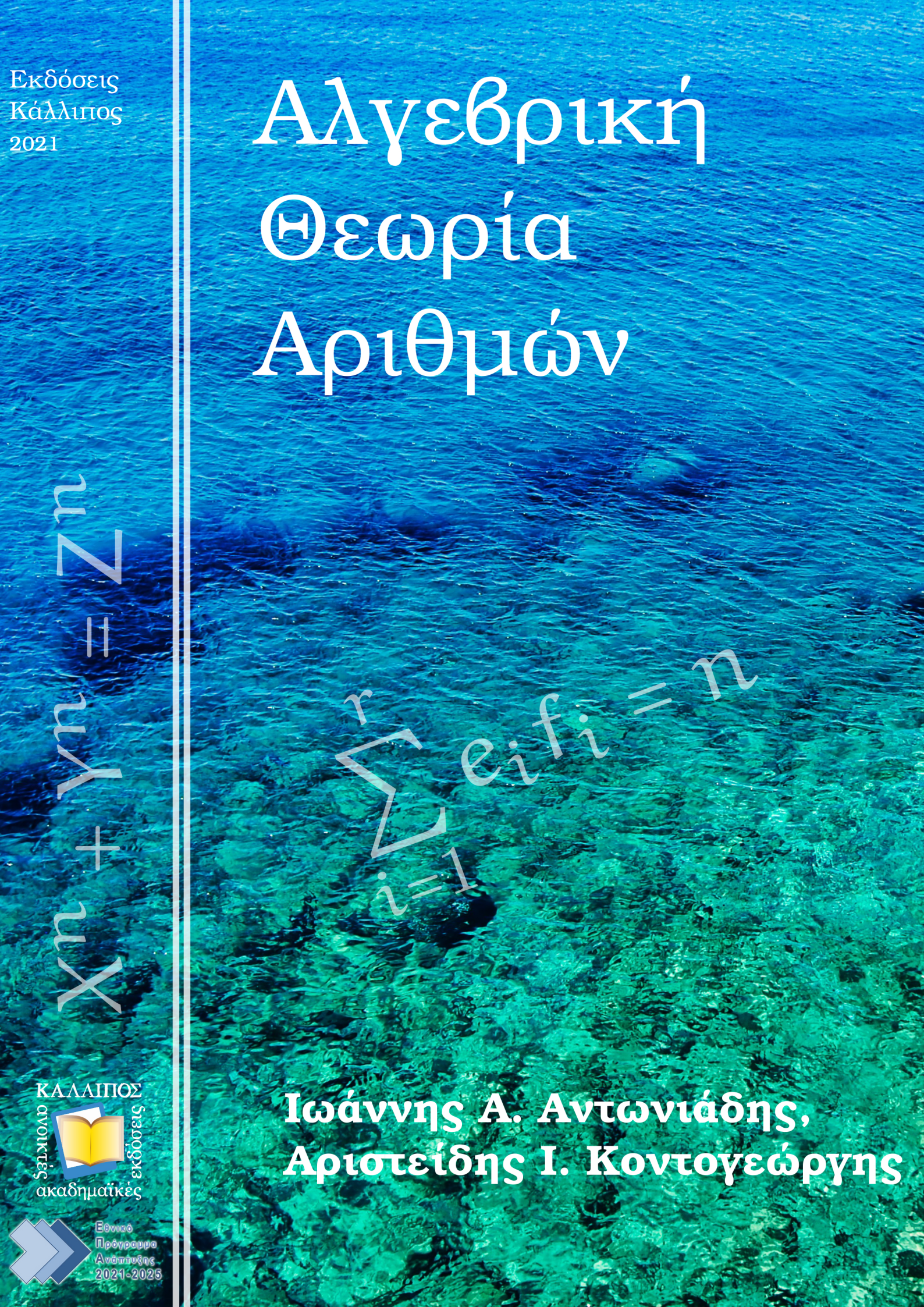
Εκδόσεις
Κάλλιπος
2021

Αλγεβρική Θεωρία Αριθμών



Ιωάννης Α. Αντωνιάδης,
Αριστείδης Ι. Κοντογεώργης

ΚΑΛΛΙΠΟΣ
ανοικτές ακαδημαϊκές εκδόσεις

Εθνικό Πρόγραμμα Ανάπτυξης 2021-2025

ΙΩΑΝΝΗΣ Α. ΑΝΤΩΝΙΑΔΗΣ

ΑΡΙΣΤΕΙΔΗΣ Ι. ΚΟΝΤΟΓΕΩΡΓΗΣ

Αλγεβρική Θεωρία Αριθμών

Αλγεβρική θεωρία Αριθμών

Συγγραφή

Ιωάννης Α. Αντωνιάδης

Αριστείδης Ι. Κοντογεώργης

Συντελεστές έκδοσης

ΓΛΩΣΣΙΚΗ ΕΠΙΜΕΛΕΙΑ: Δημήτριος Καλλιάρας

ΤΕΧΝΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ: Αριστείδης Ι. Κοντογεώργης

ISBN: 978-618-85370-4-0

΄Εκδοση 1.1 – 10 Σεπτεμβρίου 2021

ΚΑΛΛΙΠΟΣ

Εθνικό Μετσόβιο Πολυτεχνείο

Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

www.kallipos.gr

Βιβλιογραφική Αναφορά: Αντωνιάδης, Ι., Κοντογεώργης, Α. (2021). *Αλγεβρική θεωρία Αριθμών* [Προπτυχιακό εγχειρίδιο]. Αθήνα: Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. http://hdl.handle.net/11419/8007

Πνευματικά Δικαιώματα:

- Η φωτογραφία του εξωφύλλου είναι του Α. Ι. Κοντογεώργη από τη θαλάσσια περιοχή του Αγ. Μάρκου στην Τήνο.
- Τα σχεδιαγράμματα έχουν γίνει με το Sage και το Mathematica.
- Η γραμματοσειρά Kerkis είναι δημιουργία του Αντώνη Τσολομύτη από το Πανεπιστήμιο Αιγαίου.
- Το βιβλίο έχει στοιχειοθετηθεί με το LaTeX.

Αφιερώνεται στις οικογένειές μας.

Αλγεβρική Θεωρία Αριθμών

Ιωάννης Α. Αντωνιάδης, Αριστείδης Ι. Κοντογεώργης

10 Σεπτεμβρίου 2021

Περιεχόμενα

Εισαγωγή

Ο στόχος του παρόντος συγγράμματος είναι μια πρώτη (κλασική) εισαγωγή στην Αλγεβρική Θεωρία Αριθμών. Όπως θα εξηγήσουμε παρακάτω, μέρος του ανταποκρίνεται στο επίπεδο διδασκαλίας ενός προπτυχιακού μαθήματος αλλά υπάρχουν και κάποια σχετικά πιο προχωρημένα κεφάλαια. Η διάταξη της ύλης είναι:

Το πρώτο κεφάλαιο είναι εισαγωγικό και αναφέρεται στο κίνητρο ανάπτυξης που δεν είναι άλλο από την εικασία Fermat, την πιο σημαντική εικασία των Μαθηματικών, η οποία αποδείχθηκε 350 χρόνια αργότερα από τη διατύπωσή της και τον σημαντικό λόγο της δυσκολίας της που δεν είναι άλλος από το ότι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών των κυκλοτομικών σωμάτων δεν είναι εν γένει περιοχή μονοσήμαντης ανάλυσης.

Στην τρίτη παράγραφο του πρώτου κεφαλαίου διατυπώνονται όλα τα σημαντικά θεωρήματα της θεωρίας για να πάρει μια πρώτη ιδέα ο ενδιαφερόμενος αναγνώστης.

Στο δεύτερο κεφάλαιο αποδεικνύονται όλα (σχεδόν) τα θεωρήματα που έχουν περιγραφεί στο πρώτο κεφάλαιο στην πιο απλή, μη-τετριμμένη, περίπτωση αυτή των τετραγωνικών σωμάτων αριθμών. Ο στόχος είναι ο ενδιαφερόμενος αναγνώστης να αποκτήσει μια πρώτη εμπειρία των ιδεών και των αποδείξεων που πρόκειται να ακολουθήσουν στα επόμενα κεφάλαια. Ο νόμος ανάλυσης περιγράφεται μόνο για δακτύλιους που είναι περιοχές μονοσήμαντης ανάλυσης και υποβάλλει την ιδέα της αντιστοιχίας του νόμου ανάλυσης ιδεωδών.

Στην προσπάθειά του ο Kummer να αποδείξει την εικασία Fermat, θεώρησε ότι όλοι οι δακτύλιοι $\mathbb{Z}[\zeta_p]$των ακεραίων αλγεβρικών των κυκλοτομικών σωμάτων $K = \mathbb{Q}(\zeta_p)$, όπου p πρώτος $\zeta_p = e^{2\pi i/p}$ είναι περιοχές μονοσήμαντης ανάλυσης και «απέδειξε» την εικασία. Του υποδείχθηκε ότι αυτό δεν ισχύει πάντοτε και ότι μάλιστα ο πιο μικρός πρώτος που δεν ισχύει είναι ο $p = 23$. Ο «παράδεισος» των περιοχών μονοσήμαντης ανάλυσης χάθηκε!

Στη συνέχεια ο «παράδεισος» των περιοχών ανακαλύφθηκε ξανά στην έννοια της περιοχής Dedekind, όπου έχουμε μονοσήμαντη ανάλυση ιδεωδών πλέον σε γινόμενο πρώτων ιδεωδών.

Η απόδειξη ότι όλοι οι δακτύλιοι ακεραίων αλγεβρικών σωμάτων αριθμών είναι δακτύλιοι Dedekind είναι το κύριο αποτέλεσμα του τρίτου κεφαλαίου.

Στο τέταρτο κεφάλαιο μελετώνται βασικές έννοιες της θεωρίας, όπως norm και ίχνος ενός στοιχείου, βάση ακεραιότητας και διακρίνουσα ενός αλγεβρικού σώματος αριθμών. Επίσης, αποδεικνύεται το θεμελιώδες θεώρημα πεπερασμένα παραγόμενων αβελιανών ομάδων, το οποίο είναι ιδιαίτερα χρήσιμο. Αναλυτικά μελετάται και το αλγοριθμικό πρόβλημα υπολογισμού μιας βάσης ακεραιότητας και της διακρίνουσας του σώματος.

Στο πέμπτο κεφάλαιο ορίζεται η έννοια της norm ενός ιδεώδους κατά τρόπο συμβατό προς την έννοια της norm ενός στοιχείου και μελετώνται οι ιδιότητες αυτής. Στη συνέχεια ορίζονται τα κλασματικά ιδεώδη και η ομάδα κλάσεων ιδεωδών. Αποδεικνύεται ότι η τάξη της ομάδας αυτής είναι πεπερασμένη. Πρόκειται για έναν φυσικό αριθμό ο οποίος μας δείχνει πόσο απέ-

χει ο δακτύλιος των ακεραίων αλγεβρικών από το να είναι περιοχή μονοσήμαντης ανάλυσης. Ακολουθεί υπολογισμός παραδειγμάτων για την καλύτερη κατανόηση της ύλης. Τέλος, επιλύεται και η διοφαντική εξίσωση η οποία είχε επιλυθεί εσκεμμένα λάθος στο πρώτο κεφάλαιο για να μας υποδείξει το λάθος στο οποίο είχε υποπέσει ο Kummer και πώς κατάφερε τελικά να επανορθώσει.

Αν L/K επέκταση αλγεβρικών σωμάτων αριθμών και P ένα πρώτο ιδεώδες του δακτυλίου των ακεραίων αλγεβρικών R_K του σώματος K, τότε το ερώτημα είναι πώς αναλύεται το ιδεώδες PR_L, του σώματος L σε γινόμενο πρώτων ιδεωδών. Πόσα είναι τα πρώτα ιδεώδη και ποιοι οι εκθέτες τους, καθώς και ποιοι είναι οι γεννήτορες των πρώτων ιδεωδών που εμφανίζονται στην ανάλυση;

Ο νόμος ανάλυσης, θέμα του έκτου κεφαλαίου, απαντά στα παραπάνω ερωτήματα. Η μορφή είναι απλούστερη όταν η επέκταση είναι επέκταση Galois. Τέλος, υπολογίζονται οι νόμοι ανάλυσης διαφόρων συγκεκριμένων κλάσεων αλγεβρικών σωμάτων αριθμών.

Στο έβδομο κεφάλαιο, στην ειδική περίπτωση που η επέκταση L/K αλγεβρικών σωμάτων αριθμών είναι επέκταση Galois, ο Hilbert ανέπτυξε μια θεωρία η οποία αποτελεί πανέμορφη σύζευξη με τον νόμο ανάλυσης. Μας περιγράφει αναλυτικά όχι μόνο την ανάλυση των πρώτων ιδεωδών του K στο L, αλλά και τι γίνεται στα ενδιάμεσα σώματα της επέκτασης αυτής.

Στο όγδοο κεφάλαιο ασχολούμαστε με τους νόμους αντιστροφής. Πέρα από τις διοφαντικές εξισώσεις, ένα άλλο εξαιρετικά σημαντικό πρόβλημα είναι αυτό της εύρεσης ενός γενικού νόμου αντιστροφής. Αποτέλεσε τον δεύτερο πυλώνα ως κινητήρια δύναμη της ραγδαίας εξέλιξης της θεωρίας αριθμών. Κλασικό παράδειγμα αποτελεί ο τετραγωνικός νόμος αντιστροφής του Gauss. Εδώ το πρόβλημα είναι σε μια επέκταση αλγεβρικών σωμάτων αριθμών L/K ο χαρακτηρισμός του συνόλου $P(L/K)$ των πρώτων ιδεωδών του K τα οποία αναλύονται πλήρως στο L σε γινόμενο διακεκριμένων πρώτων παραγόντων μέσω εννοιών αποκλειστικά του σώματος K.

Κατά εντελώς όμοιο τρόπο όπως στη θεωρία των μιγαδικών συναρτήσεων, σύμφωνα με το θεώρημα του Cauchy, μια συνάρτηση καθορίζεται πλήρως από τις τιμές της στο «σύνορο» όπως έλεγε και ο L. Kronecker.

Αν παραδείγματος χάρη $K = \mathbb{Q}$ και $L = \mathbb{Q}(\zeta_n)$ τότε το

$$P(L/K) = \{p \text{ πρώτος αριθμός} : p \equiv 1 \mod n\}.$$

Αν πάλι K αλγεβρικό σώμα και H_K το σώμα Hilbert αυτού, έννοια η οποία θα αναλυθεί στο μάθημα, τότε το σύνολο

$$P(H_K/K) = \{P \text{ πρώτα ιδεώδη του } K : P \text{ κύριο ιδεώδες}\}.$$

Για αβελιανές επεκτάσεις L/K του K ισχύει ο νόμος αντιστροφής του Artin, τον οποίο και θα μελετήσουμε. Για μη-αβελιανές επεκτάσεις L/K ένας γενικός χαρακτηρισμός του συνόλου $P(L/K)$ δεν είναι μέχρι σήμερα γνωστός. Το πρόβλημα αποτελεί μέρος ενός προγράμματος που προχωράει πολύ σε βάθος. Τρέχει με το όνομα «Φιλοσοφία του Langlands» και εξελίσσεται τα τελευταία χρόνια με σφοδρή ταχύτητα.

Το ένατο κεφάλαιο αποτελεί μια εισαγωγή στη Γεωμετρία των Αριθμών. Αποδεικνύονται το σημαντικό θεώρημα του Minkowski, το οποίο αφορά την ύπαρξη σημείου με ακέραιες συντεταγμένες σε κατάλληλο χωρίο του $\mathbb{R}^n$ και οι σημαντικότατες εφαρμογές του. Επίσης, αποδεικνύεται το θεώρημα του Dirichlet το οποίο μας εξασφαλίζει τη δομή της ομάδας των μονάδων του δακτυλίου των ακεραίων αλγεβρικών αριθμών R_K ως πεπερασμένα παραγόμενης αβελιανής ομάδας συγκεκριμένου βαθμού.

Το δέκατο κεφάλαιο περιέχει το θεώρημα της διακρίνουσας, το οποίο χαρακτηρίζει όλα τα πρώτα ιδεώδη του αλγεβρικού σώματος αριθμών τα οποία διακλαδίζονται στην επέκταση L/K. Αποδεικνύονται το θεώρημα της διαφορίζουσας, το οποίο χαρακτηρίζει όλα τα πρώτα ιδεώδη του L τα οποία διακλαδίζονται στην ανάλυση ενός πρώτου ιδεώδους του K και, τέλος, το θεώρημα των Kronecker-Weber, ότι κάθε αβελιανή επέκταση του $\mathbb{Q}$ περιέχεται σε ένα κυκλοτομικό σώμα αριθμών.

Στο ενδέκατο κεφάλαιο περιέχονται τα αποτελέσματα της θεωρίας σχετικά με την εικασία Fermat μέσω της χρήσης Αλγεβρικής Θεωρίας Αριθμών και μέχρι τα μέσα της δεκαετίας του 1980 όταν η προσέγγιση του προβλήματος άλλαξε ριζικά.

Η εικασία χωρίζεται σε δύο περιπτώσεις. Στην πρώτη υποθέτουμε ότι υπάρχει μη-τετριμμένη λύση (x, y, z) της

$$X^p + Y^p = Z^p, p \text{ πρώτος }, p \neq 2 \text{ και } p \nmid xyz$$

ενώ στη δεύτερη περίπτωση υποθέτουμε ότι ο πρώτος p διαιρεί ακριβώς ένα από τα x, y, z.

Το δωδέκατο κεφάλαιο, ξεφεύγει αρκετά από τα προηγούμενα και έχει κυρίως περιγραφικό χαρακτήρα. Στα μέσα της δεκαετίας του 1980 το πρόβλημα της απόδειξης της εικασίας Fermat μεταφέρθηκε σε μια άλλη περιοχή της θεωρίας Αριθμών, τη λεγόμενη περιοχή της θεωρίας των ελλειπτικών καμπυλών. Η φιλοσοφία είναι ότι αν η εξίσωση Fermat έχει μη-τετριμμένη λύση (x, y, z), τότε η ελλειπτική καμπύλη που ορίζεται από αυτή τη λύση έχει τόσο όμορφες ιδιότητες που ουσιαστικά δεν υπάρχει.

Για να επιτευχθεί αυτό χρειάστηκαν και η θεωρία των modular συναρτήσεων, αναλυτικό κομμάτι της θεωρίας αριθμών, καθώς και οι p-αδικοί αριθμοί που αποτελούν την πλήρωση του $\mathbb{Q}$ ως προς την p-αδική εκτίμηση.

Το δέκατο τρίτο κεφάλαιο αποτελεί παράρτημα και περιέχει την επισκόπηση βασικών εννοιών της αντιμεταθετικής θεωρίας δακτυλίων, αυτής των modules καθώς και την έννοια της απόλυτης τιμής και εκτίμησης σε ένα αλγεβρικό σώμα αριθμών, άπειρες επεκτάσεις Galois, τοπολογία Krull και προβολικά όρια.

Προαπαιτούμενες γνώσεις για την κατανόηση του περιεχομένου του παρόντος, πέρα από το περιεχόμενο των παραγράφων 1 και 2 του παραρτήματος, είναι η γραμμική άλγεβρα, η στοιχειώδης θεωρία αριθμών και βασικές γνώσεις ενός προπτυχιακού μαθήματος της θεωρίας Galois.

Προαπαιτούμενο για τη μελέτη και κατανόηση του δωδέκατου κεφαλαίου αποτελεί η παράγραφος 3 του παραρτήματος.

Βασική ύλη περιεχομένου διδασκαλίας ενός προπτυχιακού εξαμηνιαίου μαθήματος αποτελούν τα πρώτα έξι κεφάλαια. Επηρεασμένοι από την παρατήρηση των A. Fröhlich και M. Taylor [1], ότι "many number theorists have never acquired sufficient technique to perform number theoretic calculations in anything but a quadratic field", προσθέσαμε και αρκετά υπολογιστικά παραδείγματα.

Τα υπόλοιπα πέντε κεφάλαια μπορούν να αποτελέσουν το περιεχόμενο διδασκαλίας ενός δεύτερου εξαμήνου ή ενός σεμιναρίου. Τέλος, το δωδέκατο κεφάλαιο μπορεί να αποτελέσει το έναυσμα για ένα προχωρημένο σεμινάριο στην περιοχή.

[1] Fröhlich, A. and Taylor, M. J., *Algebraic number theory*. Cambridge Studies in Advanced Mathematics, 1993.

I

Εισαγωγικά

I.1 Διοφαντικές εξισώσεις

Ένα από τα πιο σημαντικά θέματα με τα οποία ασχολείται η Θεωρία Αριθμών είναι η επίλυση διοφαντικών εξισώσεων.

Μια διοφαντική εξίσωση είναι μια εξίσωση της μορφής

$$f(x_1, x_2, \ldots, x_n) = 0$$

όπου το $f(x_1, x_2, \ldots, x_n)$ είναι ένα πολυώνυμο n μεταβλητών με συντελεστές ακεραίους αριθμούς και n ένας φυσικός αριθμός $n \geq 2$. Επίλυση μιας διοφαντικής εξίσωσης είναι η εύρεση όλων των n-άδων ακεραίων αριθμών $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ οι οποίες επαληθεύουν την εξίσωση.

Η ονομασία των εξισώσεων αυτών ως διοφαντικών έχει δοθεί προς τιμήν του Διόφαντου του Αλεξανδρινού (3ος μ.Χ. αιώνας) ο οποίος θεωρείται ο πατέρας της Άλγεβρας. Το βιβλίο του «Αριθμητικά» δημοσιεύτηκε από τον Bachet στα 1621 στο ελληνικό πρωτότυπο, μαζί με λατινική μετάφραση και εκτεταμένα σχόλια. Ένα αντίτυπο αυτού προμηθεύτηκε ο Fermat και έτσι η Θεωρία Αριθμών ξαναγεννήθηκε.

Οι γραμμικές διοφαντικές εξισώσεις αποτελούν αντικείμενο μελέτης στο μάθημα της στοιχειώδους θεωρίας αριθμών, για παράδειγμα [7, σελ. 55-61].

Ιδιαίτερα σημαντική είναι η δομή των ακεραίων αριθμών. Αποτελούν περιοχή μονοσήμαντης ανάλυσης (ΠΜΑ). Άμεση συνέπεια της ιδιότητας αυτής είναι και το ακόλουθο:

Πόρισμα I.1.1. *Αν a, b, c θετικοί ακέραιοι με $(b, c) = 1$ και $a^n = bc$ για κάποιο φυσικό αριθμό $n > 1$, τότε υπάρχουν ακέραιοι a_1, a_2 πρώτοι μεταξύ τους ώστε $a = a_1 a_2$ και $b = a_1^n, c = a_2^n$, βλέπε [7, p. 1.7.6].*

Παράδειγμα I.1.2. Να λυθεί η διοφαντική εξίσωση

$$y^3 = x^2 - 16.$$

Η εξίσωση γράφεται ως

$$y^3 = (x - 4)(x + 4).$$

Έστω $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ κάποια λύση αυτής και $d = (x - 4, x + 4)$. Αν ο x είναι περιττός, τότε $d = 1$ οπότε $x - 4 = a^3, x + 4 = b^3$ με $a, b \in \mathbb{Z}$ περιττούς και $(a, b) = 1$. Επομένως $b^3 - a^3 = 8$, το οποίο είναι αδύνατο.

Αν ο x είναι άρτιος, τότε και ο y είναι άρτιος, συνεπώς $8 \mid x^2$ οπότε $4 \mid x$. Ας γράψουμε το $x = 4x_1$, $x_1 \in \mathbb{Z}$. Η εξίσωση γίνεται $16x_1^2 - 16 = y^3$, άρα $4 \mid y$, δηλαδή $y = 4y_1$, $y_1 \in \mathbb{Z}$.

Από τα παραπάνω, προκύπτει ότι

$$x_1^2 = 4y_1^3 + 1, \qquad x_1 \text{ περιττός}$$

Το $x_1 = 2m+1$ για $m \in \mathbb{Z}$. Συνεπώς $m^2+m = y_1^3$, δηλαδή $m(m+1) = y_1^3$ και $(m, m+1) = 1$. Επομένως, $m = t^3, m+1 = s^3$, $t, s \in \mathbb{Z}$ και $(t, s) = 1$. Αλλά οι μόνοι διαδοχικοί κύβοι ακεραίων ανήκουν στο σύνολο $\{-1, 0, 1\}$. Αυτό σημαίνει ότι ο m ή ο $m+1$ είναι ίσος με μηδέν, δηλαδή $y_1 = 0$ οπότε και $y = 0$. Τελικά η μοναδική λύση της εξίσωσης είναι η $(x, y) = (\pm 4, 0)$.

Παράδειγμα Ι.1.3 (Πυθαγόρειες τριάδες)**.** Να λυθεί η διοφαντική εξίσωση

$$X^2 + Y^2 = Z^2 \tag{Ι.1}$$

στο σύνολο των θετικών ακεραίων. Είναι φανερό ότι μια τέτοια λύση είναι η $(3, 4, 5)$.

Ορισμός Ι.1.4. Τριάδες θετικών ακεραίων (x, y, z) οι οποίες επαληθεύουν την (Ι.1) θα λέγονται *πυθαγόρειες τριάδες*.

Αν (x, y, z) πυθαγόρεια τριάδα και $d \in \mathbb{Z}$, τότε και η (dx, dy, dz) είναι επίσης πυθαγόρεια τριάδα, αφού $(dx)^2 + (dy)^2 = (dz)^2$. Επομένως και οι τριάδες $(6, 8, 10)\,(9, 12, 15), \ldots$ είναι επίσης πυθαγόρειες.

Αν γνωρίζουμε όλες τις πυθαγόρειες τριάδες (a, b, c) για τις οποίες $(a, b, c) = 1$, τότε γνωρίζουμε και *όλες* τις λύσεις της (Ι.1).

Ορισμός Ι.1.5. Μία πυθαγόρεια τριάδα (a, b, c) θα λέγεται *πρωταρχική* ή *πρωτογενής* (primitive) όταν

$$(a, b, c) = 1$$

Η $(3, 4, 5)$ λοιπόν είναι πρωταρχική. Υπάρχουν και άλλες; Η απάντηση είναι «ναι». Οι πυθαγόρειες τριάδες $(5, 12, 13), (8, 5, 17), (7, 24, 25), (9, 40, 41)$ είναι πρωταρχικές.

Αν (x, y, z) πρωταρχική πυθαγόρεια τριάδα, τότε ένας ακριβώς από τους x, y θα είναι άρτιος και ο άλλος περιττός.

Πράγματι, αν x και y άρτιοι, τότε και z άρτιος, οπότε $(x, y, z) \geq 2$, άτοπο.

Αν πάλι x και y περιττοί, τότε $x^2 = 1 + 4l$, $l \in \mathbb{Z}$ και $y^2 = 1 + 4m$, $m \in \mathbb{Z}$, οπότε $z^2 = x^2 + y^2 = 2 + 4t$ με $t \in \mathbb{Z}$. Αυτό όμως είναι αδύνατο, αφού το τετράγωνο ακεραίου είναι πάντοτε της μορφής $4l$ ή $4l + 1$, $l \in \mathbb{Z}$.

Απάντηση στο πρόβλημα της εύρεσης όλων των πρωταρχικών πυθαγορείων τριάδων μας δίνει η ακόλουθη:

Πρόταση Ι.1.6. *Οι θετικοί ακέραιοι x, y, z αποτελούν πρωταρχική πυθαγόρεια τριάδα με y άρτιο ακριβώς τότε όταν υπάρχουν θετικοί ακέραιοι r, s με $r > s$, $(r, s) = 1$ ένας εκ των οποίων είναι άρτιος και ο άλλος περιττός (ετερότυποι), τέτοιοι ώστε*

$$(x = r^2 - s^2,\ y = 2rs,\ z = r^2 + s^2)$$

Απόδειξη. Αφού y άρτιος, τα x και z θα είναι περιττοί. Επομένως $z + x$ και $z - x$ θα είναι άρτιοι. Αν ονομάσουμε $k := \frac{z+x}{2} \in \mathbb{Z}$ και $l := \frac{z-x}{2} \in \mathbb{Z}$ έχουμε

$$k \cdot l = \frac{(z+x)(z-x)}{4} = \frac{z^2 - x^2}{4} = \frac{y^2}{4} = \left(\frac{y}{2}\right)^2.$$

Ο $(k, l) = 1$, διότι αν $d := (k, l) > 1$ θα είχαμε $d|k = \frac{z+x}{2}$ και $d|l = \frac{z-x}{2}$, δηλαδή $d|(k + l) = z$ και $d|(k - l) = x$, οπότε $(x, z) \geq d > 1$, άτοπο.

Επομένως, από το πόρισμα Ι.1.1 προκύπτει ότι $k = r^2$, $l = s^2$ και $(r, s) = 1$, (αφού $(k, l) = 1$). Συνεπώς $x = r^2 - s^2$, $y = 2rs$ και $z = r^2 + s^2$.

Τέλος, ο ένας από τους r και s είναι άρτιος και άλλος περιττός. Αυτό ισχύει, διότι δεν είναι δυνατό να είναι και οι δύο άρτιοι, αφού $(r, s) = 1$, αλλά ούτε και οι δύο περιττοί, αφού τότε οι x, y, z θα ήταν άρτιοι και η πυθαγόρεια τριάδα *δεν* θα ήταν πρωταρχική.

Αντίστροφα, υποθέτουμε ότι τα x, y, z έχουν τη σωστή μορφή και θα αποδείξουμε ότι αποτελούν πρωταρχική πυθαγόρεια τριάδα.

Πρώτα απ' όλα είναι φανερό ότι $x^2 + y^2 = z^2$, δηλαδή ότι (x, y, z) πυθαγόρεια τριάδα.

Αν $d := (x, y, z) > 1$ και $p \in \mathbb{P}$ τέτοιος ώστε $p|d$, τότε $p|x$, $p|y$ και $p|z$. Το $p \neq 2$, διότι x περιττός.

Από $p|x$ και $p|z$, έπεται ότι $p|(z + x)$ και $p|(z - x)$ δηλαδή $p|2r^2$ και $p|2s^2$, οπότε $p|(2r^2, 2s^2) = 2(r, s)^2 = 2$, άτοπο.

Συνεπώς η τριάδα (x, y, z) είναι πρωταρχική πυθαγόρεια τριάδα. □

Παράδειγμα I.1.7. Να λυθεί η διοφαντική εξίσωση

$$Y^3 = X^2 + 1. \tag{I.2}$$

Παρατηρούμε ότι εδώ το δεξιό μέλος δεν παραγοντοποιείται στο $\mathbb{Z}$. Αν υποθέσουμε ότι $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ λύση της παραπάνω εξίσωσης και μπορούμε να παραγοντοποιήσουμε το δεξιό μέλος

$$y^3 = (x + i)(x - i), \qquad x \in \mathbb{Z}.$$

Η παραγοντοποίηση έλαβε χώρα στον δακτύλιο του Gauss

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

και επομένως μας ενδιαφέρει η αριθμητική του δακτυλίου αυτού. Δείτε και στο παράρτημα την παράγραφο XIII.5.

Η παραπάνω εξίσωση (I.2) αποτελεί ειδική περίπτωση για $\kappa = 1$, της γενικής εξίσωσης του Mordell,

$$y^2 = x^2 + \kappa, \qquad \kappa \in \mathbb{Z}.$$

Έστω $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ μια λύση της εξίσωσης (I.2). Παραγοντοποίηση του δεξιού μέλους δίνει

$$y^3 = (x + i)(x - i),$$

όπου $x + i, x - i \in \mathbb{Z}[i]$ και

$$R = \mathbb{Z}[i] = \{a + bi : (a, b) \in \mathbb{Z} \times \mathbb{Z}\}$$

είναι, όπως θα δούμε αργότερα, ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του σώματος του

$$\mathbb{Q}(i) = \{a + bi : (a, b) \in \mathbb{Q} \times \mathbb{Q}\}.$$

Αν $\xi = a + bi \in \mathbb{Z}[i]$, η norm του ξ ορίζεται ως

$$N(\xi) = (a + ib)(a - bi) = a^2 + b^2 \in \mathbb{N}.$$

Η ομάδα των μονάδων του $\mathbb{Z}[i]$ είναι η

$$E(\mathbb{Z}[i]) = \{\xi \in \mathbb{Z}[i] : N(\xi) = \pm 1\} = \{\pm 1, \pm i\} = \langle i \rangle.$$

Με βάση την παραπάνω norm, ο $\mathbb{Z}[i]$ είναι ευκλείδειος δακτύλιος και συνεπώς δακτύλιος κυρίων ιδεωδών και επομένως δακτύλιος μονοσήμαντης αναλύσης.

Παρατηρούμε ότι $2 = (-i)(1 + i)^2$, όπου $-i \in E(\mathbb{Z}[i])$ και $\pi := 1 + i$ ανάγωγο στοιχείο του $\mathbb{Z}[i]$. Έστω $d = (x + i, x - i)$, $d \mid 2$. Ισχυριζόμαστε ότι $d \cong 1$. Πράγματι αν $d \not\cong 1$, τότε $1 + i \mid d$ και συνεπώς $1 + i \mid x + i$ άρα $N(1 + i) \mid N(x + i)$. Καταλήγουμε λοιπόν στο συμπέρασμα ότι $2 \mid x^2 + 1 = y^3$ άρα $2 \mid y$. Τότε $2^3 \mid y^3$ άρα $8 \mid x^2 + 1$ και $x^2 \equiv -1 \mod 8$, το οποίο είναι άτοπο.

Ώστε $d \cong 1$ οπότε η $y^3 = (x + i)(x - i)$ λόγω της μονοσημάντης αναλύσης δίνει $x + i \cong \xi^3$ και $\xi \in \mathbb{Z}[i]$, δηλαδή $x + i = \epsilon\xi^3$, όπου $\epsilon \in E(\mathbb{Z}[i])$. Αφού $E(\mathbb{Z}[i]) = \langle i \rangle$ κυκλική ομάδα τάξεως 4, έπεται ότι η συνάρτηση $\epsilon \mapsto \epsilon^3$ είναι αυτομορφισμός της ομάδας των μονάδων $E(\mathbb{Z}[i])$. Μπορούμε να αντικαταστήσουμε το ϵ με το ϵ^3 και να πάρουμε $x + i = \eta^3$ με $\eta = a + ib \in \mathbb{Z}[i]$.

Καταλήγουμε στη σχέση

$$x + i = (a^3 - 3ab^2) + i(3a^2b - b^3),$$

οπότε $1 = b(3a^2 - b^2)$ συνεπώς το $b \mid 1$, άρα $b = \pm 1$. Έχουμε $3a^2 - 1 = \pm 1$ και $a = 0$ είναι η μόνη λύση στο $\mathbb{Z}$. Τότε $x = a^3 - 3ab^2 = 0$ το οποίο δίνει $y = 1$.

Ώστε το σύνολο λύσεων της (I.2) είναι το $(x, y) = (0, 1)$.

Παρατήρηση Ι.1.8. Αποφασιστικά για την απόδειξη είναι

1. Το $\mathbb{Z}[i]$ είναι δακτύλιος μονοσήμαντης ανάλυσης
2. Η γνώση της δομής της ομάδας των μονάδων $E(\mathbb{Z}[i])$.

Παράδειγμα Ι.1.9. Ζητούνται οι ακέραιες λύσεις της εξίσωσης

$$2y^3 = x^2 + 5 \tag{I.3}$$

Και εδώ το δεξιό μέλος δεν παραγοντοποιείται στο $\mathbb{Z}$. Μπορούμε όμως να το παραγοντοποιήσουμε στον δακτύλιο

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in Z\}.$$

Πράγματι, αν $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ λύση της εξίσωσης, τότε

$$2y^3 = (x + \sqrt{-5})(x - \sqrt{-5}).$$

Σε αυτή την περίπτωση θα πρέπει να εργαστούμε στο σύνολο

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\},$$

το οποίο και πάλι αποτελεί ακέραια περιοχή. Η ομάδα των μονάδων του δακτυλίου $\mathbb{Z}[\sqrt{-5}]$ είναι $E(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}$. Το 2 είναι ανάγωγο στοιχείο του $\mathbb{Z}[\sqrt{-5}]$. Πράγματι, αν $2 = a \cdot b$ με $a, b \in \mathbb{Z}[\sqrt{-5}]$ όχι μονάδες, τότε $N(a)N(b) = 4$, οπότε $N(a) = N(b) = \pm 2$. Αυτό όμως είναι αδύνατο αφού αν

$$a = \kappa + \lambda\sqrt{-5},\ \kappa, \lambda \in \mathbb{Z}, N(a) = \kappa^2 + 5\lambda^2 \neq \pm 2.$$

«Επομένως»

$$2 \mid (x + \sqrt{-5}) \text{ είτε } 2 \mid (x - \sqrt{-5})$$

που σημαίνει ότι ή

$$\frac{x + \sqrt{-5}}{2} = \frac{x}{2} + \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

ή

$$\frac{x - \sqrt{-5}}{2} = \frac{x}{2} - \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}],$$

το οποίο είναι άτοπο, αφού $\frac{1}{2} \notin \mathbb{Z}$.

Καταλήξαμε στο συμπέρασμα ότι η διοφαντική εξίσωση

$$2Y^3 = X^2 + 5$$

δεν έχει ακέραια λύση.

Και «όμως κινείται» που θα έλεγε και ο Γαλιλαίος! Η εξίσωση έχει τουλάχιστον μία λύση, την $(x, y) = (\pm 7, 3)$. Πού είναι το λάθος;

Απάντηση: Το 2 είναι *ανάγωγο στοιχείο* του $\mathbb{Z}[\sqrt{-5}]$ αλλά *όχι πρώτο* στοιχείο αυτού. Αυτό σε αντίθεση προς την περιοχή του Gauss.

Γιατί συμβαίνει αυτό;

Απάντηση: Η περιοχή $\mathbb{Z}[\sqrt{-5}]$ δεν είναι *περιοχή μονοσήμαντης ανάλυσης*. Αποτελεί εύκολη άσκηση η απόδειξη ότι ο

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

έχει δύο διαφορετικές μεταξύ τους γνήσιες αναλύσεις σε γινόμενα αναγώγων στοιχείων του $\mathbb{Z}[\sqrt{-5}]$.

I.2 Η εικασία Fermat

Αποφασιστικής σημασίας για την ανάπτυξη της αλγεβρικής θεωρίας αριθμών υπήρξε η εικασία του Fermat.

Ο Fermat μελέτησε συστηματικά το έργο του Διόφαντου. Δίπλα στο περιθώριο του προβλήματος 8, Βιβλίο II των Αριθμητικών του Διοφάντου, το οποίο αναφέρεται στις πυθαγόρειες τριάδες:

«Τόν ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους»

«Να αναλύσετε δοθέν τέλειο τετράγωνο σε (άθροισμα) δύο τέλειων τετραγώνων»

Ο Fermat συμπλήρωσε, στα Λατινικά, τα ακόλουθα:

" Cubum in duos cubos aut quadro-quadratum in duos quadro-quadratos et generaliter nullam in infinitum, ultra quadratum, potestam in duas ejusdem nominis fas est dividere. Cujus rei demonstrationem mirabilem sone detexi, hanc marginis exiguitas non caperet."

