολογισμό του συμβόλου Hilbert:

(i) Εάν $p = \infty$, δηλαδή $\mathbb{Q}_p = \mathbb{R}$ έχουμε: $(a,b)_p = 1$ αν a ή $b > 0$ και $(a,b)_p = -1$ αν a και $b < 0$.

(ii) Εάν $p < \infty$ και $a = p^{v_p(a)}a'$, $b = p^{v_p(b)}b'$, όπου a', $b' \in \mathbb{Z}_p^*$, τότε:

$$(a,b)_p = (-1)^{v_p(a)v_p(b)\epsilon(p)} \left(\frac{a'}{p}\right)^{v_p(a)} \left(\frac{b'}{p}\right)^{v_p(b)} \qquad \text{για } p \neq 2$$

$$(a,b)_2 = (-1)^{\epsilon(a')\epsilon(b')+v_p(a)\omega(b')+v_p(b)\omega(a')} \qquad \text{για } p = 2,$$

όπου

- $\left(\frac{x}{p}\right) = 1$, εάν και μόνον εάν το x είναι τετράγωνο στο $\mathbb{Z}_p^*$,
- $\epsilon(x) \equiv (x - 1/2) \pmod 2$, και
- $\omega(x) \equiv (x^2 - 1/8) \pmod 2$.

Θεώρημα 20 (Hilbert) *Εάν $a, b \in \mathbb{Q}^*$, τότε $(a,b)_p = 1$ για σχεδόν όλους τους πρώτους $p \leq \infty$. Επιπλέον:*

$$\prod_{p \leq \infty} (a,b)_p = 1.$$

Απόδειξη: Λόγω της διγραμμικότητας του συμβόλου Hilbert η απόδειξη του παραπάνω θεωρήματος ανάγεται στο να θεωρήσουμε τα a, b να είναι -1 ή πρώτοι αριθμοί, και σε απαρίθμηση των περιπτώσεων. □

Τέλος, για ρητούς αριθμούς και τα σχετικά με αυτούς σύμβολα Hilbert, ισχύει το ακόλουθο:

Θεώρημα 21 *Έστω $(a_i)_{i \in I}$ πεπερασμένη οικογένεια στοιχείων του $\mathbb{Q}^*$ και έστω $(\epsilon_{i,p})_{i \in I,\, p \leq \infty}$ οικογένεια αριθμών, με $\epsilon_{i,p} = \pm 1$. Τότε, ικανή και αναγκαία συνθήκη για να υπάρχει $x \in \mathbb{Q}^*$, τέτοιο ώστε $(a_i, x)_p = \epsilon_{i,p}$ για κάθε $i \in I$ και κάθε πρώτο $p \leq \infty$, είναι να ικανοποιούνται τα ακόλουθα:*

(i) *σχεδόν όλα τα $\epsilon_{i,p}$ να είναι 1,*

(ii) *για κάθε $i \in I$ να ισχύει $\prod_{p \leq \infty} \epsilon_{i,p} = 1$,*

(iii) *για κάθε πρώτο $p \leq \infty$ υπάρχει $x_p \in \mathbb{Q}_p^*$, τέτοιο ώστε $(a_i, x_p)_p = \epsilon_{i,p}$ για κάθε $i \in I$.*

Απόδειξη: Το ευθύ για τα (i),(ii) προκύπτει άμεσα από το Θεώρημα Hilbert. Για το (iii) μπορούμε να πάρουμε $x_p = x$, οπότε έχουμε το ζητούμενο.

Για το αντίστροφο, θέτουμε S το σύνολο που περιέχει το 2, το ∞ και όλους τους πρώτους που εμφανίζονται στις παραγοντοποιήσεις των a_i. Ακόμα, θέτουμε T το σύνολο των πρώτων $p \leq \infty$, τέτοιων ώστε για κάποιο $i \in I$ να ισχύει $\epsilon_{i,p} = -1$. Και τα δύο σύνολα είναι πεπερασμένα.

Για τη συνέχεια της απόδειξης θα μας χρειαστούν τα ακόλουθα λήμματα:

Λήμμα 13 (Κινέζικο Θεώρημα Υπολοίπων) *Έστω $m_1, m_2, \ldots, m_n$, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, με τους m_i ανά δύο πρώτους μεταξύ τους. Τότε υπάρχει $a \in \mathbb{Z}$, τέτοιος ώστε:*

$$a \equiv a_i \pmod{m_i} \quad \text{για κάθε } i \in I.$$

Λήμμα 14 (Θεώρημα Dirichlet) *Έστω $a, m \in \mathbb{Z}$, πρώτοι μεταξύ τους και μεγαλύτεροι ή ίσοι της μονάδας. Τότε, υπάρχουν άπειροι το πλήθος πρώτοι p, τέτοιοι ώστε $p \equiv a \pmod{m}$.*

Λήμμα 15 *Έστω $V = \{p_i : p_i \text{ πρώτος}, p_i \leq \infty\}$ πεπερασμένο σύνολο. Η εικόνα του $\mathbb{Q}$ στο $\prod_{p_i \in V} \mathbb{Q}_{p_i}$ είναι πυκνή στο $\prod_{p_i \in V} \mathbb{Q}_{p_i}$.*

Μελετούμε τώρα τις ακόλουθες δύο περιπτώσεις: $T \cap S = \emptyset$ και $T \cap S \neq \emptyset$. Για την πρώτη περίπτωση επαληθεύεται ότι το στοιχείο $x = ap$, όπου

$$a = \prod_{\substack{l \in T \\ l \neq \infty}} l \quad \text{και} \quad m = 8 \prod_{\substack{l \in S \\ l \neq 2, \infty}} l$$

και p πρώτος αριθμός, τέτοιος ώστε $p \notin T \cup S$ και $p \equiv a \pmod{m}$ (από Λήμμα 14), ικανοποιεί ότι $(a_i, x)_p = \epsilon_{i,p}$, εφόσον πληρούνται οι (i), (ii), (iii).