« Δεν είναι δυνατόν να αναλύσουμε έναν κύβο σε άθροισμα δύο κύβων, ούτε μια τέταρτη δύναμη σε (άθροισμα) δύο τετάρτων δυνάμεων και γενικά μια δύναμη μεγαλύτερη του δύο σε άθροισμα δύο δυνάμεων με τον ίδιο εκθέτη. Έχω ανακαλύψει μια καταπληκτική απόδειξη αυτού, αλλά το περιθώριο (του βιβλίου) είναι πολύ μικρό για να τη χωρέσει. »

Οι σημειώσεις του Fermat στο αντίτυπο των Αριθμητικών δημοσιεύτηκαν για πρώτη φορά από τον γιο του Samuel Fermat στα 1670. Σε Γερμανική μετάφραση έχουν δημοσιευθεί στο Pierre de Fermat, *Bemerkungen zu Diophant*, μετάφραση από τα Λατινικά του Max Miller, Akademische Verlagsgesellschaft, Leipzig 1932.

Η μαθηματική έκφραση της εικασίας είναι η εξής: Η διοφαντική εξίσωση

$$X^n + Y^n = Z^n,\ n \in \mathbb{N}, n \geq 3$$

δεν έχει, μη-τετριμμένη, δηλαδή για $xyz \neq 0$, ακέραια λύση. Δεν υπάρχει επομένως τριάδα ακεραίων $(x, y, z) \in \mathbb{Z}^3$ με $xyz \neq 0$, τέτοια ώστε

$$x^n + y^n = z^n,$$

για οποιοδήποτε εκθέτη $n \geq 3$. Δεν είναι μέχρι σήμερα γνωστό αν πράγματι ο Fermat έχει αποδείξει την εικασία του. Η πρώτη γνωστή πλήρης απόδειξη τελειώνει με την εργασία του A. Wiles [6] και το απαραίτητο συμπλήρωμα των R. Taylor, A. Wiles [5], 350 χρόνια αργότερα. θα συνιστούσαμε ως εισαγωγή τη μελέτη του βιβλίου του Simon Singh [4].

Αλλά ας πάρουμε τα πράγματα με τη σειρά. Εύκολα αποδεικνύεται ότι αρκεί να ελέγξουμε την ισχύ της εικασίας για $n = 4$ και για κάθε περιττό πρώτο αριθμό p. Για $n = 4$ ο Fermat απέδειξε με τη μέθοδο της καθόδου ότι η διοφαντική εξίσωση

$$x^4 + y^4 = z^2$$

δεν έχει θετικές ακέραιες λύσεις. Άμεση συνέπεια της πρότασης αυτής είναι η αλήθεια της εικασίας Fermat για $n = 4$, [7, προτ. 2.3.3].

Έναν αιώνα αργότερα, ο Euler χρησιμοποίησε την αριθμητική του δακτυλίου

$$\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\},$$

όπου ω μια πρωταρχική 3-ρίζα της μονάδας και απέδειξε την εικασία για $n = 3$.

Ακολούθησαν οι αποδείξεις των Dirichlet (1825) για $n = 5$ καθώς και του Lamé (1839) για $n = 7$. Η δυσκολία των αποδείξεων έδειξε ότι είναι αδύνατο να συνεχίσει κανείς κατ' αυτόν τον τρόπο.

Έστω τώρα p πρώτος $p > 3$. Η εξίσωση Fermat είναι

$$X^p + Y^p = Z^p.$$

Αν ζ_p είναι η p-οστή πρωταρχική ρίζα της μονάδας, $\zeta_p := e^{\frac{2\pi i}{p}}$, τότε, επειδή όλες οι ρίζες της εξίσωσης $t^p - 1$ είναι οι ζ_p^i, $i = 0, 1, \dots, p-1$, έπεται ότι

$$t^p - 1 = (t-1)(t-\zeta_p)(t-\zeta_p^2)\cdots(t-\zeta_p^{p-1})$$

και αν θέσουμε στη θέση του t το $-X/Y$ έχουμε

$$Z^p = X^p + Y^p = \prod_{\nu=0}^{p-1}(X + \zeta_p^\nu Y).$$

Ο Kummer στα 1837 δέχθηκε ότι ο δακτύλιος

$$\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta^{p-2} : a_i \in \mathbb{Z}, i = 0, 1, \dots, p-1\}$$

είναι περιοχή μονοσήμαντης ανάλυσης, απέδειξε ότι οι $X + \zeta_p^\mu Y$ είναι πρώτοι μεταξύ τους ανά δύο, συνεπώς κάθε παράγοντας του γινομένου έχει τη μορφή $\epsilon\alpha^p$, όπου $\alpha \in \mathbb{Z}[\zeta_p]$, ϵ μονάδα του $\mathbb{Z}[\zeta_p]$ και με αυτόν τον τρόπο «απέδειξε» την εικασία Fermat.

Πρώτος ο Dirichlet παρατήρησε ότι η απόδειξη του Kummer είναι λάθος, διότι ο δακτύλιος $\mathbb{Z}[\zeta_p]$ δεν είναι εν γένει δακτύλιος μονοσήμαντης ανάλυσης. Ο Kummer (1845) στην προσπάθειά του να διορθώσει το λάθος του εισήγαγε τους «ιδεώδεις αριθμούς» και κατάφερε να αποδείξει την εικασία του Fermat για τους λεγόμενους «ομαλούς», τους οποίους θα ορίσουμε στη συνέχεια. Περισσότερο συγκεκριμένα, οι μέθοδοι του Kummer αποδεικνύουν την εικασία για όλους τους πρώτους $p < 100$ εκτός από τους $p \neq 37, 59, 67$.

Ακολουθεί η εργασία του Dedekind (1831-1916), ο οποίος εισάγει δύο έννοιες θεμελιώδους σημασίας για τη θεωρία των αριθμών, την άλγεβρα και τα μαθηματικά γενικότερα. Αυτές είναι η έννοια του *ιδεώδους* και του *module*.

Ας γυρίσουμε για λίγο πίσω στον δακτύλιο $\mathbb{Z}[\sqrt{-5}]$. Έχουμε δύο γνήσιες αναλύσεις του 6 στον $Z[\sqrt{-5}]$ ως γινόμενο αναγώγων, όχι ανά δύο συνεταιρικών, στοιχείων

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Αργότερα θα δούμε ότι το κύριο ιδεώδες που παράγεται από το 2, $\langle 2\rangle = \mathfrak{P}_2^2$, όπου το $\mathfrak{P}_2 = \langle 2, 1 + \sqrt{-5}\rangle$ είναι ένα πρώτο ιδεώδες του $\mathbb{Z}[\sqrt{-5}]$. Ομοίως $\langle 3\rangle = \mathfrak{P}_3\overline{\mathfrak{P}}_3$, όπου $\mathfrak{P}_3 = \langle 3, 1 + \sqrt{-5}\rangle$ και $\overline{\mathfrak{P}}_3 = \langle 3, 1 - \sqrt{-5}\rangle$ είναι πρώτα ιδεώδη του $\mathbb{Z}[\sqrt{-5}]$. Επιπλέον ισχύει ότι

$$\langle 1 + \sqrt{-5}\rangle = \mathfrak{P}_2\mathfrak{P}_3 \qquad \langle 1 - \sqrt{-5}\rangle = \mathfrak{P}_2\overline{\mathfrak{P}}_3,$$

οπότε το ιδεώδες που παράγεται από το 6 έχει μονοσήμαντη ανάλυση σε γινόμενο πρώτων ιδεωδών

$$\langle 6\rangle = \mathfrak{P}_2^2\mathfrak{P}_3\overline{\mathfrak{P}}_3.$$

Δακτύλιοι που έχουν αυτή την ιδιότητα λέγονται δακτύλιοι του Dedekind και σύντομα θα δούμε ότι οι δακτύλιοι των ακεραίων αλγεβρικών αριθμών αλγεβρικών σωμάτων αριθμών είναι δακτύλιοι του Dedekind.

Όλες οι προσπάθειες απόδειξης της εικασίας του Fermat μέχρι τη δεκαετία του 1980 στηρίζονταν στις ιδέες του Kummer. Αναλυτικά θα αναφερθούμε στο κεφάλαιο XI όπου και θα διαπιστώσουμε και τα όρια της μεθόδου αυτής.

Στα 1986 ο Gerhard Frey είχε την επαναστατική ιδέα να συνδέσει την εικασία Fermat με την ταχύτατα αναπτυσσόμενη τότε θεωρία των ελλειπτικών καμπυλών. Η βασική ιδέα είναι ότι αν η εικασία του Fermat δεν ισχύει και υπάρχει μια μη-τετριμμένη λύση, τότε η αντίστοιχη ελλειπτική καμπύλη έχει τόσο όμορφες ιδιότητες που δεν υπάρχει!

Ακολούθησαν σημαντικά αποτελέσματα των Serre και Ribet και η απόδειξη της εικασίας λήγει με το Θεώρημα του A. Wiles (1995). Στο κεφάλαιο XII θα αναπτύξουμε τις βασικές ιδέες των αποδείξεων αυτών.

Παρατήρηση I.2.1. Ότι από τη μορφή της εξίσωσης δεν μπορεί να προσδιοριστεί η ύπαρξη ή μη λύσης μιας διοφαντικής εξίσωσης φαίνεται από τα παρακάτω παραδείγματα:

Ένα γενικό πρόβλημα είναι η παράσταση φυσικών αριθμών ως άθροισμα τριών κύβων ακεραίων αριθμών. Έτσι για $n = 29$ η εξίσωση

$$x^3 + y^3 + z^3 = 29$$

έχει την προφανή λύση $(x, y, z) = (3, 1, 1)$. Και η εξίσωση

$$x^3 + y^3 + z^3 = 30$$

έχει ακέραια λύση. Η πιο μικρή όμως είναι η $(x, y, z) = (283059965, -2218888517, 2220422932)$. Οι εξισώσεις

$$x^3 + y^3 + z^3 = 31, \qquad x^3 + y^3 + z^3 = 32$$

δεν έχουν ακέραια λύση, αφού $x^3, y^3, z^3 \equiv -1$ ή 0 ή 1 modulo 9. και $31 \equiv 4 \mathrm{mod} 9$ ενώ $32 \equiv 5 \mathrm{mod} 9$. Μέχρι το τέλος του 20ού αιώνα από τους φυσικούς αριθμούς $n, n < 100$ δεν είχε απαντηθεί η ύπαρξη ή μη λύσης για τους $33, 42$ και 74.

Για τον 74 δόθηκε μια λύση από τον S. Huisman το 2016 [1], για τον 33 δόθηκε μια λύση από τον A. Booker (Bristol) το 2019 και για τον 42 δόθηκε μια λύση από τον A. Sutherland (MIT) το 2020 [1]

Επίσης, από το 1953 ήταν ανοιχτό το ερώτημα αν η διοφαντική εξίσωση

$$x^3 + y^3 + z^3 = 3$$

έχει άλλη λύση πέρα από τις προφανείς $(x, y, z) = (1, 1, 1)$ και $(x, y, z) = (-5, 4, 4)$. Στην εργασία τους αυτή οι A. Booker και A. Sutherland δίνουν και μία τρίτη λύση. Δεν είναι γνωστό αν η εξίσωση αυτή έχει πεπερασμένο ή άπειρο πλήθος λύσεων.

I.3 Σύντομη επισκόπηση της θεωρίας των αλγεβρικών σωμάτων αριθμών

Στην παράγραφο αυτή θα περιγράψουμε όλα τα σημαντικά θεωρήματα του μαθήματος. Ο στόχος είναι να πάρει μια βασική ιδέα ο αναγνώστης. Θα εμβαθύνει στη συνέχεια κατά την αναλυτική παρουσίαση της ύλης.

Η αλγεβρική θεωρία των αριθμών ασχολείται με τη μελέτη των αλγεβρικών σωμάτων αριθμών.

Ορισμός I.3.1. Ένα σώμα K θα λέγεται αλγεβρικό σώμα αριθμών ακριβώς τότε όταν το K είναι υπόσωμα του $\mathbb{C}$ και $[K : \mathbb{Q}] < \infty$.

Πρότυπο στη μελέτη μας είναι το σώμα των ρητών αριθμών. Τον ρόλο που παίζουν οι ακέραιοι $\mathbb{Z}$ (από εδώ και κάτω θα τους ονομάζουμε ρητούς ακέραιους) στο σώμα των ρητών αριθμών $\mathbb{Q}$, παίζουν οι ακέραιοι αλγεβρικοί αριθμοί του K στο σώμα K. Αποτελούν όπως και ο $\mathbb{Z}$, έναν δακτύλιο R_K τον λεγόμενο δακτύλιο των ακεραίων αλγεβρικών αριθμών του K.

Ορισμός I.3.2. Για ένα $\alpha \in K$ ο α είναι ακέραιος αλγεβρικός αν και μόνο αν $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$, όπου $\mathrm{Irr}(\alpha, \mathbb{Q})$ είναι το ανάγωγο πολυώνυμο του α υπεράνω του $\mathbb{Q}$.

Κατ' αρχήν, αν K επέκταση σώματος χαρακτηριστικής μηδέν (του **Q**) έπεται ότι το $K/\mathbb{Q}$ είναι απλή αλγεβρική, δηλαδή υπάρχει ένα στοιχείο $\theta \in K$ ώστε $K = \mathbb{Q}(\theta)$. Έστω $f(x) = \mathrm{Irr}(\theta, \mathbb{Q}) = (x - \theta^{(1)})(x - \theta^{(2)}) \cdots (x - \theta^{(n)})$ το ανάγωγο πολυώνυμο του $\theta = \theta^{(1)}$ υπέρ το $\mathbb{Q}$. Γνωρίζουμε από την άλγεβρα ότι ο βαθμός της επέκτασης $[K : \mathbb{Q}] = \deg \mathrm{Irr}(\theta, \mathbb{Q}) = n$ και ότι μια βάση της επέκτασης $K/\mathbb{Q}$ είναι το $\{1, \theta, \theta^2, \ldots, \theta^{(n-1)}\}$. Έστω R_K ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του σώματος K. Ισχύει το

[1] Δείτε: `https://www.ntwebseminar.org/previous-talks` και συγκεκριμένα στη διάλεξη του Sutherland 7 Μαΐου 2020 όπως και `https://drive.google.com/file/d/1qzD__dviONTqHQH7DBFmsQ0MdCa7ePRg/view`.

Θεώρημα Ι.3.3. *Ο δακτύλιος* R_K *είναι δακτύλιος του Dedekind, δηλαδή κάθε ιδεώδες του* R_K *αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών αυτού. Δείτε το Θεώρημα ΙΙΙ.3.14.*

Στη θεωρία αριθμών όταν μιλάμε για ιδεώδη θα εννοούμε πάντοτε τα διάφορα του μηδενικού ιδεώδη.

Ορισμός Ι.3.4. Αν $w_1, w_2, \ldots, w_n$ είναι στοιχεία του R_K γραμμικά ανεξάρτητα υπέρ το $\mathbb{Q}$ και

$$R_K = \mathbb{Z}w_1 + \mathbb{Z}w_2 + \cdots + \mathbb{Z}w_n$$

δηλαδή το R_K είναι ένα *ελεύθερο $\mathbb{Z}$-module* που παράγεται από τα $w_1, \ldots, w_n$. Το σύνολο $\{w_1, \ldots, w_n\}$ λέγεται μια *βάση ακεραιότητας* του σώματος K.

Θεώρημα Ι.3.5. *Κάθε αλγεβρικό σώμα αριθμών* K *έχει μια βάση ακεραιότητας υπέρ του* $\mathbb{Q}$. *Δείτε το θεωρήμα IV.4.2 και του ορισμό IV.4.4.*

Πρόβλημα: Να βρεθεί μία βάση ακεραιότητας.

Σημείωση Ι.3.6. Αν πάρουμε δύο αλγεβρικά σώματα αριθμών K, L και υποθέσουμε ότι $K \subset L$, τότε μπορούμε να ορίσουμε ανάλογα όλα τα παραπάνω, το τελευταίο όμως θεώρημα δεν ισχύει, δηλαδή δεν είναι πάντοτε ο R_L ελεύθερο R_K-module.

Με τη βοήθεια των παραπάνω εννοιών ορίζουμε *διακρίνουσα* για κάθε σύνολο $\{\alpha_1, \ldots, \alpha_n\}$ n το πλήθος στοιχείων του K η οποία έχει τη χαρακτηριστική ιδιότητα ότι είναι ίση με μηδέν ακριβώς τότε όταν το σύνολο είναι γραμμικά εξαρτημένο υπεράνω του $\mathbb{Q}$. Στη συνέχεια ορίζουμε διακρίνουσα D_K του σώματος K. Η διακρίνουσα είναι ένας ακέραιος αριθμός. Είναι γνωστό ότι υπάρχουν πεπερασμένου πλήθους σώματα με δοσμένη διακρίνουσα. Ισχύει το εξής βασικό

Θεώρημα Ι.3.7. *Αν* $p \nmid D_K$ *και* $\langle p \rangle = pR_K = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ *με* $\mathfrak{P}_i$ *διαφορετικά μεταξύ τους πρώτα ιδεώδη του* R_K, *τότε κατ' ανάγκη* $e_1 = e_2 = \cdots = e_g = 1$. *Δείτε το θεώρημα X.2.4.*

Ορισμός Ι.3.8. Ο αριθμός e_i λέγεται *δείκτης διακλάδωσης* του πρώτου ιδεώδους $\mathfrak{P}_i$ του R_K υπεράνω του $\mathbb{Q}$, συμβολίζεται δε με $e_{K/\mathbb{Q}}(\mathfrak{P}_i)$. Το ιδεώδες $\mathfrak{P}_i$ λέγεται *διακλαδιζόμενο* (ramified) αν και μόνο αν $e_{K/\mathbb{Q}}(\mathfrak{P}_i) > 1$, αλλιώς λέγεται *όχι διακλαδιζόμενο*. Θα λέμε ότι το p διακλαδίζεται στο K όταν υπάρχει ένα τουλάχιστον $\mathfrak{P}_i$ με $e_{K/\mathbb{Q}}(\mathfrak{P}_i) > 1$.

Ώστε, διακλαδιζόμενα μπορεί να είναι μόνο τα ιδεώδη που εμφανίζονται στην ανάλυση των ιδεωδών πρώτων αριθμών που διαιρούν τη διακρίνουσα. Το θεώρημα της διακρίνουσας μας εξασφαλίζει και το αντίστροφο.

Σε κάθε ιδεώδες του R_K αντιστοιχούμε έναν φυσικό αριθμό που τον λέμε norm του ιδεώδους. Για πρώτα ιδεώδη $\mathfrak{P}$ του K, ισχύει $N_K(\mathfrak{P}) = p^f$ όπου $f \in \mathbb{N} - \{0\}$ και p ο μοναδικός πρώτος που ανήκει στο $\mathfrak{P}$. Ο f λέγεται βαθμός του $\mathfrak{P}$ και γράφεται $f_{K/\mathbb{Q}}(\mathfrak{P})$.

Ισχύει το παρακάτω:

Θεώρημα Ι.3.9 (Νόμος Ανάλυσης)**.**

$$\langle p \rangle = pR_K = pR_K = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$$

και $N_K(\mathfrak{P}_i) = p^{f_i}$ *τότε*

$$e_1f_1 + e_2f_2 + \cdots + e_gf_g = n.$$

Δείτε και το θεώρημα VI.3.4.

Σημείωση Ι.3.10. Αν η επέκταση $K/\mathbb{Q}$ είναι επέκταση Galois, ο παραπάνω νόμος είναι πολύ απλός στη μορφή.

Το σώμα $K = \mathbb{Q}(\theta)$, $\theta \in R_K$. Είναι φανερό ότι η προσθετική ομάδα $\mathbb{Z}[\theta]$ είναι υποομάδα της R_K. Ισχύει το ακόλουθο θεώρημα των Kummer-Dedekind:

Θεώρημα I.3.11. *Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$ και έστω p πρώτος αριθμός, $p \nmid [R_K : \mathbb{Z}[\theta]$ και $f(x) = \mathrm{Irr}(\theta, \mathbb{Q})$. Αν*

$$\overline{f}(x) = \overline{f}_1(x)^{e_1}\overline{f}_2(x)^{e_2}\cdots\overline{f}_g(x)^{e_g}$$

είναι η μονοσήμαντη ανάλυση του $\overline{f}(x)$ σε γινόμενο αναγώγων πολυωνύμων του δακτυλίου $\mathbb{F}_p[x]$ τότε ισχύει

$$\langle p\rangle = pR_K = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g},$$

όπου $\mathfrak{P}_i$ πρώτα ιδεώδη του R_K και μάλιστα $\mathfrak{P}_i = \langle p_i, f_i(\theta)\rangle = pR_K + f_i(\theta)R_K$ για $i = 1, 2, \ldots, g$. Δείτε και το θεώρημα VI.5.16.

Όπως από τους ακεραίους κατασκευάζουμε τους ρητούς έτσι και από τα (από εδώ και κάτω ακέραια ονομαζόμενα) ιδεώδη του R_K ορίζουμε τα *κλασματικά ιδεώδη* του (καταχρηστικώς λεγόμενα) σώματος K.

Εύκολα βλέπει κανείς ότι έχουμε άπειρα ιδεώδη. Τα χωρίζουμε σε κλάσεις ως προς την ισοδυναμία $\mathfrak{A} \cong \mathfrak{B}$ αν και μόνο αν $\mathfrak{A}\mathfrak{B}^{-1}$ είναι ακέραιο ιδεώδες. Ισχύει το

Θεώρημα I.3.12. *Το πλήθος των κλάσεων είναι για κάθε αλγεβρικό σώμα αριθμών πεπερασμένο. Δείτε και το θεώρημα V.2.8.*

Ορισμός I.3.13. Ο αριθμός που μας δείχνει το πλήθος των κλάσεων λέγεται *αριθμός κλάσεων* ιδεωδών του σώματος K και συμβολίζεται με h_K.

Η σημασία του φαίνεται μεταξύ άλλων και από το

Θεώρημα I.3.14. *Ισχύει ότι $h_K = 1$ αν και μόνο αν ο R_K είναι δακτύλιος μονοσήμαντης ανάλυσης. Δείτε και την πρόταση V.2.8.*

Πρόβλημα: Δίνεται ένα αλγεβρικό σώμα αριθμών. Ζητείται ο h_K.

Στις κλάσεις ιδεωδών μπορούμε να ορίσουμε μια πράξη πολλαπλασιασμού, οπότε το σύνολο των κλάσεων γίνεται αβελιανή ομάδα (η τάξη της είναι h_K). Η εύρεση της δομής αυτής της ομάδας είναι όπως είναι φυσικό, πολύ πιο δύσκολο και πιο σημαντικό ίσως πρόβλημα από την εύρεση του αριθμού κλάσεων ιδεωδών.

Ένα άλλο πρόβλημα ήταν η εύρεση της δομής των μονάδων $E(R_K)$ του R_K το οποίο όμως λύθηκε από τον Dirichlet

Θεώρημα I.3.15. *Για κάθε αλγεβρικό σώμα αριθμών K υπάρχει ένας φυσικός $r = r(K)$ και μονάδες $\epsilon_1, \epsilon_2, \ldots, \epsilon_r$ του R_K (λέγονται θεμελιώδεις μονάδες) έτσι ώστε κάθε μονάδα του R_K να έχει μία μονοσήμαντη παράσταση της μορφής*

$$\epsilon = \zeta^s\epsilon_1^{s_1}\epsilon_2^{s_2}\cdots\epsilon_r^{s_r},$$

όπου $s, s_1, s_2, \ldots, s_r$ φυσικοί αριθμοί και ζ μία ρίζα της μονάδας του σώματος K. Δείτε και το θεώρημα IX.2.1.

Πρόβλημα: Δοθέντος ενός αλγεβρικού σώματος K να βρεθεί ένα πλήρες σύστημα θεμελιωδών μονάδων της ομάδας των μονάδων του.

Όλα τα παραπάνω θα τα εξετάσουμε κατ' αρχήν στα πιο απλά σώματα τα οποία δεν είναι άλλα από τα *τετραγωνικά σώματα αριθμών*, δηλαδή σώματα της μορφής $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z} - \{0\}$ και d όχι τέλειο τετράγωνο. Προφανώς $K/\mathbb{Q}$ είναι κυκλική επέκταση του Galois, βαθμού 2.

Τα *κυκλοτομικά σώματα αριθμών* $K = \mathbb{Q}(\zeta_n)$, $\zeta_n = e^{\frac{2\pi i}{n}}$, αποτελούν ιδιαιτέρως ενδιαφέρουσα κλάση. Ως γνωστόν οι επεκτάσεις $K/\mathbb{Q}$ είναι αβελιανές, δηλαδή επεκτάσεις του Galois με ομάδα Galois $G(K/\mathbb{Q})$ αβελιανή.

Ισχύει και το αντίστροφο:

Θεώρημα Ι.3.16 (Kronecker-Weber)**.** *Κάθε αβελιανή επέκταση του* $\mathbb{Q}$, $K/\mathbb{Q}$ *περιέχεται σε ένα κυκλοτομικό σώμα, δηλαδή υπάρχει* $n \in \mathbb{N}$ *ώστε* $K \subset \mathbb{Q}(\zeta_n)$. *Δείτε και τα θεωρήματα VIII.5.1 και X.4.1.*

Το θεώρημα αυτό αποτελεί την αρχή ενός κλάδου της θεωρίας των αριθμών του λεγόμενου class field theory, τον οποίο ο H. Koch στην κριτική του [2] για το βιβλίο του Neukirch [3] τον χαρακτήρισε όχι μόνο σαν την καρδιά της αλγεβρικής θεωρίας αριθμών αλλά και «χωρίς αμφιβολία μία από τις πιο σημαντικές επιδόσεις του πολιτισμού του 20ου αίωνα», «*Die Klassenkörpertheorie ist das Herzstück der algebraischen Zahlentheorie und zweifellos eine der bedeutendsten Kulturleistungen des 20 Jahrhunderts*».

Η ύλη θα μπορούσε να αναπτυχθεί και με τη βοήθεια της *θεωρίας των εκτιμήσεων*, προτιμήθηκε όμως η *θεωρία των ιδεωδών* για διδακτικούς κυρίως λόγους. Για την κατανόηση του μαθήματος προϋποτίθενται βασικές γνώσεις από τη θεωρία δακτυλίων και τη θεωρία του Galois.

I.4 Ασκήσεις

1. Να λυθεί η διοφαντική εξίσωση
$$y^2 = x^3 + x$$

2. Να αποδείξετε ότι η διοφαντική εξίσωση
$$y^2 = x^3 + 7$$
δεν έχει ακέραια λύση.

3. Να αποδείξετε ότι ο φυσικός αριθμός 26 είναι ο μοναδικός αριθμός με την ιδιότητα: «Ο $n-1$ είναι τέλειο τετράγωνο και ο $n+1$ είναι τρίτη δύναμη φυσικού».

   Σημείωση: Η άσκηση αυτή προτάθηκε προς λύση από τον Fermat στους Βρετανούς μαθηματικούς της εποχής.

4. Αν (x, y, z) πρωταρχική πυθαγόρεια τριάδα, να αποδείξετε ότι

   (α′) Το x ή το y διαιρείται με 3

   (β′) Ένα ακριβώς από τα x, y, z διαιρείται με 5.

   (γ′) Ένα τουλάχιστο από τα x, y, z διαιρείται με 4.

5. Να αποδείξετε ότι η ακτίνα του εγγεγραμμένου κύκλου ορθογωνίου τριγώνου με πλευρές πυθαγόρεια τριάδα είναι φυσικός αριθμός.

6. Υποθέτουμε ότι η διοφαντική εξίσωση
$$X^n + Y^n = Z^n$$
δεν έχει μη τετριμμένη λύση (x, y, z) για $n = 4$ και $n = p$, πρώτος αριθμός $p \neq 2$. Να αποδείξετε ότι δεν έχει μη-τετριμμένη λύση για κάθε φυσικό αριθμό n, $n \geq 3$.

Βιβλιογραφία

[1] Huisman, S. G. *Newer sums of three cubes* (2016). URL: arXiv:1604.07746.

[2] Koch, H. *Jahresbericht der DMV*. 89.3 (1987). σελ. 32.

[3] Neukirch, J. *Algebraische Zahlentheorie*. German. Springer-Verlag Berlin, 1992.

[4] Simon, S. *Το τελευταίο θεώρημα του Φερμά*. Η γοητεία της γνώσης. Τραυλός, Αθήνα, 1998, p. 400. ISBN: 9789607122971.

[5] Taylor, R. & Wiles, A. *Ring-theoretic properties of certain Hecke algebras*. *Ann. of Math. (2)* 141.3 (1995), pp. 553–572. ISSN: 0003-486X. URL: https://doi.org/10.2307/2118560.

[6] Wiles, A. *Modular Elliptic Curves and Fermat's Last Theorem*. *Ann. of Math. (2)* 141.3 (1995), pp. 443–551. ISSN: 0003-486X. URL: https://doi.org/10.2307/2118559.

[7] Αντωνιάδης, I. A. & Κοντογεώργης, Α. *Θεωρία Αριθμών και Εφαρμογές*. Κάλλιπος, 2015, pp. ix+315. ISBN: 978-618-82124-5-9. URL: https://eclass.uoa.gr/modules/document/file.php/MATH443/NumberTheoryNov2016.pdf.

II

Τετραγωνικά σώματα αριθμών

Πριν προχωρήσουμε στη γενική θεωρία θα ασχοληθούμε ειδικά με τα τετραγωνικά σώματα αριθμών. Ο λόγος είναι ότι πρόκειται για την πιο απλή μη-τετριμμένη περίπτωση και ότι αρκετά από τα σημαντικά θεωρήματα δεν χρειάζονται τη γενική θεωρία και αποδεικνύονται ανεξάρτητα.

II.1 Ακέραιοι αλγεβρικοί αριθμοί

Υπενθυμίζουμε ότι ένας μιγαδικός αριθμός α θα λέγεται *αλγεβρικός* όταν είναι ρίζα ενός πολυωνύμου $f(x) \in \mathbb{Q}[x]$, $f(x) \neq 0$.

Ορισμός II.1.1. Ο αλγεβρικός αριθμός α θα λέγεται *ακέραιος αλγεβρικός* τότε και μόνο τότε όταν ο α είναι ρίζα ενός πολυωνύμου

$$f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in \mathbb{Z}[x], f(x) \neq 0.$$

Είναι φανερό ότι κάθε ρητός αριθμός α είναι αλγεβρικός αφού είναι ρίζα του πολυωνύμου $f(x) = x - \alpha \in \mathbb{Q}[x]$.

Παρατήρηση II.1.2. Ένας ρητός αριθμός α είναι ακέραιος αλγεβρικός τότε και μόνο τότε όταν ο $\alpha \in \mathbb{Z}$. Πράγματι, κάθε ακέραιος αριθμός α είναι αλγεβρικός αφού είναι ρίζα του πολυωνύμου $f(x) = x - \alpha \in \mathbb{Z}[x]$.

Αντίστροφα, έστω $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$ και $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$ και $b > 1$. Υποθέσαμε ότι ο α είναι ακέραιος αλγεβρικός. Επομένως υπάρχει ένα πολυώνυμο

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

το οποίο να έχει τον α ως ρίζα. Δηλαδή

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

Πολλαπλασιάζουμε με b^n και έχουμε

$$a^n + ba_{n-1}a^{n-1} + \cdots b^n a_0 = 0.$$

Το $b > 1$ έχει έναν πρώτο διαιρέτη p. Άρα $p \mid a^n$, συνεπώς $p \mid a$ άτοπο, αφού $(a, b) = 1$. Επομένως $b = 1$ και $\alpha = a/b = a \in \mathbb{Z}$.

Πρόταση II.1.3. *Το σύνολο*

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \text{ όπου } \alpha \text{ αλγεβρικός αριθμός}\}$$

είναι υπόσωμα του σώματος των μιγαδικών αριθμών.

Απόδειξη. Υποθέτουμε ότι $\alpha, \beta \in \overline{\mathbb{Q}}$. Από τη σχέση

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]$$

έχουμε: Ο α είναι αλγεβρικός, επομένως $[\mathbb{Q}(\alpha):\mathbb{Q}] < \infty$. Ο β είναι αλγεβρικός, άρα είναι αλγεβρικός και υπεράνω του $\mathbb{Q}(\alpha)$, συνεπώς $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] < \infty$. Επομένως $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] < \infty$, δηλαδή η επέκταση $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ είναι αλγεβρική.

Αυτό σημαίνει ότι τα $\alpha \pm \beta, \alpha\beta$, και για $\beta \neq 0$, α/β είναι αλγεβρικοί αριθμοί. Συνεπώς το $\overline{\mathbb{Q}}$ είναι σώμα. □

Παρατήρηση II.1.4. Για μια πιο στοιχειώδη απόδειξη παραπέμπουμε στο βιβλίο [16] του Κ. Λάκκη, *Θεωρία Αριθμών*.

Στη συνέχεια θεωρούμε το σύνολο

$$\mathcal{A} := \{\alpha \in \overline{\mathbb{Q}} \text{ όπου } \alpha \text{ ακέραιος αλγεβρικός}\}$$

Θα αποδείξουμε ότι το σύνολο $\mathcal{A}$ αποτελεί *ακέραια περιοχή*, υποδακτύλιο του $\overline{\mathbb{Q}}$. Για να το πετύχουμε, χρειαζόμαστε μια βοηθητική

Πρόταση II.1.5. *Ο μιγαδικός αριθμός α είναι αλγεβρικός ακέραιος αν και μόνο αν η προσθετική ομάδα η οποία παράγεται από όλες τις δυνάμεις του α,*

$$1, \alpha, \alpha^2, \ldots$$

είναι πεπερασμένα παραγόμενη.

Απόδειξη. Είναι σαφές ότι αν ο α είναι ακέραιος αλγεβρικός ικανοποιεί μια εξίσωση της μορφής

$$f(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

$a_i \in Z$, για κάθε $i = 0, \ldots, n-1$. Ας θεωρήσουμε μια οποιαδήποτε πολυωνυμική έκφραση του α, $F(\alpha)$, όπου $F(x) \in \mathbb{Q}[x]$. Έχουμε

$$F(x) = \pi(x)f(x) + u(x),$$

όπου το $u(x)$ είναι ή μηδενικό πολυώνυμο ή $\deg(u) < n$. Συνεπώς $F(\alpha) = u(\alpha)$, και αρκούν οι δυνάμεις $1, \alpha, \ldots, \alpha^{n-1}$ για να παράξουν τη ζητούμενη ομάδα.

Αντιστρόφως ας υποθέσουμε ότι τα στοιχεία $z_1, \ldots, z_n$ παράγουν την προσθετική ομάδα $\mathbb{Q}[\alpha]$. Αυτό σημαίνει ότι για κάθε $1 \leq i \leq n-1$ υπάρχουν $\lambda_{ij} \in \mathbb{Q}$ ώστε

$$\alpha z_i = \sum_{\nu=0}^{n-1} \lambda_{\nu,i} z_i.$$

Με άλλα λόγια το σύστημα

$$\left(\alpha\mathbb{I}_n - (\lambda)_{i,j}\right)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

επιδέχεται εκτός της μηδενικής λύσης και την $(z_1, \ldots, z_n)^t$. Άρα $\det(\alpha\mathbb{I}_n - (\lambda)_{i,j}) = 0$ η οποία είναι μια ορίζουσα της μορφής

$$x^n + b_1 x^{n-1} + \cdots + b_1 x + b_0 = 0, \qquad b_i \in \mathbb{Z}$$

που ικανοποιείται από το α, άρα ο α είναι ακέραιος αλγεβρικός.

□

Θα αποδείξουμε τώρα ότι ο $\mathcal{A}$ είναι υποδακτύλιος του $\overline{\mathbb{Q}}$.

Έστω $\alpha, \beta \in \mathcal{A}$. Θα πρέπει να αποδείξουμε ότι $\alpha+\beta$ και $\alpha\cdot\beta$ είναι στοιχεία του $\mathcal{A}$.

Σύμφωνα με την πρόταση II.1.5 το α ανήκει σε μια πεπερασμένα παραγόμενη προσθετική ομάδα G_α, υποομάδα του $\mathbb{C}$. Ομοίως και το β ανήκει σε μια πεπερασμένα παραγόμενη προσθετική ομάδα G_β.

Επόμενως τα $\alpha+\beta$ και $\alpha\beta$ είναι ακέραιοι γραμμικοί συνδυασμοί των στοιχείων $\alpha^i\beta^j$ τα οποία ανήκουν στην ομάδα $G_\alpha G_\beta$ η οποία είναι φανερό ότι είναι πεπερασμένα παραγόμενη.

Από τα παραπάνω συμπεραίνουμε ότι και όλες οι δυνάμεις των $\alpha+\beta$ και $\alpha\beta$ ανήκουν σε μια πεπερασμένα παραγόμενη προσθετική υποομάδα του $\mathbb{C}$. Από την προηγούμενη πρόταση προκύπτει ότι $\alpha+\beta$ και $\alpha\cdot\beta \in \mathcal{A}$, επομένως $\mathcal{A}$ υποδακτύλιος του $\overline{\mathbb{Q}}$.

Ουσιαστικά το κύριο αντικείμενο της αλγεβρικής θεωρίας αριθμών είναι η μελέτη της αριθμητικής του σώματος $\overline{\mathbb{Q}}$. Επειδή όμως αυτό είναι αρκετά δύσκολο θα περιορίσουμε τις ... φιλοδοξίες μας!

Ορισμός II.1.6. Ένα σώμα K υπόσωμα του $\mathbb{C}$ θα λέγεται *αλγεβρικό σώμα αριθμών* ακριβώς τότε όταν η επέκταση $K/\mathbb{Q}$ είναι πεπερασμένη.

Αφού $K/\mathbb{Q}$ είναι πεπερασμένη, έπεται ότι είναι αλγεβρική, δηλαδή το K είναι υπόσωμα του $\overline{\mathbb{Q}}$.

Σημείωση II.1.7. Η επέκταση $\overline{\mathbb{Q}}/\mathbb{Q}$ είναι άπειρη αλγεβρική.

Η επέκταση $K/\mathbb{Q}$ είναι πεπερασμένη και διαχωρίσιμη. Επομένως είναι απλή, δηλαδή υπάρχει ένα $\theta \in K$ τέτοιο ώστε $K = \mathbb{Q}(\theta)$.

Παρατήρηση II.1.8. Αν $\alpha \in \overline{\mathbb{Q}}$, τότε υπάρχει ακέραιος m, τέτοιος ώστε $m\alpha \in \mathcal{A}$.

Πράγματι, $\alpha \in \overline{\mathbb{Q}}$ σημαίνει ότι υπάρχει ένα πολυώνυμο

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Q}[X],$$

τέτοιο ώστε $f(\alpha) = 0$. Επιλέγουμε έναν ακέραιο m, τέτοιον ώστε $ma_i \in \mathbb{Z}$ για κάθε $i = 0, 1, 2, \ldots, m-1$. Επομένως έχουμε

$$(m\alpha)^n + ma_{n-1}(m\alpha)^{n-1} + \cdots + m^n a_0 = 0,$$

δηλαδή ότι $m\alpha \in \mathcal{A}$.

Άμεση συνέπεια της παρατήρησης αυτής είναι ότι αν K αλγεβρικό σώμα αριθμών, τότε υπάρχει $\theta \in \mathcal{A}$ τέτοιο ώστε $K = \mathbb{Q}(\theta)$.

Πράγματι, $K = \mathbb{Q}(h)$ με $h \in \overline{\mathbb{Q}}$. Έστω $m \in \mathbb{Z}$ ώστε $\theta := mh \in \mathcal{A}$. Είναι φανερό ότι $K = \mathbb{Q}(h) = \mathbb{Q}(\theta)$.

Η περιοχή των ακεραίων αλγεβρικών αριθμών του K είναι $R_K := K \cap \mathcal{A} \leq K$.

Στη συνέχεια θα περιοριστούμε στα *τετραγωνικά σώματα αριθμών* δηλαδή αλγεβρικά σώματα αριθμών K με $[K : \mathbb{Q}] = 2$.

Αποτελούν μετά το $\mathbb{Q}$, την απλούστερη περίπτωση αλγεβρικών σωμάτων αριθμών. Έχουν όμως το πλεονέκτημα ότι όλες οι βασικές ιδιότητες των αλγεβρικών σωμάτων αριθμών εμφανίζονται ήδη στα τετραγωνικά σώματα αριθμών και θα διατυπώσουμε τις γενικές προτάσεις χωρίς απόδειξη.

Έστω θ αλγεβρικός αριθμός του τετραγωνικού σώματος αριθμών K, τέτοιος ώστε $K = \mathbb{Q}(\theta)$. Αφού $[K, \mathbb{Q}] = 2$ θα πρέπει ο βαθμός του αναγώγου πολυωνύμου $\mathrm{Irr}(\theta, \mathbb{Q})$ να είναι δύο, δηλαδή το ανάγωγο πολυώνυμο του θ υπέρ το $\mathbb{Q}$ να έχει τη μορφή

$$\mathrm{Irr}(\theta, \mathbb{Q}) = X^2 - aX - b.$$

Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $a = 0$, διότι αλλιώς παίρνουμε τον αριθμό $\theta^* = \theta - \frac{a}{2}$ ο οποίος είναι ρίζα του πολυωνύμου

$$X^2 - b',$$

όπου $b' = \frac{a^2}{4} + b$ και $K = \mathbb{Q}(\theta^*)$. Ο ρητός b' δεν είναι τέλειο τετράγωνο στο $\mathbb{Q}$, διότι το $X^2 - b'$ είναι ανάγωγο στο $\mathbb{Q}[X]$.

Γράφουμε το $b' = mr^2$, $r \in \mathbb{Q}$ όπου $m \in \mathbb{Z}$ ο οποίος δεν διαιρείται με το τετράγωνο πρώτου αριθμού. Προφανώς $m \neq 1$ διότι αλλιώς θα είχαμε $b' = r^2$. Αν $r \neq 1$, τότε θεωρούμε τον αριθμό

$$\theta'' := \frac{\theta'}{r} \in K$$

ο οποίος είναι ρίζα του πολυωνύμου

$$X^2 - m.$$

Αποδείξαμε το

Θεώρημα II.1.9. *Κάθε τετραγωνικό σώμα αριθμών K προκύπτει από το $\mathbb{Q}$ με επισύναψη της τετραγωνικής ρίζας ενός ακέραιου αριθμού $m \neq 1$ ελεύθερου τετραγώνου.*

Γνωρίζουμε από την άλγεβρα ότι

$$K = \mathbb{Q}(\sqrt{m}) = \mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m}, a, b \in \mathbb{Q}\}.$$

Αν $m > 0$, τότε $K = \mathbb{Q}(\sqrt{m}) \subset \mathbb{R}$ και το K λέγεται *πραγματικό τετραγωνικό σώμα αριθμών*. Αν όμως $m < 0$, τότε κάθε στοιχείο του K που δεν είναι ρητός είναι μιγαδικός και το σώμα λέγεται *μιγαδικό τετραγωνικό σώμα αριθμών*.

Το K είναι σώμα αναλύσεως του διαχωρίσιμου πολυωνύμου $X^2 - m$. Συνεπώς η επέκταση $K/\mathbb{Q}$ είναι επέκταση του Galois. Η ομάδα Galois της επέκτασης αυτής είναι η

$$G = \mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\},$$

όπου $\sigma(a + b\sqrt{m}) = a - b\sqrt{m}$ για $a, b \in \mathbb{Q}$.

Κάθε στοιχείο $\alpha = a + b\sqrt{m}$ έχει ίχνος

$$S_K(\alpha) = \alpha + \sigma(\alpha) = 2a$$

και νόρμα

$$N_K(\alpha) = \alpha \cdot \sigma(\alpha) = a^2 - mb^2.$$

Προφανώς το ανάγωγο πολυώνυμο του $\alpha = a + b\sqrt{m}$ υπέρ το $\mathbb{Q}$ είναι το

$$(X - \alpha)(X - \sigma(\alpha)) = X^2 - S_K(\alpha)X + N_K(\alpha).$$

Ώστε:

Θεώρημα II.1.10. *Έστω $\alpha \in K = \mathbb{Q}(\sqrt{m})$. Ο α είναι ακέραιος αλγεβρικός ακριβώς τότε όταν $S_K(\alpha) \in \mathbb{Z}$ και $N_K(\alpha) \in \mathbb{Z}$.*

Γράφουμε $\alpha = a + b\sqrt{m} \in K$ και θέτουμε $2a = \gamma$, $2b = \delta$, οπότε το ίχνος είναι ακέραιος τότε και μόνο τότε ο γ είναι ακέραιος και η norm του α είναι ακέραιος τότε και μόνο τότε όταν ο

$$a^2 - mb^2 = \frac{\gamma^2}{4} - m\frac{\delta^2}{4} = \frac{\gamma^2 - m\delta^2}{4},$$

είναι ακέραιος. Επομένως ο α είναι ακέραιος αλγεβρικός αν και μόνο αν

$$\gamma, \delta \in \mathbb{Z} \text{ και } \gamma^2 \equiv m\delta^2 \mod 4.$$

Αν $m \equiv 2, 3 \mod 4$, επειδή για κάθε $x \in \mathbb{Z}$ έχουμε $x^2 \equiv 0, 1 \mod 4$ για να έχει η $\gamma^2 \equiv m\delta^2 \mod 4$ λύση θα έπρεπε $\gamma \equiv \delta \equiv 0 \mod 2$ δηλαδή $\alpha, \beta \in \mathbb{Z}$.

Αν $m \equiv 1 \mod 4$, τότε για να έχει η ισοτιμία $\gamma^2 \equiv m\delta^2 \mod 4$ λύση θα πρέπει

$$\gamma \equiv \delta \mod 2$$

οπότε ο $\frac{\gamma - \delta}{2} \in \mathbb{Z}$ και

$$\alpha = a + b\sqrt{m} = \frac{\gamma}{2} + \frac{\delta}{2}\sqrt{m} = \frac{\gamma - \delta}{2} + \delta\frac{1 + \sqrt{m}}{2}.$$

Παράδειγμα II.1.11. Αν $K = \mathbb{Q}(i)$, τότε η περιοχή των ακεραίων αλγεβρικών αριθμών του K είναι $R_K = \mathbb{Z}[i]$. Αν $K = \mathbb{Q}(\sqrt{-5})$, τότε η περιοχή των ακεραίων αλγεβρικών είναι $R_K = \mathbb{Z}[\sqrt{-5}]$.

II.2 Βάση και διακρίνουσα

Έστω τώρα $K = \mathbb{Q}(\sqrt{m})$ ένα τετραγωνικό σώμα αριθμών και

$$\omega_m = \begin{cases} \frac{1}{2}(1+\sqrt{m}) & \text{όταν } m \equiv 1 \mod 4 \\ \sqrt{m} & \text{όταν } m \equiv 2,3 \mod 4 \end{cases}$$

Σύμφωνα με τα προηγούμενα της παραγράφου II.1 προκύπτει αμέσως η αλήθεια της επόμενης

Πρόταση II.2.1. *Μια βάση ακεραιότητας του* R_K *είναι το σύνολο* $\{1, \omega_m\}$.

Παρατήρηση II.2.2. Αντίστοιχη πρόταση ισχύει και στην περίπτωση των γενικών σωμάτων αριθμών.

Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$ και R_K η περιοχή των ακεραίων αλγεβρικών αριθμών του K. Η R_K έχει μια βάση ακεραιότητας βαθμού n.

Φυσικά δεν είναι τόσο εύκολος ο υπολογισμός της, όπως στα τετραγωνικά σώματα αριθμών.

Στη συνέχεια υποθέτουμε ότι $K = \mathbb{Q}(\sqrt{m})$ ένα τετραγωνικό σώμα αριθμών και $\{1, \omega_m\}$ η βάση ακεραιότητας της πρότασης II.2.1.

Ορισμός II.2.3. Διακρίνουσα D_K του τετραγωνικού αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ λέγεται η ορίζουσα

$$D_K = \left(\det\begin{pmatrix} 1 & 1 \\ \omega_m & \overline{\omega}_m \end{pmatrix}\right)^2 = \begin{cases} m & \text{αν } m \equiv 1 \mod 4 \\ 4m & \text{αν } m \equiv 2,3 \mod 4 \end{cases}.$$

Παρατήρηση II.2.4. Αποδεικνύεται ότι η διακρίνουσα είναι ανεξάρτητη της επιλογής της βάσης του δακτυλίου των ακεραίων αλγεβρικών.

Ο λόγος είναι ότι αν έχουμε δύο βάσεις ακεραιότητας του R_K, τότε η μία προκύπτει από την άλλη διά πολλαπλασιασμού με έναν unimodular πίνακα, δηλαδή πίνακα με στοιχεία ακεραίους αριθμούς και ορίζουσα ± 1 (άσκηση).

Παρατήρηση II.2.5. Είναι φανερό ότι στα τετραγωνικά σώματα αριθμών η διακρίνουσα ορίζεται μονοσήμαντα από το σώμα $K = \mathbb{Q}(\sqrt{m})$.

Παρατήρηση II.2.6. Η διακρίνουσα ορίζεται σε κάθε αλγεβρικό σώμα αριθμών. Αποδεικνύεται ότι υπάρχουν πεπερασμένου πλήθους αλγεβρικά σώματα αριθμών με διακρίνουσα δοσμένο ακέραιο αριθμό.

II.3 Η ομάδα των μονάδων

Έστω $K = \mathbb{Q}(\sqrt{m})$ τετραγωνικό αλγεβρικό σώμα αριθμών και R_K η περιοχή των ακεραίων αλγεβρικών αριθμών. Θα μελετήσουμε την ομάδα των μονάδων του R_K.

Ως γνωστό το στοιχείο $\epsilon \in R_K$ είναι μονάδα της περιοχής R_K ακριβώς τότε όταν η norm $N_{K/\mathbb{Q}}(\epsilon) = \epsilon\epsilon' = \pm 1$, όπου ϵ' είναι το συζυγές του ϵ.

Ώστε το στοιχείο $\epsilon = a + b\omega_m$ είναι μονάδα του δακτυλίου R_K ακριβώς τότε όταν

$$a^2 - b^2 m = \pm 1, \text{ για } m \equiv 2,3 \mod 4$$

και

$$a^2 + ab + \frac{1-m}{4}b^2 = \pm 1, \text{ για } m \equiv 1 \mod 4.$$

Ξεχωρίζουμε τώρα δύο περιπτώσεις:

Περίπτωση I $m < 0$ δηλαδή το $K = \mathbb{Q}(\sqrt{m})$ είναι μιγαδικό τετραγωνικό σώμα αριθμών. Έστω πάλι $m \equiv 2, 3 \mod 4$. Αφού $a^2 - b^2 m > 0$ αρκεί να εξετάσουμε μόνο την περίπτωση

$$a^2 + |m|b^2 = 1.$$

Αν $|m| > 1$, τότε για να ισχύει η ισότητα θα πρέπει $b = 0$ οπότε $a = \pm 1$ και τελικά $\epsilon = \pm 1$.

Αν $m = -1$ έχουμε

$$a^2 + b^2 = 1$$

δηλαδή της τέσσερις λύσεις $a = \pm 1, b = 0$ και $a = 0, b = \pm 1$, δηλαδή $\epsilon = \pm 1, \pm i$.

Έστω τώρα ότι $m \equiv 1 \mod 4$. Αφού

$$a^2 + ab + \frac{1-m}{4}b^2 = (a + b/2)^2 + \frac{|m|}{4}b^2 \geq 0$$

αρκεί να θεωρήσουμε την

$$a^2 + ab + \frac{1-m}{4}b^2 = (a + b/2)^2 + \frac{|m|}{4}b^2 = 1.$$

Αν $|m| > 4$ τότε $b = 0$ δηλαδή και πάλι $a = \pm 1$ άρα $\epsilon = \pm 1$. Αν $|m| \leq 4$ αφού $m \equiv 1 \mod 4$, η μοναδική προς εξέταση τιμή του m είναι η $m = -3$. Σε αυτή την περίπτωση έχουμε

$$a^2 + ab + \frac{1-m}{4}b^2 = (a + b/2)^2 + \frac{3}{4}b^2 = 1.$$

Για $|b| \geq 2$ δεν υπάρχουν λύσεις. Για $b = 1$ καταλήγουμε στην $a^2 + a + 1 = 1$ η οποία έχει λύσεις $a = 0$ ή $a = 1$.

Για $b = 0$ οι λύσεις είναι $a = \pm 1$ και για $b = -1$ έχουμε $a = 0$. Άρα οι μονάδες είναι οι

$$\pm 1, \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}.$$

Επομένως έχουμε αποδείξει το

Θεώρημα II.3.1. *Έστω $K = \mathbb{Q}(\sqrt{m})$ μιγαδικό τετραγωνικό σώμα αριθμών. Η ομάδα των μονάδων της περιοχής R_K είναι η*

$$E(R_K) = \begin{cases} \{\pm 1\} & \text{αν } m < -4 \\ \{\pm 1, \pm i\} & \text{αν } m = -4 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} & \text{αν } m = -3 \end{cases}$$

Περίπτωση II Έστω ότι $m > 0$, δηλαδή το K είναι ένα πραγματικό σώμα αριθμών. Η περίπτωση αυτή είναι πολύ πιο δύσκολη από την προηγούμενη.

Στον R_K υπάρχουν άπειρες το πλήθος μονάδες και αυτό είναι συνέπεια ότι η εξίσωση του Pell

$$X^2 - mY^2 = 1$$

έχει άπειρες λύσεις, και της απλούστατης παρατήρησης ότι κάθε αριθμός του K της μορφής $x + y\sqrt{m}$, $x, y \in \mathbb{Z}$ είναι ακέραιος αλγεβρικός.

Λήμμα II.3.2. *Έστω $B \in \mathbb{R}$. Υπάρχουν πεπερασμένου πλήθους μονάδες του R_K για τις οποίες ισχύει $1 < \epsilon < B$.*

Απόδειξη. Έστω ϵ μια ρίζα του πολυωνύμου

$$X^2 - S_K(\epsilon)X \pm 1.$$

Τώρα $\epsilon > 1$ και $N_K(\epsilon) = \pm 1$ συνεπώς αν ϵ' είναι η άλλη ρίζα του παραπάνω πολυωνύμου $|\epsilon'| = \epsilon^{-1} < 1$, οπότε

$$|S_K(\epsilon)| = |\epsilon + \epsilon'| \leq |\epsilon| + |\epsilon'| < B + 1.$$

Δηλαδή ο ϵ είναι ρίζα ένος πολυωνύμου της μορφής

$$X^2 + \lambda X \pm 1$$

όπου $\lambda \in \mathbb{Z}$ και $|\lambda| \leq B + 1$. Υπάρχουν πεπερασμένου πλήθους τέτοια πολυώνυμα και κάθε ένα από αυτά έχει δύο ρίζες, άρα καταλήγουμε σε πεπερασμένου πλήθους επιλογές για το ϵ. □

Έστω $\epsilon \in E(R_K)\backslash\{\pm 1\}$. Τότε κάποια από τις $\epsilon, -\epsilon, \epsilon^{-1}, -\epsilon^{-1}$ θα είναι μεγαλύτερη του 1.

Υποθέτουμε λοιπόν ότι $\epsilon \in E(R_K)$ με $\epsilon > 1$. Παρατηρούμε ότι ανάμεσα στο 1 και στο ϵ υπάρχουν πεπερασμένες το πλήθος μονάδες του R_K, θα υπάρχει και μία ελάχιστη έστω η ϵ_0, με $1 < \epsilon_0 \leq \epsilon$.

Θα αποδείξουμε τώρα ότι

Θεώρημα II.3.3. *Η ομάδα των μονάδων δίνεται από*

$$E(R_K) = \{\pm\epsilon_0^n : n \in \mathbb{Z}\}.$$

Απόδειξη. Έστω $\epsilon \geq 1$ μια μονάδα του R_K. Αφού $\epsilon_0 > 1$ έπεται ότι $\epsilon_0^n \to \infty$ για $n \to \infty$. Άρα υπάρχει φυσικός n, ώστε

$$\epsilon_0^n \leq \epsilon < \epsilon_0^{n+1}.$$

Οπότε $1 \leq \epsilon_0^{-n}\epsilon < \epsilon_0$ και αφού ϵ_0 η ελάχιστη μεγαλύτερη του 1 μονάδα, έχουμε ότι $\epsilon\epsilon_0^{-n} = 1$ συνεπώς $\epsilon = \epsilon_0^n$.

Αν ϵ τυχαία μονάδα του R_K, μία από τις $\pm\epsilon, \pm\epsilon^{-1}$ θα είναι μεγαλύτερη της μονάδας και τελικά η ϵ θα είναι της μορφής $\pm\epsilon_0^n$ με $n \in \mathbb{Z}$. □

Το ερώτημα είναι γιατί τα τετραγωνικά σώματα αριθμών έχουν πεπερασμένο πλήθος μονάδων και τα τετραγωνικά πραγματικά άπειρο πλήθος; Τι γίνεται στη γενική περίπτωση;

Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$, $K = \mathbb{Q}(\theta)$. Αν $f(X)$ το ανάγωγο πολυώνυμο του θ υπεράνω του $\mathbb{Q}$, τότε $\deg f(X) = n$ και

$$f(X) = (X - \theta^{(1)})(X - \theta^{(2)})\cdots(X - \theta^{(n)}),$$

$\theta^{(1)} = \theta$. Υποθέτουμε ότι r_1 είναι το πλήθος των πραγματικών ριζών του $f(X)$ και $2r_2$ είναι το πλήθος των μιγαδικών. Οι μιγαδικές ρίζες έχουν άρτιο πλήθος γιατί αν ένα πολυώνυμο με συντελεστές πραγματικούς αριθμούς έχει μια μιγαδική ρίζα τότε έχει και τη συζυγή της. Επομένως $r_1 + 2r_2 = n$.

Θεώρημα II.3.4 (μονάδων του Dirichlet)**.** *Υπάρχουν* $r := r_1 + r_2 - 1$ *μονάδες* $\epsilon_1, \epsilon_2, \ldots, \epsilon_r$ *μονάδες της ομάδας* $E(R_K)$ *έτσι ώστε κάθε μονάδα του* R_K *να έχει μονοσήμαντη παράσταση της μορφής*

$$\epsilon = \zeta\epsilon_1^{s_1}\epsilon_2^{s_2}\cdots\epsilon_r^{s_r},$$

όπου $s_i \in \mathbb{Z}$ *για* $i \in 1, 2, \ldots, r$ *και* ζ *είναι μια ρίζα της μονάδας.*

Εφαρμογή: Αν $K = \mathbb{Q}(\sqrt{m})$ είναι τετραγωνικό μιγαδικό σώμα αριθμών, το $f(X) = X^2 - m$ έχει δύο μιγαδικές ρίζες και συνεπώς $r_1 = 0$ και $r_2 = 1$. Άρα $r = r_1 + r_2 - 1 = 0$.

Αν πάλι $K = \mathbb{Q}(\sqrt{m})$ τετραγωνικό πραγματικό σώμα αριθμών, τότε $r_1 = 2$ και $r_2 = 0$, συνεπώς $r = r_1 + r_2 - 1 = 1$.

Πρόβλημα: Πώς θα βρούμε μια θεμελιώδη μονάδα ενός πραγματικού τετραγωνικού σώματος αριθμών;

Η θεωρία των συνεχών κλασμάτων είναι και πάλι χρήσιμη. Προκειμένου να διατυπώσουμε το θεώρημα, χρειαζόμαστε να «ομογενοποιήσουμε» τη βάση ακεραιότητας του R_K, όπου K τετραγωνικό σώμα αριθμών, έτσι ώστε να μην υπάρχει ανάγκη να ξεχωρίζουμε δύο περιπτώσεις.

Πρόταση II.3.5. *Έστω K τετραγωνικό σώμα αριθμών διακρίνουσας D_K. Τότε $K = \mathbb{Q}(\sqrt{D_K})$ και $R_K = \mathbb{Z}\left[\frac{D_K+\sqrt{D_K}}{2}\right]$*

Απόδειξη. Αν $K = \mathbb{Q}(\sqrt{m})$, τότε $D_K \in \{m, 4m\}$. Επομένως $K = \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{D_K})$. Υπολογίζουμε ότι

$$\frac{D_K + \sqrt{D_K}}{2} = \begin{cases} \frac{4m+\sqrt{4m}}{2} = 2m + \sqrt{m} & \text{αν } m \equiv 2,3 \mod 4 \\ \frac{m+\sqrt{m}}{2} = \frac{m-1}{2} + \frac{1+\sqrt{m}}{2} & \text{αν } m \equiv 1 \mod 4 \end{cases}$$

το οποίο modulo $\mathbb{Z}$ είναι ισοδύναμο με $\sqrt{m}$ και $\frac{1+\sqrt{m}}{2}$, αντίστοιχα. □

Θεώρημα II.3.6. *Έστω K πραγματικό τετραγωνικό σώμα αριθμών διακρίνουσας D_K και $R_K = \mathbb{Z}[\omega]$, με $\omega = \frac{D_K+\sqrt{D_K}}{2}$, η περιοχή των ακεραίων αλγεβρικών αριθμών αυτού.*

Έστω ακόμη $\theta := \frac{1}{\omega - [\omega]}$. Ο αριθμός θ είναι ανάγωγος (reduced) και συνεπώς απλά περιοδικός.

Υποθέτουμε ότι $\theta = [\overline{a_0, a_1, \ldots, a_{r-1}}]$ με την ελάχιστη περίοδο.

Ο αριθμός $\epsilon_0 := q_{r-1}\theta + q_{r-2}$ είναι η θεμελιώδης μονάδα του R_K. Τα q_k είναι φυσικοί αριθμοί που ορίζονται με τη βοήθεια της θεωρίας των συνεχών κλάσματων.

Απόδειξη. Η απόδειξη είναι μακροσκελής και ως εκ τούτου παραλείπεται. Τον ενδιαφερόμενο αναγνώστη παραπέμπουμε στο [15].

□

II.4 Νόμος Ανάλυσης στα τετραγωνικά σώματα αριθμών

II.4.1 Περιοχές μονοσήμαντης ανάλυσης

Έστω τώρα $K = \mathbb{Q}(\sqrt{m})$, και R_K δακτύλιος μονοσήμαντης ανάλυσης. Ας ρίξουμε μια ματιά στα ανάγωγα στοιχεία (πρώτα), χωρίς φυσικά να κάνουμε διάκριση μεταξύ συνεταιρικών, δηλαδή στοιχεία που διαφέρουν κατά μονάδα.

Αν π λοιπόν *ανάγωγο* στοιχείο του K, τότε υπάρχει τουλάχιστον ένας φυσικός αριθμός n, η norm του π, $(\pi) = \pi\pi'$, η οποία διαιρείται με π, δηλαδή υπάρχει (ρητός) πρώτος p ώστε $\pi \mid p$. Προφανώς ο p είναι ο μοναδικός πρώτος που διαιρείται με π.

Ορισμός II.4.1. Αν $\pi \mid p$ θα λέμε ότι ο p είναι ρητός πρώτος που ανήκει στο π ή αλλιώς ο π είναι ένας πρώτος διαιρέτης του p στο σώμα K.

Η σχέση $\pi \mid p$ δίνει $N_K(\pi) \mid p^2$, και επομένως $N_K(\pi) \cong p$ ή p^2.

Αν $N_K(\pi) \cong p$ τότε $p \cong \pi\pi'$, με π' πρώτο στοιχείο του K. Ξεχωρίζουμε δύο περιπτώσεις. Την $\pi \not\cong \pi'$ και $\pi \cong \pi'$.

Αν πάλι $N_K(\pi) \cong p^2$ τότε $p^2 = \pi\pi'$ και λόγω του μονοσημάντου της ανάλυσης $p \cong \pi \cong \pi'$.

Όταν λοιπόν το p διατρέχει όλους τους ρητούς πρώτους, τότε οι πρώτοι π, π' (εξαιρούμε έναν από τους δύο αν $\pi \cong \pi'$) διατρέχουν ένα πλήρες σύστημα πρώτων του K.

Εντελώς φυσιολογικά τώρα τίθεται το ερώτημα της εύρεσης ενός κανόνα που να μας δίνει ποια από τις τρεις περιπτώσεις

$$\begin{array}{ccc} p \cong \pi\pi', & \text{με} & N_K(\pi) = N_K(\pi') \cong p \\ p \cong \pi^2, & \text{με} & N_K(\pi) = N_K(\pi') \cong p \\ p \cong \pi, & \text{με} & N_K(\pi) = N_K(\pi') = p^2, \end{array}$$

ισχύει. Ένας τέτοιος κανόνας θα λέγεται *νόμος ανάλυσεως* για το $K = \mathbb{Q}(\sqrt{m})$ και η εύρεσή του είναι ένα από τα πιο βασικά και σπουδαία προβλήματα της θεωρίας των τετραγωνικών σωμάτων αριθμών.

Προτού διατυπώσουμε τον νόμο αναλύσεως, παρατηρούμε ότι κάθε ακέραιος αλγεβρικός αριθμός του K γράφεται στη μορφή

$$\alpha = \frac{a + b\sqrt{D}}{2},$$

με $a, b \in \mathbb{Z}$ και

$$a \equiv Db \mod 2,$$

όπου D η διακρίνουσα του σώματος.

Επιπλέον, χρειαζόμαστε μια γενίκευση του συμβόλου του Legendre.

Ορισμός II.4.2. Αν D διακρίνουσα ενός τετραγωνικού σώματος αριθμών, τότε το σύμβολο του Kronecker $\left(\frac{D}{p}\right)$για κάθε πρώτο αριθμό p ορίζεται ως:

- Αν $p \neq 2$ και $p \nmid D$, τότε το $\left(\frac{D}{p}\right)$ ταυτίζεται με το σύμβολο του Legendre.
- Αν $p \mid D$, τότε $\left(\frac{D}{p}\right) = 0$.
- Αν $D \equiv 1 \mod 4$, τότε $\left(\frac{D}{2}\right) = \left(\frac{2}{D}\right)$ = σύμβολο του Jacobi δηλαδή

$$\left(\frac{D}{2}\right) = \begin{cases} 1 & \text{αν } D \equiv 1 \mod 8 \\ -1 & \text{αν } D \equiv 5 \mod 8 \end{cases}$$

Θεώρημα II.4.3 (Νόμος ανάλυσης στο K)**.** *Έστω $K = \mathbb{Q}(\sqrt{m})$, τετραγωνικό σώμα αριθμών με R_K δακτύλιος μονοσήμαντης ανάλυσης και D η διακρίνουσα αυτού. Οι τρεις περιπτώσεις*

$$p \cong \pi\pi', \qquad p \cong \pi^2, \qquad p \cong \pi$$

αντιστοιχούν στις τιμές του συμβόλου του Kronecker

$$\left(\frac{D}{p}\right) = 1, \qquad \left(\frac{D}{p}\right) = 0, \qquad \left(\frac{D}{p}\right) = -1.$$

Απόδειξη. Αρκεί να δείξουμε ότι

1. $p \cong \pi^2$ αν και μόνο αν $\left(\frac{D}{p}\right) = 0$ και
2. $p \cong \pi\pi'$ αν και μόνο αν $\left(\frac{D}{p}\right) = 1$

Για το 1. Θα αποδείξουμε ότι αν $\left(\frac{D}{p}\right) = 0$ τότε $p \cong \pi^2$. Έστω $p \mid D$. Υποθέτουμε κατ' αρχήν ότι $p \cong \pi$ δηλαδή ότι ο p παραμένει στο K και πάλι πρώτος. Σε όλες τις άλλες περιπτώσεις, εκτός της $p = 2$ και $m \equiv 3 \mod 4$ έχουμε $p \mid \sqrt{m}$ και καταλήγουμε στο ότι $p^2 \mid m$, άτοπο, αφού ο m είναι ελεύθερος τετραγώνου.

Αν $p = 2$ και $m \equiv 3 \mod 4$ τότε

$$2 \mid 1 - m = (1 - \sqrt{m})(1 + \sqrt{m})$$

συνεπώς $2 \mid (1 - \sqrt{m})$ ή $2 \mid (1 + \sqrt{m})$. Άρα $4 \mid (1 - m)$ και $m \equiv 1 \mod 4$, άτοπο.

Επομένως $p \cong \pi\pi'$ και αρκεί να δείξουμε ότι $\pi \cong \pi'$. Γράφουμε το

$$\pi = \frac{a + b\sqrt{D}}{2}, a, b \in \mathbb{Z}, a \equiv bD \mod 2$$

$$\pi' = \frac{a - b\sqrt{D}}{2}, a, b \in \mathbb{Z}, a \equiv bD \mod 2$$

άρα

$$\pi - \pi' = b\sqrt{D}.$$

Τώρα $\pi \mid p \mid D = \sqrt{D}\sqrt{D}$ συνεπώς $\pi \mid \sqrt{D}$ και έχουμε $\pi \mid (\pi - \pi')$, άρα $\pi \mid \pi'$ και καταλήγουμε στο $\pi \cong \pi'$, δηλαδή $p \cong \pi^2$.

Αντιστρόφως έστω ότι $p \cong \pi^2$ άρα $\pi' \cong \pi$ συνεπώς $\pi \mid \pi'$ και $\pi \mid (\pi - \pi')$ οπότε $\pi \mid (\pi - \pi') \mid b\sqrt{D}$ και τελικά $p \mid b^2D$.

Θα δείξουμε ότι $p \nmid b$. Αν $p \neq 2$ και $p \mid b$ τότε αφού

$$p \cong \frac{a^2 - b^2D}{4} \Rightarrow p \mid a \Rightarrow p^2 \mid \frac{a^2 - b^2D}{4} \cong p,$$

άτοπο.

Αν πάλι $p = 2$ και $p \mid b$ τότε η

$$2 \cong \frac{a^2 - Db^2}{4}$$

δίνει για $D \equiv 0 \mod 4$

$$2 \equiv \left(\frac{a}{2}\right)^2 \mod 4$$

το οποίο είναι άτοπο, ενώ για $D \equiv 1 \mod 4$ δίνει

$$2 \cong \left(\frac{a}{2}\right)^2 - \left(\frac{b}{2}\right)^2 \mod 4$$

το οποίο είναι και πάλι άτοπο. Δηλαδή $p \nmid b$ άρα $p \mid D$ το οποίο εξ ορισμού δίνει $\left(\frac{D}{p}\right) = 0$.

Θα αποδείξουμε τώρα το 2.

Έστω $\left(\frac{D}{p}\right) = 1$. Αν $p \neq 2$, τότε η ισοδυναμία

$$x^2 \equiv D \mod p,$$

έχει λύση. Για έναν πρώτο διαιρέτη $\pi \mid p$ στο K, ισχύει

$$(x - \sqrt{D})(x + \sqrt{D}) \equiv 0 \mod \pi$$

και, χωρίς περιορισμό της γενικότητας, υποθέτουμε ότι

$$x - \sqrt{D} \equiv 0 \mod \pi.$$

Η τελευταία όμως ισοδυναμία δεν ισχύει για το p διότι

$$\frac{x - \sqrt{D}}{p} \notin R_K,$$

οπότε $p \nmid \pi$, δηλαδή $p \cong \pi\pi'$. Αν ήταν $\pi \cong \pi'$, τότε λόγω του 1. θα είχαμε $p \mid D$, το οποίο είναι άτοπο.

Αν τώρα $p = 2$, τότε $\left(\frac{D}{p}\right) = 1$ δίνει εξ ορισμού $D \equiv 1 \mod 8$ συνεπώς

$$\left(1 - \frac{1+\sqrt{D}}{2}\right)\left(1 - \frac{1-\sqrt{D}}{2}\right) = \frac{1-D}{4} \equiv 0 \mod 2$$

οπότε για κάποιον πρώτο διαιρέτη π του 2 στο K θα έχουμε

$$1 - \frac{1+\sqrt{D}}{2} \equiv 0 \mod \pi,$$

ενώ, όπως παραπάνω, $2 \nmid \left(1 - \frac{1+\sqrt{D}}{2}\right)$ στο K, δηλαδή $2 \cong \pi\pi'$ με $\pi \nmid \pi'$.

Αντιστρόφως, έστω $p \cong \pi\pi'$ με $\pi \nmid \pi'$,

$$\pi = \frac{a + b\sqrt{D}}{2} \qquad \pi' = \frac{a - b\sqrt{D}}{2}.$$

Στην απόδειξη του 1. δείξαμε ότι $p \nmid b$.

$$p \cong \frac{a^2 - Db^2}{4} \Rightarrow \frac{a^2 - Db^2}{4} \equiv 0 \mod p \text{ στο },$$

οπότε για $p \neq 2$ έχουμε

$$a^2 \equiv Db^2 \mod p \Rightarrow \left(\frac{Db^2}{p}\right) = \left(\frac{D}{p}\right) = 1,$$

αφού $p \nmid b$. Τέλος για $p = 2$

$$a^2 \equiv Db^2 \mod 8 \Rightarrow D \equiv 1 \mod 8 \Rightarrow \left(\frac{D}{2}\right) = 1.$$

□

Παρατήρηση II.4.4. Αφού λόγω της υποθέσεως ότι R_K περιοχή μονοσήμαντης ανάλυσης το κύριο ιδεώδες που παράγεται από τον πρώτο αριθμό π, $(\pi) = \pi R_K$ είναι πρώτο ιδεώδες, θα μπορούσαμε να γράψουμε το θεώρημα II.4.3 και για πρώτα ιδεώδη. Το παραπάνω θεώρημα ισχύει για κάθε δακτύλιο R_Kακόμη και αν δεν είναι περιοχή μονοσήμαντης ανάλυσης.

II.5 Ιδεώδη και αριθμός κλάσεων

Ορισμός II.5.1. Ένα υποσύνολο A του K θα λέγεται ιδεώδες του K αν και μόνο αν ισχύουν τα παρακάτω:

1. Για κάθε $a_1, a_2 \in A$ η διαφορά $a_1 - a_2 \in A$
2. Για κάθε $\lambda \in R_K$ και για κάθε $a \in A$ το $\lambda a \in A$
3. $A \neq (0)$
4. Υπάρχει $R_K \ni \delta \neq 0$, ώστε $\delta A \subseteq R_K$.

Αν $A \subseteq R_K$ θα λέγεται *ακέραιο ιδεώδες*, αλλιώς θα λέγεται *κλασματικό*.

Σημαντική παρατήρηση: Έχουμε ήδη διαπιστώσει ότι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών R_K, ενός αλγεβρικού σώματος αριθμών K δεν είναι, εν γένει, περιοχή μονοσήμαντης ανάλυσης. Ισχύει όμως το

Θεώρημα II.5.2. *Αν* K *αλγεβρικό σώμα αριθμών και* R_K *η περιοχή των ακεραίων αλγεβρικών αριθμών αυτού, τότε κάθε ακέραιο ιδεώδες* A *του* K *αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών, δηλαδή*

$$A = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_s^{\alpha_s},$$

με P_i *πρώτα ιδεώδη του* R_K *και* $\alpha_i \in \mathbb{N}$ *για* $i = 1, 2, \dots, s$.

Αυτό είναι άμεση συνέπεια της ιδιότητας της περιοχής R_K να είναι *περιοχή του Dedekind*.

Μπορούμε λοιπόν να ρωτήσουμε το εξής: Αν $p\mathbb{Z}$ είναι ένα κύριο πρώτο ιδεώδες του $\mathbb{Z}$. Αν θεωρήσουμε το κύριο ιδεώδες pR_K του δακτυλίου R_K τότε αυτό δεν είναι κατ' ανάγκη πρώτο. Ο νόμος ανάλυσης σε τετραγωνικά σώματα αριθμών απαντά ακριβώς σε αυτό το ερώτημα:

Θεώρημα II.5.3 (Νόμος ανάλυσης, στα τετραγωνικά σώματα αριθμών, γενική περίπτωση)**.** *Το ιδεώδες* pR_K *στον δακτύλιο ακεραίων του τετραγωνικού σώματος αριθμών* $\mathbb{Q}(\sqrt{m})$ *γράφεται ως γινόμενο πρώτων ιδεωδών του* R_K *ως εξής:*

$$\begin{aligned}
pR_K &= Q^2, N(Q) = p && \text{αν} \quad \left(\frac{D_K}{p}\right) = 0 \\
pR_K &= Q, N(Q) = p^2 && \text{αν} \quad \left(\frac{D_K}{p}\right) = -1 \\
pR_K &= Q_1 Q_2, N(Q_1) = N(Q_2) = p && \text{αν} \quad \left(\frac{D_K}{p}\right) = 1
\end{aligned}$$

Απόδειξη. Η απόδειξη θα δοθεί ως ειδική περίπτωση του γενικού θεωρήματος αργότερα. □

II.5.1 Αριθμός Κλάσεων Ιδεωδών

Στο σύνολο όλων των ιδεωδών (κλασματικών και ακέραιων) ορίζουμε *ισοδυναμία ιδεωδών*:

$$A \sim B \text{ αν και μόνο αν υπάρχει } K \ni \xi \neq 0, A = (\xi) \cdot B$$

και *ισοδυναμία ιδεωδών με στενή έννοια*:

$$A \sim_\sigma B \text{ αν και μόνο αν υπάρχει } K \ni \xi, N(\xi) > 0, A = (\xi) \cdot B$$

Ορισμός II.5.4. Ο αριθμός κλάσεων $h(D)$ (αντίστοιχα ο αριθμός κλάσεων με τη στενή έννοια $h_\sigma(D)$) ορίζεται να είναι το πλήθος των κλάσεων σε κάθε μία από τις παραπάνω κλάσεις ισοδυναμίας.

Χωρίς απόδειξη αναφέρουμε το

Θεώρημα II.5.5. *Για κάθε αλγεβρικό σώμα αριθμών* K *η ομάδα κλάσεων ιδεωδών του* K *είναι πεπερασμένη.*

Το σύνολο όλων των ιδεωδών ακεραίων και κλασματικών I_K ενός αλγεβρικού σώματος αριθμών K αποτελεί αβελιανή ομάδα. Το σύνολο των κυρίων ιδεωδών αυτού αποτελεί αβελιανή ημιομάδα της I_Kτ την οποία θα συμβολίζουμε με H_K. Το σύνολο των κλάσεων ισοδυναμίας είναι η ομάδα πηλίκο

$$\mathfrak{K}_K = \frac{I_K}{H_K},$$

και λέγεται *ομάδα κλάσεων ιδεωδών*.