Για τη δεύτερη περίπτωση το κατάλληλο στοιχείο είναι το $x = yx'$, όπου:

$$x' \in \mathbb{Q}^* \text{ ώστε } \frac{x'}{x_p} \in (\mathbb{Q}_p^*)^2 \qquad (\text{Λήμμα 15})$$

και το $y \in \mathbb{Q}^*$ προκύπτει από την πρώτη περίπτωση, για την οικογένεια αριθμών $\eta_{i,p} = \epsilon_{i,p} \cdot (a_i, x')_p$. □

Τετραγωνικές μορφές

Στην προηγούμενη ενότητα, συγκεκριμένα στην τρίτη εφαρμογή του Λήμματος του Hensel, ορίσαμε την έννοια της τετραγωνικής μορφής από ένα διανυσματικό χώρο V σε ένα σώμα $\mathbb{K}$. Παρακάτω θα δώσουμε κάποιες σημαντικές αναλλοίωτες ποσότητες σχετικές με κάθε τετραγωνική μορφή, οι οποίες τις ταξινομούν σε κλάσεις ισοδυναμίας.

Έχουμε αναφέρει ότι κάθε τετραγωνική μορφή μπορεί να αναχθεί στη μορφή:

$$f(x) = a_1 x_1^2 + \cdots + a_n x_n^2 = \sum_{k=1}^{n} a_k x_k^2,$$

όπου $x = (x_1, x_2, \ldots, x_n)$. Επειδή θα μας απασχολήσουν τετραγωνικές μορφές που ορίζονται πάνω στα σώματα $\mathbb{Q}_p$ και $\mathbb{Q}$, θα έχουμε $a_i \in \mathbb{Q}_p, p \leq \infty$, ή $a_i \in \mathbb{Q}$. Για τον ίδιο λόγο θεωρούμε $V = \mathbb{Q}_p^n$ ή $\mathbb{Q}^n$ και $\mathbb{K} = \mathbb{Q}_p$ ή $\mathbb{Q}$.

Ορίζουμε ως *τάξη* $n(f)$ της τετραγωνικής μορφής f τον αριθμό των δεικτών i, για τους οποίους έχουμε $a_i \neq 0$. Επιπλέον, θα καλούμε *διακρίνουσα* της τετραγωνικής μορφής f το γινόμενο $d(f) = a_1 \dots a_n$. Αποδεικνύεται ότι μπορούμε να θεωρούμε την d ως στοιχείο του $I\!K^\star/(I\!K^\star)^2$, όπου $I\!K$ το σώμα πάνω στο οποίο ορίζεται η f.

Τετραγωνικές μορφές πάνω στο $Q\!\!\!Q_p$

Έστω f τετραγωνική μορφή πάνω από στο $Q\!\!\!Q_p$. Ορίζουμε το σχετικό με την τετραγωνική μορφή f σύμβολο Hilbert, ως το γινόμενο:

$$\epsilon_p(f) = \prod_{i<j} (a_i, a_j)_p,$$

όπου $(a_i, a_j)_p$ το σύμβολο Hilbert, όπως το ορίσαμε παραπάνω.

Θεώρημα 22 *Η διακρίνουσα $d(f)$ και το σύμβολο Hilbert $\epsilon_p(f)$ μιας τετραγωνικής μορφής f πάνω στο $Q\!\!\!Q_p$ αποτελούν αναλλοίωτες ποσότητες για την f.*

Για την απόδειξη του θεωρήματος παραπέμπουμε στο [16].

Ορισμός 33 Δύο τετραγωνικές μορφές f, g είναι ισοδύναμες, όταν έχουν την ίδια τάξη n, την ίδια διακρίνουσα d και το ίδιο σύμβολο Hilbert ϵ. Την ισοδυναμία των f, g συμβολίζουμε με $f \sim g$.

Θα λέμε ότι μία τετραγωνική μορφή f *αναπαριστά* ένα στοιχείο $a \in I\!K$, εάν υπάρχει $x \in I\!K^n$, $x \neq 0$, τέτοιο ώστε $f(x) = a$.

Ακόμα, ορίζουμε $h = f \widehat{+} g$, $h = f \widehat{-} g$ για δύο τετραγωνικές μορφές f, g, να είναι μία τετραγωνική μορφή h με τάξη $n(h) = n(f) + n(g)$ και συντελεστές τους συντελεστές των f, g ή των $f, (-g)$ αντίστοιχα.