Ανάλογες ιδιότητες ισχύουν και για την ομάδα κλάσεων ιδεωδών με τη στενή έννοια.

Ένα σημαντικότατο πρόβλημα της Αλγεβρικής Θεωρίας Αριθμών είναι δοθέντος σώματος K, ο προσδιορισμός του αριθμού κλάσεων ιδεωδών αυτού.

Στην περίπτωση που το K είναι μιγαδικό τετραγωνικό σώμα αριθμών, διακρίνουσας D_K αυτό είναι εύκολο, αφού οι κλάσεις ιδεωδών του K αντιστοιχούν αμφιμονοσήμαντα στις κλάσεις ισοδυναμίας (θετικά ορισμένων) τετραγωνικών μορφών διακρίνουσας D_K, σύμφωνα με το ακόλουθο

Θεώρημα II.5.6. *Έστω* $K = \mathbb{Q}(\sqrt{m})$ *μιγαδικό τετραγωνικό σώμα αριθμών διακρίνουσας* D_K. *Υπάρχει μια αμφιμονοσήμαντη αντιστοιχία ανάμεσα στις κλάσεις ισοδυναμίας (θετικά ορισμένων) τετραγωνικών μορφών διακρίνουσας* D *και στις κλάσεις ισοδυναμίας με στενή έννοια ιδεωδών του* K.

Η αντιστοιχία αυτή δίνεται ως εξής: Στο ιδεώδες $A = \mathbb{Z}\alpha + \mathbb{Z}\beta$ *με* $\frac{\alpha'\beta - \alpha\beta'}{\sqrt{D_K}} >$ *αντιστοιχεί η τετραγωνική μορφή*

$$f(X, Y) = aX^2 + bXY + cY^2$$

όπου

$$a = \frac{\alpha\alpha'}{N(A)}, \qquad b = \frac{\alpha\beta' + \alpha'\beta}{N(A)}, \qquad c = \frac{\beta\beta'}{N(A)}.$$

Αντιστρόφως στην τετραγωνική μορφή

$$f(X, Y) = ax^2 + bXY + cY^2,$$

αντιστοιχεί το κλασματικό ιδεώδες

$$\mathbb{Z}\lambda + \mathbb{Z}\frac{b + \sqrt{D}}{2a}\lambda,$$

όπου $\lambda \in K$ *και διαλέχτηκε ώστε* $N(\lambda)a > 0$.

Απόδειξη. Δείτε στο [13]. □

Παρατήρηση II.5.7. Αξίζει να σημειωθεί ότι για μιγαδικά τετραγωνικά σώματα αριθμών οι έννοιες ισοδυναμία ιδεωδών και ισοδυναμία ιδεωδών με τη στενή έννοια συμπίπτουν, αφού κάθε στοιχείο του σώματος K έχει θετική norm.

Δεδομένου λοιπόν ότι η τάξη της αβελιανής ομάδας $\mathfrak{K}_K = I_K/H_K$ των κλάσεων ιδεωδών του K, h είναι πεπερασμένη, έπεται ότι αν A ιδεώδες του R_K, A^h είναι κύριο ιδεώδες.

Πρόταση II.5.8. *Αν τώρα* A^μ *κύριο ιδεώδες του* K *και* $(\mu, h_K) = 1$, *τότε το* A *είναι κύριο ιδεώδες του* K

Απόδειξη. Γράφουμε $1 = x\mu + yh$, για κατάλληλα $x, y \in \mathbb{Z}$. Στη συνέχεια υπολογίζουμε ότι:

$$A = A^{x\mu + yh} = (A^\mu)^x (A^h)^y \in H_K.$$

□

II.6 Ασκήσεις

1. Να υπολογιστεί ο αριθμός κλάσεων ιδεωδών των τετραγωνικών σωμάτων αριθμών
$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-23}), \mathbb{Q}(\sqrt{-47}).$$
2. Ποιοι πρώτοι αριθμοί μπορούν να παρασταθούν ως άθροισμα δύο τετραγώνων ακεραίων αριθμών;
3. Να υπολογισθούν οι θεμελιώδεις μονάδες των (πραγματικών) τετραγωνικών σωμάτων αριθμών
$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$$
4. Ποιοι φυσικοί αριθμοί n μπορούν να παρασταθούν ως άθροισμα δύο τετραγώνων ακεραίων αριθμών;
5. Να υπολογίσετε τον αριθμό κλάσεων ιδεωδών του σώματος $K = \mathbb{Q}(\sqrt{-163})$ και να διατυπώσετε τον νόμο ανάλυσης αυτού.

Βιβλιογραφία

[1] Adams, W. W. & Goldstein, L. J. *Introduction to Number Theory*. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1976, pp. xiii+362.

[2] Cox, D. A. *Primes of the Form x^2+ny^2, Fermat, class field theory, and complex multiplication*. 2nd edition. Pure and Applied Mathematics. John Wiley & Sons, Inc., 2013, pp. xviii+356. ISBN: 978-1-118-39018-4.

[3] Gauss, C. F. *Disquisitiones Arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966, pp. xx+472.

[4] Goldman, J. R. *The Queen of Mathematics, A historically motivated guide to Number Theory*. A K Peters, Ltd., Wellesley, MA, 1998, pp. xxiv+525. ISBN: 1-56881-006-7.

[5] Halter-Koch, F. *Quadratic Irrationals, An Introduction to Classical Number Theory*. Pure and Applied Mathematics (Boca Raton). CRC Press, Boca Raton, FL, 2013, pp. xvi+415. ISBN: 978-1-4665-9183-7. URL: https://doi.org/10.1201/b14968.

[6] Hasse, H. *Vorlesungen über Zahlentheorie*. Zweite neubearbeitete Auflage. Die Grundlehren der Mathematischen Wissenschaften, Band 59. Springer-Verlag, Berlin, 1964, pp. xv+504.

[7] Hunter, J. *Αριθμοθεωρία (μετάφραση Ν. Κρητικού)*. Σύλλογος προς διάδοσιν ωφελίμων βιβλίων, 1980.

[8] Lemmermeyer, F. *Quadratische Zahlkörper: Eine Einführung mit vielen Beispielen*. Springer Berlin, 2017. ISBN: 9783662538227. URL: https://books.google.gr/books?id=z5ErDwAAQBAJ.

[9] Niven, I., Zuckerman, H. S. & Montgomery, H. L. *An Introduction to the Theory of Numbers*. Fifth. John Wiley & Sons, Inc., New York, 1991, pp. xiv+529. ISBN: 0-471-62546-9.

[10] Pollack, P. *A Conversational Introduction to Algebraic Number Theory, Arithmetic beyond $\mathbb{Z}$*. Vol. 84. Student Mathematical Library. American Mathematical Society, Providence, RI, 2017, pp. ix + 316. ISBN: 978-1-4704-3653-7.

[11] Redmond, D. *Number Theory, An introduction*. Vol. 201. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, Inc., New York, 1996, pp. xiv+749. ISBN: 0-8247-9696-9.

[12] Weil, A. *Number Theory, An approach through history from Hammurapi to Legendre, Reprint of the 1984 edition*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007, pp. xxii+377. ISBN: 978-0-8176-4565-6; 0-8176-4565-9.

[13] Zagier, D. B. *Zetafunktionen und quadratische Körper*. Eine Einführung in die höhere Zahlentheorie. [An introduction to higher number theory], Hochschultext. [University Text]. Springer-Verlag, Berlin, 1981, pp. viii+144. ISBN: 3-540-10603-0.

[14] Αντωνιάδης, Ι. Α. *Θεωρία Αριθμών κατά τον 17ο και 18ο αιώνα*. Ηράκλειο: Πανεπιστήμιο Κρήτης, 1999.

[15] Αντωνιάδης, Ι. Α. & Κοντογεώργης, Α. *Θεωρία Αριθμών και Εφαρμογές*. Κάλλιπος, 2015, pp. ix+315. ISBN: 978-618-82124-5-9. URL: https://eclass.uoa.gr/modules/document/file.php/MATH443/NumberTheoryNov2016.pdf.

[16] Λάκκης, Κ. *Θεωρία Αριθμών*. Εκδ. Ζήτη, 1990.

III

Ακέραια Εξάρτηση και δακτύλιοι του Dedekind

III.1 Απλές επεκτάσεις σωμάτων

Από το παρόν κεφάλαιο οι επεκτάσεις που θα θεωρήσουμε είναι οι λεγόμενες *σχετικές επεκτάσεις αλγεβρικών σωμάτων αριθμών*, δηλαδή K θα είναι ένα αλγεβρικό σώμα αριθμών και L μια πεπερασμένη επέκταση αυτού. Ο λόγος είναι ότι υπάρχει σημαντική ομοιότητα με τις απόλυτες επεκτάσεις όταν το σώμα K είναι αυτό των ρητών αριθμών $\mathbb{Q}$. Βέβαια υπάρχουν και διαφορές. Αυτές θα τονιστούν στη συγκεκριμένη περίπτωση και αν χρειαστεί θα περιοριστούμε και αποκλειστικά στην απόλυτη περίπτωση.

Έστω λοιπόν L/K μια επέκταση αλγεβρικών σωμάτων αριθμών. Το σώμα K έχει χαρακτηριστική 0 αφού $\mathbb{Q} \subset K$. Η επέκταση L/K είναι πεπερασμένη και διαχωρίσιμη. Επομένως είναι και απλή (Κ. Λάκκη, *Άλγεβρα*, σελ. 237 [8].

Σημείωση III.1.1. Αν $K \leq \mathbb{C}$ και $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ αλγεβρικά υπεράνω του σώματος K, τότε επαγωγικά εργαζόμενοι έχουμε ότι υπάρχει ένα $\alpha \in \mathbb{C}$ αλγεβρικό υπεράνω του K για το οποίο ισχύει

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha).$$

Από την απόδειξη του θεωρήματος των απλών επεκτάσεων συνάγεται ότι για κάθε βήμα αρκεί να βρούμε έναν ρητό αριθμό $c \in \mathbb{Q}$, για τον οποίο όλα τα στοιχεία $\alpha' + \beta' c$ είναι διαφορετικά, καθώς τα α' και β' διατρέχει ένα πλήρες σύνολο συζυγών των α και β αντιστοίχως, οπότε $K(\alpha, \beta) = K(\alpha + c\beta)$.

Παράδειγμα III.1.2. Το σώμα $K = \mathbb{Q}$ και $L = \mathbb{Q}(\sqrt{3}, \sqrt[2]{2})$. Συζυγή της $\sqrt{3}$ είναι η $\sqrt{3}$ και $-\sqrt{3}$. Συζυγή της $\sqrt[3]{2}$ είναι τα $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, όπου ω είναι μια πρωταρχική κυβική ρίζα της μονάδας.

Επομένως έχουμε

$$\sqrt{3} + \sqrt[3]{2}, -\sqrt{3} + \sqrt[3]{2}, \sqrt{3} + \omega\sqrt[3]{2}, -\sqrt{3} + \omega\sqrt[3]{2}, \sqrt{3} + \omega^2\sqrt[3]{2}, -\sqrt{3} + \omega^2\sqrt[3]{2}$$

όλα μεταξύ τους διαφορετικά. Συνεπώς,

$$\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{3} + \sqrt[3]{2}).$$

Η επέκταση L/K είναι πεπερασμένη. Έστω $[L : K] = n$. Αφού $L = K(\alpha)$ ισχύει

$$[L : K] = \deg \mathrm{Irr}(\alpha, K) = n.$$

Αφού το α είναι διαχωρίσιμο υπεράνω του K, το ανάγωγο πολυώνυμο του α υπεράνω του K έχει όλες τις ρίζες του απλές.

Έστω K αλγεβρικό σώμα αριθμών και L πεπερασμένη επέκταση αυτού. Αφού η χαρακτηριστική του σώματος K είναι 0, έπεται ότι η επέκταση είναι διαχωρίσιμη, άρα υπάρχει ένα στοιχείο

$\theta \in L$, τέτοιο ώστε $L = K(\theta)$. Έστω $n = [L : K]$ ο βαθμός της επέκτασης L/K, και έστω $\mathrm{Irr}(\theta, K)$ το ανάγωγο πολυώνυμο του θ το οποίο είναι προφανώς βαθμού n. Όλες οι ρίζες του $\mathrm{Irr}(\theta, K)$ είναι απλές, αφού η επέκταση είναι διαχωρίσιμη.

Έστω $\widetilde{K}$ μια αλγεβρική θήκη του σώματος K που περιέχει το L.

Ορισμός III.1.3. Κάθε μονομορφισμός σωμάτων $\sigma : L \to \widetilde{K}$ ώστε $\sigma|_K = \mathrm{Id}_K$ θα λέγεται μια *εμφύτευση της επέκτασης* L/K στο $\widetilde{K}$.

Αν $\alpha \in L$, τότε

$$\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1},$$

με $a_i \in K$. Σε αυτή την περίπτωση η εμφύτευση $\sigma(\alpha)$ δίνεται από

$$\sigma(\alpha) = a_0 + a_1\sigma(\theta) + \cdots + a_{n-1}\sigma(\theta^{n-1}).$$

Επιπλέον, είναι σαφές ότι $\sigma(\theta)$ είναι μια ρίζα του αναγώγου πολυωνύμου $\mathrm{Irr}(\theta, K)$

$$f(x) := \mathrm{Irr}(\theta, K) = \prod_{i=1}^{n}(x - \theta^{(i)}),$$

όπου $\theta^{(1)} = \theta$, αφού

$$0 = \sigma(f(\theta)) = f(\sigma(\theta)).$$

Ώστε, όλες οι εμφυτεύσεις δίνονται με την παρακάτω επέκταση της ταυτότητας του K,

$$\begin{array}{ccc} L = K(\theta) & \xrightarrow{\sigma_i} & L_i = K(\theta^{(i)}) \\ \Big| & & \Big| \\ K & \xrightarrow{\mathrm{Id}_K} & K \end{array}$$

Αποδείξαμε το παρακάτω

Θεώρημα III.1.4. *Υπάρχουν ακριβώς n εμφυτεύσεις του L/K στο $\widetilde{K}$.*

Ορισμός III.1.5. Οι εικόνες ενός στοιχείου $\alpha \in L$ μέσω των εμφυτεύσεων σ_i λέγονται συζυγή στοιχεία του α.

Παρατήρηση III.1.6. Τα συζυγή στοιχεία του $\alpha \in L$ δεν είναι εν γένει μεταξύ τους διαφορετικά.

Παραδείγματα III.1.7.

1. Θεωρούμε το σώμα $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$. Το ανάγωγο πολυώνυμο του $\sqrt{m}$ είναι το $\mathrm{Irr}(\sqrt{m}, \mathbb{Q}) = x^2 - m$, το οποίο έχει ρίζες τα $\pm\sqrt{m}$.

   Υπάρχουν δύο εμφυτεύσεις, η ταυτοτική $\sqrt{m} \mapsto \sqrt{m}$ και η σ η οποία στέλνει το $\sqrt{m} \mapsto -\sqrt{m}$. Δηλαδή $\sigma(a + b\sqrt{m}) = a - b\sqrt{m}$, για $a, b \in \mathbb{Q}$.

2. Θεωρούμε την κυκλοτομική επέκταση $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, όπου $\zeta_n = e^{2\pi i/n}$ είναι μια *πρωταρχική n-στη ρίζα του* 1. Το ανάγωγο πολυώνυμο του ζ_n είναι το n-στο *κυκλοτομικό πολυώνυμο* $\Phi_n(x)$ και ορίζεται:

   $$\Phi_n(x) = \mathrm{Irr}(\zeta_n, \mathbb{Q}) = \prod_{\substack{\nu=1 \\ (\nu,n)=1}}^{n} (x - \zeta_n^{\nu}).$$

   Η εμφύτευση σ_ν για $(n, \nu) = 1$ ορίζεται ως

   $$\begin{aligned} \sigma_\nu : \mathbb{Q}(\zeta_n) &\to \mathbb{Q}(\zeta_n) \\ \zeta_n &\mapsto \zeta_n^{\nu} \end{aligned}$$

3. Θεωρούμε την επέκταση $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Παρατηρούμε ότι το ελάχιστο πολυώνυμο του $\sqrt[3]{2}$ είναι ίσο με
$$\mathrm{Irr}(\sqrt[3]{2},\mathbb{Q}) = x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}),$$
όπου $\omega = (-1+\sqrt{-3})/2 = \zeta_3$ είναι μια πρωταρχική 3-τη ρίζα της μονάδας. Οι εμφυτεύσεις δίνονται από τον τύπο
$$\begin{aligned}\sigma_\nu : \mathbb{Q}(\sqrt[3]{2}) &\mapsto \mathbb{Q}(\sqrt[3]{2}\omega^\nu)\\ \sqrt[3]{2} &\mapsto \sqrt[3]{2}\omega^\nu\end{aligned}$$
για $\nu = 0,1,2$. Παρατηρήστε ότι μόνο για $\nu = 0$ η εικόνα της σ_ν περιέχεται στο σώμα των πραγματικών αριθμών.

Θεωρούμε τα σώματα K, L και τις διαφορετικές μεταξύ τους εμφυτεύσεις $\sigma_1,\dots,\sigma_n$ του K στο L. Οι μονομορφισμοί αυτοί θα λέγονται *γραμμικά ανεξάρτητοι* στο L αν η σχέση
$$\lambda_1\sigma_1(x) + \lambda_2\sigma_2(x) + \cdots\lambda_n\sigma_n(x) = 0 \text{ με } \lambda_i \in L$$
ισχύει για κάθε $x \in K$ μόνο αν $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

Πρόταση III.1.8. *Οι n εμφυτεύσεις του σώματος L στο σώμα $\widetilde{K}$ είναι γραμμικά ανεξάρτητες στο $\widetilde{K}$.*

Απόδειξη. Θα το αποδείξουμε με επαγωγή. Για $k = 1$ η πρόταση ισχύει, γιατί η σχέση $\lambda_1\sigma_1(x) = 0$ ισχύει για κάθε $x \in L$ έχει ως συνέπεια $\lambda_1 = 0$.

Έστω ότι η πρόταση είναι αληθής για $k-1$ το πλήθος διαφορετικές εμφυτεύσεις του L στο $\widetilde{K}$. Θα αποδείξουμε ότι η πρόταση ισχύει για k το πλήθος εμφυτεύσεις του L στο $\widetilde{K}$. Θεωρούμε τη σχέση
$$\lambda_1\sigma_1(x) + \lambda_2\sigma_2(x) + \cdots + \lambda_k\sigma_k(x) = 0 \text{ με } \lambda_i \in \widetilde{K} \text{ για κάθε } x \in L \qquad \text{(III.1)}$$
Θεωρούμε ένα στοιχείο $a \in L$, $a \neq 0$ και γράφουμε την (III.1) για το στοιχείο ax οπότε έχουμε
$$\lambda_1\sigma_1(a)\sigma_1(x) + \lambda_2\sigma_2(a)\sigma_2(x) + \cdots + \lambda_k\sigma(a)\sigma_k(x) = 0 \text{ με } \lambda_i \in \widetilde{K} \text{ για κάθε } x \in L \qquad \text{(III.2)}$$
Πολλαπλασιάζουμε την (III.1) με $\sigma_k(a)$ και αφαιρούμε από την (III.2) για να πάρουμε
$$\lambda_1(\sigma_1(a) - \sigma_k(a))\sigma_1(x) + \lambda_2(\sigma_1(a) - \sigma_k(a))\sigma_2(x) + \cdots + \lambda_{k-1}(\sigma_1(a) - \sigma_k(a))\sigma_{k-1}(x) = 0$$
η οποία ισχύει για κάθε $x \in L$. Σύμφωνα με την επαγωγική σχέση έχουμε
$$\lambda_i((\sigma_1(a) - \sigma_k(a))) = 0 \text{ για κάθε } i = 1,2,\dots,k-1.$$
Επειδή οι σχέσεις αυτές ισχύουν για κάθε $a \in L$ και οι ισομορφισμοί $\sigma_1,\dots,\sigma_k$ είναι διαφορετικοί μεταξύ τους έχουμε ότι $\lambda_1 = \cdots\lambda_{k-1} = 0$ και τελικά από την (III.1) έχουμε επίσης $\lambda_k\sigma_k(x) = 0$ για κάθε $x \in L$ από όπου καταλήγουμε στο $\lambda_k = 0$. □

Αν F είναι το σώμα των σταθερών στοιχείων των n εμφυτεύσεων, δηλαδή το σώμα των στοιχείων $a \in L$ με
$$\sigma_1(a) = \sigma_2(a) = \cdots = \sigma_n(a)$$
τότε ισχύει ότι $[L:F] \geq n$ Πράγματι, έστω $[K:F] = m < n$ και $\omega_1,\omega_2,\dots,\omega_m$ είναι μια βάση της επέκτασης L/F. Θεωρούμε το γραμμικό σύστημα
$$x_1\sigma_1(\omega_i) + x_2\sigma_2(\omega_i) + \cdots + x_n\sigma_n(\omega_i) = 0 \text{ για } i = 1,2,\dots,m$$
Το πλήθος των εξισώσεων είναι μικρότερο από αυτό των αγνώστων. Επομένως, το σύστημα θα έχει τουλάχιστον μία λύση την $\xi_1,\xi_2,\dots,\xi_n$ διάφορη της τετριμμένης. Ισχύει
$$\xi_1\sigma_1(a) + \xi_2\sigma_2(a) + \cdots\xi_n\sigma_n(a) = 0 \text{ για κάθε } a \in L.$$
Το τελευταίο όμως είναι άτοπο, γιατί οι εμφυτεύσεις $\sigma_1,\dots,\sigma_n$ είναι γραμμικά ανεξάρτητες.

Άρα για το σώμα των σταθερών στοιχείων F έχουμε $[L:F] \geq n$ και λόγω ότι $K \subset F$ και $[L:K] = n$ έπεται ότι $K = F$.

Θεώρημα III.1.9. *Ισχύει για $\alpha \in L$ ότι $\alpha \in K$ αν και μόνο αν $\sigma_\nu(\alpha) = \alpha$ για κάθε $\nu = 1,2,\dots,n$.*

III.2 Ιδεώδη αλγεβρικού σώματος αριθμών

Έστω R ακέραια περιοχή με μοναδιαίο και K το σώμα πηλίκων αυτού.

Ορισμός III.2.1. Ένα υποσύνολο A του σώματος K θα λέγεται *ιδεώδες του* K αν και μόνο αν

1. Για κάθε $a_1, a_2 \in A$ έχουμε ότι $a_1 - a_2 \in A$
2. Για κάθε $\lambda \in R$ και για κάθε $a \in A$ έχουμε ότι $\lambda a \in A$
3. $A \neq \langle 0 \rangle$
4. Υπάρχει $K \ni \delta \neq 0$ ώστε $\delta A \subset R$

Αν $A \subset R$ τότε το A θα λέγεται *ακέραιο ιδεώδες* αλλιώς θα λέγεται *κλασματικό*.

Στο σύνολο των ιδεωδών ορίζουμε ισοδυναμία ιδεωδών

$$A \sim B \Leftrightarrow \text{ υπάρχει } \xi \neq 0, \xi \in K \text{ με } A = \langle \xi \rangle B.$$

Ένα κλασματικό ιδεώδες του K δεν είναι τίποτε άλλο παρά ένα, μη μηδενικό, R-module για το οποίο ισχύει επιπλέον η ιδιότητα

$$\text{Υπάρχει } \delta \in K \backslash \{0\} \text{ με } \delta A \subset R.$$

Αν A, B είναι δύο ιδεώδη του K τότε ορίζεται το γινόμενό τους

$$A \cdot B = \left\{ \sum_{\text{πεπερασμένο}} a_i b_i : a_i \in A, b_i \in B \right\}$$

όπου το άθροισμα είναι πεπερασμένο. Προφανώς το γινόμενο AB είναι επίσης R-module και μάλιστα ιδεώδες του K διότι, αν $xA \subset R$ και $yB \subset R$ και

$$\alpha = a_1 b_1 + a_2 b_2 + \cdots + a_m b_m,$$

τυχαίο στοιχείο του $A \cdot B$ τότε

$$(xy)\alpha = (xa_1)(yb_1) + (xa_2)(yb_2) + \cdots + (xa_m)(yb_m) \in R.$$

Από τον ορισμό του γινομένου ιδεωδών προκύπτει ότι

$$A \cdot B = B \cdot A$$

και

$$(A \cdot B) \cdot \Gamma = A(B \cdot \Gamma).$$

Ακόμη το ακέραιο ιδεώδες R είναι μοναδιαίο

$$A \cdot R = R \cdot A = A.$$

Ώστε, το σύνολο των ιδεωδών του K με πράξη τον πολλαπλασιασμό ιδεωδών αποτελεί αντιμεταθετική ημιομάδα με μοναδιαίο. Το ερώτημα τώρα είναι αν μερικά (ή όλα) από τα ιδεώδη αυτά είναι αντιστρέψιμα.

Ορισμός III.2.2. Ένας αντιμεταθετικός δακτύλιος R με μοναδιαίο, λέγεται *δακτύλιος της Noether* όταν ισχύει μία (συνεπώς και οι τρεις) από τις παρακάτω ισοδύναμες προτάσεις:

1. Κάθε αύξουσα ακολουθία ιδεωδών γίνεται σταθερά

2. Κάθε διάφορο του κενού σύνολο ιδεωδών του R έχει μέγιστα στοιχεία

3. Κάθε ιδεώδες του R είναι πεπερασμένα παραγόμενο.

Ας αποδείξουμε την ισοδυναμία των παραπάνω τριών προτάσεων. Θα δείξουμε πρώτα ότι από το (1) συνεπάγεται το (2). Πράγματι, έστω Ω ένα μη κενό σύνολο ιδεωδών του δακτυλίου R. Έστω ότι $A_0 \in \Omega$. Αν το A_0 δεν είναι μέγιστο, τότε υπάρχει $A_1 \in \Omega$ με $A_0 \subsetneq A_1$. Αν και το A_1 δεν είναι μέγιστο, τότε υπάρχει $A_2 \in \Omega$ με $A_0 \subsetneq A_1 \subsetneq A_2$. Συνεχίζοντας με αυτόν τον τρόπο καταλήγουμε σε μία γνήσια αύξουσα ακολουθία στοιχείων του Ω που είναι τελικά σταθερή.

Για να δείξουμε ότι από το (2) συνεπάγεται το (3) θεωρούμε το σύνολο W των πεπερασμένα παραγόμενων ιδεωδών που περιέχονται σε ένα δεδομένο ιδεώδες A. Το σύνολο W έχει ένα μέγιστο στοιχείο A_0 το οποίο οφείλει να ταυτιστεί με το A. Σε διαφορετική περίπτωση το A θα είχε ένα στοιχείο $x \in A \backslash A_0$ και το $A_0 + xR \in W$ θα ήταν γνήσια μεγαλύτερο του A_0.

Τέλος θα δείξουμε ότι από το (3) συνεπάγεται το (1). Θεωρούμε μια αύξουσα ακολουθία ιδεωδών $A_0 \subset A_1 \subset A_2 \subset \cdots$. Η ένωση $A = \bigcup_{i=0}^{\infty} A_i$ είναι ιδεώδες και συνεπώς πεπερασμένα παραγόμενο, δηλαδή $A = \langle a_1, \ldots, a_r \rangle$. Υπάρχει κάποιο κ ώστε $a_1, \ldots, a_r \in A_\kappa$ και η αύξουσα ακολουθία σταθεροποιείται στο A_κ.

Πρόταση III.2.3. *Κάθε δακτύλιος κυρίων ιδεωδών είναι δακτύλιος της Noether.*

Ορισμός III.2.4. Έστω R αντιμεταθετικός δακτύλιος με μοναδιαίο και M ένα R-module. Το module M θα λέγεται *module της Noether* αν ισχύει μία (και συνεπώς και οι τρεις) από τις παρακάτω ισοδύναμες προτάσεις:

1. Κάθε αύξουσα ακολουθία υπομodules του M γίνεται σταθερά.

2. Κάθε διάφορη του κενού οικογένεια υπομodules του M περιέχει μέγιστα στοιχεία.

3. Κάθε υπομodule του M είναι πεπερασμένα παραγόμενο.

Σημείωση III.2.5. Η απόδειξη της ισοδυναμίας των παραπάνω προτάσεων γίνεται ακριβώς όπως και στα ιδεώδη, [7, σελ. 20].

Θεώρημα III.2.6.
- *Το ευθύ άθροισμα πεπερασμένου πλήθους modules της Noether είναι module της Noether.*
- *Η ομομορφική εικόνα ενός module της Noether είναι επίσης module της Noether.*

Η απόδειξη του θεωρήματος στηρίζεται στο

Λήμμα III.2.7. *Αν M είναι ένα module της Noether και η ακολουθία*

$$0 \to M_1 \hookrightarrow M \xrightarrow{\phi} M_2 \to 0 \tag{III.3}$$

είναι ακριβής, τότε τα modules M_1 και M_2 είναι επίσης modules της Noether. Αντιστρόφως, αν M_1, M_2 είναι modules της Noether και η ακολουθία (III.3) είναι ακριβής, τότε και το M είναι module της Noether.

Απόδειξη. Αφού M_1 υπο-module του M, έπεται ότι κάθε υπο-module του M_1 θα είναι και υπο-module του M, δηλαδή M_1 είναι module της Noether.

Έστω τώρα $\{I_m\}_{m \in \mathbb{N}}$ μια άπειρη αύξουσα ακολουθία υπό-modules του M_2. Για κάθε $m \in \mathbb{N}$ τώρα ορίζουμε

$$I'_m = \{a \in M | \phi(a) \in I_m\}.$$

Προφανώς I'_m είναι ένα υπό-module του M και μάλιστα αν $I_{m_1} \subsetneq I_{m_2}$, τότε $I'_{m_1} \subsetneq I'_{m_2}$, δηλαδή $\{I'_m\}$ είναι μια άπειρη αύξουσα ακολουθία υπό-modules του M, άτοπο, συνεπώς M_2 είναι ένα module της Noether.

Αντιστρόφως τώρα. Έστω $\{I_m\}_{m\in\mathbb{N}}$ μια τυχούσα αύξουσα ακολουθία υπό-modules του M. Θεωρούμε τις εικόνες των I_m στο M_2,

$$J_m = \{a \in M_2 | \exists b \in I_m, \phi(b) = a\}.$$

Η $\{J_m\}_{m\in\mathbb{N}}$ είναι αύξουσα ακολουθία υπό-modules του M_2 και συνεπώς γίνεται σταθερή, δηλαδή υπάρχει $n_1 \in \mathbb{N}$ με

$$J_{n_1} = J_{n_1+1} = J_{n_1+2} = \cdots$$

Ομοίως θεωρούμε την αύξουσα ακολουθία $\{N_m\}_{m\in\mathbb{N}}$, $N_m = M_1 \cap I_m$, η οποία γίνεται σταθερά, δηλαδή υπάρχει ένα n_2 με

$$N_{n_2} = N_{n_2+1} = N_{n_2+2} = \cdots$$

Έστω $\lambda = \max\{n_1, n_2\}$ και έστω $r \geq \lambda$. Προφανώς $I_\lambda \subset I_r$. Έστω $\alpha \in I_r$ συνεπώς $\phi(\alpha) \in J_r = J_\lambda$. Συνεπώς υπάρχει $\beta \in I_\lambda$ με $\phi(\alpha) = \phi(\beta)$, δηλαδή $\phi(\alpha - \beta) = 0$ συνεπώς το $\alpha - \beta \in \ker\phi = \mathrm{Im}(i)$ και $\alpha - \beta \in M_1$. Τώρα $\alpha \in I_r$, $b \in I_\lambda$, $I_\lambda \subset I_r$ συνεπώς $\alpha - \beta \in I_r \cap M_1$. Το $\alpha - \beta \in N_r = N_\lambda = M_1 \cap I_\lambda$ οπότε $\alpha - \beta \in I_\lambda$ και αφού $\beta \in I_\lambda$ έχουμε $\alpha \in I_\lambda$, δηλαδή $I_\lambda = I_r$ και το M είναι module της Noether.

□

Για να αποδείξουμε το θεώρημα III.2.6 παρατηρούμε ότι το δεύτερο μέρος έχει ήδη αποδειχτεί στην απόδειξη του λήμματος III.2.7. Για το πρώτο μέρος αρκεί να θεωρήσουμε την ακριβή ακολουθία

$$0 \to A \to A \oplus B \to B \to 0$$

και να εφαρμόσουμε επαγωγή.

Από εδώ και κάτω το R θα είναι μια ακέραια περιοχή (δηλαδή αντιμεταθετικός δακτύλιος με μοναδιαίο, χωρίς διαιρέτες του μηδενός) και K θα είναι το σώμα πηλίκων αυτού.

Αν A είναι ιδεώδες του K, τότε με A^* θα συμβολίζουμε το σύνολο

$$A^* = \{x \in K | xA \subset R\} \text{ Ανάστροφο του } A.$$

Προφανώς το A^* είναι R-module, διάφορο του κενού. Είναι ιδεώδες του K, διότι αν $y \in A$, $y \neq 0$ και $r \in R$ τέτοιο ώστε $ry \in R$ τότε $ry \in R \cap A$ και για κάθε $a \in A^*$ έχουμε ότι $ary \in R$.

Αν A_1 και A_2 είναι ιδεώδη του K τέτοια ώστε $A_1 \subset A_2$ τότε $A_2^* \subset A_1^*$. Ακόμα ισχύει ότι $A^*A \subset R$, αλλά εν γένει η ισότητα δεν ισχύει.

Έστω

$$\mathcal{I} = \{A | A \text{ ιδεώδες του } K\}.$$

Υποθέτουμε ότι κάποιο ιδεώδες A του I έχει αντίστροφο, δηλαδή υπάρχει $A^{-1} \in \mathcal{I}$, με $A^{-1}A = R$. Αν $x \in A^{-1}$, αφού $A^{-1}A = R$ έχουμε ότι $xa \in R$ για κάθε $a \in A$, συνεπώς $A^{-1} \subset A^*$.

Από την άλλη μεριά $AA^* \subset R$ συνεπώς $A^{-1}(AA^*) \subset A^{-1}R$, δηλαδή $A^* \subset A^{-1}$ και τελικά $A^* = A^{-1}$.

Ώστε αν το ιδεδώδες A έχει αντίστροφο αυτό ταυτίζεται με το ανάστροφό του.

Λήμμα III.2.8. *Κάθε κύριο ιδεώδες του K είναι αντιστρέψιμο και επομένως το σύνολο*

$$H = \{aR | a \in K\backslash\{0\}\}$$

είναι πολλαπλασιαστική ομάδα.

Απόδειξη. Προφανώς για κάθε ιδεώδες $\langle a\rangle = aR, a \in K\backslash\{0\}$ υπάρχει $a^{-1} \in K\backslash\{0\}$ ώστε $\langle a^{-1}\rangle = a^{-1}R$ να ικανοποιεί

$$aRa^{-1}R = 1 \cdot R = R.$$

□

Αν $A_1 \cdot A_2 = R$, τότε $A_2 = A_1^{-1}$. Πράγματι από τη σχέση $A_1A_2 = R$ έπεται ότι $A_2 \subset A_1^*$, οπότε $R = A_1A_2 \subset A_1A_1^* \subset R$. Επομένως $A_1A_1^* = R$. Επίσης

$$A_1^* = A_1^*R = A_1^*(A_1A_2) = (A_1^*A_1)A_2 = RA_2 = A_2.$$

Τέλος είναι προφανές ότι το αντίστροφο του γινομένου δύο αντιστρέψιμων κλασματικών ιδεωδών ισούται με το αντίστροφο γινόμενο των αντιστρόφων τους και ότι ισχύει $A = (A^{-1})^{-1}$.

Πρόταση III.2.9. *Έστω*

$$\mathcal{I}' = \{A \in \mathcal{I} : \text{ ώστε υπάρχει } A^{-1} \in \mathcal{I}, AA^{-1} = R\}.$$

Τότε το $\mathcal{I}'$ είναι πολλαπλασιαστική ομάδα.

Απόδειξη. Αν $A \in \mathcal{I}', B \in \mathcal{I}'$, τότε $A \cdot B \in \mathcal{I}'$ και αν $A \in \mathcal{I}'$, τότε $A^{-1} \in \mathcal{I}'$. □

Ορισμός III.2.10. Έστω R μια ακέραια περιοχή και K το σώμα πηλίκων αυτής. Ο δακτύλιος R θα λέγεται *δακτύλιος του Dedekind* ακριβώς τότε αν κάθε ιδεώδες του K έχει αντίστροφο.

Δύο σπουδαίες ιδιότητες ενός *δακτυλίου του Dedekind* δίνονται από το παρακάτω:

Θεώρημα III.2.11. *Έστω R δακτύλιος του Dedekind. Τότε ο R είναι δακτύλιος της Noether και κάθε πρώτο μη-μηδενικό ιδεώδες του R είναι μέγιστο.*

Απόδειξη. Έστω $A \neq \langle 0 \rangle$ ιδεώδες του R. Από τη σχέση $A \cdot A^{-1} = R$ έπεται ότι υπάρχουν $a_i \in A$ και $b_i \in A^{-1}$, $1 \leq i \leq m$ ώστε

$$1 = a_1b_1 + a_2b_2 + \cdots + a_mb_m.$$

Τώρα αν $x \in A$ έχουμε ότι

$$x = (xb_1)a_1 + \cdots (xb_m)a_m$$

με $xb_j \in R$. Συνεπώς

$$A = a_1R + \cdots a_mR,$$

δηλαδή το ιδεώδες A είναι πεπερασμένα παραγόμενο και ο R είναι δακτύλιος της Noether.

Έστω τώρα $P \neq \langle 0 \rangle$ ένα πρώτο ιδεώδες του R και έστω N ένα μέγιστο ιδεώδες του R που περιέχει το P. Αφού $P \subset N$ έχουμε $PN^{-1} \subset N \cdot N^{-1} = R$, δηλαδή PN^{-1} είναι ακέραιο ιδεώδες του K. Αφού $(PN^{-1})N = P$ και P πρώτο έχουμε ότι $PN^{-1} \subset P$ ή $N \subset P$.

Πράγματι αν γενικά $A \cdot B \subset P$ με A, B γνήσια ιδεώδη του R, τότε $A \subset P$ ή $B \subset P$. Αν κάθε στοιχείο $b \in B$ ανήκει στο P, τότε $B \subset P$ και έχουμε τελειώσει. Αν υπάρχει $b \in B$ με $b \notin P$, θεωρούμε το γινόμενο $a \cdot b$ με $a \in A$ τυχαίο. Έχουμε ότι $ab \in A \cdot B \subset P$ και από τον ορισμό του πρώτου ιδεώδους $a \in P$.

Επιστρέφουμε στην απόδειξη του θεωρήματος. Αν ισχύει $PN^{-1} \subset P$, τότε $N^{-1} \subset P^{-1}PN^{-1} \subset P^{-1}P = R$. Προφανώς $R \subset N^{-1}$ διότι για κάθε $x \in R$, $xN \subset R$ και επομένως $N^{-1} = R$ δηλαδή $N = R$, άτοπο.