Θεώρημα 23 *Εάν η τετραγωνική μορφή f αναπαριστά το 0 και $d(f) \neq 0$, τότε ισχύει $f \sim f_1 + g$, όπου $f_1 \sim x_1^2 - x_2^2$. Επιπλέον, η f αναπαριστά κάθε στοιχείο του $I\!K$.*

Πόρισμα 12 *Έστω $g = g(x_1, \dots, x_{n-1})$ τετραγωνική μορφή τάξης $n-1$, με $d(g) \neq 0$ και έστω $a \in I\!K$. Τα ακόλουθα είνα ισοδύναμα:*

(i) *Η g αναπαριστά το a.*

(ii) *Έχουμε $g \sim h \widehat{+} az^2$, όπου h είναι μια τετραγωνική μορφή τάξης $n-2$.*

(iii) *Η τετραγωνική μορφή $f = g \widehat{-} az^2$ αναπαριστά το 0.*

Πόρισμα 13 *Έστω $g,\ h$ τετραγωνικές μορφές με $d(g),\ d(h) \neq 0$ και $n(g),\ n(h) \geq 1$. Τα ακόλουθα είναι ισοδύναμα:*

(i) *Η $f = g \widehat{-} h$ αναπαριστά το 0.*

(ii) *Υπάρχει $a \in I\!K^\star$ το οποίο αναπαρίσταται από την g και την h.*

(iii) *Υπάρχει $a \in I\!K^\star$, τέτοιο ώστε οι $g \widehat{-} az^2$ και $h \widehat{-} az^2$ να αναπαριστούν το 0.*

Οι αποδείξεις του θεωρήματος και των πορισμάτων απαιτούν εκτενή ανάλυση και βασίζονται σε προχωρημένη γραμμική άλγεβρα. Για αυτές παραπέμπουμε και πάλι στο [16].

Το ακόλουθο θεώρημα είναι ανάλογο του Θεωρήματος 16. Μας λέει πότε μια τετραγωνική μορφή έχει ρίζες, χρησιμοποιώντας τις έννοιες των τριών αναλλοίωτων $n,\ d,\ \epsilon$ μιας τετραγωνικής μορφής. Το παραθέτουμε χωρίς απόδειξη.

Θεώρημα 24 *Έστω η τετραγωνική μορφή f τάξης n με διακρίνουσα d και σύμβολο Hilbert ϵ. Για να αναπαριστά η f το 0 είναι ικανό και αναγκαίο να ικανοποιούνται οι ακόλουθες συνθήκες:*

(i) *$n = 2$ και $d = -1$ (στο $I\!K^\star/(I\!K^\star)^2$),*

(ii) *$n = 3$ και $(-1, -d)_p = \epsilon$,*

(iii) *$n = 4$ και είτε $d \neq 1$ ή $d = 1$ και $\epsilon = (-1, -1)_p$,*

(iv) *$n \geq 5$.*

Τετραγωνικές μορφές πάνω από το $\mathbb{R}$

Μια τετραγωνική μορφή τάξης n πάνω από το $\mathbb{R}$ είναι ισοδύναμη με τη μορφή

$$x_1^2 + \ldots + x_r^2 - y_1^2 - \ldots - y_s^2,$$

όπου r και s μη αρνητικοί ακέραιοι αριθμοί, τέτοιοι ώστε $r+s=n$. Το ζευγάρι (r,s) εξαρτάται μόνο από την f, και καλείται *προσήμανση (signature)* της f. Λέμε ότι η f είναι ορισμένη (definite) αν r ή $s=0$, δηλαδή όταν δεν αλλάζει πρόσημο. Διαφορετικά, λέμε ότι είναι αόριστη (indefinite) (και σε αυτή την περίπτωση η f αναπαριστά το 0).

Το σύμβολο Hilbert $\epsilon(f)$ ορίζεται όπως και προηγουμένως. Συγκεκριμένα, επειδή $(-1,-1)_\infty = -1$, έχουμε:

$$\epsilon(f) = (-1)^{s(s-1)/2} = \begin{cases} 1, & \text{αν } s \equiv 0,1 \pmod 4, \\ -1, & \text{αν } s \equiv 2,3 \pmod 4. \end{cases}$$

Επιπλέον:

$$d(f) = (-1)^s = \begin{cases} 1, & \text{αν } s \equiv 0 \pmod 2, \\ -1, & \text{αν } s \equiv 1 \pmod 2. \end{cases}$$

Τετραγωνικές μορφές πάνω από το $\mathbb{Q}$

Έστω $f = a_1x_1^2 + \cdots + a_nx_n^2$, $a_i \in \mathbb{Q}$ τετραγωνική μορφή τάξης n. Ορίζουμε τις ακόλουθες αναλλοίωτες για την f:

(i) Τη διακρίνουσα $d(f) = a_1 \ldots a_n \ \in \mathbb{Q}^\star/(\mathbb{Q}^\star)^2$. Εφόσον κάθε στοιχείο a_i ανήκει στο $\mathbb{Q}$, μπορούμε επίσης να το βλέπουμε και ως στοιχείο του $\mathbb{Q}_p$, για κάθε $p \leq \infty$. Επομένως, έχει νόημα να συμβολίζουμε την $d(f)$ ως $d_p(f)$, για κάθε πρώτο $p \leq \infty$.

(ii) Επιπλέον, για τον παραπάνω λόγο, θα θεωρήσουμε για την f τα σύμβολα Hilbert $\epsilon_p(f)$, για κάθε πρώτο $p \leq \infty$:

$$\epsilon_p(f) = \prod_{i<j} (a_i, a_j)_p.$$

(iii) Τέλος, θεωρώντας την f ως πραγματική τετραγωνικής μορφή, η προσήμανση (r,s) της f αποτελεί επίσης μιά αναλλοίωτη ποσότητα για την f.

Από το Θεώρημα Hilbert προκύπτει ότι για τα σύμβολα Hilbert $\epsilon_p(f)$ της ρητής τετραγωνικής μορφής f ισχύει:

$$\prod_{p\leq\infty} \epsilon_p(f) = 1.$$

Απόδειξη Θεωρήματος 17 (Hasse-Minkowski)

Μπορούμε τώρα να περάσουμε στην απόδειξη του Θεωρήματος Hasse-Minkowski. Κάνουμε επαγωγή στο πλήθος των μεταβλητών, δηλαδή στην τάξη της τετραγωνικής μορφής.

(1) *Η περίπτωση* $n = 2$ Είναι η Πρόταση 43.

(2) *Η περίπτωση* $n = 3$ Είναι το Θεώρημα 19. Μπορούμε να το δείξουμε και με επαγωγή στο άθροισμα των συντελεστών. Πιο συγκεκριμένα, έχουμε ότι η τετραγωνική μορφή με τρεις μεταβλητές είναι της μορφής

$$f = x_1^2 - ax_2^2 - bx_3^2,$$

και μπορούμε να υποθέσουμε ότι τα a, b είναι ελεύθερα τετραγώνων. Επίσης, μπορούμε να υποθέσουμε ότι $|a| \leq |b|$, όπου $|\cdot|$ η συνήθης απόλυτη τιμή. Θα δείξουμε ότι αν η f έχει ρίζα σε κάθε $\mathbb{Q}_p$, $p \leq \infty$, τότε θα έχει και στο $\mathbb{Q}$.

Χρησιμοποιούμε επαγωγή στο $m = |a| + |b|$. Για $m = 2$ έχουμε:

$$f = x_1^2 \pm x_2^2 \pm x_3^2.$$

Επειδή η f έχει λύσεις στο $\mathbb{R}$, δεν μπορεί να είναι της μορφής $x_1^2 + x_2^2 + x_3^2$. Σε κάθε άλλη περίπτωση όμως, η f έχει λύση, για παράδειγμα μια *πυθαγόρεια τριάδα*.

Έστω, τώρα, $m > 2$, και χωρίς βλάβη της γενικότητας, έστω $|b| > 2$. Μπορούμε να γράψουμε το b ως

$$b = \pm p_1 \dots p_k,$$

όπου p_i πρώτοι διαφορετικοί μεταξύ τους. Από την Πρόταση 44 έχουμε ότι για κάθε p το a θα ανήκει στην ομάδα των νορμών $N\mathbb{Q}_{pb}^{\star}$ των στοιχείων του $\mathbb{Q}_p(\sqrt{b})$, και άρα θα είναι της μορφής $a = t^2 - bs^2$, δηλαδή το a είναι τετράγωνο modulo b. Μάλιστα, μπορούμε να επιλέξουμε το t έτσι ώστε $|t| \leq |b|/2$ και $a = t^2 - bb'$.

Έτσι, μπορούμε να γράψουμε ότι $bb' = t^2 - a$, το οποίο μας δείχνει ότι το bb' είναι νόρμα της επέκτασης $I\!K(\sqrt{a})$ πάνω από το $I\!K$, όπου $I\!K = \mathbb{Q}$ ή $\mathbb{Q}_p$. Από την ιδιότητα (iii) του συμβόλου Hilbert, καταλήγουμε στο ότι η f αναπαριστά το 0 στο $I\!K$, αν και μόνο αν ισχύει το ίδιο και για την

$$f' = x_1^2 - ax_2^2 - b'x_3^2.$$

Συγκεκριμένα έχουμε ότι η f' αναπαριστά το 0 σε κάθε $\mathbb{Q}_p$, και επιπλέον έχουμε:

$$|b'| = \left|\frac{t^2 - a}{b}\right| \leq \frac{b}{4} + 1 < b, \quad \text{καθώς } |b| \geq 2.$$

Αν γράψουμε $b' = b''u^2$, όπου u ακέραιοι αριθμοί και b'' ελεύθερο τετραγώνων, τότε η f' είναι ισοδύναμη με την $f'' = x_1^2 - aX_2^2 - b''x_3^2$, και ισχύει ότι $|b''| < |b|$. Επομένως, μπορούμε να εφαρμόσουμε την επαγωγική υπόθεση για την f'', η οποία τελικά είναι ισοδύναμη με την f.

(3) *Η περίπτωση* $n = 4$ Γράφουμε την f ως διαφορά δύο τετραγωνικών μορφών τάξης δύο:

$$f = h \widehat{-} g = ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2).$$

Από το Λήμμα 13, εφόσον η f αναπαριστά το 0 σε κάθε $\mathbb{Q}_p$, υπάρχει $x_p \in \mathbb{Q}_p^\star$ που αναπαρίσταται και από τις δύο τετραγωνικές μορφές h και g. Ισοδύναμα, από το Θεώρημα 24, αυτό σημαίνει ότι

$$(x_p, -ab)_p = (a, b)_p \ \text{ και } \ (x_p, -cd)_p = (c, d)_p \ \text{ για κάθε } p \leq \infty.$$