Αν $N \subset P$, τότε $N = P$ δηλαδή P μέγιστο. □

III.3 Ακέραια εξάρτηση

Έστω R ακέραια περιοχή και K το σώμα πηλίκων αυτής.

Ορισμός III.3.1. Ένα στοιχείο $x \in K$ θα λέγεται R-*ακέραιο* αν υπάρχουν $a_i \in R$, $0 \leq i \leq n-1$ ώστε

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

Σημείωση III.3.2. Μπορούσαμε αντί για K να πάρουμε L σώμα με $R \subset L$. Αν R σώμα, τότε τα ακέραια στοιχεία του L υπεράνω του R συμπίπτουν με τα αλγεβρικά υπεράνω του R.

Θεώρημα III.3.3. *Έστω $x \in L$. Ισχύουν ισοδύναμα:*

1. *Το x είναι R-ακέραιο*
2. *Ο δακτύλιος $R[x]$ που παράγεται από τα R και x είναι πεπερασμένα παραγόμενος.*
3. *Υπάρχει ένα πεπερασμένα παραγόμενο μη-μηδενικό R-module $M \subset K$, τέτοιο ώστε $xM \subset M$*

Απόδειξη. Για να δείξουμε ότι $(1) \Rightarrow (2)$ παρατηρούμε ότι ο δακτύλιος $R[x]$ παράγεται από τα $1, x, x^2, \ldots, x^{n-1}$

Για να δείξουμε ότι $(2) \Rightarrow (3)$ παρατηρούμε ότι αρκεί να πάρουμε για $M := R[x]$.

Τέλος θα δείξουμε ότι $(3) \Rightarrow (1)$. Έστω ότι το πεπερασμένα παραγόμενο R module M γράφεται ως

$$M = Rz_1 + Rz_2 + \cdots + Rz_r, z_i \in K$$

και υποθέτουμε ότι $xM \subset M$, δηλαδή $xz_i \in M$ για κάθε $i = 1, 2, \ldots, r$. Αυτό σημαίνει ότι υπάρχει πίνακας $A = (a_{ij}) \in M_{r\times r}(R)$ ώστε

$$x\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_r \end{pmatrix} = A\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_r \end{pmatrix} \to (xId_r - A)\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_r \end{pmatrix} = 0.$$

Θέτουμε $B = (xId_r - A)$ και πολλαπλασιάζουμε με τον adjoint $\widetilde{B}$ οπότε αφού

$$\widetilde{B}B = (\delta_{i,j}\det(B))$$

έχουμε

$$\widetilde{B}B\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_r \end{pmatrix} = \widetilde{B}0 = 0 \text{ συνεπώς } \det(B)I_r\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_r \end{pmatrix} = 0.$$

Επειδή $M \neq 0$ τουλάχιστον ένας γεννήτορας z_i είναι διαφορετικός του μηδενός οπότε $\det(B) = 0$. Το ανάπτυγμα της ορίζουσας μας δίνει ένα πολυώνυμο της μορφής

$$x^n + \lambda_1 x^{n-1} + \cdots + \lambda_n = 0,$$

με $\lambda_i \in R$, $1 \leq i \leq n$. Δηλαδή το x είναι R-ακέραιο. □

Επαγωγικά αποδεικνύεται ότι

Πόρισμα III.3.4. *Αν $x_1, \ldots, x_m \in L$ είναι R-ακέραια, τότε $R[x_1, x_2, \ldots, x_m]$ είναι πεπερασμένα παραγόμενο υπο-module του R-module L.*

Πόρισμα III.3.5. *Το σύνολο όλων των στοιχείων του L που είναι R-ακέραια είναι υποδακτύλιος του L που περιέχει τον R.*

Απόδειξη. Αν $a, b \in L$ είναι R-ακέραια, τότε υπάρχουν πεπερασμένα παραγόμενα R-modules M, N ώστε $aM \subset M$ και $bN \subset N$. Συνεπώς $(a-b)MN \subset MN$ και $abMN \subset MN$ δηλαδή $a-b$ και ab είναι R-ακέραια. □

Ορισμός III.3.6. Ο δακτύλιος $R' = \{x \in L | x \text{ είναι } R-\text{ακέραιο}\}$ λέγεται η ακέραια θήκη του R στο L. Αν $R' = R$, τότε ο δακτύλιος R λέγεται ακέραια κλειστός στο L. Αν $L = K$ και ο δακτύλιος R είναι ακέραια κλειστός στο K, τότε λέμε οτι ο δακτύλιος R είναι ακέραια κλειστός.

Θεώρημα III.3.7. *Έστω R ακέραια περιοχή, K σώμα $R \subset K$ και L επέκταση του K. Αν S είναι η ακέραια θήκη του R στον K, τότε οι ακέραιες θήκες των R και S στο L συμπίπτουν.*

Απόδειξη. Έστω $x \in L$, S-ακέραιο συνεπώς υπάρχουν $a_0, a_1, \ldots, a_{n-1} \in S$ με

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Από την άλλη το $R_1 = R[a_0, a_1, \ldots, a_{n-1}]$ είναι πεπερασμένα παραγόμενος υπεράνω του R, ο x είναι R_1 ακέραιος. Συνεπώς και το $R_1[x]$ είναι πεπερασμένα παραγόμενο R_1-module και συνεπώς είναι και πεπερασμένα παραγόμενο R-module και $xR_1[x] \subset R_1[x]$, δηλαδή το x είναι R-ακέραιο. □

Πόρισμα III.3.8. *Η ακέραια θήκη S της ακέραιας περιοχής R στο σώμα L, $R \subset L$ είναι ακέραια κλειστή.*

Απόδειξη. Θεωρούμε $L = K$ το σώμα πηλίκο της S στο προηγούμενο θεώρημα. □

Θεώρημα III.3.9. *Η ακέραια περιοχή R είναι δακτύλιος του Dedekind αν και μόνο αν ισχύουν οι παρακάτω προτάσεις:*

1. *Ο R είναι δακτύλιος της Noether*
2. *Κάθε μη μηδενικό πρώτο ιδεώδες του R είναι μέγιστο.*
3. *Ο R είναι ακέραια κλειστός.*

Απόδειξη. Τα (1) και (2) έχουν αποδειχθεί στο θεώρημα III.2.11. Θα αποδείξουμε ότι ο R είναι ακέραια κλειστός. Έστω $x \in K$, K σώμα πηλίκων του R και x είναι R-ακέραιο. Τότε το $R[x]$ είναι πεπερασμένα παραγόμενο R-module, δηλαδή

$$R[x] = a_1R + a_2R + \cdots + a_mR, a_i \in K.$$

Διαλέγουμε ένα $b \neq 0$ ώστε $ba_i \in R$ για όλα τα $i = 1, \ldots, m$. Τότε $bR[x] \subset R$, δηλαδή το $R[x]$ είναι κλασματικό ιδεώδες του K. Αφού το $R[x]$ είναι δακτύλιος έχουμε $R[x]^2 = R[x]$ οπότε

$$R[x] = R[x]^2R[x]^{-1} = R[x]R[x]^{-1} = R,$$

δηλαδή $x \in R$ και ο R είναι ακέραια κλειστός.

Για να αποδείξουμε ότι τα (1),(2),(3) δίνουν ότι ο R είναι δακτύλιος Dedekind θα χρειαστεί να αποδείξουμε τρία λήμματα πρώτα. □

Λήμμα III.3.10. *Έστω R δακτύλιος της Noether και A ένα μη-μηδενικό ιδεώδες του R, $A \neq R$. Τότε υπάρχουν πρώτα ιδεώδη $P_1, \ldots, P_r$ ώστε*

$$P_1P_2 \cdots P_r \subset A \subset P_1 \cap P_2 \cap \cdots \cap P_r.$$

Απόδειξη. Έστω

$$\mathcal{A} = \{A \text{ ιδεώδες του } R, A \neq \langle 0 \rangle, A \neq R \text{ για τα οποία η απαίτηση του λήμματος δεν ισχύει.}\}$$

Έστω ότι $\mathcal{A} \neq \varnothing$ και αφού ο R είναι δακτύλιος της Noether έχει μέγιστο στοιχείο M_0, το οποίο δεν είναι πρώτο γιατί τότε θα ικανοποιούσε την απαίτηση του λήμματος. Συνεπώς υπάρχουν $a, b \notin M_0$ με $ab \in M_0$. Θεωρούμε τώρα τα ιδεώδη $A = M_0 + aR$ και $B = M_0 + bR$. Είναι σαφές ότι

$$AB \subset M_0 \subset A \cap B.$$

Ακόμα $A \neq R$ και $B \neq R$ διότι αν $A = R$, τότε $B \subset M_0 \subset B$ συνεπώς $M_0 = B$ και $b \in M_0$, άτοπο.

Επίσης $M_0 \subsetneq A$, $M_0 \subsetneq B$ διότι $a \notin M_0$ και $b \notin M_0$. Αφού το M_0 μέγιστο στοιχείο του $\mathcal{A}$ έχουμε ότι για τα A, B ισχύει η απαίτηση του λήμματος οπότε ισχύει και για το M_0, άτοπο. □

Λήμμα III.3.11. *Αν R είναι ακέραια περιοχή που επαληθεύει τα (1),(2),(3) του θεωρήματος III.3.9, τότε κάθε πρώτο διάφορο του μηδενικού ιδεώδους R είναι αντιστρέψιμο.*

Απόδειξη. Έστω P πρώτο ιδεώδες του R, $P \neq \langle 0 \rangle$. Διαλέγουμε ένα στοιχείο $\alpha \in P \backslash \{0\}$ έτσι ώστε το αR να περιέχει ένα γινόμενο πρώτων ιδεωδών

$$P_1 \cdots P_{r_0} \subset \alpha R \subset P$$

με r_0 τον μικρότερο δυνατό φυσικό αριθμό. Την ύπαρξη ενός τέτοιου γινομένου την εξασφαλίζει το λήμμα III.3.10.

Υπάρχει $i \in \{1, \ldots, r_0\}$ με $P_i \subset P$. Λόγω της υπόθεσης (2) του θεωρήματος III.3.9 έχουμε ότι $P = P_i$ και χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $P = P_1$. Λόγω της επιλογής του r_0 έχουμε ότι

$$P_2 \cdots P_{r_0} \notin \alpha R$$

άρα υπάρχει $b \in P_2 \cdots P_{r_0} - \alpha R$. Αφού $b \notin \alpha R$ έχουμε ότι $b/\alpha \notin R$. Ισχύει όμως

$$bP \subset P_1 P_2 \cdots P_r \subset \alpha R$$

συνεπώς $a^{-1}bP \subset R$ δηλαδή $b/\alpha \in P^* = \{x \in K | xP \subset R\}$ και αφού $b/\alpha \notin R$, $R \subsetneq P^*$.

Το PP^* είναι ιδεώδες του R και ισχύει

$$P \subset RP \subset P^*P \subset R.$$

Αρκεί να δείξουμε ότι $P^*P = R$. Αν $P^*P \neq R$, τότε αφού P πρώτο, δηλαδή εξ υποθέσεως μέγιστο έπεται ότι $P = P^*P$ και επαγωγικά $(P^*)^n P = P$ για κάθε φυσικό αριθμό n. Δηλαδή θα είχαμε για κάθε $x \in P \backslash \{0\}$ και για κάθε $y \in P^* \backslash R$ (μόλις δείξαμε ότι υπάρχουν τέτοια y) ότι $xy^n \in P \subset R$, για όλους τους φυσικούς n.

Επομένως θα είχαμε $xR[y] \subset R$ και συνεπώς το $xR[y]$ είναι ιδεώδες του R. Από την υπόθεση (1) του θεωρήματος III.3.9 έχουμε ότι το $xR[y]$ είναι πεπερασμένα παραγόμενο, δηλαδή

$$xR[y] = a_1 R + a_2 R + \cdots + a_m R$$

και

$$R[y] = x^{-1}a_1 R + x^{-1}a_2 R + \cdots + x^{-1}a_m R$$

δηλαδή το $R[y]$ πεπερασμένα παραγόμενο R-module, οπότε το θεώρημα III.3.3 δίνει ότι y είναι R-ακέραιο και σύμφωνα με την υπόθεση (3) του III.3.9 έχουμε ότι $y \in R$, άτοπο. □

Λήμμα III.3.12. *Αν μια ακέραια περιοχή R πληροί τις υποθέσεις (1),(2),(3) του III.3.9, τότε κάθε ιδεώδες του R διάφορο του R είναι ίσο με ένα γινόμενο πρώτων ιδεωδών.*

Απόδειξη. Έστω

$$\mathcal{A} = \{A \text{ ιδεώδες του } R, A \neq R, A \neq \langle 0 \rangle, A \text{ δεν γράφεται ως γινόμενο πρώτων ιδεωδών}\}$$

και έστω $\mathcal{A} \neq \varnothing$. Από τα ιδεώδη του $\mathcal{A}$ διαλέγουμε εκείνο το οποίο περιέχει τον μικρότερο αριθμό από γινόμενα πρώτων ιδεωδών.

$$P_1 P_2 \cdots P_{r_0} \subset A.$$

Έστω P πρώτο ιδεώδες ώστε $A \subset P$, συνεπώς χωρίς περιορισμό της γενικότητας $P_1 \subset P$. Τότε όμως $P_1 = P$ αφού το P_1 ως πρώτο είναι μέγιστο. Συνεπώς (χρησιμοποιώντας το λήμμα III.3.11 που εξασφαλίζει ότι τα πρώτα είναι αντιστρέψιμα)

$$P_2 P_3 \cdots P_{r_0} \subset P^{-1} A \subset P^{-1} P = R.$$

Καταλήξαμε στο ότι το $P^{-1}A$ είναι ιδεώδες του R και περιέχει γινόμενο πρώτων ιδεωδών με πλήθος μικρότερο του r_0 άρα

$$P^{-1} A = Q_1 Q_2 \cdots Q_s$$

όπου $Q_1, \ldots, Q_s$ πρώτα ιδεώδη του R. Άρα

$$A = P Q_1 Q_2 \cdots Q_s$$

και το $\mathcal{A} = \varnothing$, δηλαδή το λήμμα έχει αποδειχτεί. □

Θα ολοκληρώσουμε τώρα την απόδειξη του θεωρήματος III.3.9. Έστω A ένα κλασματικό ιδεώδες του R και έστω $a \neq 0$, $a \in R$ ώστε $aA \subset R$. Αφού το aA είναι ακέραιο ιδεώδες του R, σύμφωνα με το λήμμα III.3.12 αυτό γράφεται ως γινόμενο πρώτων ιδεωδών

$$aA = P_1 P_2 \cdots P_s$$

με P_i πρώτα ιδεώδη του R, $1 \leq i \leq s$. Δηλαδή το A γράφεται ως

$$A = a^{-1} R P_1 \cdots P_s$$

και συνεπώς είναι γινόμενο αντιστρέψιμων ιδεωδών και είναι αντιστρέψιμο. Αποδείξαμε ότι ο R είναι δακτύλιος του Dedekind.

Πόρισμα III.3.13. *Αν R είναι δακτύλιος του Dedekind, τότε κάθε μη-τετριμμένο ιδεώδες του γράφεται ως γινόμενο πρώτων ιδεωδών.*

Θεώρημα III.3.14. *Αν R δακτύλιος του Dedekind, τότε κάθε μη-τετριμμένο ιδεώδες του γράφεται μονοσήμαντα ως γινόμενο πρώτων ιδεωδών, όπου φυσικά η σειρά των πρώτων παραγόντων δεν λαμβάνεται υπόψιν.*

Απόδειξη. Το μόνο που χρειάζεται να αποδειχθεί είναι η μοναδικότητα της ανάλυσης. Έστω A ιδεώδες του R με δύο διαφορετικές αναλύσεις

$$A = P_1 P_2 \cdots P_r = Q_1 Q_2 \cdots Q_s.$$

Μπορούμε να υποθέσουμε ότι το A είναι εκείνο για το οποίο η μία από τις δύο αναλύσεις έχει το ελάχιστο δυνατό μήκος. Έχουμε

$$Q_1 Q_2 \cdots Q_s \subset P_1 \text{ συνεπώς } Q_1 \subset P_1$$

χωρίς περιορισμό της γενικότητας, οπότε αφού Q_1 μέγιστο $P_1 = Q_1$. Άρα

$$P_2 P_3 \cdots P_r = P_1^{-1} P_1 P_2 \cdots P_r = P_1^{-1} Q_1 Q_2 \cdots Q_s = Q_2 Q_3 \cdots Q_s.$$

Λόγω της υπόθεσης των δύο διαφορετικών αναλύσεων του A σε γινόμενο πρώτων, το ιδεώδες $P_2 \cdots P_r$ έχει δύο διαφορετικές αναλύσεις, όπου μία έχει μήκος μικρότερο του ελαχίστου, άτοπο. Συνεπώς η αλήθεια του θεωρήματος. □

Πόρισμα III.3.15. *Η ομάδα των ιδεωδών ενός δακτυλίου του Dedekind* R *είναι μια ελεύθερη αβελιανή ομάδα που παράγεται από τα πρώτα ιδεώδη του* R.

Απόδειξη. Έστω A ένα κλασματικό ιδεώδες του R και $a \neq 0, a \in R$ ώστε $aA \subset R$, δηλαδή το aA είναι ιδεώδες του R. Συνεπώς το $A = (aR)^{-1}(aA)$ είναι ένα γινόμενο δυνάμεων πρώτων ιδεωδών με εκθέτη ακέραιο, όχι κατ' ανάγκη φυσικό αριθμό. Επομένως τα πρώτα ιδεώδη παράγουν την ομάδα των ιδεωδών του R και μάλιστα μονοσήμαντα λόγω του θεωρήματος III.3.14. □

III.4 Το θεμελιώδες Θεώρημα

Από τα προηγούμενα γίνεται φανερό ότι κάθε ιδεώδες A, δακτυλίου του Dedekind R έχει τη μορφή

$$A = \prod_P P^{a(P)}, \tag{III.4}$$

όπου το γινόμενο διατρέχει όλα τα πρώτα ιδεώδη P του R και οι εκθέτες $a(P)$ είναι ακέραιοι αριθμοί σχεδόν όλοι μηδέν. Κατ'αυτό τον τρόπο ξανακερδίζουμε για τα ιδεώδη του R πολλά αποτελέσματα της στοιχειώδους θεωρίας των αριθμών.

Ορισμός III.4.1. Θα λέμε ότι το ιδεώδες A διαιρείται από το ιδεώδες B αν και μόνο αν υπάρχει C ιδεώδες του R ώστε $A = BC$.

Αν $C \mid A$ και $C \mid B$ και για κάθε $C' \mid A$ και $C' \mid B$ έχουμε $C' \mid C$, τότε ο C θα λέγεται ο μέγιστος κοινός διαιρέτης των A, B.

Η ύπαρξη και μοναδικότητα του C είναι αποτέλεσμα του μονοσήμαντου της ανάλυσης από την εξίσωση (III.4). Προφανώς αν $A = \prod_P P^{a(P)}$ και $B = \prod_P P^{b(P)}$ είναι ακέραια ιδεώδη, τότε τα $a(P)$ και $b(P)$ είναι φυσικοί αριθμοί.

Ακόμα $A \mid B$ αν και μόνο αν $a(P) \leq b(P)$ για όλα τα P. Οπότε ο μέγιστος κοινός διαιρέτης C είναι

$$C = (A, B) = \prod_P P^{\min\{a(P), b(P)\}}.$$

Ανάλογα ορίζεται το ελάχιστο κοινό πολλαπλάσιο και ισχύει

$$D := [A, B] = \prod_P P^{\max\{a(P), b(P)\}}.$$

Προφανώς ισχύει

$$(A, B)[A, B] = AB.$$

Πρόταση III.4.2. *Αν* R *δακτύλιος του Dedekind, τότε*

1. *Αν* A, B *κλασματικά ιδεώδη του* R*, τότε* $A \subset B$ *αν και μόνο αν υπάρχει ιδεώδες* $C \subset R$ *με* $A = BC$.
2. *Αν* A *κλασματικό ιδεώδες του* R*, τότε υπάρχει ένα κύριο κλασματικό ιδεώδες του* R *το* aR*, τέτοιο ώστε* $aRA^{-1} \subset R$.
3. *Αν* A, B *ακέραια ιδεώδη, πρώτα μεταξύ τους, τότε* $AB = A \cap B$.
4. *Αν* A, B *είναι ακέραια ιδεώδη του* R*, τότε* $(A, B) = \langle A, B\rangle = A + B$.

Απόδειξη. 1. Ας υποθέσουμε ότι $A = BC$, τότε είναι σαφές ότι $A \subset B$. Αντιστρόφως αν $A \subset B$, τότε $AB^{-1} \subset BB^{-1} = R$, οπότε το $C = AB^{-1}$ είναι ιδεώδες του R και $BC = A$.

2. Έστω $a \in A - \{0\}$, συνεπώς $aR \subset A$ και σύμφωνα με ό,τι δείξαμε υπάρχει $C \subset R$ με $aR = AC$ δηλαδή $C = (aR)A^{-1} \subset R$.

3. Αν A, B είναι μεταξύ τους πρώτα, τότε από $A \mid A \cap B$ και $B \mid A \cap B$ έχουμε ότι $AB \mid A \cap B$ συνεπώς $A \cap B \subset AB$. Από τις ιδιότητες του ιδεώδους προκύπτει ότι $AB \subset A \cap B$ και συνεπώς η ισότητα.

4. Ισχύει ότι $A, B \subset A + B$ άρα $A + B \mid A, B$ συνεπώς από τις ιδιότητες του μέγιστου κοινού διαιρέτη $A + B \mid (A, B)$. Από την άλλη το $A + B$ είναι το ελάχιστο ιδεώδες που περιέχει τα A, B άρα θα πρέπει $(A, B) \mid A + B$, δηλαδή το ζητούμενο.

□

Ορισμός III.4.3. Ένας δακτύλιος Dedekind θα λέμε ότι ικανοποιεί τη *συνθήκη της πεπερασμένης norm* (FN) αν για κάθε μη-μηδενικό ακέραιο ιδεώδες ο δακτύλιος πηλίκο R/A έχει πεπερασμένο πλήθος στοιχείων.

Ορισμός III.4.4. Σε έναν δακτύλιο Dedekind που ικανοποιεί τη συνθήκη (FN) θα λέμε απόλυτη norm του ιδεώδους A το πλήθος των στοιχείων του R/A.

Το σημαντικότερο θεώρημα της παραγράφου είναι το

Θεώρημα III.4.5. *Έστω R δακτύλιος του Dedekind και K το σώμα πηλίκων του. Έστω L/K μια πεπερασμένη και διαχωρίσιμη επέκταση του K και έστω S η ακέραια θήκη του R στο L. Τότε το S είναι επίσης δακτύλιος του Dedekind. Επιπλέον αν ο R πληροί τη συνθήκη (FN), τότε και ο S την πληροί.*

Απόδειξη. Θα αποδείξουμε ότι ισχύουν τα (i),(ii), (iii) του θεωρήματος III.3.9. Η επέκταση L/K είναι απλή ως πεπερασμένη και διαχωρίσιμη. Δηλαδή υπάρχει ένα $\theta \in L$ με $L = K(\theta)$. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $\theta \in S$, διότι αν θ είναι ρίζα του πολυωνύμου

$$A_n x^n + A_{n-1} x^{n-1} + \cdots + A_0 = 0, \quad A_n \neq 0, A_i \in R,$$

τότε το στοιχείο $A_n\theta$ είναι ρίζα της εξίσωσης

$$x^n + A_{n-1} x^{n-1} + A_{n-2} A_n x^{n-2} + \cdots + A_0 A_n^{n-1} = 0,$$

δηλαδή $A_n\theta \in S$ και προφανώς $L = K(A_n\theta)$.

Θα δείξουμε ότι υπάρχει $c \in K$, ώστε $S \subset cR[\theta]$. Έστω $L^{(i)}$ οι εμφυτεύσεις του σώματος L σε μια αλγεβρική θήκη του σώματος K, για $i = 1, 2, \ldots, n$. Αν $x \in L$, το $x^{(i)}$ είναι το i-στο συζυγές του x. Έστω $a \in S$ τυχαίο στοιχείο το οποίο δέχεται μια γραφή:

$$a = \sum_{k=0}^{n-1} a_k \theta^k \text{ με } a_k \in K, k = 0, 1, \ldots, n-1$$

συνεπώς

$$a^{(i)} = \sum_{k=0}^{n-1} a_k (\theta^{(i)})^k \text{ με } i = 0, 1, \ldots, n-1$$

Με αυτόν τον τρόπο καταλήγουμε σε ένα σύστημα n εξισώσεων με n αγνώστους (τα a_k). Το σύστημα αυτό μπορούμε να το λύσουμε με τη μέθοδο του Crammer και να έχουμε

$$a_k = \frac{A_k}{D}, i = 0, 1, \ldots, n-1,$$

όπου $A_k \in S$, $D \in S$ και η ορίζουσα υπολογίζεται με τη μέθοδο του Vandermode:

$$D = \prod_{1 \leq i < j \leq n} (\theta^{(i)} - \theta^{(j)}) \neq 0,$$

Προφανώς $D \neq 0$. Έστω N η ελάχιστη κανονική θήκη του K που περιέχει το L. Δηλαδή η N/K είναι επέκταση του Galois και κάθε K-αυτομορφισμός του $N = K(\theta^{(1)}, \theta^{(2)}, \dots, \theta^{(n)})$ δίνεται μέσω μιας μετάθεσης του συνόλου $\{1, 2, \dots, n\}$ οπότε το

$$D^2 = \prod_{1 \leq i < j \leq n} \left(\theta^{(i)} - \theta^{(j)}\right)^2$$

παραμένει αναλλοίωτο κάτω από τη δράση όλων των K-αυτομορφισμών του N και συνεπώς $D^2 \in K$. Αφού $D^2 \in S$ έχουμε ότι $D^2 \in S \cap K = R$. Γράφουμε $a_k = \frac{A_k D}{D^2}$ με $a_k \in K$, $D^2 \in R$, συνεπώς $a_k D^2 \in K$ και αφού $a_k D^2 = A_k D \in S$ καταλήγουμε ότι $A_k D \in R$. Επομένως, για κάθε $a \in S$ έχουμε $a = \sum_{k=0}^{n-1} a_k \theta^k$ και

$$D^2 a = \sum_{k=0}^{n-1} D^2 a_k \theta^k = \sum_{k=0}^{n-1} (A_k D)\theta^k \in R[\theta].$$

Δηλαδή

$$a \in cR[\theta], \text{ όπου } c = D^{-2} \in K.$$

Θεωρούμε τη συνάρτηση $f : R^n \to cR[\theta]$ με

$$f : (x_1, x_2, \dots, x_n) \mapsto c(x_1 + x_2\theta + \cdots + x_n\theta^{n-1})$$

είναι επιμορφισμός από R-modules. Συνεπώς το $cR[\theta]$ είναι R-module της Noether. Αφού δε $S \subset cR[\theta]$, έχουμε ότι και ο S είναι επίσης R-module της Noether. Αλλά κάθε ιδεώδες του S είναι προφανώς R-module και καταλήγουμε ότι ο S είναι δακτύλιος της Noether.

Αφού τώρα $S \subset L$ το L περιέχει το σώμα πηλίκων του S και καταλήγουμε ότι ο S είναι ακέραια κλειστός.

Παρατήρηση III.4.6. Από την απόδειξη προκύπτει το εξής συμπέρασμα: Αν R δακτύλιος του Dedekind και K το σώμα πηλίκων αυτού L/K μια πεπερασμένη και διαχωρίσιμη επέκταση, S η ακέραια θήκη του R στο L, $L = K(\theta)$, $\theta \in S$, τότε

$$R[\theta] \subset S \subset \frac{1}{D^2} R[\theta], \tag{III.5}$$

όπου

$$D = \prod_{1 \leq i < j \leq n} (\theta^{(i)} - \theta^{(j)}).$$

Η απόδειξη θα ολοκληρωθεί μόλις δείξουμε ότι τα πρώτα ιδεώδη του S είναι και μέγιστα.

Λήμμα III.4.7. *Δεχόμαστε τις υποθέσεις του θεωρήματος III.4.5. Τότε αν P πρώτο ιδεώδες του S έχουμε ότι $P' = P \cap R$ είναι πρώτο ιδεώδες του R. Αν πάλι P_1, P_2 πρώτα ιδεώδη του S και $P_1 \subset P_2$ και ότι $P_1 \cap R = P_2 \cap R$, τότε $P_1 = P_2$.*

Απόδειξη. Παρατηρούμε ότι το $P \cap R$ είναι ο πυρήνας της σύνθεσης των ομομορφισμών

$$\phi : R \hookrightarrow S \to S/P$$

$$r \mapsto r \mapsto r + P.$$

Συνεπώς η συνάρτηση

$$\phi' : \frac{R}{R \cap P} \mapsto S/P$$

με

$$\phi'(a + (R \cap P)) = a + P$$

είναι μονομορφισμός δακτυλίων. Αφού δε το S/P είναι ακέραια περιοχή και το $R/R \cap P$ είναι ακέραια περιοχή, άρα το $P \cap R$ είναι πρώτο ιδεώδες του R.

Τώρα έστω $P_1 \cap R = P_2 \cap R$ αλλά $P_1 \subsetneq P_2$. Θεωρούμε ένα $x \in P_2 - P_1$. Το $x \in S$ συνεπώς είναι R-ακέραιο, δηλαδή υπάρχουν $a_i \in R$, $i = 0, 1, 2, \ldots, n-1$ με

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Αν όλοι οι συντελεστές $a_i \in P_1 \cap R$, τότε $x^n \in P_1$ και συνεπώς και το $x \in P_1$, αφού το P_1 είναι πρώτο ιδεώδες.

Ας θεωρήσουμε j τον μικρότερο δείκτη ώστε $a_j \notin P_1 \cap R$. Έχουμε ότι

$$x^j \left(x^{n-j} + a_{n-1}x^{n-j-1} + \cdots + a_j\right) \in P_1.$$

Αφού $x \notin P_1$ έχουμε ότι $x^j \notin P_1$ και συνεπώς

$$x^{n-j} + a_{n-1}x^{n-j-1} + \cdots + a_j \in P_1 \subset P_2$$

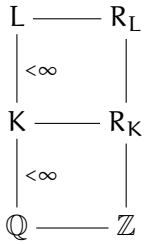
και αφού $x \in P_2$ έχουμε ότι $a_j \in P_2$. Όμως $a_j \in P_1 \cap R = P_2 \cap R$ από όπου έχουμε $a_j \in P_1$, άτοπο. □

Συνεχίζουμε με την απόδειξη του θεωρήματος III.4.5. Ας θεωρήσουμε το P_1 ένα διάφορο του μηδενικού πρώτο ιδεώδες του S το οποίο δεν είναι μέγιστο. Συνεπώς υπάρχει μέγιστο - και συνεπώς πρώτο - ιδεώδες P_2 του S με $P_1 \subsetneq P_2$ συνεπώς $P_1 \cap R \subset P_2 \cap R$. Σύμφωνα με το λήμμα III.4.7 έχουμε ότι $P_1 \cap R \neq P_2 \cap R$ και $P_1 \cap R, P_2 \cap R$ πρώτα ιδεώδη του R δηλαδή μέγιστα, άτοπο.

Παρατηρούμε ότι $R \cap P \neq R$, αφού δεν περιέχει το κοινό μοναδιαίο των δακτυλίων R, S. Επίσης, το $R \cap P$ είναι μη μηδενικό, αφού το P είναι μη μηδενικό γιατί για $0 \neq x \in P$ το $0 \neq N(x) \in R \cap P$.

Έστω τέλος ότι ο R επαληθεύει τη συνθήκη της πεπερασμένης norm. Είδαμε ότι το σώμα S/P είναι επέκταση του σώματος $R/(R \cap P)$, το οποίο εξ υποθέσεως είναι πεπερασμένο. Από την άλλη $S \subset cR[\theta]$, $\deg \mathrm{Irr}(\theta, K) = n$. Άρα κάθε στοιχείο του S είναι ρίζα μιας εξίσωσης το πολύ βαθμού n με συντελεστές από το R, άρα κάθε στοιχείο του S/P είναι ρίζα πολυωνύμου βαθμού το πολύ n με συντελεστές από το σώμα $R/(R \cap P)$. Αφού όμως το τελευταίο είναι πεπερασμένο σώμα και το S/P είναι πεπερασμένο σώμα. Για τυχαία ιδεώδη A θέλει ένα επιχείρημα κινέζικου θεωρήματος υπολοίπων και ένα επιχείρημα για το S/P^i

Θεωρούμε τις επεκτάσεις αλγεβρικών σωμάτων αριθμών:



Ο $\mathbb{Z}$ είναι περιοχή κυρίων ιδεωδών άρα κάθε κύριο κλασματικό ιδεώδες του $\mathbb{Q}$ είναι αντιστρέψιμο, οπότε το $\mathbb{Z}$ είναι δακτύλιος του Dedekind. Επίσης, κάθε ιδεώδες του $\mathbb{Z}$ είναι της μορφής $m\mathbb{Z}$, και $\mathbb{Z}/m\mathbb{Z}$ είναι πεπερασμένο, οπότε οι δακτύλιοι R_K, R_L είναι δακτύλιοι του Dedekind και πληρούν τη συνθήκη της πεπερασμένης norm.

□

Ο ενδιαφερόμενος αναγνώστης μπορεί να συμβουλευτεί τη βιβλιογραφία τα [1],[3], [4], [5], [6], [7].

Παρατήρηση III.4.8. Έχουμε χαρακτηρίσει τις *περιοχές Dedekind* ως ακέραιες περιοχές στις οποίες ισχύουν οι τρεις ιδιότητες:

1. Είναι περιοχές της Noether
2. Είναι ακέραια κλειστή

3. Όλα τα πρώτα ιδεώδη εκτός του μηδενικού είναι μέγιστα

και αποδείξαμε ότι σε κάθε περιοχή Dedekind έχουμε μονοσήμαντη ανάλυση σε γινόμενο πρώτων (μέγιστων) ιδεωδών.

Υπάρχουν αντιπαραδείγματα ακεραίων περιοχών οι οποίες πληρούν τα 1 και 2 αλλά όχι το 3, τα 2, 3 αλλά όχι το 1 ή την 1 και 3 αλλά όχι την 2.

Παρατήρηση III.4.9. Υπάρχουν και άλλοι ισοδύναμοι χαρακτηρισμοί των περιοχών Dedekind. Έστω R μια ακέραια περιοχή. Οι προτάσεις που ακολουθούν είναι μεταξύ τους ισοδύναμες:

1. Η R είναι ακέραια περιοχή.
2. Κάθε μη-μηδενικό, γνήσιο ιδεώδες της R είναι γινόμενο πρώτων ιδεωδών.
3. Κάθε μη-μηδενικό γνήσιο ιδεώδες της R είναι μονοσήμαντα γινόμενο πρώτων ιδεωδών.
4. Κάθε μη-μηδενικό, ιδεώδες της R είναι αντιστρέψιμο, ως κλασματικό R-module.
5. Κάθε, μη-μηδενικό ιδεώδες της R είναι ένα προβολικό R-module. Την έννοια του προβολικού R-module δεν θα την ορίσουμε εδώ.
6. Η περιοχή R είναι περιοχή της Noether και ο εντοπισμός R_P είναι περιοχή κυρίων ιδεωδών για κάθε μη-μηδενικό πρώτο ιδεώδες της R. Η έννοια του εντοπισμού θα οριστεί αργότερα σε επόμενο κεφάλαιο.

Η απόδειξη βρίσκεται στο [2, 16.3 Θεώρημα 15 σελ. 765].

III.5 Ασκήσεις

1. Να αποδειχτεί ότι κάθε αλγεβρικός αριθμός γράφεται ως πηλίκο ακεραίου αλγεβρικού και φυσικού αριθμού.
2. Να αποδειχτεί ότι ο
$$\frac{1}{3}\left(1 + 10^{\frac{1}{3}} + 10^{\frac{2}{3}}\right)$$
είναι ακέραιος αλγεβρικός αριθμός.
3. Να εκφράσετε τον αλγεβρικό αριθμό
$$\left(\frac{1+\sqrt{2}}{9}\right)^{1/3} + \left(\frac{1-\sqrt{2}}{9}\right)^{1/3}$$
ως πηλίκο ενός ακεραίου αλγεβρικού αριθμού και ενός φυσικού αριθμού.
4. Να αποδειχτεί ότι οι ρίζες του πολυωνύμου
$$x^2 - 37 - 12\sqrt{7},$$
ανήκουν στο σώμα $\mathbb{Q}(\sqrt{7})$.
5. Να αποδειχτεί ότι οι αριθμοί $3 + 2\sqrt{-5}$ και $1 + 2\sqrt{-5}$ είναι ανάγωγα στοιχεία της περιοχής των ακεραίων αλγεβρικών του σώματος $K = \mathbb{Q}(\sqrt{-5})$.
6. Αν θ ρίζα του πολυωνύμου $x^3 + 6x + 64$ να αποδείξετε ότι η ακέραια περιοχή
$$\mathbb{Z}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 : a_i \in Z\}$$
δεν είναι ακέραια κλειστή. Είναι περιοχή Dedekind;

7. Αν ένας δακτύλιος Dedekind έχει πεπερασμένο πλήθος πρώτων ιδεωδών να αποδείξετε ότι είναι περιοχή κυρίων ιδεωδών.

8. Έστω A, B δύο ιδεώδη ενός δακτυλίου Dedekind R. Να αποδείξετε ότι υπάρχει ιδεώδες C του R για το οποίο ισχύουν $(C, AB) = R$ και CA κύριο ιδεώδες.

9. Να αποδείξετε ότι σε κάθε περιοχή Dedekind, οποιοδήποτε ιδεώδες αυτής παράγεται από δύο στοιχεία.

10. Είναι η ακέραια περιοχή $K[X, Y]$ περιοχή Dedekind;

Βιβλιογραφία

[1] Alaca, Ş. & Williams, K. S. *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, 2004, pp. xviii+428. ISBN: 0-521; 0-521-54011-9.

[2] Dummit, D. S. & Foote, R. M. *Abstract Algebra*. 3rd edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9.

[3] Fröhlich, A. & Taylor, J. M. *Algebraic number theory*. Vol. 27. Cambridge Studies in advanced mathematics. Cambridge: Cambridge University Press, 1993, pp. xiv+355. ISBN: 0-521-43834-9.

[4] Janusz, G. J. *Algebraic Number Fields*. 2nd edition. Vol. 7. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 1996, pp. x+276. ISBN: 0-8218-0429-4.

[5] Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*. 3rd edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004, pp. xii+708. ISBN: 3-540-21902-1.

[6] Neukirch, J. *Algebraische Zahlentheorie*. German. Springer-Verlag Berlin, 1992.

[7] Samuel, P. *Algebraic Theory of Numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970, p. 109.

[8] Λάκκης, Κ. *Άλγεβρα*. Εκδ. Ζήτη, 1991.

IV

Norm, Ίχνος, Βάση και Διακρίνουσα

IV.1 Norm και Ίχνος

Έστω L, K αλγεβρικά σώματα αριθμών $K \subset L$, θ ένα πρωταρχικό στοιχείο της επέκτασης L/K δηλαδή $L = K(\theta)$, $B = \{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ βάση της επέκτασης. Έστω $\alpha \in L$, τότε υπάρχουν $a_{j,i} \in K$ ώστε

$$\alpha\theta^i = \sum_{j=0}^{n-1} a_{j,i}\theta^j.$$

Συμβολίζουμε τον πίνακα $A(\alpha) = (a_{j,i}) \in M_n(K)$, τον οποίο θα ονομάζουμε πίνακα παράστασης του α.

Προφανώς ισχύουν

$$A(\alpha + \beta) = A(\alpha) + A(\beta) \text{ για κάθε } \alpha, \beta \in L \tag{IV.1}$$

$$A(\lambda\alpha) = \lambda A(\alpha) \text{ για κάθε } \lambda \in K, \alpha \in L \tag{IV.2}$$

$$A(\alpha\beta) = A(\alpha)A(\beta) \text{ για κάθε } \alpha, \beta \in L \tag{IV.3}$$

$$A(1_L) = \mathbb{I}_n \tag{IV.4}$$

Επομένως ο $A : L \to M_n(K)$ είναι ομομορφισμός δακτυλίων και συνεπώς μονομορφισμός του L σε κάποιο υπόσωμα της K-άλγεβρας $M_n(K)$. Επιπλέον, λόγω των (IV.1),(IV.2) είναι και μονομορφισμός διανυσματικών χώρων.

Αν θεωρήσουμε τώρα τον ενδομορφισμό

$$\phi_\alpha : L \ni x \mapsto \alpha x \in L$$

βλέπουμε αμέσως ότι ο $A(\alpha)$ είναι ο πίνακας που αντιστοιχεί στον ενδομορφισμό ϕ_α ως προς τη βάση B.

Ορισμός IV.1.1. Ίχνος του α ως προς την επέκταση L/K θα λέγεται το ίχνος του πίνακα $A(\alpha)$. Norm του α ως προς την επέκταση L/K θα λέγεται η ορίζουσα του πίνακα $A(\alpha)$. Θα συμβολίζουμε το ίχνος με $\mathrm{Tr}_{L/K}(\alpha)$ και την Norm με $N_{L/K}(\alpha)$.

Το χαρακτηριστικό πολυώνυμο του πίνακα $A(\alpha)$ θα το ονομάζουμε *χαρακτηριστικό πολυώνυμο του* α ως προς την επέκταση L/K και θα το συμβολίζουμε με $\chi_{\alpha,L/K}$, δηλαδή

$$\chi_{\alpha,L/K}(x) = \det(x\mathbb{I}_n - A(\alpha)).$$

Πρόταση IV.1.2. *Έστω ότι*

$$\chi_{\alpha,L/K}(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0,$$

το χαρακτηριστικό πολυώνυμο του α. Ισχύουν οι παρακάτω ιδιότητες:

1. $N_{L/K}(\alpha) = (-1)^n c_0$, $\mathrm{Tr}_{L/K}(\alpha) = -c_{n-1}$
2. *Το α είναι ρίζα του χαρακτηριστικού του πολυωνύμου.*
3. *Το χαρακτηριστικό πολυώνυμο και συνεπώς και η norm καθώς και το ίχνος είναι ανεξάρτητα της επιλογής της βάσης*
4. $\mathrm{Tr}_{L/K}(\lambda\alpha + \mu\beta) = \lambda\mathrm{Tr}_{L/K}(\alpha) + \mu\mathrm{Tr}_{L/K}(\beta)$, *δηλαδή το ίχνος είναι μια γραμμική μορφή*

$$\mathrm{Tr} : L \to K.$$

5. $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$. *Επιπλέον* $N_{L/K}(\alpha) = 0$ *αν και μόνο αν* $\alpha = 0$, *δηλαδή*

$$N_{L/K} : L^* \to K^*$$

είναι ομομορφισμός ομάδων.

Απόδειξη. 1. Γνωρίζουμε ότι $c_0 = \chi_{\alpha,L/K}(0) = \det(-A(\alpha)) = (-1)^n \det A(\alpha)$. Από την άλλη, γράφουμε

$$\chi_{\alpha,L/K}(x) = x^n - \sum_{i=0}^{n-1} a_{ii}X^{n-1} + h(x),$$

με $\deg(h(x)) \le n-2$. Συνεπώς $c_{n-1} = -\sum_{i=0}^{n-1} a_{ii}$.

2. Παρατηρούμε ότι για $B = \{1, \theta, \ldots, \theta^{n-1}\}$ έχουμε $\alpha B = B\alpha = BA(\alpha)$. Συνεπώς $B(\alpha\mathbb{I}_n - A(\alpha)) = 0$. Με αυτόν τον τρόπο καταλήγουμε σε ένα ομογενές γραμμικό σύστημα με συντελεστές από το L με μία τετριμμένη λύση B. Άρα η ορίζουσα $\det(\alpha\mathbb{I}_n - A(\alpha)) = 0$, οπότε α είναι ρίζα του χαρακτηριστικού πολυωνύμου.

3. Έστω B' μια άλλη βάση της L/K. Οι δύο βάσεις συνδέονται μέσω της σχέσης $B' = BC$ για κάποιο πίνακα $C \in GL_n(K)$. Άρα

$$B'\alpha = B'A'(\alpha) = BCA'(\alpha)$$

και

$$B'\alpha = BC\alpha = (B\alpha)C = BA(\alpha)C$$

Από τις δύο παραπάνω σχέσεις έχουμε

$$CA'(\alpha) = A(\alpha)C$$

και, αφού ο C είναι αντιστρέψιμος, έχουμε

$$A'(\alpha) = C^{-1}A(\alpha)C$$

και όμοιοι πίνακες έχουν το ίδιο χαρακτηριστικό πολυώνυμο.

4. Προφανές, λόγω του ορισμού του $\mathrm{Tr}_{L/K}(\alpha)$ και της πρώτης πρότασης.

5. Προφανές, αφού η ορίζουσα είναι πολλαπλασιαστική. Η συνάρτηση $A : L \to M_n(K)$ ως μονομορφισμός δίνει ότι αν $A(\alpha) = 0$ τότε και μόνο τότε όταν $\alpha = 0$. Επίσης το $A(L)$ είναι σώμα οπότε $A(L) - \{0_n\} \subset GL_n(K)$, οπότε $\det(A(\alpha)) = 0$ αν και μόνο αν $A(\alpha) = 0_n$.

□

Πόρισμα IV.1.3. 1. *Το ανάγωγο πολυώνυμο* $\mathrm{Irr}(\alpha, K)$ *διαιρεί το χαρακτηριστικό πολυώνυμο του* α.

2. *Αν* α *πρωταρχικό δηλαδή* $L = K(\alpha)$, *τότε* $\mathrm{Irr}(\alpha, K) = \chi_{\alpha, L/K}(x)$.

3. $\mathrm{Tr}_{L/K}(L) \neq 0$

Απόδειξη. 1. Είναι σαφές ότι το σύνολο των πολυωνύμων του $K[x]$ που μηδενίζονται στο α είναι κύριο ιδεώδες του $K[x]$ του οποίου εξ ορισμού το $\mathrm{Irr}(\alpha, K)$ αποτελεί μονικό γεννήτορα.

2. Τα $\mathrm{Irr}(\alpha, K)$ και $\chi_{\alpha, L/K}(x)$ είναι μονικά πολυώνυμα ίδιου βαθμού (rank) και το πρώτο διαιρεί το δεύτερο, άρα ταυτίζονται.

3. Παρατηρούμε ότι
$$\mathrm{Tr}_{L/K}(1_L) = \mathrm{tr}(A(1_L)) = \mathrm{tr}\mathbb{I}_n = n \neq 0,$$
αφού η χαρακτηριστική του σώματος K είναι 0.

□

Θεωρούμε την αλυσίδα σωμάτων $K \subset K(\alpha) \subset L = K(\theta)$, ώστε $[L : K] = n$, $[L : K(\alpha)] = m$ και $[K(\alpha) : K] = \ell$. Είναι γνωστό ότι αν $\{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ βάση της $L/K(\alpha)$ και $\underline{\beta} := \{\beta_1, \beta_2, \ldots, \beta_\ell\}$ βάση της $K(\alpha)/K$, τότε
$$B = \{\gamma_i\beta_j : i = 1, \ldots, m, j = 1, \ldots, \ell\} = \{\gamma_1\underline{\beta}, \ldots, \gamma_m\underline{\beta}\}$$
είναι μια βάση της L/K. Θέλουμε να βρούμε τον πίνακα $A_{L/K}(\alpha)$ ως προς βάση B. Υπολογίζουμε:

$$B\alpha = (\gamma_1\underline{\beta}\alpha, \ldots, \gamma_m\underline{\beta}\alpha).$$

Όμως
$$\underline{\beta}\alpha = A_{K(\alpha)/K}(\alpha)$$

Άρα
$$B\alpha = \left(\gamma_1 A_{K(\alpha)/K}(\alpha), \gamma_2 A_{K(\alpha)/K}(\alpha), \ldots, \gamma_m A_{K(\alpha)/K}(\alpha)\right).$$

Δηλαδή
$$A_{L/K}(\alpha) = \begin{pmatrix} A_{K(\alpha)/K}(\alpha) & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & A_{K(\alpha)/K}(\alpha) \end{pmatrix}_{m\times m}$$

και τελικά καταλήγουμε στο ότι
$$\chi_{\alpha, L/K}(x) = \chi_{\alpha, K(\alpha)/K}(x)^m.$$

Με αυτόν τον τρόπο αποδείχτηκε η

Πρόταση IV.1.4. 1. *Ισχύει* $\chi_{\alpha, L/K}(x) = \mathrm{Irr}_{\alpha, K}(x)^{[L:K(\alpha)]}$

2. $N_{L/K}(\alpha) = \left(N_{K(\alpha)/K}(\alpha)\right)^{[L:K(\alpha)]}$

3. $\mathrm{Tr}_{L/K}(\alpha) = [L : K(\alpha)]\mathrm{Tr}_{K(\alpha)/K}(\alpha)$.

Παράδειγμα IV.1.5. Έστω $f(x) = x^3 - x^2 - 2x - 8 \in \mathbb{Q}[x]$. Το $f(x)$ είναι ανάγωγο υπεράνω του $\mathbb{Q}$, οπότε αν θ μία ρίζα του πολυωνύμου $f(x)$, $f(\theta) = 0$ και $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$. Έστω $\alpha = \frac{\theta^2-\theta}{2}$.Θέλουμε να βρούμε τη χαρακτηριστική εξίσωση του α. Προφανώς $\theta^3 = \theta^2 + 2\theta + 8$. Συνεπώς

$$\begin{aligned} \alpha &= \frac{\theta^2 - \theta}{2} \\ \alpha\theta &= \frac{\theta^2 - \theta}{2}\theta = \frac{1}{2}(\theta^3 - \theta^2) = \theta + 4 \\ \alpha\theta^2 &= \frac{\theta^2 - \theta}{2}\theta^2 = \theta^2 + 4\theta \end{aligned}$$

Το χαρακτηριστικό πολυώνυμο είναι το

$$\det \begin{pmatrix} \alpha & -4 & 0 \\ \frac{1}{2} & \alpha - 1 & -4 \\ -\frac{1}{2} & 0 & \alpha - 1 \end{pmatrix} = \alpha^3 - 2\alpha^2 + 3\alpha - 10.$$

Δηλαδή ο α είναι ακέραιος αλγεβρικός αριθμός του $\mathbb{Q}(\theta)$. Επιπλέον παρατηρούμε ότι $N_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha) = 10$ και $\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha) = 2$.

Τέλος παρατηρούμε ότι $\alpha \notin \mathbb{Z}[\theta]$.

Έστω $K \subset L \subset M$, αλγεβρικά σώματα αριθμών $L = K(\theta)$ και $M = L(\eta)$. Γνωρίζουμε ότι υπάρχουν $n = [L : K] = \deg \mathrm{Irr}(\theta, K)$ K-μονομορφισμοί του L σε μία αλγεβρική θήκη $\widetilde{K}$ του K που περιέχει το M (συνεπώς και το L). Αν $[M : L] = \deg \mathrm{Irr}(\eta, L) = m$, τότε κάθε K-μονομορφισμός του L στο $\widetilde{K}$ έχει m δυνατότητες επέκτασης σε K-μονομορφισμούς του M στο $\widetilde{K}$. Συνολικά δηλαδή μπορούμε να σχηματίσουμε mn-μονομορφισμούς του M στο $\widetilde{K}$ και αφού $[M : K] = nm$, αυτές είναι όλες.

Πρόταση IV.1.6. *Έστω $K \subset L \subset M$, αλγεβρικά σώματα αριθμών. Τότε κάθε εμφύτευση του L/K στο $\widetilde{K}$ επεκτείνεται σε $m = [M : L]$ ακριβώς εμφυτεύσεις του M/K.*

Παράδειγμα IV.1.7.

$$\begin{array}{ccc} \mathbb{Q}(i, \sqrt[3]{2}) & \xrightarrow{\sigma_{\mu,\nu}} & \mathbb{Q}(i, \omega^\mu \sqrt[3]{2}) \\ \Big| & & \Big| \\ \mathbb{Q}(i) & \xrightarrow{\sigma_\mu} & \mathbb{Q}(i) \\ \Big| & & \Big| \\ \mathbb{Q} & \xrightarrow{\mathrm{id}} & \mathbb{Q} \end{array}$$

με

$$\sigma_{\mu,\nu}(\sqrt[3]{2}) = \omega^\nu \sqrt[3]{2}, \ \ \nu = 0, 1, 2, \qquad \sigma_\mu(i) = (-1)^\mu, \ \ \mu = 0, 1$$

Πρόταση IV.1.8. *Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών. Έστω $\alpha \in L$. Τότε*

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \text{ και } \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

όπου σ_i οι K-εμφυτεύσεις του L στο $\mathbb{C}$.

Απόδειξη. Ξεχωρίζουμε δύο περιπτώσεις:

- Έστω ότι $L = K(\alpha)$.Τότε το χαρακτηριστικό πολυώνυμο $f(x)$ του α συμπίπτει με το ανάγωγο πολυώνυμο του α υπεράνω του $\mathbb{Q}$. Έστω

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, (a_i \in K)$$

Έχουμε $N_{L/K}(\alpha) = (-1)^n a_0$ και $Tr_{L/K}(\alpha) = -a_{n-1}$. Από την άλλη μεριά γνωρίζουμε ότι

$$f(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$$

οπότε

$$a_0 = (-1)^n \prod_{i=1}^{n} \sigma_i(\alpha) \text{ και } a_{n-1} = -\sum_{i=1}^{n} \sigma_i(\alpha).$$

- Έστω τώρα $K_0 = K(\alpha) \subsetneq L$. Σε αυτή την περίπτωση γνωρίζουμε ότι

$$N_{L/K}(\alpha) = \left(N_{K_0/K}(\alpha)\right)^{[L:K_0]}$$

και

$$Tr_{L/K}(\alpha) = [L : K_0]Tr_{K_0/K}(\alpha).$$

Έχουμε όμως ότι

$$N_{K_0/K}(\alpha) = \prod_{j=1}^{\ell} \rho_j(\alpha),$$

όπου ρ_j, $j = 1, 2, \ldots, \ell$ οι ℓ εμφυτεύσεις της K_0/K, όπου $\ell = [K_0 : K]$. Αφού κάθε μία από αυτές επεκτείνεται σε $[L : K_0]$ εμφυτεύσεις της L/K θα έχουμε

$$N_{L/K}(\alpha) = \left(\prod_{j=1}^{\ell} \rho_j(\alpha)\right)^{[L:K_0]} = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Ομοίως

$$Tr_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

□

Αν τώρα L/K επέκταση αλγεβρικών σωμάτων αριθμών και R, S οι αντίστοιχοι δακτύλιοι των ακεραίων αλγεβρικών αριθμών, τότε για κάθε $\alpha \in S$ έχουμε $N_{L/K}(\alpha) \in R$ και $Tr_{L/K}(\alpha) \in R$, διότι $\alpha \in S$ και τα $\sigma_i(\alpha)$ είναι R-ακέραιοι για κάθε $i = 1, 2, \ldots, \ell$ (όχι κατ' ανάγκη στοιχεία του S), οπότε $N_{L/K}(\alpha)$ και $Tr_{L/K}(\alpha)$ είναι R-ακέραιοι. Επειδή δε $N_{L/K}(\alpha)$ και $Tr_{L/K}(\alpha) \in K$ έχουμε $N_{L/K}(\alpha), Tr_{L/K}(\alpha) \in R$.

Πρόταση IV.1.9. *Έστω K αλγεβρικό σώμα αριθμών, R ο δακτύλιος των ακεραίων αλγεβρικών αριθμών αυτού και $E(R)$ η ομάδα των μονάδων του R. Ισχύει ότι*

$$E(R) = \{\epsilon \in R : N_{K/\mathbb{Q}}(\epsilon) = \pm 1\}.$$

Απόδειξη. Έστω $\epsilon \in E(R)$ συνεπώς υπάρχει $\epsilon' \in R$ με $\epsilon\epsilon' = 1$, άρα $N_{K/\mathbb{Q}}(\epsilon)N_{K/\mathbb{Q}}(\epsilon') = 1$, άρα αφού $N_{K/\mathbb{Q}}(\epsilon), N_{K/\mathbb{Q}}(\epsilon') \in \mathbb{Z}$ οπότε $N_{K/\mathbb{Q}}(\epsilon) = N_{K/\mathbb{Q}}(\epsilon') = \pm 1$.

Αν πάλι $N_{K/\mathbb{Q}}(\epsilon) = \pm 1$, τότε

$$\epsilon\sigma_2(\epsilon)\cdots\sigma_n(\epsilon) = \pm 1$$

συνεπώς υπάρχει ϵ' με $\epsilon\epsilon' = \pm 1$. Αφού $\epsilon \in R$ έχουμε ότι ϵ' ακέραιος αλγεβρικός υπεράνω του R. Αλλά $\epsilon' = \pm\frac{1}{\epsilon} \in K$ και αφού είναι ακέραιος αλγεβρικός έχουμε ότι $\epsilon' \in R$ άρα $\epsilon \in E(R)$. □

Πρόταση IV.1.10. *Έστω* K, L, M *αλγεβρικά σώματα αριθμών με* $K \subset L \subset M$. *Τότε για κάθε* $\alpha \in M$ *ισχύει:*

$$\mathrm{Tr}_{L/K}\big(\mathrm{Tr}_{M/L}(\alpha)\big) = \mathrm{Tr}_{M/K}(\alpha)$$

και

$$N_{L/K}\big(N_{M/L}(\alpha)\big) = N_{M/K}(\alpha).$$

Απόδειξη. Έστω N μια κανονική επέκταση του $\mathbb{Q}$ τέτοια ώστε $M \subset N$. Επεκτείνουμε τις $n = [L : K]$ K-εμφυτεύσεις $\sigma_1, \ldots, \sigma_n$ σε K-αυτομορφισμούς του N. Θέτουμε $m = [M : L]$ και επεκτείνουμε και τις m το πλήθος L-εμφυτεύσεις $\tau_1, \ldots, \tau_m$ του M σε L-αυτομορφισμούς του N, διαλέγουμε κάθε φορά μόνο μία από τις επεκτάσεις και την ξανασυμβολίζουμε πάλι με σ_i και τ_j οπότε έχουμε

$$\mathrm{Tr}_{L/K}\big(\mathrm{Tr}_{M/L}(\alpha)\big) = \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \tau_j(\alpha) \right) = \sum_{i,j} \sigma_i\tau_j(\alpha)$$

$$N_{L/K}\big(N_{M/L}(\alpha)\big) = \prod_{i=1}^{n} \sigma_i \left(\prod_{j=1}^{m} \tau_j(\alpha) \right) = \prod_{i,j} \sigma_i\tau_j(\alpha)$$

Τα $\sigma_i\tau_j$ είναι K-εμφυτεύσεις του M στο N. Αν αποδείξουμε ότι είναι ανά δύο μεταξύ τους διαφορετικές, τότε αφού είναι σε πλήθος nm θα έχουμε τελειώσει.

Έστω $\sigma_i\tau_j = \sigma_{i'}\tau_{j'}$. Έστω τυχαίο $\alpha \in L$, τότε $\sigma_i(\tau_j(\alpha)) = \sigma_{i'}(\tau_{j'}(\alpha)$ άρα $\sigma_i(\alpha) = \sigma_{i'}(\alpha)$ για κάθε $\alpha \in L$. Συνεπώς $\sigma_i = \sigma_{i'}$, δηλαδή $i = i'$ οπότε $\tau_j = \tau_{j'}$. □

IV.2 Διακρίνουσα μιας n-άδας

Έστω L/K μια πεπερασμένη και διαχωρίσιμη επέκταση σωμάτων. Ξαναθυμίζουμε ακόμη μια φορά ότι υπάρχουν ακριβώς $n = [L : K]$ -εμφυτεύσεις του L σε κάποια κανονική θήκη του K έστω N, τέτοια ώστε $L \subset N$. Έστω $\sigma_1, \sigma_2, \ldots, \sigma_n$ αυτές οι εμφυτεύσεις και έστω $(a_1, a_2, \ldots, a_n) \in L^n$ μια n-άδα του L.

Ορισμός IV.2.1. Η ποσότητα

$$D_{L/K}(a_1, \ldots, a_n) = \big(\det(\sigma_i(a_j))\big)^2$$

θα λέγεται *διακρίνουσα* της n-άδας $(a_1, \ldots, a_n)$.

Για παράδειγμα αν $K = \mathbb{Q}(\sqrt{2})$, $D_K(1, \sqrt{2}) = 8$.

Πρόταση IV.2.2. *Έστω* L/K *επέκταση και* $(a_1, a_2, \ldots, a_n)$ *όπως παραπάνω. Τότε* $D_{L/K}(a_1, \ldots, a_n) \in K$.

Απόδειξη. Υπολογίζουμε

$$\begin{aligned} D_{L/K}(a_1, \ldots, a_n) &= \det \begin{pmatrix} a_1 & a_1 & \cdots & a_n \\ \sigma_2(a_1) & \sigma_2(a_2) & \cdots & \sigma_2(a_n) \\ \sigma_3(a_1) & \sigma_3(a_2) & \cdots & \sigma_3(a_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(a_1) & \sigma_n(a_2) & \cdots & \sigma_n(a_n) \end{pmatrix}^2 \\ &= \det \begin{pmatrix} \mathrm{Tr}_{L/K}(a_1^2) & \mathrm{Tr}_{L/K}(a_1a_2) & \cdots & \mathrm{Tr}_{L/K}(a_1a_n) \\ \mathrm{Tr}_{L/K}(a_2a_1) & \mathrm{Tr}_{L/K}(a_2^2) & \cdots & \mathrm{Tr}_{L/K}(a_2a_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{L/K}(a_na_1) & \mathrm{Tr}_{L/K}(a_na_2) & \cdots & \mathrm{Tr}_{L/K}(a_n^2) \end{pmatrix} \end{aligned}$$

Η τελευταία ποσότητα είναι στοιχείο του K αφού το ίχνος είναι στοιχείο του K. □

Παρατήρηση IV.2.3. Αν L, K είναι αλγεβρικά σώματα αριθμών $K \subset L$ με αντίστοιχους δακτυλίους ακεραίων S, R και $a_i \in S$ για κάθε $i = 1, \dots, n$, τότε $D_{L/K}(a_1, \dots, a_n) \in R$.

Θεώρημα IV.2.4. *Έστω* L/K *πεπερασμένη και διαχωρίσιμη επέκταση σωμάτων* $[L : K] = n$ *και* $L = K(\theta)$. *Έστω* $f(x) = \mathrm{Irr}(\theta, K) = \prod_{\nu=1}^{n}(x - \theta_\nu)$, *με* $\theta_\nu \in \widetilde{K}$. *Ισχύει* $\sigma_\nu(\theta) = \theta_\nu$. *Τότε*

$$D_{L/K}(1, \theta, \theta^2, \dots, \theta^{n-1}) = \prod_{1 \le \nu < \mu \le n} (\theta_\nu - \theta_\mu)^2 \neq 0,$$

και

$$D_{L/K}(1, \theta, \theta^2, \dots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\theta))$$

Απόδειξη. Παρατηρούμε ότι

$$\begin{aligned}
D_{L/K}(\theta) &= \prod_{1 \le \nu < \mu \le n} (\theta_\nu - \theta_\mu)^2 \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{\nu=1}^{n} \prod_{\substack{\mu=1 \\ \mu \neq \nu}}^{n} (\theta_\nu - \theta_\mu) \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{\nu=1}^{n} \left(\prod_{\substack{\mu=1 \\ \mu \neq \nu}}^{n} (x - \theta_\mu) \right) \Bigg|_{x=\theta_\nu} \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{\nu=1}^{n} f'(\theta_\nu) \\
&= (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\theta)).
\end{aligned}$$

□

Ορισμός IV.2.5. Η διακρίνουσα $D_{L/K}(\theta) = D_{L/K}(1, \theta, \dots, \theta^{n-1})$ λέγεται η *διακρίνουσα του στοιχείου* θ υπεράνω του K.

Από το θεώρημα IV.2.4 προκύπτει ότι

$$L = K(a) \Leftrightarrow D_{L/K}(a) \neq 0.$$

Πράγματι η συνεπαγωγή «⇒» προκύπτει άμεσα από τον ορισμό της διακρίνουσας και την παρατήρηση ότι όλα τα συζυγή είναι μεταξύ τους διαφορετικά.

Αντιστρόφως αν $D_{L/K}(a) = \prod_{i>j}(\sigma_i(a) - \sigma_j(a))^2 \neq 0$, τότε $\sigma_i(a) \neq \sigma_j(a)$ για κάθε $i \neq j$, δηλαδή όλα τα συζυγή του a είναι ανά δύο μεταξύ τους διαφορετικά, δηλαδή το ανάγωγο πολυώνυμο του a είναι ίσο με το χαρακτηριστικό πολυώνυμο του a υπεράνω του K, συνεπώς

$$\deg \mathrm{Irr}(a, K) = n = [L : K].$$

Αφού $K \subset K(a) \subset L$ και $[K(a) : K] = \deg \mathrm{Irr}(a, K)$ έπεται ότι $L = K(a)$.

Ακόμα ισχύει το

Πόρισμα IV.2.6. *Έστω* $a_1, a_2, \dots, a_n \in L$. *Τότε ισχύει*

$$D_{L/K}(a_1, a_2, \dots, a_n) \neq 0 \Leftrightarrow \{a_1, a_2, \dots, a_n\} \textit{ βάση της επέκτασης } L/K$$

Απόδειξη. Αν το σύνολο $\{\alpha_1, \dots, \alpha_n\}$, $\alpha_i \in L$ είναι γραμμικά εξαρτημένο υπεράνω του K, τότε υπάρχουν $\lambda_1, \dots, \lambda_n \in K$ όχι όλα μηδέν ώστε

$$\lambda_1 \alpha_1 + \cdots + \lambda_n \alpha_n = 0.$$

Εφαρμόζουμε τα σ_i και έχουμε

$$\lambda_1\sigma_i(a_1) + \lambda_2\sigma_i(a_2) + \cdots + \lambda_n\sigma_i(a_n) = 0$$

για κάθε $i \in 1, \ldots, n$. και βλέπουμε ότι έχει μια μη τετριμμένη λύση $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$ συνεπώς $\det(\alpha_1, \ldots, \alpha_n) = 0$ και κατά συνέπεια $D_{L/K}(\alpha_1, \ldots, \alpha_n) = 0$.

Τώρα υποθέτουμε το $\alpha_1, \ldots, \alpha_n$, $\alpha_i \in L$ είναι K-γραμμικά ανεξάρτητα. Αφού $[L : K] = n$ αυτά αποτελούν μια K-βάση του L. Αν $L = K(\theta)$ μια άλλη βάση είναι η $\{1, \theta, \ldots, \theta^{n-1}\}$. Συνεπώς υπάρχουν $\mu_{ij} \in K$ για τα οποία έχουμε

$$\begin{aligned} 1 &= \mu_{11}\alpha_1 + \cdots + \mu_{1n}\alpha_n \\ \theta &= \mu_{21}\alpha_1 + \cdots + \mu_{2n}\alpha_n \\ &\ldots\ldots\ldots\ldots\ldots \\ \theta^{n-1} &= \mu_{n1}\alpha_1 + \cdots + \mu_{nn}\alpha_n \end{aligned}$$

άρα $D_{L/K}(\theta) = D_{L/K}(1, \theta, \ldots, \theta^{n-1}) = \det(\mu_{ij})^2 D_{L/K}(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$. Αλλά $K = \mathbb{Q}(\theta)$ οπότε $D_{L/K}(\theta) \neq 0$.

□

Παράδειγμα IV.2.7. Έστω $K = \mathbb{Q}$ και $L = \mathbb{Q}(\zeta_p)$, όπου $\zeta_p = e^{2\pi i/p}$, με $p \neq 2$ πρώτος.

Γνωρίζουμε ότι $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, αφού

$$f(x) = \mathrm{Irr}(\zeta_p, \mathbb{Q}) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{\nu=1}^{p-1}(x - \zeta_p^\nu).$$

Επίσης

$$x^p - 1 = (x-1)f(x) \Rightarrow px^{p-1} = f(x) + (x-1)f'(x) \Rightarrow f'(\zeta_p) = \frac{p\zeta_p^{p-1}}{\zeta_p - 1}.$$

Προφανώς $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(p) = p^{p-1}$, και $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = (-1)^{p-1} \cdot 1 = 1$. Επίσης

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1) = \prod_{\nu=1}^{p-1}(\zeta_p^\nu - 1) = (-1)^{p-1}\prod_{\nu=1}^{p-1}(1 - \zeta_p^\nu) = p.$$

Συνεπώς

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(f'(\zeta_p)) = p^{p-2},$$

οπότε η διακρίνουσα είναι ίση με

$$D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}.$$

IV.3 Ελεύθερες αβελιανές ομάδες πεπερασμένου βαθμού (rank)

Μια αβελιανή ομάδα $(M, +)$ θα λέγεται *ελεύθερη αβελιανή ομάδα* πεπερασμένου βαθμού (rank) αν και μόνο αν υπάρχουν $m_1, \ldots, m_n \in M$ ώστε

1.
$$M = m_1\mathbb{Z} + m_2\mathbb{Z} + \cdots + m_n\mathbb{Z} = \left\{\sum_{i=1}^{n} m_i x_i | x_i \in \mathbb{Z}, i = 1, \ldots, n\right\}$$

2. Η παραπάνω παράσταση είναι μοναδική, δηλαδή αν

$$x_1m_1 + \cdots + x_nm_n = 0 \Rightarrow x_1 = \ldots = x_n = 0.$$

Τα $(m_1, \ldots, m_n)$ λέγονται σε αυτή την περίπτωση $\mathbb{Z}$-ελεύθερα.

Κάθε σύνολο $\{m_1, \ldots, m_n\}$ λέγεται σε αυτή την περίπτωση $\mathbb{Z}$-βάση της M.

Παρατήρηση IV.3.1. Σε κάθε ελεύθερη αβελιανή ομάδα πεπερασμένου βαθμού (rank) όλες οι βάσεις έχουν το ίδιο πλήθος στοιχείων. Πράγματι από τον ορισμό έπεται ότι αν η M έχει μια βάση με n το πλήθος στοιχεία, τότε $M \cong \mathbb{Z}^n$ αν είχε και μια βάση με διαφορετικό πλήθος στοιχείων, τότε θα έπρεπε $\mathbb{Z}^n \cong \mathbb{Z}^m$, το οποίο είναι άτοπο όπως βλέπει κανείς θεωρώντας την M modulo ένα πρώτο p.

Συγκεκριμένα για $p = 2$ η απεικόνιση

$$\phi : \frac{M}{2M} \ni x_1 m_1 + x_2 m_2 + \cdots + x_n m_n \mapsto (x_1 + 2\mathbb{Z}, x_2 + 2\mathbb{Z}, \ldots, x_n + 2\mathbb{Z}) \in (\mathbb{Z}/2\mathbb{Z})^n$$

είναι ένας ισομορφισμός ομάδων, επομένως $\#M/2M = 2^n$. Αν $M \cong \mathbb{Z}^m$, τότε και $\#M/2M = 2^m$. Επομένως $2^n = 2^m$, δηλαδή $n = m$.

Ορισμός IV.3.2. Το πλήθος των στοιχείων μιας βάσης θα λέγεται βαθμός (rank) της M.

Ορισμός IV.3.3. Ένας $n \times n$ πίνακας $A = (a_{ij})$ με συντελεστές από το $\mathbb{Z}$ θα λέγεται unimodular αν και μόνο αν η ορίζουσά του είναι ± 1.

Θεώρημα IV.3.4. *Έστω M ελεύθερη αβελιανή ομάδα πεπερασμένου βαθμού (rank) και $m_1, m_2, \ldots, m_n$ μια βάση αυτής. Έστω ακόμα $m'_1, m'_2, \ldots, m'_n \in M$. Τότε ισχύει $m'_1, \ldots, m'_n$ είναι μια βάση της M αν και μόνο αν υπάρχει unimodular πίνακας A ώστε*

$$\begin{pmatrix} m'_1 \\ m'_2 \\ \vdots \\ m'_n \end{pmatrix} = A \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}.$$

Απόδειξη. Αν $m'_1, \ldots, m'_n$ βάση της M, τότε υπάρχει πίνακας $A \in M_n(\mathbb{Z})$ με

$$\begin{pmatrix} m'_1 \\ m'_2 \\ \vdots \\ m'_n \end{pmatrix} = A \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}$$

και

$$\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = A' \begin{pmatrix} m'_1 \\ m'_2 \\ \vdots \\ m'_n \end{pmatrix}.$$

Συνδυάζοντας τις παραπάνω σχέσεις έχουμε ότι

$$\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = AA' \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}$$

Επομένως, αφού $(m_1, \ldots, m_n)$ βάση της M έχουμε ότι $A'A = \mathbb{I}_n$ και $\det(A)\det(A') = 1$ από όπου προκύπτει ότι $\det(A) = \pm 1$.

Για το αντίστροφο αρκεί να δείξουμε ότι τα $m'_1, \ldots, m'_n$ είναι $\mathbb{Z}$-ελεύθερα. Αφού $\det(A) = \pm 1$ υπάρχει $A^{-1} \in M_n(\mathbb{Z})$ οπότε από

$$\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = A^{-1} \begin{pmatrix} m'_1 \\ m'_2 \\ \vdots \\ m'_n \end{pmatrix}$$

έχουμε ότι $m'_1, \dots, m'_n$ είναι βάση του M.

□

Θεώρημα IV.3.5 (Elementarteilersatz). *Έστω $(M,+)$ ελεύθερη αβελιανή ομάδα πεπερασμένα παραγόμενη με rank n και έστω T μια υποομάδα της M. Τότε ισχύουν:*

1. *T είναι ελεύθερη αβελιανή ομάδα με $\mathrm{rank}(T) \le n$*
2. *Υπάρχει μια βάση $\omega_1, \dots, \omega_n$ του M και $\epsilon_1, \dots, \epsilon_d \in \mathbb{Z} - \{0\}$, $d \le n$ ώστε*
   (α') $\epsilon_1\omega_1, \dots, \epsilon_d\omega_d$ είναι βάση του T
   (β') $\epsilon_1 \mid \epsilon_2$, $\epsilon_2 \mid \epsilon_3$, ..., $\epsilon_{d-1} \mid \epsilon_d$
3. *Τα κύρια ιδεώδη $\langle\epsilon_1\rangle, \langle\epsilon_2\rangle, \dots, \langle\epsilon_d\rangle$, ορίζονται μονοσήμαντα από το T.*

Καταρχήν αποδεικνύουμε το ακόλουθο:

Λήμμα IV.3.6. *Έστω M μια ελεύθερη αβελιανή ομάδα πεπερασμένου βαθμού (rank) και T μια υποομάδα της M. Τότε ισχύουν:*

1. *Η T είναι ελεύθερη αβελιανή ομάδα πεπερασμένου βαθμού (rank)*
2. $\mathrm{rank}T \le \mathrm{rank}M$

Παρατήρηση IV.3.7. Μπορεί να συμβεί $T \subset M$ και $\mathrm{rank}(T) = \mathrm{rank}(M)$, για παράδειγμα $2\mathbb{Z} \subset \mathbb{Z}$.

Απόδειξη. (του IV.3.6.1) Επαγωγικά ως προς την rank n του M.

Αν $n = 1$, τότε $M = m_1\mathbb{Z} \cong \mathbb{Z}$. Άρα η υποομάδα είναι $T = \langle 0\rangle$ ή $T = t\mathbb{Z}, t \in \mathbb{N}$, δηλαδή το λήμμα ισχύει.

Έστω ότι ισχύει για ελεύθερες αβελιανές ομάδες με rank $n-1$. Θεωρούμε μια βάση $m_1, m_2, \dots, m_n$ του M, όπου

$$M = m_1\mathbb{Z} \oplus m_2\mathbb{Z} \oplus \cdots \oplus m_n\mathbb{Z}$$

και ονομάζουμε

$$M_{n-1} := m_1\mathbb{Z} \oplus \cdots \oplus m_{n-1}\mathbb{Z}, \quad T_{n-1} := T \cap M_{n-1}.$$

Λόγω της επαγωγικής υπόθεσης έχουμε ότι T_{n-1} είναι ελεύθερη αβελιανή ομάδα με rank $\mathrm{rank}T_{n-1} \le \mathrm{rank}M_{n-1} = n - 1$.

Ισχυριζόμαστε ότι υπάρχει $t_n \in T$ ώστε $T = T_{n-1} \oplus t_n\mathbb{Z}$. Παρατηρούμε ότι αν αποδειχτεί ο παραπάνω ισχυρισμός, τότε έχουμε αποδείξει αυτό που θέλουμε, δηλαδή ότι T ελεύθερη και $\mathrm{rank}T \le n$.

Κάθε $m \in M$ έχει μια μονοσήμαντη παράσταση της μορφής:

$$m = x_1m_1 + \cdots + x_nm_n : \text{ με } x_i \in \mathbb{Z}$$

Γράφουμε $x_i := x_i(m)$ για $i = 1, 2, \dots, n$. Ορίζουμε το σύνολο

$$\mathcal{A} = \{x \in \mathbb{Z} : \text{ υπάρχει } t \in T \text{ με } x = x_n(t)\}.$$

Προφανώς $\mathcal{A}$ είναι ιδεώδες του $\mathbb{Z}$. Ξεχωρίζουμε δύο περιπτώσεις:

- $\mathcal{A} = \langle 0\rangle$. Σε αυτή την περίπτωση $T = T_{n-1}$ δηλαδή το T είναι ελεύθερη ομάδα με rank $\le n - 1 < n$.
- Σε αυτή την περίπτωση $\mathcal{A} \neq \langle 0\rangle$, δηλαδή υπάρχει $a_n \in \mathbb{N} - \{0\}$, ώστε $\mathcal{A} = a_n\mathbb{Z}$. Διαλέγουμε ένα $t_n \in T$, ώστε $x_n(t_n) = a_n$. Η σχέση

$$T \supset T_{n-1} + t_n\mathbb{Z}$$

είναι προφανής. Έστω $t \in T$ συνεπώς $x_n(t) = xa_n$, $x \in \mathbb{Z}$, διότι $x_n(t) \in \mathcal{A} = \mathbb{Z}a_n$, οπότε γράφουμε

$$t = (t - xt_n) + xt_n.$$

Αρκεί $t - xt_n \in T_{n-1}$, δηλαδή αρκεί να δείξουμε ότι η n-στή συνιστώσα του $t - xt_n$ είναι μηδενική. Πράγματι,

$$x_n(t - xt_n) = x_n(t) - x_n(xt_n) = x_n(t) - xx_n(t_n) = xa_n - xa_n = 0.$$

Επομένως, δείξαμε ότι $T = T_{n-1} + \mathbb{Z}t_n$.