Εφόσον $\prod_{p\leq\infty}(a,b)_p = \prod_{p\leq\infty}(c,d)_p = 1$, μπορούμε να εφαρμόσουμε το Θεώρημα 21. Εξασφαλίζουμε έτσι την ύπαρξη ρητού αριθμού $x \in \mathbb{Q}^\star$, τέτοιου ώστε:

$$(x, -ab)_p = (a, b)_p \ \text{ και } \ (x, -cd)_p = (c, d)_p \ \text{ για κάθε } p \leq \infty.$$

Λόγω των παραπάνω, βλέπουμε ότι η τετραγωνική μορφή $ax_1^2 + bx_2^2 - xz^2$ αναπαριστά το 0 σε κάθε $\mathbb{Q}_p$, άρα και στο $\mathbb{Q}$ λόγω του (ii). Επομένως, η h αναπαριστά το x στο $\mathbb{Q}$. Την ίδια σκέψη ακολουθούμε και για την g. Έπεται άμεσα ότι η f αναπαριστά το 0 στο $\mathbb{Q}$.

(4) *Η περίπτωση* $n \geq 5$ Γράφουμε την f ως:

$$f = h\widehat{-}g = a_1x_1^2 + a_2x_2^2 - (a_3x_3^2 + \cdots a_nx_n^2).$$

Έστω S το σύνολο που περιέχει το άπειρο, το δύο και όλους τους πρώτους p που διαιρούν τους συντελεστές της g. Το S είναι ένα πεπερασμένο σύνολο.

Έστω $v \in S$. Εφόσον η f αναπαριστά το 0 στο $\mathbb{Q}_v$, τότε θα υπάρχει κάποιο $a_v \in \mathbb{Q}_v^*$ που αναπαρίσταται από την h και από την g, δηλαδή θα υπάρχουν x_i^v, τέτοια ώστε:

$$h(x_1^v, x_2^v) = a_v = g(x_3^v, \ldots, x_n^v).$$

Επειδή το σύνολο των τετραγώνων του $\mathbb{Q}_v^*$ είναι ανοικτό σύνολο, μπορούμε να προσεγγίσουμε κάποιο από τα στοιχεία του. Δηλαδή, μπορούμε να βρούμε $x_1, x_2 \in \mathbb{Q}$ με $a = h(x_1, x_2)$, τέτοια ώστε $a/a_v \in \mathbb{Q}_v^2$,για κάθε $v \in S$.

Θεωρούμε τώρα την τετραγωνική μορφή $f_1 = az^2\widehat{-}g$. Εάν $v \in S$, τότε η g αναπαριστά κάποιο $a_v \in \mathbb{Q}_v$, και επομένως αναπαριστά και το a. Πράγματι,

$$g(x_3^v, \ldots, x_n^v) = a_v \Rightarrow ag(x_3^v, \ldots, x_n^v) = aa_v \Rightarrow$$

$$\frac{a}{a_v} g(x_3^v, \ldots, x_n^v) = a,$$

και επειδή το a/a_v είναι τετράγωνο, μπορεί να απορροφηθεί στις μεταβλητές της g. Επομένως, η f αναπαριστά το 0 στο $\mathbb{Q}$.

Έστω τώρα $v \notin S$. Τότε, όλοι οι συντελεστές $-a_3, \ldots, -a_n$ είναι p-αδικές μονάδες, και επομένως το ίδιο και η διακρίνουσα $d_v(g)$. Επιπλέον, επειδή $v \neq 2$, έχουμε ότι $\epsilon_v(g) = 1$. Σε κάθε περίπτωση, η f_1 αναπαριστά το 0 σε κάθε $\mathbb{Q}_v$, και άρα, εφόσον έχει τάξη $n-1$, αναπαριστά το 0 στο $\mathbb{Q}$, λόγω της επαγωγικής υπόθεσης. Δηλαδή, η g αναπαριστά το a στο $\mathbb{Q}$. Επειδή και η h αναπαριστά το a στο $\mathbb{Q}$, προκύπτει άμεσα ότι η f αναπαριστα το 0 στο $\mathbb{Q}$. □

Κεφάλαιο 5

Άλλες εφαρμογές των p-αδικών αριθμών

Όπως είδαμε σε προηγούμενη ενότητα, το σώμα των p-αδικών αριθμών και το σώμα των πραγματικών αριθμών έχουν πολλές ομοιότητες, όμως ταυτόχρονα και πάρα πολλές διαφορές. Για παράδειγμα, ενώ και τα δύο είναι πληρώσεις των ρητών αριθμών, έχουν διαφορετική γεωμετρία και άλγεβρα. Μάλιστα, επειδή απλοποιούνται πολύ τα πράγματα στα p-αδικά σώματα, μία χρησιμότητά τους είναι η απλούστερη απόδειξη γνωστών αποτελεσμάτων, όπως για παράδειγμα το Θεώρημα του Fermat. Το τελυεταίο κεφάλαιο δίνει επίσης μία σημαντική εφαρμογή των p-αδικών στη Θεωρία Αριθμών.

Εφαρμογές στη Φυσική

Από τη δεκαετία του '80 περίπου, οι φυσικοί εκμεταλλεύτηκαν τις διαφορές μεταξύ πραγματικών και p-αδικών αριθμών και αναπτύχθηκε έτσι ο κλάδος της p-αδικής Μαθηματικής Φυσικής. Η ουλτραμετρική ιδιότητα της p-αδικής μετρικής δίνει ένα παράδειγμα δομής που φαίνεται κατάλληλο για την περιγραφή μερικών φυσικών διαδικασιών.