Αν $xt_n \in T$, τότε έχουμε $x_n(xt_n) = 0$ και συνεπώς $xx_n(t_n) = 0$ δηλαδή $xa_n = 0$. Αφού $a_n \neq 0$ καταλήγουμε στο $x = 0$, δηλαδή $T_{n-1} \cap \mathbb{Z}t_n = \{0\}$ και το άθροισμα είναι ευθύ:

$$T = T_{n-1} \oplus \mathbb{Z}t_n.$$

□

Παρατηρούμε ότι, αν $\phi : M \to \mathbb{Z}$ ομομορφισμός ομάδων, τότε

$$\phi(xm + x'm') = x\phi(m) + x'\phi(m') \text{ για κάθε } x, x' \in \mathbb{Z}, m, m' \in M.$$

Δηλαδή το ϕ είναι γραμμικό συναρτησιοειδές επί του M. Για παράδειγμα αν

$$M = \mathbb{Z}m_1 \oplus \mathbb{Z}m_2 \oplus \cdots \oplus \mathbb{Z}m_n$$

και $m \in M$,

$$m = x_1(m)m_1 + \cdots + x_n(m)m_n,$$

τότε η $\phi_i : M \to \mathbb{Z}$, $m \mapsto x_i(m)$ είναι ομομορφισμός ομάδων. Είναι προφανές ότι αν $\phi : M \to \mathbb{Z}$, τότε

$$\phi(T) := \{x \in \mathbb{Z} : \text{ υπάρχει } t \in T, \phi(t) = x\}$$

είναι ένα ιδεώδες του $\mathbb{Z}$. Από τα παραπάνω φαίνεται ότι το, διάφορο του κενού, σύνολο ιδεωδών

$$J := \{\phi(T) : \phi : M \to \mathbb{Z} \text{ ομομορφισμός ομάδων}\}$$

έχει μέγιστα στοιχεία. Έστω $\phi_0(T)$ ένα μέγιστο στοιχείο του J.

Τότε είναι προφανές ότι υπάρχει $\epsilon_0 \in \mathbb{N}$ με $\phi_0(T) = \mathbb{Z}\epsilon_0$ και υπάρχει $t_0 \in T$ με $\phi_0(t_0) = \epsilon_0$. Ισχυριζόμαστε τώρα ότι για το t_0 υπάρχει $\omega_0 \in M$ έτσι ώστε $t_0 = \epsilon_0\omega_0$.

Πράγματι, θεωρούμε τυχούσα βάση $\{m_1, m_2, \ldots, m_n\}$ της M. Αρκεί να αποδείξουμε ότι $\epsilon_0 \mid x_i(t_0)$ για κάθε $i = 1, 2, \ldots n$.

Για $i = 1$. Θεωρούμε τους ομομορφισμούς

$$\phi_{A,B} = A\phi_0 + Bx_1 : m \mapsto A\phi_0(m) + B\phi_1(m) \in \mathbb{Z}, A, B \in \mathbb{Z}.$$

Συνεπώς

$$\phi_{A,B}(t_0) = A\phi_0(t_0) + B\phi_1(t_0) = A\epsilon_0 + Bx_1(t_0).$$

Θεωρούμε τώρα το άθροισμα των κυρίων ιδεωδών $\langle\epsilon_0\rangle$ και $\langle x_1(t_0)\rangle = \mathbb{Z}x_1(t_0)$ το οποίο προφανώς είναι κύριο ιδεώδες, δηλαδή υπάρχουν $A, B \in \mathbb{Z}$ με

$$\mathbb{Z}\epsilon_0 + \mathbb{Z}x_1(t_0) = \mathbb{Z}(A\epsilon_0 + Bx_1(t_0))$$

συνεπώς

$$\phi_0(T) = \mathbb{Z}\epsilon_0 \subseteq \mathbb{Z}(A\epsilon_0 + Bx_1(t_0)) \subseteq \phi_{A,B}(T).$$

Επειδή το $\phi_0(T)$ μέγιστο στο σύνολο J και $\phi_{A,B}(T) \in J$ έχουμε ότι

$$\phi_0(T) = \mathbb{Z}\epsilon_0 = \mathbb{Z}(A\epsilon_0 + Bx_1(t_0)) = \phi_{A,B}(T),$$

δηλαδή

$$\mathbb{Z}\epsilon_0 = \mathbb{Z}\epsilon_0 + \mathbb{Z}x_1(t_0)$$

και $x_1(t_0) \in \mathbb{Z}\epsilon_0$ άρα $\epsilon_0 \mid x_1(t_0)$.

Υποθέτουμε τώρα ότι $T \neq 0$ και διαλέγουμε $\phi_0, \epsilon_0, \omega_0, t_0$ όπως παραπάνω. Προφανώς $t_0 \neq 0$, οπότε $\epsilon_0, \omega_0 \neq 0$. Θα αποδείξουμε τώρα ότι

$$M = \mathbb{Z}\omega_0 \oplus \ker\phi_0 \tag{IV.5}$$

$$T = \mathbb{Z}\epsilon_0\omega_0 \oplus (\ker\phi_0 \cap T). \tag{IV.6}$$

Προφανώς $\mathbb{Z}\omega_0 \oplus \ker\phi_0 \subseteq M$ και $\mathbb{Z}\epsilon_0\omega_0 \oplus (\ker\phi_0 \cap T) \subset T$. Αρκεί λοιπόν να αποδείξουμε τη σχέση του περιέχεσθαι προς την αντίθετη κατεύθυνση.

$$t_0 = \epsilon_0\omega_0 \text{ συνεπώς } \phi_0(t_0) = \epsilon_0\phi_0(\omega_0)$$

συνεπώς $\epsilon_0 = \epsilon_0\phi_0(\omega_0)$ και τελικά $\phi_0(\omega_0) = 1$. Το τυχαίο στοιχείο $m \in M$ το γράφουμε

$$m = \phi_0(m)\omega_0 + (m - \phi_0(m)\omega_0).$$

Αρκεί να δείξουμε ότι $m - \phi_0(m)\omega_0 \in \ker\phi_0$. Πράγματι,

$$\phi_0(m - \phi_0(m)\omega_0) = \phi_0(m) - \phi_0(m)\phi_0\omega_0 = 0.$$

Συνεπώς $M = \mathbb{Z}\omega_0 \oplus \ker\phi_0$.

Έστω τώρα τυχαίο $t \in T$, $\phi_0(t) \in \phi_0(T) = \mathbb{Z}\epsilon_0$, δηλαδή $\phi_0(t) = x\epsilon_0$, $x \in \mathbb{Z}$. Γράφουμε

$$t = \phi_0(t)\omega_0 + (t - \phi_0(t)\omega_0) = x\epsilon_0\omega_0 + (t - \phi_0(t)\omega_0).$$

Αρκεί να δείξουμε ότι

$$t - \phi_0(t)\omega_0 \in \ker\phi_0 \cap T.$$

Όπως παραπάνω για το m, έτσι και για το t, έχουμε

$$t - \phi_0(t)\omega_0 \in \ker\phi_0.$$

Ακόμη

$$t - \phi_0(t)\omega_0 = t - x\epsilon_0\omega_0 = t - xt_0 \in T.$$

Συνεπώς

$$T = \mathbb{Z}\epsilon_0\omega_0 \oplus (\ker\phi_0 \cap T),$$

και συνεχίζουμε επαγωγικά.

Τώρα θα αποδείξουμε το 2 του θεώρηματος IV.3.5. Η απόδειξη θα γίνει επαγωγικά ως προς τον βαθμό του n. Αν το $n = 0$ δεν έχουμε κάτι να αποδείξουμε.

Από την απόδειξη $M = \mathbb{Z}\omega_0 \oplus \ker\phi_0$ στο πρώτο μέρος και αφού ο βαθμός του $\mathbb{Z}\omega_0$ είναι ένα, έπεται ότι ο $\ker\phi_0$ είναι μια ελεύθερη αβελιανή ομάδα βαθμού (rank) $n - 1$. Εφαρμόζουμε την υπόθεση της μαθηματικής επαγωγής για την $\ker\phi_0$ βαθμού $n-1$ και την υποομάδα της $\ker\phi_0 \cap T$.

Επομένως αν $\ker\psi_0 \cap T \neq \{0\}$, τότε υπάρχει ένα $d \leq n$ και μια βάση $\{\omega_2, \ldots, \omega_n\}$ του $\ker\phi_0$ καθώς και, μη-μηδενικοί, ακέραιοι $\epsilon_2, \epsilon_3, \ldots, \epsilon_d \in \mathbb{Z}$ ώστε το σύνολο $\{\epsilon_2\omega_2, \epsilon_3\omega_3, \ldots, \epsilon_d\omega_d\}$ να αποτελεί μια βάση του $T \cap \ker\phi_0$. Επιπλέον για τα $\epsilon_2, \epsilon_3, \ldots, \epsilon_d$ ισχύει $\epsilon_i \mid \epsilon_{i+1}$, $2 \leq i \leq d - 1$. Ονομάζουμε $\omega_1 := \omega_0$ και $\epsilon_1 := \epsilon_0$ στους τύπους (IV.5) και (IV.6). Επομένως λόγω της (IV.5) έχουμε ότι το $\{\omega_1, \omega_2, \ldots, \omega_n\}$ είναι μια βάση του M, και λόγω της (IV.6) και ότι $\epsilon_1\omega_1 = \epsilon_0\omega_0$ έχουμε ότι το $\{\epsilon_1\omega_1, \ldots, \epsilon_d\omega_d\}$ είναι μια βάση του T. Απομένει να αποδειχθεί ότι $\epsilon_1 \mid \epsilon_2$. Αν f

είναι το γραμμικό συναρτησιοειδές της M που ορίζεται από τις σχέσεις $f(\omega_1) = f(\omega_2) = 1$ και $f(\omega_i) = 0$ για $i \geq 3$, τότε $\epsilon_1 = \epsilon_0 = f(\epsilon_0\omega_0) = f(\epsilon_1\omega_1) \in f(T)$. Αυτό σημαίνει ότι $R\epsilon_1 \subset f(T)$ αφού το $f(T)$ είναι ιδεώδες του R. Επειδή από την απόδειξη του 1. το $R\epsilon_0$ είναι μέγιστο ιδεώδες έχουμε $f(T) = R\epsilon_0 = R\epsilon_1$. Τώρα

$$\epsilon_2 = f(\epsilon_2\omega_2) \in f(T) = R\epsilon_1$$

δηλαδή $\epsilon_2 \in R\epsilon_1$ οπότε $\epsilon_1 \mid \epsilon_2$.

Παρατήρηση IV.3.8. Και η 3η ιδιότητα είναι σημαντική, αφού τα ιδεώδη ορίζονται μονοσήμαντα από το T και όχι από τα στοιχεία της βάσης του M που έχουμε επιλέξει. Αυτό δεν το χρειαζόμαστε στα επόμενα και ως εκ τούτου δεν θα το αποδείξουμε. Ο ενδιαφερόμενος αναγνώστης παραπέμπεται σε διάφορα βιβλία Άλγεβρας, για παράδειγμα T.W. Hungerford, [7, σελ. 225] ή S. Bosch [4, σελ. 66-78].

Παρατήρηση IV.3.9. Εντελώς όμοια είναι η απόδειξη αν αντί για το $\mathbb{Z}$ είχαμε περιοχή κυρίων ιδεωδών R και M ένα R-module.

Αποδείξαμε λοιπόν το μέρος του Θεωρήματος IV.3.5 που θα χρειαστούμε στα παρακάτω. Θα κλείσουμε την παράγραφο με μία εφαρμογή.

Θεώρημα IV.3.10. *Έστω*

$$M = \mathbb{Z}m_1 \oplus \mathbb{Z}m_2 \oplus \cdots \oplus \mathbb{Z}m_n$$

και

$$T = \mathbb{Z}t_1 \oplus \mathbb{Z}t_2 \oplus \cdots \oplus \mathbb{Z}t_n$$

ελεύθερες αβελιανές ομάδες με rank n*, και* $T \leq M$*. Έστω* $A \in M_n(\mathbb{Z})$*, ο μονοσήμαντα ορισμένος* $n \times n$ *πίνακας με στοιχεία από το* $\mathbb{Z}$ *ώστε*

$$\begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = A \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}$$

Τότε ισχύει $[M : T] = \#M/T = |\det A|$.

Απόδειξη. Διαλέγουμε βάση για τα M και , σύμφωνα με το Θεώρημα IV.3.5.

$$\begin{aligned} T &= \mathbb{Z}\epsilon_1\omega_1 \oplus \cdots \oplus \mathbb{Z}\epsilon_n\omega_n \\ M &= \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n \end{aligned}$$

Κατά την αλλαγή βάσεων έχουμε

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = B \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix},$$

και

$$\begin{pmatrix} \epsilon_1\omega_1 \\ \epsilon_2\omega_2 \\ \vdots \\ \epsilon_n\omega_n \end{pmatrix} = \Gamma \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix},$$

όπου B, Γ unimodular πίνακες $B, \Gamma \in M_n(\mathbb{Z})$, $\det B = \pm 1, \det \Gamma = \pm 1$. Τελικά καταλήγουμε στο

$$\begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = \Gamma^{-1} \begin{pmatrix} \epsilon_1\omega_1 \\ \epsilon_2\omega_2 \\ \vdots \\ \epsilon_n\omega_n \end{pmatrix} = \Gamma^{-1}\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n) \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = \Gamma^{-1}\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n)B \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}.$$

Δηλαδή

$$A = \Gamma^{-1}\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n)B \Rightarrow |\det A| = |\epsilon_1\epsilon_2\cdots\epsilon_n|.$$

Από την άλλη μεριά

$$\frac{M}{T} = \frac{\mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n}{\mathbb{Z}\epsilon_1\omega_1 \oplus \cdots \oplus \mathbb{Z}\epsilon_n\omega_n} \cong \frac{\mathbb{Z}}{\epsilon_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{\epsilon_n\mathbb{Z}}$$

από όπου προκύπτει ότι

$$|M/T| = |\epsilon_1\cdots\epsilon_n|,$$

δηλαδή το ζητούμενο. □

IV.4 Διακρίνουσα σώματος και βάση ακεραιότητας αυτού

Έστω K αλγεβρικό σώμα αριθμών $K = \mathbb{Q}(\theta)$ με $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, και $\omega_1, \ldots, \omega_n$ μια βάση της επέκτασης $K/\mathbb{Q}$. Έστω

$$\alpha_i = \sum_{j=1}^{n} a_{ij}\omega_j : i = 1, 2, \ldots, n$$

n-στοιχεία του σώματος K, $a_{ij} \in \mathbb{Q}$ για $1 \le i, j \le n$.

Πρόταση IV.4.1. *Ισχύει*

$$D_K(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2 D_K(\omega_1, \ldots, \omega_n).$$

Απόδειξη.

$$\begin{aligned} \mathrm{Tr}_K(\alpha_\kappa\alpha_\lambda) &= \mathrm{Tr}_K\left(\sum_{i=1}^{n} a_{\kappa i}\omega_i \cdot \sum_{j=1}^{n} a_{\lambda j}\omega_j\right) \\ &= \mathrm{Tr}_K\left(\sum_{i,j=1}^{n} a_{\kappa i}a_{\lambda j}\omega_i\omega_j\right) \\ &= \sum_{i,j=1}^{n} a_{\kappa i}a_{\lambda j}\mathrm{Tr}_K(\omega_i\omega_j). \end{aligned}$$

Συνεπώς καταλήγουμε στην ισότητα πινάκων

$$(\mathrm{Tr}_K(\alpha_\kappa\alpha_\lambda)) = (a_{\kappa i})\mathrm{Tr}_K(\omega_i\omega_j)(a_{\lambda j})^t$$

και θεωρώντας την ορίζουσα προκύπτει η ζητούμενη πρόταση. □

Κύριος σκοπός αυτής της παραγράφου είναι η απόδειξη του παρακάτω θεωρήματος:

Θεώρημα IV.4.2. *Έστω* K *αλγεβρικό σώμα αριθμών, και* R_K *ο δακτύλιος των ακεραίων αλγεβρικών του* K. *Αν* $[K : \mathbb{Q}] = n$, *τότε ο* R_K *είναι μια ελεύθερη αβελιανή ομάδα με βαθμού* n, *δηλαδή υπάρχει ένα σύστημα* $\{\omega_1, \omega_2, \ldots, \omega_n\}$ *στοιχείων του* R_K *ώστε*

$$R_K = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \oplus \cdots \oplus \mathbb{Z}\omega_n.$$

Παρατήρηση IV.4.3. Από το μονοσήμαντο της ανάλυσης έπεται ότι το σύνολο $\{\omega_1, \omega_2, \ldots, \omega_n\}$ είναι και βάση της επέκτασης $K/\mathbb{Q}$.

Ορισμός IV.4.4. Ένα σύστημα $\omega_1, \omega_2, \ldots, \omega_n$ ακεραίων αλγεβρικών αριθμών του K οι οποίοι είναι γραμμικά ανεξάρτητοι υπεράνω του $\mathbb{Q}$ και παράγουν το R ως $\mathbb{Z}$-module, θα λέγεται *βάση ακεραιότητας* του K.

Παρατήρηση IV.4.5. Αν L/K σχετική επέκταση αλγεβρικών σωμάτων αριθμών και $[L : K] = n$, τότε η ύπαρξη ενός συστήματος στοιχείων $\omega_1, \omega_2, \ldots, \omega_n$ του R_L το οποίο είναι K-γραμμικά ανεξάρτητα και το οποίο παράγει το R_L ως R_K-module είναι ισοδύναμο με το γεγονός ότι ο R_L είναι ελεύθερο R_K-module. Αυτό όμως, όπως θα δούμε παρακάτω, δεν ισχύει εν γένει. Όταν ισχύει, τότε το σύνολο $\{\omega_1, \omega_2, \ldots, \omega_n\}$ θα λέγεται σχετική βάση ακεραιότητας του L ως προς το K.

Αν $\{\omega_1, \ldots, \omega_n\}$ και $\{\omega'_1, \ldots, \omega'_n\}$ βάσεις ακεραιότητας του R, τότε λόγω του IV.4.1 έχουμε ότι

$$D_K(\omega_1, \ldots, \omega_n) \mid D_K(\omega'_1, \ldots, \omega'_n) \text{ και } D_K(\omega'_1, \ldots, \omega'_n) \mid D_K(\omega_1, \ldots, \omega_n)$$

και επειδή έχουν το ίδιο πρόσημο έχουμε

$$D_K(\omega_1, \ldots, \omega_n) = D_K(\omega'_1, \ldots, \omega'_n).$$

Από τα παραπάνω συμπεραίνουμε ότι η διακρίνουσα μιας βάσης ακεραιότητας δεν εξαρτάται από την εκλογή της βάσης και μπορούμε να δώσουμε τον παρακάτω:

Ορισμός IV.4.6. Έστω K αλγεβρικό σώμα αριθμών και $\{\omega_1, \ldots, \omega_n\}$ μια βάση ακεραιότητας της $K/\mathbb{Q}$. Η διακρίνουσα

$$D_K = D_{K/\mathbb{Q}} = D_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n)$$

θα λέγεται *διακρίνουσα του σώματος* K.

Παρατηρούμε ότι κάθε βάση ακεραιότητας της $K/\mathbb{Q}$ είναι και βάση της επέκτασης $K/\mathbb{Q}$.

Πρόταση IV.4.7. *Έστω K αλγεβρικό σώμα αριθμών βαθμού $[K : \mathbb{Q}] = n$ και έστω $\omega_1, \ldots, \omega_n \in R_K$ γραμμικά ανεξάρτητα υπεράνω του σώματος $\mathbb{Q}$. Τότε*

$$D_K(\omega_1, \ldots, \omega_n) = m^2 D_K,$$

όπου $m = [R : \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n]$.

Απόδειξη. Ας θεωρήσουμε μια βάση ακεραιότητας $\tau_1, \ldots, \tau_n$ και ας εκφράσουμε τα $\omega_1, \ldots, \omega_n$ σε σχέση με τη βάση αυτή:

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A \begin{pmatrix} \tau_1 \\ \vdots \\ \tau_n \end{pmatrix},$$

με $A \in M_n(\mathbb{Z})$. Τότε από το IV.4.1 έχουμε ότι

$$D_K(\omega_1, \ldots, \omega_n) = \det(A)^2 D_K$$

ενώ από το IV.3.10 έχουμε ότι $\det(A) = m$, δηλαδή το ζητούμενο. □

Κριτήριο IV.4.8. Έστω K ένα αλγεβρικό σώμα αριθμών και $\omega_1, \ldots, \omega_n \in R_K$ γραμμικά ανεξάρτητα υπεράνω του $\mathbb{Q}$. Τότε αν ο ακέραιος $D_K(\omega_1, \ldots, \omega_n)$ είναι ελεύθερος τετραγώνου, τότε τα $\{\omega_1, \ldots, \omega_n\}$ είναι βάση ακεραιότητας της $K/\mathbb{Q}$.

Σημείωση IV.4.9. Το παραπάνω κριτήριο δεν εφαρμόζεται πάντα για παράδειγμα $D_{\mathbb{Q}(i)} = -4$ και όμως $\{1, i\}$ είναι βάση ακεραιότητας της $\mathbb{Q}(i)/\mathbb{Q}$.

Θεώρημα IV.4.10 (Stickelberger). *Για κάθε αλγεβρικό σώμα αριθμών K η διακρίνουσά του είναι*

$$D_K \equiv 0, 1 \mod 4$$

Απόδειξη. Έστω $\omega_1, \dots, \omega_n$ μια βάση ακεραιότητας του K και έστω $\omega_i^{(j)}$ $i, j = 1, \dots, n$ τα συζυγή των ω_i. Υπολογίζουμε

$$D_K^{1/2} = \det(\omega_i^{(j)}) = \sum_{\substack{\sigma \in S_n \\ \text{άρτια}}} \omega_1^{(\sigma(1))} \omega_2^{(\sigma(2))} \cdots \omega_n^{(\sigma(n))} - \sum_{\substack{\sigma \in S_n \\ \text{περιττή}}} \omega_1^{(\sigma(1))} \omega_2^{(\sigma(2))} \cdots \omega_n^{(\sigma(n))} = A - B.$$

Συνεπώς

$$D_K = (A-B)^2 = (A+B)^2 - 4AB \equiv (A+B)^2 \mod 4.$$

Τώρα έστω N η κανονική θήκη του $\mathbb{Q}$ που περιέχει το K. Προφανώς $A, B \in R_N$.

Επιπλέον, κάθε $\mathbb{Q}$-αυτομορφισμός του N αφήνει τα στοιχεία $A+B$ και AB σταθερά, δηλαδή $A+B, AB \in \mathbb{Q}$ και επειδή είναι και ακέραια έχουμε ότι $A+B, AB \in \mathbb{Z}$. Το ζητούμενο προκύπτει αφού τα μοναδικά τετράγωνα modulo 4 είναι τα $0, 1$. □

Μερικές φορές μπορούμε να χρησιμοποιήσουμε το θεώρημα Stickelberger για τον υπολογισμό μιας βάσης ακεραιότητας.

Παράδειγμα IV.4.11. Το πολυώνυμο $x^3 - x - 2 \in \mathbb{Z}[x]$ είναι ανάγωγο. Έστω θ μια ρίζα αυτού και $K = \mathbb{Q}(\theta)$. Ο βαθμός της επέκτασης είναι $[K : \mathbb{Q}] = 3$. Η διακρίνουσα του θ είναι $D_K(\theta) = -104 = -26 \cdot 2^2$. Ως γνωστό ο δείκτης είναι τετράγωνο ακεραίου $D_K(\theta)/D_K$ τέλειο τετράγωνο. Επομένως $D(\theta)/D(K)$ είναι 1 ή $4 = 2^2$.

Αν $D_K(\theta)/D_K = 1$, τότε $D(K) = -104$. Αν $D_K(\theta)/D_K = 4$, τότε $D_K = -26$. Άλλα $D_K = -26 \neq 0, 1 \mod 4$, συνεπώς $D_K = D(\theta) = -104$ και το $\{1, \theta, \theta^2\}$ είναι βάση ακεραιότητας του $K = \mathbb{Q}(\theta)$.

Απόδειξη. (του θεωρήματος IV.4.2) Θεωρούμε το $K = \mathbb{Q}(\theta)$ με $\theta \in R_K$. Έχουμε ότι $D_K(\theta) \in \mathbb{Z} - \{0\}$ αφού $\{1, \theta, \dots, \theta^{n-1}\}$ είναι βάση της $K/\mathbb{Q}$.

Έχουμε αποδείξει ότι

$$\mathbb{Z}[\theta] \subset R_K \subset \frac{1}{D_K(\theta)} \mathbb{Z}[\theta].$$

Από την άλλη $\operatorname{rank}\mathbb{Z}[\theta] = \operatorname{rank} D_K(\theta)^{-1}\mathbb{Z}[\theta] = n$ από όπου προκύπτει ότι $\operatorname{rank} R_K = n$. □

Θεώρημα IV.4.12. *Έστω K αλγεβρικό σώμα αριθμών και $n = [K : \mathbb{Q}]$ και R_K ο δακτύλιος των ακεραίων αλγεβρικών αριθμών αυτού. Τότε κάθε κλασματικό ιδεώδες του R_K είναι ελεύθερη αβελιανή ομάδα με rank n.*

Απόδειξη. Έστω A ακέραιο ιδεώδες του R_K. Θεωρούμε ένα $\alpha \in A - \{0\}$ και έχουμε

$$\alpha R_K \subset A \subset R_K$$

και αφού το αR_K είναι ελεύθερη αβελιανή ομάδα με rank n έχουμε το ζητούμενο.

Αν τώρα το A είναι ένα κλασματικό ιδεώδες του R_K, τότε υπάρχει $r \in R_K - \{0\}$ με $rA \subset R_K$ και rA ακέραιο από όπου προκύπτει ότι η τάξη του τυχαίου κλασματικού είναι επίσης n. □

Στη συνέχεια θα υπολογίσουμε το πρόσημο της διακρίνουσας. Θεωρούμε το $K = \mathbb{Q}(\theta)$ και έστω

$$\operatorname{Irr}(\theta, \mathbb{Q}) = (x - \theta^{(1)})(x - \theta^{(2)}) \cdots (x - \theta^{(n)})$$

το ανάγωγο πολυώνυμο του θ, όπου $\theta = \theta^{(1)}, \theta^{(2)}, \dots, \theta^{(n)}$ είναι τα συζυγή του θ. Έστω $\sigma_1, \sigma_2, \dots, \sigma_n$ οι διάφορες εμφυτεύσεις του K στο $\mathbb{C}$, $\sigma_1 = \mathrm{Id}$, $\sigma(K) = K(\theta^{(i)})$.

Ορισμός IV.4.13. Μια εμφύτευση σ_i θα λέγεται *πραγματική* αν $\sigma(K) = K_i \subset \mathbb{R}$ αλλιώς θα λέγεται *μιγαδική*.

Προφανώς αν σ_i είναι μιγαδική εμφύτευση του K, τότε $\overline{\sigma}$ είναι επίσης μια εμφύτευση του K, δηλαδή το πλήθος των μιγαδικών εμφυτεύσεων του K είναι άρτιο στο πλήθος. Αν r_1 είναι το πλήθος των πραγματικών εμφυτεύσεων και $2r_2$ είναι το πλήθος των μιγαδικών, τότε

$$n = r_1 + 2r_2.$$

Αν $r_2 = 0$, τότε το σώμα θα λέγεται *πλήρως πραγματικό* και αν $r_1 = 0$, τότε θα λέγεται *πλήρως μιγαδικό*. Το ζευγάρι $[r_1, r_2]$ θα λέγεται *ταυτότητα (signature)* του K.

Χωρίς απόδειξη αναφέρουμε ότι υπάρχουν πεπερασμένου πλήθους αλγεβρικά σώματα αριθμών με δοσμένη ταυτότητα. Για μια απόδειξη παραπέμπουμε στον Narkiewicz [12, σελ. 52].

Σχετικά με το πρόσημο της διακρίνουσας ισχύει το εξής:

Θεώρημα IV.4.14. *Αν $[r_1, r_2]$ είναι η ταυτότητα (signature) του αλγεβρικού σώματος αριθμών K, τότε*

$$\operatorname{sgn} D_K = (-1)^{r_2}.$$

Απόδειξη. Έστω $\omega_1, \ldots, \omega_n$ μια βάση ακεραιότητας του K και έστω $\omega_i^{(j)}$ τα συζυγή του ω_i. Γράφουμε την ορίζουσα

$$\det(\omega_i^{(j)}) = d_1 + id_2, d_1, d_2 \in \mathbb{R}$$

Τα συζυγή του $d_1 + id_2$, $d_1 - id_2$ τα παίρνουμε αν αλλάξουμε τις $2r_2$ συζυγείς γραμμές ανά δύο. Επομένως

$$d_1 - id_2 = (-1)^{r_2} \det(\omega_i^{(j)}) = (-1)^{r_2}(d_1 + id_2).$$

- Αν $r_2 \equiv 0 \mod 2$, τότε $D_K = d_1^2 \in \mathbb{R}$ σε αυτή την περίπτωση $D_K > 0$.
- Αν $r_2 \equiv 1 \mod 2$, τότε $d_1 = 0$ και $D_K = (id_2)^2 = -d_2^2 < 0$.

□

Στη συνέχεια θα διατυπώσουμε και αποδείξουμε ένα θεώρημα το οποίο μας εξασφαλίζει την ύπαρξη κάποιας ειδικής βάσης.

Θεώρημα IV.4.15. *Έστω K αλγεβρικό σώμα αριθμών με $[K : \mathbb{Q}] = n$ και $\alpha_1, \alpha_2, \ldots, \alpha_n \in R_K$ γραμμικά ανεξάρτητα υπεράνω του $\mathbb{Q}$. Υπάρχει μια βάση ακεραιότητας $\omega_1, \omega_2, \ldots, \omega_n$ του K για την οποία ισχύει:*

$$\alpha_j = c_{j1}\omega_1 + c_{j2}\omega_2 + \cdots + c_{jj}\omega_j : j = 1, 2, \ldots, n, c_{ij} \in \mathbb{Z}.$$

Απόδειξη. Για κάθε $i = 1, 2, \ldots, n$ ορίζουμε ως d_{ii} τον ελάχιστο φυσικό αριθμό ($\neq 0$) με την ιδιότητα ότι για κατάλληλα επιλεγμένους ακέραιους $d_{i1}, d_{i2}, \ldots, d_{i,i-1}$ οι αριθμοί

$$\omega_i = D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1} \sum_{j=1}^{i} d_{ij}\alpha_j \in R_K$$

Θα αποδείξουμε ότι τα $\omega_1, \omega_2, \ldots, \omega_n$ αποτελούν βάση ακεραιότητας του K. Πρώτα από όλα το σύνολο $\{\omega_1, \omega_2, \ldots, \omega_n\}$ είναι $\mathbb{Q}$-γραμμικά ανεξάρτητο. Πράγματι,

$$D_K(\omega_1, \omega_2, \ldots, \omega_n) = \left(D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-n} \det(d_{ij})\right)^2 D_K(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$$

αφού $D_K(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ και $\det(d_{ij}) \neq 0$. Θα αποδείξουμε ότι το σύνολο $\{\omega_1, \omega_2, \ldots, \omega_n\}$ παράγει τον R_K.

Αλλά πρώτα απ' όλα ως ενδιάμεσο βήμα αποδεικνύουμε ότι, αν $c \in R_K$ και γράφεται στη μορφή

$$c = D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1}(c_1\alpha_1 + c_2\alpha_2 + \cdots + c_j\alpha_j)$$

για κάποιο j, με $c_i \in \mathbb{Z}$ για $i = 1, 2, \ldots, j$, τότε το $d_{jj} \mid c_j$. Πράγματι, έστω $c_j = d_{jj}\pi + u$, $0 \leq u < d_{jj}$. Αν $u \neq 0$, τότε ο

$$c - \pi\omega_j = D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1}\big((c_1 - d_{j1})\alpha_1 + \cdots + u a_j\big) \in R_K.$$

Αυτό όμως είναι άτοπο, αφού $u \in \mathbb{N} - \{0\}$, $u < d_{jj}$ λόγω του ορισμού του d_{jj}.

Έστω τώρα M_0 το $\mathbb{Z}$-module που παράγεται από τα $\omega_1, \omega_2, \ldots, \omega_n$. Θα αποδείξουμε επαγωγικά ότι κάθε στοιχείο του R_K της μορφής

$$D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1}(x_1\alpha_1 + x_2\alpha_2 + \cdots + x_j\alpha_j)$$

με $x_j \in \mathbb{Z}$ ανήκει στο M_0. Για $j = n$, θα έχουμε $M_0 = R_K$.

Για $j = 1$, το στοιχείο που ανήκει στο R_K έχει τη μορφή $D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1}x_1\alpha_1$ και το $\omega_1 = D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1}d_{11}\alpha_1$. Όπως αποδείξαμε το $d_{11} \mid x_1$, $x_1 = d_{11}t$, οπότε

$$D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1}x_1\alpha_1 = \big(D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1}d_{11}\alpha_1\big)t = \omega_1 t \in R_K.$$

Συνεπώς ισχύει για $j = 1$. Υποθέτουμε τώρα ότι ισχύει για $i = j - 1$ και έστω

$$y = D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)^{-1}(x_1\alpha_1 + \cdots + x_j\alpha_j),$$

με $x_j \in \mathbb{Z}$, ανήκει στο R_K. Επομένως, όπως αποδείξαμε παραπάνω $x_j = sd_{jj}$, για κατάλληλο $s \in \mathbb{Z}$. Αυτό σημαίνει ότι το $y - s\omega_j \in R_K$ και λόγω της υπόθεσης της μαθηματικής επαγωγής, αυτό ανήκει και στο M_0. Το $s\omega_j \in M_0$, εξ ορισμού του M_0. Τελικά έχουμε $y \in M_0$. □

IV.5 Παραδείγματα και υπολογισμοί

Παράδειγμα IV.5.1. Υπολογισμός δακτυλίου ακεραίων αλγεβρικών για ένα τετραγωνικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{d})$, με d ελεύθερο τετραγώνου. Ισχύει ότι

$$R_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{αν } d \not\equiv 1 \mod 4 \\ \mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right] & \text{αν } d \equiv 1 \mod 4 \end{cases}$$

Πράγματι κάθε στοιχείο $\alpha \in \mathbb{Q}(\sqrt{d})$ είναι της μορφής

$$\alpha = x + y\sqrt{d},$$

για $x, y \in \mathbb{Q}$. Συνεπώς μπορούμε να γράψουμε

$$\alpha = \frac{k + l\sqrt{d}}{m},$$

με $k, l, m \in \mathbb{Z}$, $m > 0$ και $(k, l, m) = 1$. Παρατηρούμε ότι ικανή και αναγκαία συνθήκη για να είναι ο α ακέραιος είναι οι συντελεστές του ελαχίστου πολυωνύμου του, δηλαδή το $\mathrm{Tr}(\alpha)$ και η $N(\alpha)$ να είναι ακέραιοι. Δηλαδή απαιτούμε

$$\frac{k^2 - l^2 d}{m^2} \in \mathbb{Z} \text{ και } \frac{2k}{m} \in \mathbb{Z}.$$

Αν τα k, m έχουν κοινό παράγοντα p, τότε η πρώτη σχέση θα μας δώσει ότι $p \mid b$ αφού το d είναι ελεύθερο τετραγώνου, άτοπο. Συνεπώς το $m = 1, 2$. Η περίπτωση $m = 1$ είναι σαφής οπότε θα εξετάσουμε την περίπτωση $m = 2$. Σε αυτή την περίπτωση θα πρέπει k, l να είναι και οι δύο περιττοί και $(k^2 - b^2 d)/4 \in \mathbb{Z}$. Συνεπώς θα πρέπει

$$k^2 - l^2 d \equiv 0 \mod 4$$

Παρατηρούμε ότι ένας περιττός αριθμός $2\nu+1$ έχει τετράγωνο $4\nu^2+4\nu+1 \equiv 1 \mod 4$, συνεπώς $k^2 \equiv l^2 \equiv 1 \mod 4$, και αυτό μας δίνει ότι $d \equiv 1 \mod 4$.

Αφού υπολογίσαμε τη βάση ακεραιότητας, μπορούμε να προχωρήσουμε στον υπολογισμό και των διακρινουσών:

$$\det\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} = 4d$$

και

$$\det\begin{pmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{d} \end{pmatrix} = d.$$

IV.6 Κυβικά σώματα αριθμών

IV.6.1 Καθαρές κυβικές επεκτάσεις

Ένα ιδιαίτερα χρήσιμο αποτέλεσμα για τον υπολογισμό μιας βάσης ακεραιότητας είναι το ακόλουθο:

Θεώρημα IV.6.1. *Έστω $K = \mathbb{Q}(\theta)$ αλγεβρικό σώμα αριθμών, $[K:\mathbb{Q}(\theta)] = n$, $\theta \in R_K$. Υποθέτουμε ότι $\mathrm{Irr}(\theta,\mathbb{Q})$ είναι τύπου Eisenstein, δηλαδή της μορφής*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

με $a_i \in \mathbb{Z}$, $p \mid a_i$ για κάθε $i = 0,\ldots,n-1$, ενώ $p^2 \nmid a_0$ για κάποιο πρώτο αριθμό p. Τότε το $p \nmid [R_K : \mathbb{Z}[\theta]]$.

Απόδειξη. Από την υπόθεση συμπεραίνουμε ότι το $p \mid \theta^n$ στο R_K, δηλαδή ότι $\theta^n/p \in R_K$. Υποθέτουμε ότι $p \mid [R_K : \mathbb{Z}[\theta]]$. Αυτό σημαίνει ότι υπάρχει ένα στοιχείο $\alpha \in R_K$,

$$\alpha = \frac{1}{p}\left(b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}\right)$$

για το οποίο δεν διαιρουνται όλα τα $b_0, b_1, \ldots, b_{n-1}$ με p. Έστω j ο ελάχιστος δείκτης για τον οποίο $p \nmid b_j$. Ο αριθμός

$$c := \frac{1}{p}\left(b_j\theta^j + \cdots + b_{n-1}\theta^{n-1}\right) = \alpha - \left(\frac{b_0}{p} + \frac{b_1\theta}{p} + \cdots + \frac{b_{j-1}}{p}\theta^{j-1}\right)$$

είναι ακέραιος αλγεβρικός. Συνεπώς και ο

$$f := b_j\theta^{n-1}p^{-1} = c\theta^{n-j-1} - \frac{\theta^n}{p}\left(b_{j+1} + b_{j+2}\theta + \cdots + b_{n-1}\theta^{n-j-2}\right)$$

Επομένως

$$p^n N_{K/Q}(f) = N_{K/\mathbb{Q}}(pf) = N_{K/\mathbb{Q}}(b_j)N_{K/\mathbb{Q}}(\theta^{n-1}) = b_j^n N_{K/\mathbb{Q}}(\theta)^{n-1}.$$

Επειδή το πολυώνυμο είναι Eisenstein το $p^2 \nmid N_{K/\mathbb{Q}}(\theta)$ οπότε κατ' ανάγκη $p \mid b_j$, άτοπο. □

Στη συνέχεια θα εφαρμόσουμε το θεώρημα στην εύρεση βάσεων ακεραιότητας καθαρών κυβικών επεκτάσεων του $\mathbb{Q}$.