Το πρώτο παράδειγμα στο οποίο φάνηκαν χρήσιμοι οι p-αδικοί αριθμοί είναι η Στατιστική Φυσική. Η θεωρία των θερμοδυναμικών ιδοτήτων των spin glasses[1] χρησιμοποιεί p-αδικές μεθόδους ως εργαλεία. Συγκεκριμένα η *τεχνική*

[1] άτακτα υλικά συστήματα που παρουσιάζουν δυσκολία στην ελαχιστοποίηση των μαγνητικών ενεργειών αλληλεπίδρασης μεταξύ των συστατικών τους (high magnetic frustration).

των Αντιγράφων (Replica trick)[2] είναι ισοδύναμη με μία σειρά ακεραίων που τείνει p-αδικά στο μηδέν για όλους τους πρώτους αριθμούς. Επίσης, οι p-αδικοί αριθμοί βρίσκουν εφαρμογή στα διάφορα μοντέλα που περιγράφουν τη *χαλάρωση (relaxation)* των γυαλιών και των μακρομορίων, της οποίας η μη εκθετική φύση φαίνεται να είναι συνέπεια της ιεραρχικής δομής των χωρικών τους καταστάσεων. Θυμίζουμε ότι οι p-αδικοί αριθμοί χαρακτηρίζονται από την ιεραρχική τους δομή (βλ. Ενότητα 3.6).

Επίσης, οι p-αδικοί χρησιμοποιούνται στη σωματιδιακή και κβαντική φυσική. Μια από τις πιο εντυπωσιακές ανακαλύψεις των τελευταίων δεκαετιών είναι ότι ο χώρος και ο χρόνος είναι *μη αρχιμήδειοι*: η αρχιμήδεια ιδιότητα παύει να ισχύει στην *κλίμακα του Planck*, δηλαδή για αποστάσεις μικρότερες των 1.6×10^{-33} μέτρων και για χρονικά διαστήματα μικρότερα των 5.4×10^{-44} δευτερολέπτων. Η μη αρχιμήδεια αυτή δομή του χωροχρόνου οδήγησε στην κατασκευή p-αδικών μοντέλων, τα οποία και φαίνεται να ανταποκρίνονται καλύτερα απ' ότι τα συνήθη μοντέλα, που βασίζονται στους πραγματικούς αριθμούς, για την περιγραφή των φαινομένων σε τόσο μικρές κλίμακες.

Τα πρώτα μοντέλα p-αδικής κβαντικής φυσικής είναι αυτά των p-αδικών Χορδών και Υπερχορδών. Η Θεωρία Χορδών (String Theory) είναι ένα μοντέλο της θεωρητικής Φυσικής, του οποίου τα θεμελιώδη δομικά στοιχεία είναι μονοδιάστατα εκτεταμένα αντικείμενα, οι Χορδές (strings), σε αντίθεση με την παραδοσιακή έννοια των σημειακών και αδιάστατων στοιχειωδών σωματιδίων. Αν και δεν έχει ως τώρα υπάρξει πειραματική επαλήθευσή της, είναι προς το παρόν η μόνη αξιόπιστη θεωρία κβαντικής βαρύτητας η οποία μπορεί εξίσου καλά να περιγράψει και τις ηλεκτρομαγνητικές και τις άλλες θεμελιώδεις αλληλεπιδράσεις. Δεδομένης λοιπόν της μη αρχιμήδειας δομής του χωροχρόνου, τα μοντέλα των p-αδικών Χορδών βρίσκουν πολλές εφαρμογές στη σύγχρονη Φυσική.

Όλες αυτές οι έρευνες πάνω στην p-αδική μαθηματική φυσική οδήγησαν στην ανάπτυξη των p-αδικών μαθηματικών σε πολλές διαφορετικές κατευθύνσεις, όπως: την p-αδική Θεωρία των Κατανομών, την p-αδική Θεωρία Πιθαν-

[2] Αν έχουμε ότι Z είναι η συνάρτηση διαμέρισης του συστήματος, η οποία μας δίνει πληροφορίες για διάφορες μακροσκοπικές ποσότητες του συστήματος όπως η εντροπία, η ελεύθερη ενέργεια κ.α., η τεχνική αυτή συνίσταται στην εφαρμογή της σχέσης $\lim_{n\to 0} \frac{Z^n-1}{n} = \log Z$ για την προσέγγιση της Z.

οτήτων [3], τη Θεωρία Τελεστών σε ένα p-αδικό ανάλογο ενός χώρου Hilbert, τα p-αδικά Δυναμικά συστήματα κ.α. Επίσης, προέκυψαν μία σειρά από p-αδικές διαφορικές εξισώσεις και έχουν μελετηθεί τα p-αδικά ανάλογα άλλων, όπως για παράδειγμα της κυματικής εξίσωσης.

Εφαρμογές στη Θεωρία Κωδίκων και τη Θεωρία Πληροφοριών

Η αναπαράσταση των p-αδικών αριθμών από ακολουθίες συγκεκριμένων ψηφίων δίνει τη δυνατότητα να χρησιμοποιηθούν για την κωδικοποίηση της πληροφορίας. Για παράδειγμα, μπορούμε να κατασκευάσουμε κώδικες, τους λεγόμενους κώδικες Hensel, οι οποίοι μπορούν να αναπαραστήσουν μοναδικά όλους του όρους μιας ακολουθίας Farey. Μία ακολουθία Farey τάξης n είναι όλα τα ανάγωγα κλάσματα που ανήκουν στο $[0, 1]$, των οποίων ο παρονομαστής δεν υπερβαίνει το n. Δηλαδή, έχουμε μοναδική απεικόνιση ρητών αριθμών που ανήκουν στο $[0, 1]$, και επιπλέον μία ιδιάιτερα εύχρηστη αριθμητική (βλ. για παράδειγμα [13]). Κάτι τέτοιο μας επιτρέπει αναπαραστάσεις και αριθμητική κλασμάτων χωρίς λάθη (error-free representations, error-free arithmetic)[4].

Φυσικά, μπορούμε να παράγουμε κώδικες όπως και στη συνήθη Θεωρία Κωδίκων. Μπορούμε να αποκτήσουμε p-αδικούς κυκλικούς κώδικες, παίρνοντας ως πολυώνυμο-γεννήτορα ένα πολυώνυμο του $\mathbb{Z}_p[x]$. Για παράδειγμα, έχουμε p-αδικούς κώδικες Golay και Hamming, με ανάλογα μήκη κωδικών λέξεων.

Επιπλέον, οι p-αδικοί αριθμοί χρησιμοποιούνται για την περιγραφή διαδικασιών πληροφορίας (information processes). Οι p-αδικοί χώροι πληροφορίας μπορούν να χρησιμοποιηθούν στην έρευνα ροών πληροφορίας για νοητικα και κοινωνικά συστήματα (cognitive and social systems). Μάλιστα, αν επιχειρήσουμε και σε αυτήν την περίπτωση μία σύγκριση με τους πραγματικούς χώρους πληροφορίας, μπορούμε να πουμε κατά τον Khrennikov[12] τα ακόλουθα:

'Το σύστημα των πραγματικών αριθμών δημιουργήθηκε ως ένα σύστημα κωδικοποίησης πληροφοριών που αντιλαμβανόμαστε από την πραγματικότητα. Τα κύρια χαρακτηριστικά του είναι η *διάταξη* του συνόλου των διανυσμάτων

[3] Μάλιστα,πάιρνουμε ένα φυσικό μοντέλο πιθανοτήτων, όπου, αντίθετα με ένα μοντέλο Kolmogorov, είναι δυνατές και αρνητικές πιθανότητες.

[4] Μάλιστα, κάτι τέτοιο βρίσκει εφαρμογές και στην επιστήμη των υπολογιστών, στο Λογισμικό και Υλικό (Software, Hardware).

πληροφορίας και η περιορισμένη δυνατότητα *συσχετίσεων*. Αντίθετα, οι p-αδικοί χώροι πληροφορίας χαρακτηρίζονται από την έλλειψη διάταξης, ενώ η p-αδική μετρική δίνει μία φυσική περιγραφή της δυνατότητας συσχετίσεων, εφόσον έχουμε ιεραρχική διάταξη των p-αδικών αριθμών.'

Εφαρμογές στη Βιολογία

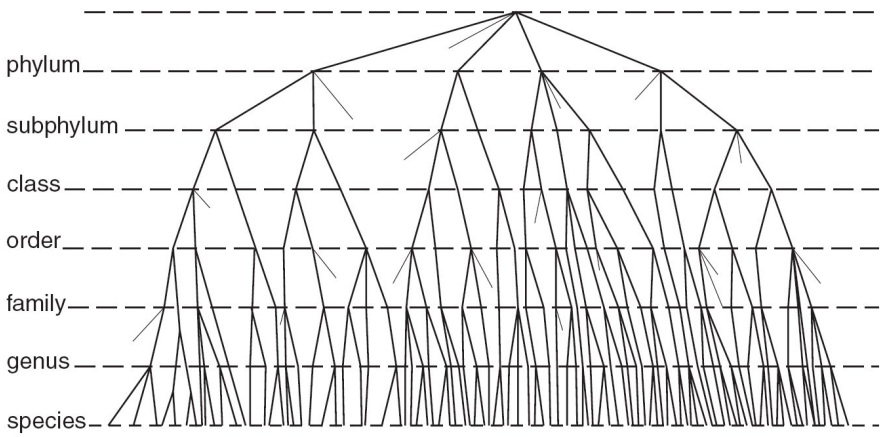
Μία πολύ ενδιαφέρουσα εφαρμογή της p-αδικής Θεωρίας Πληροφοριών στη Βιολογία είναι η κατασκευή μοντέλων για να εκφραστεί ο γενετικός κώδικας. Όλη η γενετική πληροφορία για τους ζωντανούς οργανισμούς περιέχεται στο DNA τους, μία ακολουθία νουκλεοτιδίων που χαρακτηρίζεται από την αλληλουχία τεσσάρων διαφορετικών βάσεων, της Αδενίνης (A), της Γουανίνης (G), της Κυτοσίνης (C) και της Θυμίνης (T). Τα γονίδια περιέχουν πληροφορίες για την παραγωγή αμινοξέων, των δομικών συστατικών των πρωτεϊνών. Ένα κωδικόνιο είναι μία τριπλέτα βάσεων, η οποία καθορίζει ποιο αμινοξύ θα παρασκευαστεί.

Ο γενετικός κώδικας αποτελεί μία παθολογική απεικόνιση κωδικονίων σε πρωτεΐνες. Το ζητούμενο είναι να βρεθεί ένα κατάλληλο μοντέλο που να αναπαράγει την παθολογική αυτή δομή του γενετικού κώδικα και η ιδέα είναι να χρησιμοποιηθεί ένας ουλτραμετρικός p-αδικός χώρος πληροφορίας, του οποίου τα στοιχεία θα είναι τα νουκλεοτίδια, τα κωδικόνια και τα γονίδια.

Συγκεκριμένα, στο άρθρο [5], προτείνεται ως καταλληλότερος ένας 5-αδικός χώρος πληροφορίας και αποδεικνύεται ότι *κωδικόνια που είναι p-αδικά κοντά αντιστοιχούν στο ίδιο αμινοξύ*. Δηλαδή, ότι η παθολογική δομή του γενετικού κώδικα μπορεί να συσχετιστεί με την p-αδική απόσταση μεταξύ των κωδωνίων.

Επίσης, έχουν κατασκευαστεί p-αδικά μοντέλα που περιγράφουν επιτυχώς την κινητικότητα ενός μακρομορίου πρωτεΐνης. Ο χώρος καταστάσεων των πρωτεϊνών αποδεικνύεται πως έχει ουλτραμετρική δομή, γι' αυτό και τα p-αδικά μοντέλα είναι κατάλληλα στην περίπτωση αυτή.

Γενικότερα, η ουλτραμετρικότητα είναι μία χρήσιμη μαθηματική έννοια και ένα χρήσιμο εργαλείο για την περιγραφή συστημάτων με ιεραρχική δομή. Θα κλείσουμε παρουσιάζοντας μία από τις προφανείς εφαρμογές των p-αδικών αριθμών στη Βιολογία, στον τομέα της ταξινόμησης και εξέλιξης των ειδών. Αν κοιτάξουμε το δέντρο της ταξινόμησης των ειδών (Σχήμα 5.1) βλέπουμε ότι μπορεί να οριστεί η ''απόσταση'' ανάμεσα σε δύο είδη b και c ως η διαφορά



Σχήμα 5.1: Ταξινόμηση των Ειδών

ανάμεσα στους γονότυπούς τους. Η απόσταση θα είναι μικρή αν ανήκουν στο ίδιο γένος, αλλά θα είναι μεγάλη εάν ανήκουν απλώς στην ίδια συνομοταξία. Η αναλογία με την απεικόνιση των p-αδικών αριθμών ως δέντρα είναι ξεκάθαρη, καθώς και εκεί η απόσταση ορίζεται με εντελώς ανάλογο τρόπο.

Βιβλιογραφία

[1] Σ. Αργυρός, *Σημειώσεις Παραδόσεων Πραγματικής Ανάλυσης*, Ε.Μ.Π., Αθήνα 2003.

[2] L. Cabusora, *Diophantine Sets, Primes, and the Resolution of Hilbert"s 10th Problem*, Thesis, Harvard University, April 2004.

[3] J.W.S. Cassels, *Local Fields*, Cambridge University Press, Cambridge, 1986.

[4] Capi Corrales Rodrigañez, *p-adic Numbers and Non-Archimedean Valuations*, Universidad Complutense de Madrid.

[5] B. Dragovich, A. Dragovich, *A p-adic Model of DNA Sequence and Genetic Code*, arXiv:q-bio/0607018v1 [q-bio.GN], July 2006.

[6] M. Davy, *Hilbert's 10th Problem*, www.jaworski.co.uk/m13/13_hilbert.html.

[7] John B. Fraleigh, *Εισαγωγή στην Άλγεβρα*, Πανεπιστημιακές Εκδοσεις Κρήτης, Ηράκλειο 2002.

[8] Fernando Q. Gouvêa, *p-adic numbers: an introduction*, Springer-Verlag, New York, Heidelberg, Berlin, 1993.

[9] Jan E. Holly, *Pictures of Ultrametric Spaces, the p-adic Numbers, and Valued Fields*, The Mathematical Association of America,108(October 2001) 721-728.

[10] J. Juyumaya, S. Lambropoulou, *p-adic framed Braids*, arXiv:math.GR/06004228v3, May 2006

[11] Svetlana Katok, *Real and p-adic Analysis Course Notes,* University of Pensylvania, 2001

[12] Andrei Khrennikov, *Classical and quantum mechanics on information spaces with applications to cognitive, psychological, social and anomalous phenomena*, arXiv:quant-ph/0003016v1, May 2006

[13] C.K.Koc, *A tutorial on p-adic Arithmetic*, Oregon State University, April 2002

[14] N. Koblitz, *p-adic numbers, p-adic Analysis and Zeta-Functions,* Springer-Verlag, New York, Heidelberg, Berlin, 1977

[15] Alain M. Robert, *A course in p-adic Analysis*, Springer-Verlag, New York, Heidelberg, Berlin, 2000

[16] J.-P. Serre, *A course in Arithmetic,* Springer-Verlag New York, Heidelberg, Berlin, 1973

[17] Α. Παπαϊωάννου, Χ. Κουκουβίνος, *Εισαγωγή στην Κρυπτογραφία*, Εκδόσεις Ε.Μ.Π., Αθήνα, 2005.

[18] G. Hardy, E. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1960.

[19] www.wikipedia.org