Ορισμός IV.6.2. Μια καθαρή κυβική επέκταση του $\mathbb{Q}$ είναι ένα σώμα $K = \mathbb{Q}(\sqrt[3]{m})$, όπου ο m είναι ένας ελεύθερος κύβου ακέραιος, δηλαδή δεν διαιρείται από κανέναν κύβο πρώτου αριθμού και είναι της μορφής $m = ab^2$, $a, b \in \mathbb{Z}$ και ο ab ελεύθερος τετραγώνου. Είναι φανερό ότι $(a,b) = 1$ και επιπλέον χωρίς βλάβη της γενικότητας αν $3 \mid m$ υποθέτουμε ότι $3 \mid a$ και $3 \nmid b$, αφού τα σώματα που παράγονται από τα $(ab^2)^{1/3}$ και $(a^2b)^{1/3}$ συμπίπτουν.

Θεώρημα IV.6.3. *Έστω* $K = \mathbb{Q}(\sqrt[3]{m})$, *(*$m$ *ελεύθερο κύβου,* $m = ab^2$, ab *ελεύθερο τετραγώνου).*

1. *Αν* $m \not\equiv 1, 8 \mod 9$, *τότε* $D_K = -3^3(ab^2)$ *και το σύνολο* $\{1, m^{1/3}, m^{2/3}b^{-1}\}$ *είναι βάση ακεραιότητας του* K.
2. *Αν* $m \equiv 1 \mod 9$, *τότε* $D_K = -3(ab)^2$ *και το σύνολο* $\{m^{1/3}, m^{2/3}b^{-1}, \frac{1+m^{1/3}+m^{2/3}}{3}\}$ *είναι μια βάση ακεραιότητας του* K.
3. *Αν* $m \equiv 8 \mod 9$, *τότε* $D_K = -3(ab)^2$ *και το σύνολο* $\{m^{1/3}, m^{2/3}b^{-1}, \frac{1-m^{1/3}+m^{2/3}}{3}\}$ *είναι μια βάση ακεραιότητας του* K

Απόδειξη. Έστω $A := m^{1/3}$. Το ανάγωγο πολυώνυμο του A υπεράνω του $\mathbb{Q}$ είναι το

$$f(X) = X^3 - m \in \mathbb{Q}[X],$$

επομένως η διακρίνουσα του A είναι

$$D_{K/\mathbb{Q}}(A) = (-1)^3 N_{K/\mathbb{Q}}(f'(A)) = -N_{K/\mathbb{Q}}(3A^2) = -(3A^2)(3\omega A^2)(3\omega^2 A^2) = -3^3A^6 = -3^3m^2 = -3^3a^2b^4.$$

Για κάθε πρώτο p που διαιρεί το a το πολυώνυμο $f(X)$ είναι πολυώνυμο Eisenstein ως προς p. Επομένως αν $3 \mid a$, τότε το $3 \nmid b$ και μάλιστα από το θεώρημα IV.6.1 έπεται ότι $3 \nmid [R_K : \mathbb{Z}[\theta]]$ καθώς και ότι $a \nmid [R_K\mathbb{Z}[\theta]]$. Συνεπώς $27a^2 \mid D_K$.

Αν το $3 \nmid a$, τότε $3a^2 \mid D_K$. Ο αριθμός $B := A^2/b$ είναι ρίζα του πολυωνύμου $X^3 - a^2b$ το οποίο είναι τύπου Eisenstein για όλους τους πρώτους που διαρούν το b συνεπώς $b^2 \mid D_K$.

Συνολικά λοιπόν έχουμε

$$D_K = -3^N(ab)^2, \qquad N = \begin{cases} 3, & \text{αν } 3 \mid m \\ 1 \text{ ή } 3 & \text{αν } 3 \nmid m \end{cases}$$

Τώρα, αν $m \neq 1, 8 \mod 9$, ισχύει $m^3 \not\equiv m \mod 9$. Αν $3 \mid m$ όπως έχουμε συμφωνήσει $3 \nmid b$. Επομένως το πολυώνυμο

$$(x + m)^3 - m = x^3 + 3mx + 3m^2X + (m^3 - m)$$

είναι πολυώνυμο του Eisenstein ως προς τον πρώτο $p = 3$ έχει ως ρίζα τον αριθμό $A - m$ και η διακρίνουσα $D_K(A - m) = -27m^2$. Από το θεώρημα IV.6.1 προκύπτει $D_K = -27(ab)^2$. Έστω τώρα $m \equiv 1 \mod 9$. Ο αριθμός $c := \frac{1+A+A^2}{3}$ είναι ακέραιος αλγεβρικός. Πράγματι, αφού $T_{K/\mathbb{Q}}(A) = T_{K/Q}(A^2) = 0$ έπεται ότι $T_{K/\mathbb{Q}}(c) = 1$ και η norm

$$N_{K/\mathbb{Q}}(c) = N_{K/\mathbb{Q}}\left(\frac{1 + A + A^2}{3}\right) = \frac{1}{27}N_{K/\mathbb{Q}}(1 + A + A^2) = \frac{1}{27}N_{K/\mathbb{Q}}\left(\frac{A^3 - 1}{A - 1}\right)$$
$$= \frac{1}{27}\frac{N_{K/\mathbb{Q}}(A^3 - 1)}{N_{K/\mathbb{Q}}(A - 1)} = \frac{(m - 1)^3}{27(m - 1)} = \frac{(m - 1)^2}{27} \in \mathbb{Z},$$

αφού $m \equiv 1 \mod 9$. Το $\mathrm{Irr}(c, \mathbb{Q})$ έχει τη μορφή

$$X^3 - X^2 + \alpha X + \frac{(m - 1)^2}{27}.$$

Θα υπολογίσουμε το α. Το $A = m^{1/3}$ συνεπάγεται $3c = 1 + \sqrt[3]{m} + \sqrt[3]{m^2}$ άρα

$$(3c - 1)^3 = \left(\sqrt[3]{m} + \sqrt[3]{m^2}\right)^3 = m + m^2 + 3\sqrt[3]{m} \cdot \sqrt[3]{m^2}(3c - 1).$$

Οπότε έχουμε

$$27c^3 - 27c^2 + 9c - 1 = m + m^2 + 3m(3c - 1),$$

δηλαδή

$$c^3 - c^2 + 9\frac{1-m}{27}c + \frac{(1-m)^2}{27} = 0.$$

Άρα $\alpha = \frac{1-m}{3} \in \mathbb{Z}$, αφού $m \equiv 1 \mod 9$ και συνεπώς ο c είναι ακέραιος αλγεβρικός, οπότε από την πρόταση IV.4.1 έπεται ότι το 3 διαιρεί τον δείκτη και η διακρίνουσα σε αυτή την περίπτωση είναι

$$D_K = -3(ab)^2.$$

Εργαζόμαστε ανάλογα όταν $m \equiv 8 \mod 9$ με το στοιχείο $c = \frac{1-A+A^2}{3}$.

Τέλος για το ότι τα σύνολα του θεωρήματος είναι βάση ακεραιότητας επαληθεύεται εύκολα ότι έχουν τη σωστή διακρίνουσα. □

Παράδειγμα IV.6.4. 1. $K = \mathbb{Q}(\sqrt[3]{2})$, $m = 2, a = 2, b = 1$. Έχουμε $m \not\equiv 1, 8 \mod 9$ άρα βάση ακεραιότητας είναι το σύνολο $\{1, \sqrt[3]{4}, \sqrt[3]{4}\}$.

2. $K = \mathbb{Q}(\sqrt[3]{5})$, $m = 5, a = 5, b = 1$, $m \not\equiv 1, 8 \mod 9$ άρα το σύνολο $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ είναι βάση ακεραιότητας του K.

3. $K = \mathbb{Q}(\sqrt[3]{f})$, $m = 175, a = 7, b = 5$, $m \not\equiv 1, 8 \mod 9$. Το σύνολο $\{1, \sqrt[3]{175}, \sqrt[3]{245}\}$ είναι βάση ακεραιότητας του K.

4. $K = \mathbb{Q}(\sqrt[3]{10})$, $m = 10, a = 10, b = 1$. Έχουμε $m = 1 \mod 9$ και μία βάση ακεραιότητας είναι $\{\sqrt[3]{10}, \sqrt[3]{100}, \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}\}$

IV.6.2 Κυβικά σώματα $K = \mathbb{Q}(\theta)$, $\theta \in R_K$ και $\mathrm{Irr}(\theta, \mathbb{Q}) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$

.

Έστω $f(x) = x^n + ax + b$, $a, b \in \mathbb{Q}$, $n \geq 2$. Υποθέτουμε ότι $f(x)$ είναι ανάγωγο υπεράνω του $\mathbb{Q}$. Αν θ μία ρίζα του $f(x)$, τότε αποδεικνύεται (άσκηση) ότι η διακρίνουσα του θ είναι η

$$D_K(\theta) = (-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n\right).$$

Επομένως

$n = 2$ $D_K(\theta) = -4b + a^2$

$n = 3$ $D_K(\theta) = -27b^2 - 4a^3$

$n = 4$ $D_K(\theta) = 256b^3 - 27a^4$

$n = 5$ $D_K(\theta) = 5^5 b^4 + 4^4 a^5$

Παράδειγμα IV.6.5. 1. Έστω $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$ και θ μια οποιαδήποτε ρίζα του $f(x)$. Το $f(x)$ είναι ανάγωγο υπεράνω του $\mathbb{Q}$. Υπολογίζουμε ότι $D_K(\theta) = -27 \cdot 1 - 4 \cdot 1 = -31$ το οποίο είναι ελεύθερο τετραγώνου. Συνεπώς μια βάση ακεραιότητας του K είναι το σύνολο $\{1, \theta, \theta^2\}$.

2. Ομοίως αν $f(x) = x^3 - x - 1 \in \mathbb{Q}[x]$, $D_K(\theta) = -23$ μια βάση ακεραιότητας είναι πάλι της μορφής $\{1, \theta, \theta^2\}$.

3. Έστω $f(x) = x^5 - x - 1 \in \mathbb{Q}[x]$.Το πολυώνυμο είναι ανάγωγο υπεράνω του $\mathbb{Q}$, αφού είναι ανάγωγο στο $\mathbb{F}_3[x]$. Η $D_K(\theta) = 19 \cdot 151$ είναι ελεύθερη τετραγώνου και συνεπώς ο δακτύλιος ακεραίων αλγεβρικών είναι το $\mathbb{Z}[\theta]$.

Το ερώτημα που τίθεται είναι αν υπάρχει πάντοτε ένας ακέραιος αλγεβρικός θ ώστε η περιοχή των ακεραίων αλγεβρικών του $\mathbb{Q}(\theta)$ να είναι το $\mathbb{Z}[\theta]$. Η απάντηση είναι αρνητική. Θα αναφέρουμε το κλασικό παράδειγμα του Dedekind.

Έστω θ μια ρίζα του πολυωνύμου

$$f(x) = x^3 - x^2 - 2x - 8 \in \mathbb{Q}[x].$$

Το πολυώνυμο είναι ανάγωγο υπέρ του $\mathbb{Q}$, επομένως αν $K = \mathbb{Q}(\theta)$, $[K : \mathbb{Q}(\theta)] = 3$. Θα αποδείξουμε ότι δεν υπάρχει βάση ακεραιότητας της μορφής $\{1, \alpha, \alpha^2\}$ όπου α ακέραιος αλγεβρικός στον R_K. Συγκεκριμένα θα αποδείξουμε ότι η διακρίνουσα $D_K = -503$ ενώ για κάθε $\alpha \in R_K$ ισχύει $D_K(\alpha) = -2012 = -4 \cdot 503$.

Υπολογίζουμε τη διακρίνουσα του θ:

$$D_K(1, \theta, \theta^2) = (-1)^{3(3-1)/2} N_{K/\mathbb{Q}}(f'(\theta)).$$

Θέτουμε

$$\begin{aligned} \eta = f'(\theta) &= 3\theta^2 - 2\theta - 2 \\ \eta\theta &= \theta^2 + 4\theta + 24 \\ \eta\theta^2 &= 5\theta^2 + 26\theta + 8 \end{aligned}$$

Ο πίνακας $A(\eta)$ είναι ο

$$A(\eta) = \begin{pmatrix} -2 & 24 & 8 \\ -2 & 4 & 26 \\ 3 & 1 & 5 \end{pmatrix}$$

ο οποίος έχει χαρακτηριστικό πολυώνυμο

$$\det(x\mathbb{I}_3 - A(\eta)) = \det \begin{pmatrix} x+2 & -24 & -8 \\ +2 & x-4 & -26 \\ -3 & -1 & x-5 \end{pmatrix} = x^3 - 7x^2 - 2012 =: g(x).$$

Άρα $N_{K/\mathbb{Q}}(\eta) = (-1)^3(-2012) = 4 \cdot 503$ Καταλήγουμε στο ότι

$$D_K(1, \theta, \theta^2) = -4 \cdot 503.$$

Έστω τώρα $\alpha = -(\theta^2 + \theta)/2$. Το χαρακτηριστικό πολυώνυμο του α είναι $x^3 - 3x^2 - 10x - 8$, δηλαδή ακέραιος αλγεβρικός του K.

$$D_K(1, \theta, \alpha) = \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & 1/2 \end{pmatrix}^2 \cdot D_K(1, \theta, \theta^2) = 1/4(-4 \cdot 503) = -503.$$

Επειδή 503 είναι πρώτος αριθμός, έπεται ότι η διακρίνουσα του σώματος είναι $D_K = -503$ και μια βάση του R_K είναι το $\{1, \theta, \alpha\}$.

Ισχυριζόμαστε ότι δεν υπάρχει $\omega \in R_K$ ώστε

$$D_K(1, \omega, \omega^2) = -503.$$

Θα αποδείξουμε ότι για κάθε $\omega \in R_K$, $2 \mid D_K(1, \omega, \omega^2)$.

Έστω $\omega = x + y\theta + z\alpha$, $x, y, z \in \mathbb{Z}$. Παρατηρούμε ότι

$$\alpha^2 = \frac{\theta^4 + 2\theta^3 + \theta^2}{4} = 6 + 2\theta + 3\alpha.$$

Οπότε

$$\begin{aligned}\omega^2 &= x^2 + y^2\theta^2 + z^2\alpha^2 + 2xy\theta + 2xz\alpha + 2yz\theta\alpha \\ &= (x^2 + 6z^2 + 8yz) + (2z^2 - y^2 + 2xy)\theta + (2y^2 + 3z^2 + 2xz + 4yz)\theta^2.\end{aligned}$$

Επομένως η διακρίνουσα του τυχαίου στοιχείου ω του R_K έχει τη μορφή:

$$D_{K/\mathbb{Q}}(\omega) = \det\begin{pmatrix} 1 & x & x^2 + 6z^2 + 8yz \\ 0 & y & 2z^2 - y^2 + 2xy \\ 0 & z & 2y^2 + 3z^2 + 2xz + 4yz \end{pmatrix}^2 \cdot (-503).$$

Υπολογίζουμε την παραπάνω διακρίνουσα modulo 2.

$$D_{K/\mathbb{Q}} \equiv -503 \cdot (yz^2 + y^2z)^2 \mod 2.$$

- Αν $yz \equiv 0 \mod 2$, τότε $D_{K/\mathbb{Q}} \equiv 0 \mod 2$
- Αν $yz \equiv 1 \mod 2$, τότε y, z περιττοί και $y + z \equiv 0 \mod 2$, οπότε πάλι $D_{K/\mathbb{Q}} \equiv 0 \mod 2$.

Αποδείξαμε δηλαδή ότι δεν υπάρχει βάση της μορφής $1, \omega, \omega^2$ στο σώμα K.

Από τα παραπάνω συμπεραίνουμε ότι $2 \mid [R_K : \mathbb{Z}[\alpha]]$ για κάθε $\alpha \in R_K$. Ένας τέτοιος πρώτος λέγεται *μη ουσιώδης διαιρέτης της διακρίνουσας*.

Ορισμός IV.6.6. Έστω K αλγεβρικό σώμα αριθμών βαθμού $n = [K : \mathbb{Q}]$. Αν υπάρχει ένα $\theta \in R_K$ για τον οποίο να ισχύει ότι το σύνολο $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ να είναι βάση ακεραιότητας του K, τότε θα λέμε ότι το K είναι *μονογενικό* και η βάση λέγεται *βάση δυνάμεων* του K.

IV.6.3 Δείκτης αλγεβρικού σώματος αριθμών

Ορισμός IV.6.7. Το $\alpha \in R_K$ θα λέγεται *γεννήτορας* του K όταν $K = \mathbb{Q}(\alpha)$. Ο *δείκτης* του α είναι $\mathrm{Ind}(\alpha) = [R_K : \mathbb{Z}[\alpha]]$ Ορίζουμε τον δείκτη του K

$$i(K) = \text{ΜΚΔ}\{\mathrm{Ind}(\alpha) : \alpha \text{ γεννήτορας της } K/\mathbb{Q}\}.$$

Ο ελάχιστος δείκτης του K

$$m(K) = \min\{\mathrm{Ind}(\alpha) : \alpha \text{ γεννήτορας της } K/\mathbb{Q}\}$$

Προφανώς $i(K) \mid m(K)$.

Πρόταση IV.6.8. *Έστω K αλγεβρικό σώμα αριθμών. Ισχύει ότι $m(K) = 1$ αν και μόνο αν το K έχει μια βάση δυνάμεων ως βάση ακεραιότητας.*

Απόδειξη. Έστω $m(K) = 1$. Αυτό σημαίνει ότι υπάρχει $\alpha \in R_K$ γεννήτορας του K με $\mathrm{Ind}(\alpha) = 1$, δηλαδή $D_K(1, \alpha, \ldots, \alpha^{n-1}) = D_K(\alpha) = \mathrm{Ind}(\alpha)^2 D_K = D_K$, δηλαδή το $\{1, \alpha, \ldots, \alpha^{n-1}\}$ βάση ακεραιότητας του K και το K έχει μια βάση ακεραιότητας δυνάμεις ενός στοιχείου.

Αντίστροφα, έστω ότι υπάρχει $\alpha \in R_K$ για το οποίο το σύνολο $\{1, \alpha, \ldots, \alpha^{n-1}\}$ είναι βάση ακεραιότητας του K. Αυτό σημαίνει ότι $D_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = D_K$. Αλλά $D_K(1, \alpha, \ldots, \alpha^{n-1}) = D_K(\alpha) = \mathrm{Ind}(\alpha)^2 D_K$. Συνεπώς $\mathrm{Ind}(\alpha) = 1$ και $m(K) = 1$.

Πόρισμα IV.6.9. *Αν το σώμα K έχει μια βάση δυνάμεων, τότε $m(K) = 1$ και αφού $i(K) \mid m(K)$ έχουμε ότι $i(K) = 1$.*

Το αντίστροφο δεν ισχύει. Πράγματι για το $K = \mathbb{Q}(\sqrt[3]{175})$ έχουμε υπολογίσει ότι $\{1, \sqrt[3]{175}, \sqrt[3]{245}\}$ και διακρίνουσα $D_K = -3^3 5^2 7^2$. Έστω $\alpha \in R_K$ συνεπώς γράφεται

$$\alpha = a + b\sqrt[3]{175} + c\sqrt[3]{245}$$

και ω μια πρωταρχική τρίτη ρίζα του 1, $\omega^3 = 1, \omega^2 + \omega + 1 = 0$. Τα συζυγή του α είναι

$$\alpha' = a + b\omega\sqrt[3]{175} + c\omega^2\sqrt[3]{245}$$
$$\alpha'' = a + b\omega^2\sqrt[3]{175} + c\omega\sqrt[3]{245}$$

Επομένως

$$\alpha - \alpha' = (1-\omega)(b\sqrt[3]{175} - c\omega^2\sqrt[3]{245})$$
$$\alpha - \alpha'' = (1-\omega^2)(b\sqrt[3]{175} - c\omega\sqrt[3]{245})$$
$$\alpha' - \alpha'' = (\omega-\omega^2)(b\sqrt[3]{175} - c\sqrt[3]{245})$$

οπότε

$$\begin{aligned} D_K(\alpha) &= (\alpha-\alpha')(\alpha-\alpha'')(\alpha'-\alpha'') \\ &= \big((1-\omega)(1-\omega^2)(\omega-\omega^2)\big)^2(175b^3 - 245c^3)^2. \end{aligned}$$

Ο δείκτης του α,

$$\mathrm{Ind}(\alpha) = [R_K : \mathbb{Z}[\alpha]] = \sqrt[3]{\frac{D_K(\alpha)}{D_K}} = \sqrt[3]{\frac{-3^3\cdot 5^2\cdot 7^2(5b^3-7c^3)^2}{-3^3\cdot 5^2\cdot 7^2}} = |5b^3 - 7c^3|.$$

Ο δείκτης του K είναι

$$i(K) = \text{ΜΚΔ}\{|5b^3 - 7c^3| : b, c \in \mathbb{Z}, 5b^3 - 7c^3 \neq 0\}$$

και ο ελάχιστος δείκτης

$$m(K) = \min\{|5b^3 - 7c^3| : b, c \in \mathbb{Z}, 5b^3 - 7c^3 \neq 0\}.$$

Τώρα $|5\cdot 1^3 - 7\cdot 1^3| = 2$ και $|5\cdot 1^3 - 7\cdot 0^3| = 5$, συνεπώς $i(K) = 1$. Το παραπάνω σημαίνει ότι $m(K) = 1$ ή 2. Αν $m(K) = 1$, τότε υπάρχουν $B, C \in Z$ ώστε

$$5B^3 - 7C^3 = \pm 1,$$

δηλαδή $5B^3 \equiv \pm 1 \mod 7$, οπότε $B^3 \equiv \pm 3 \mod 7$. Όμως για κάθε $x \in \mathbb{Z}$ ισχύει $x^3 \equiv \pm 1, 0 \mod 7$. Συνεπώς $m(K) = 2$ που σημαίνει ότι το K δεν έχει μονογενή βάση ακεραιότητας. □

Ορισμός IV.6.10 (Μη ουσιώδης διαιρέτης διακρίνουσας)**.** Έστω K-αλγεβρικό σώμα αριθμών $[K : \mathbb{Q}] = n$. Ένας πρώτος αριθμός p θα λέγεται ένας *μη-ουσιαστικός διαιρέτης διακρίνουσας* όταν $p \mid \mathrm{Ind}(\alpha) = [R_K : \mathbb{Z}[\alpha]]$, για κάθε γεννήτορα του σώματος $K = \mathbb{Q}(\alpha)$.

Παρατήρηση IV.6.11. Το σώμα $K = \mathbb{Q}(\sqrt[3]{175})$ αποτελεί ένα παράδειγμα σώματος που ενώ δεν έχει μη-ουσιαστικό διαιρέτη (non-essensial discriminant divisor), όπως το παράδειγμα του Dedekind είχε το 2, δεν έχει και μονογενή βάση ακεραιότητας.

Παρατήρηση IV.6.12. Γενικά η διακρίνουσα ενός κυβικού σώματος αριθμών $K = \mathbb{Q}(\theta)$, θ ρίζα του αναγώγου πολυωνύμου $f(x) = x^3 + ax + b$, $a, b \in \mathbb{Z}$ έχει υπολογιστεί από τους Llorente και Nart στο [8]. Αποδεικνύεται ότι αν ένας πρώτος αριθμός p διαιρεί τον δείκτη $i(K)$ του σώματος, τότε κατ' ανάγκη $p < n = [K : \mathbb{Q}]$. Συνεπώς για κυβικές επεκτάσεις ο μόνος πρώτος που θα μπορούσε να διαιρεί τον δείκτη είναι ο $p = 2$. Επομένως ισχύει $i(K) = 1$ ή $i(K) = 2$. Το θεώρημα των Llorente

και Nart είναι: Έστω $s_2 = \nu_2(\Delta)$ ο μεγαλύτερος εκθέτης του 2 ο οποίος διαιρεί τη διακρίνουσα $\Delta = -4a^3 - 27b^2$ του $f(x)$ και $\Delta_2 = \Delta/p^{s_2}$. Ισχύει $i(K) = 2$ αν και μόνο αν a περιττός, ο b άρτιος, ο s_2 άρτιος και ο $\Delta_2 \equiv 1 \mod 8$. Μια βάση κυβικού αλγεβρικού σώματος $K = \mathbb{Q}(\theta)$ στη γενική περίπτωση που το θ είναι ρίζα του ανάγωγου πολυωνύμου $f(x) = x^3 + ax + b$, $a, b \in \mathbb{Z}$ έχει δοθεί από τον Alaca [1]. Είναι τεχνικά δύσκολο να παρουσιαστεί εδώ.

Είναι φανερό ότι οι μη ουσιώδεις διαιρέτες διακρίνουσας είναι επακριβώς οι πρώτοι διαιρέτες του δείκτη $i(K)$ του K. Χωρίς απόδειξη αναφέρουμε το ακόλουθο θεώρημα το οποίο αποτελεί ένα κριτήριο του πότε ένας πρώτος $p \nmid i(K)$. Ο ορισμός του βαθμού αδρανείας $f_{K/\mathbb{Q}}$ θα οριστεί αναλυτικά σε επόμενο κεφάλαιο.

Θεώρημα IV.6.13. *Έστω p πρώτος αριθμός (είναι βολικό να του ταυτίσουμε με το κύριο ιδεώδες $p\mathbb{Z}$) και έστω*

$$pR_K = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$$

η ανάλυση του pR_K σε γινόμενο πρώτων ιδεωδών του K. Έστω επίσης $f_i = f_{K/\mathbb{Q}}(P_i)$. Τότε το $p \nmid i(K)$ αν και μόνο αν υπάρχουν διακεκριμένα πολυώνυμα $V_1, V_2, \ldots, V_g \in \mathbb{F}_p[x]$, ανάγωγα υπεράνω του σώματος $\mathbb{F}_p$ με βαθμούς $f_1, f_2, \ldots, f_g$ αντίστοιχα [12, Th. 4.13 σελ. 170].

Για να χρησιμοποιήσουμε αυτό το θεώρημα είναι απαραίτητο να γνωρίζουμε το πλήθος $r_P(n)$ των μη-συνεταιρικών μεταξύ τους, αναγώγων πολυωνύμων υπεράνω του σώματος $\mathbb{F}_p$ βαθμού n.

Αυτό είναι γνωστό και για κάθε πρώτο p και $n \geq 1$ δίνεται από τον τύπο

$$r_P(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d},$$

όπου $\mu(d)$ η γνωστή συνάρτηση του Möbius. Η γνώση αυτή μας επιτρέπει να φράξουμε από πάνω τους πρώτους διαιρέτες του $i(K)$.

Πρόταση IV.6.14. *Αν p πρώτος διαιρέτης του $i(K)$, τότε $p < n = [K : \mathbb{Q}]$.*

Απόδειξη. Αν $p \mid i(K)$ και $p \geq n$, τότε μεταξύ των αριθμών $f_{K/\mathbb{Q}}(P)$ (το P διατρέχει όλους τους πρώτους παράγοντες του pR_K) θα πρέπει να είναι το πολύ n/κ ίσοι με κ, ενώ σύμφωνα με το προηγούμενο θεώρημα, θα πρέπει να υπάρχει ένα κ_0 τέτοιο ώστε $r_P(\kappa_0) < n/\kappa_0 \leq r/\kappa_0$. Αλλά ο τύπος για τον αριθμό $r_P(\kappa_0)$ είναι πολλλαπλάσιο του p και διάφορο του μηδενός, οπότε $r_P(\kappa_0) \geq p \geq p/\kappa_0$, άτοπο. □

Έστω τώρα K μια κυβική επέκταση του $\mathbb{Q}$ και p πρώτος αριθμός $p \mid i(K)$. Τότε, κατ' ανάγκη, $p < 3 = [K : \mathbb{Q}]$, δηλαδή $p = 2$. Το 2 είναι διαιρέτης του δείκτη $i(K)$ αν και μόνο αν $2R_K = P_1P_2P_3$ με διακεκριμένα πρώτα ιδεώδη P_i, $i = 1, 2, 3$, δηλαδή όταν το $2R_K$ αναλυεται πλήρως στο K. Αυτό ισχύει αφού υπάρχουν μόνο δύο ανάγωγα πολυώνυμα πρώτου βαθμού στον δακτύλιο $\mathbb{F}_2[x]$ και αυτά είναι το x και το $x + 1$.

IV.7 Διακρίνουσα και βάση ακεραιότητας κυκλοτομικών σωμάτων

IV.7.1 Το κυκλοτομικό σώμα $\mathbb{Q}(\zeta_p)$, p πρώτος

Για εκπαιδευτικούς σκοπούς θα μελετήσουμε πρώτα την απλούστερη περίπτωση $K = \mathbb{Q}(\zeta_p)$ και θα δείξουμε ότι ο δακτύλιος ακέραιων $R_K = \mathbb{Z}[\zeta_p]$, όπου $\zeta = \zeta_p = e^{2\pi i/p}$.

Το ανάγωγο πολυώνυμο του ζ είναι το

$$f(X) = \mathrm{Irr}(\zeta, \mathbb{Q}) = 1 + X + X^2 + \cdots + X^{p-1} = \frac{X^p - 1}{X - 1}.$$

Έστω

$$F(X) := f(X+1) = X^{p-1} + pX^{p-2} + \binom{p}{2}X^{p-3} + \cdots + \binom{p}{p-2}X + p,$$

το οποίο είναι Eisenstein για το p. Υπολογίσαμε τη διακρίνουσα:

$$D_{K/\mathbb{Q}}(\zeta) = (-1)^{\frac{p-1}{2}}p^{p-2} = \pm p.$$

Έχουμε

$$D_{K/\mathbb{Q}}(\zeta) = m^2 D_{K/\mathbb{Q}} \Rightarrow p^{p-2} = m^2 D_{K/\mathbb{Q}}.$$

Το $F(X)$ είναι Eisenstein, άρα ανάγωγο υπεράνω του $\mathbb{Q}$ και $F(X) = \mathrm{Irr}(\zeta - 1, \mathbb{Q})$. Επιπλέον, είναι φανερό ότι ισχύει:

$$D_{K/\mathbb{Q}}(\zeta - 1) = D_{K/\mathbb{Q}}(\zeta).$$

Καταλήγουμε στο ότι $p \nmid m$ και $R_K = \mathbb{Z}[\zeta]$.

IV.7.2 Η γενική περίπτωση

Σε πρώτο βήμα θα μελετήσουμε την ειδική περίπτωση που ζ είναι μια πρωταρχική p^n-ρίζα της μονάδας, όπου p πρώτος. Θεωρούμε το κυκλοτομικό σώμα $K = \mathbb{Q}(\zeta)$.

Θεώρημα IV.7.1. *Η επέκταση $K/\mathbb{Q}$ είναι Galois και $[K : \mathbb{Q}] = \phi(p^n) = p^{n-1}(p-1)$. Το σύνολο $\{1, \zeta, \zeta^2, \ldots, \zeta^r\}$ για $r = \phi(p^n) - 1$ αποτελεί βάση ακεραιότητας του K και η διακρίνουσα $D_K = (-1)^{\frac{p(p-1)}{2}}p^N$ όπου $N = n\phi(p^n) - p^{n-1}$.*

Η ομάδα Galois $\mathrm{Gal}(K/\mathbb{Q})$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα $E(\mathbb{Z}/p^n\mathbb{Z})$ των μονάδων του δακτυλίου $\mathbb{Z}/p^n\mathbb{Z}$.

Απόδειξη. Για να αποδείξουμε ότι $[K : \mathbb{Q}] = p^n - p^{n-1}$ αρκεί να αποδείξουμε ότι το πολυώνυμο

$$P(X) := \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1}$$

είναι ανάγωγο υπεράνω του $\mathbb{Q}$. Το $P(X)$ έχει ρίζα το ζ. Θέτουμε $F(X) = P(X+1)$. Επαγωγικά (άσκηση) μπορούμε να αποδείξουμε ότι για $j \geq 1$ ισχύει

$$(1+X)^{jp^{n-1}} = \left(1 + X^{p^{n-1}}\right)^j + pP_j(X)$$

με $P_j(X) \in \mathbb{Z}[X]$ και $\deg P_j(X) < jp^{n-1}$. Το

$$F(X) = \frac{(1+X)^{p^n} - 1}{(1+X)^{p^{n-1}} - 1} = \sum_{j=0}^{p-1}(1+X)^{jp^{n-1}},$$

από τον επαγωγικό τύπο μας δίνει

$$F(X) = \sum_{j=1}^{p-1}\left(\left(1 + X^{p^{n-1}}\right)^j + pP_j(X)\right) = \sum_{j=1}^{p-1}\left(1 + X^{p^{n-1}}\right)^j + pV(X),$$

όπου $V(X) \in \mathbb{Z}[X]$ πολυώνυμο με

$$\deg V(X) < (p-1)p^{n-1} \text{ αφού } \deg P_j(X) < jp^{n-1} \text{ για } j = 1, 2, \ldots, p-1.$$

Επομένως

$$F(X) = pV(X) + \sum_{j=1}^{p-1}\binom{p}{j}X^{p^{n-1}(j-1)}$$

καθώς και $F(0) = P(1) = p$. Όλοι οι άλλοι συντελεστές διαιρούνται με p. Αυτό σημαίνει ότι το πολυώνυμο $F(X)$ είναι πολυώνυμο Eisenstein ως προς τον πρώτο p, δηλαδή ανάγωγο υπεράνω του $\mathbb{Q}$, συνεπώς και το $P(X)$.

Στη συνέχεια υπολογίζουμε τη διακρίνουσα

$$D_{K/\mathbb{Q}}(\zeta) = (-1)^{\frac{p(p-1)}{2}} N_{K/\mathbb{Q}}(P'(\zeta)).$$

Τώρα $P(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$ άρα

$$P'(X) = \frac{p^n X^{p^n-1}\left(X^{p^{n-1}}-1\right) - \left(X^{p^n}-1\right)p^{n-1}X^{p^{n-1}-1}}{\left(X^{p^{n-1}}-1\right)^2}$$

οπότε

$$P'(X)(X^{p^{n-1}}-1) = p^n X^{p^n-1} - p^{n-1}X^{p^{n-1}-1}\frac{X^{p^n}-1}{X^{p^{n-1}}-1},$$

δηλαδή

$$P'(X)(X^{p^{n-1}}-1) + p^{n-1}X^{p^{n-1}-1}P(X) = p^n X^{p^n-1}.$$

Έστω $\theta = \zeta^{p^{n-1}}$. Το θ είναι μια πρωταρχική p ρίζα της μονάδας. Από την παραπάνω σχέση προκύπτει ότι

$$P'(\zeta)(\theta-1) = p^n\zeta^{-1}.$$

Υπολογίζουμε την norm

$$\begin{aligned} N_{K/\mathbb{Q}}(P'(\zeta)) &= N_{K/\mathbb{Q}}(p^n(\theta-1)^{-1}\zeta^{-1}) = N_{K/\mathbb{Q}}(p^n)\left(N_{K/\mathbb{Q}}(\theta-1)\zeta\right)^{-1} \\ &= p^{n\phi(p^n)}\left(N_{K/\mathbb{Q}}(\zeta)N_{K/\mathbb{Q}}(\theta-1)\right)^{-1}. \end{aligned}$$

Άλλα $N_{K/\mathbb{Q}}(\zeta) = 1$ και το $\theta - 1$ είναι ρίζα του πολυωνύμου

$$(x+1)^{p-1} + \cdots + (x+1) + 1.$$

Έστω $K_0 = \mathbb{Q}(\theta)$.

$$\begin{aligned} N_{K/\mathbb{Q}}(\theta-1) &= N_{K_0/\mathbb{Q}}(N_{K/K_0}(\theta-1)) = N_{K_0/\mathbb{Q}}\left((\theta-1)^{p^{n-1}}\right) \\ &= N_{K_0/\mathbb{Q}}(\theta-1)^{p^n-1} = p^{p^n-1}. \end{aligned}$$

Συνεπώς από το θεώρημα IV.2.4

$$D_{K/\mathbb{Q}}(\zeta) = (-1)^{\frac{p(p-1)}{2}}p^N, \qquad N := \phi(p^n) - p^{n-1}.$$

Τέλος παρατηρούμε ότι

$$D_{K/\mathbb{Q}}(\zeta) = D_{K/\mathbb{Q}}(\zeta-1)$$

και $\zeta - 1$ επαληθεύει μια εξίσωση του Eisenstein ως προς το p. Αυτό σημαίνει ότι $D_{K/\mathbb{Q}}(\zeta) = D_K$ και ότι το σύνολο $\{1, \zeta, \ldots, \zeta^r\}$, $r = \phi(p^n) - 1$ αποτελεί βάση ακεραιότητας του K. □

Στη συνέχεια θα μελετήσουμε κυκλοτομικές επεκτάσεις $K = \mathbb{Q}(\zeta)$ όπου $\zeta = \zeta_N = e^{\frac{2\pi i}{N}}$ μία N-στη ρίζα της μονάδας για κάποιο φυσικό αριθμό $N > 1$. Πρέπει όμως πιο μπροστά να μελετήσουμε πώς σχετίζεται ο δακτύλιος των ακεραίων αλγεβρικών αριθμών και η διακρίνουσα ενός αλγεβρικού σώματος αριθμών το οποίο είναι η σύνθεση δύο αλγεβρικών σωμάτων αριθμών. Αυτό θα γίνει βέβαια κάτω από κάποιους περιορισμούς.

Πρόταση IV.7.2. *Πρόταση έστω* K *και* L *δύο πεπερασμένες επεκτάσεις του* $\mathbb{Q}$ *για τις οποίες ισχύει*

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}].$$

Έστω επίσης $d = ΜΚΔ(D_K, D_L)$. *Τότε ισχύει* $R_{KL} \subset \frac{1}{d} R_K R_L$.

Απόδειξη. Έστω $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ βάση ακεραιότητας του K και $\{\beta_1, \beta_2, \ldots, \beta_n\}$ βάση ακεραιότητας του L. Προφανώς τα δύο σύνολα είναι $\mathbb{Q}$-γραμμικά ανεξάρτητα. Επομένως το σύνολο

$$\{\alpha_i \beta_j : i = 1, 2, \ldots, m, j = 1, 2, \ldots, n\}$$

αποτελεί βάση του σώματος KL υπέρ του $\mathbb{Q}$. Δηλαδή κάθε $\gamma \in R_{KL}$ γράφεται μονοσήμαντα στη μορφή:

$$\gamma = \sum_{i,j} \frac{a_{ij}}{r} \alpha_i \beta_j,$$

$a_{ij}, r \in \mathbb{Z}$. Αν απλοποιήσουμε τους κοινούς παράγοντες από τα a_{ij} και r, τότε έχουμε ότι δεν υπάρχει πρώτος παράγοντας του r ο οποίος να διαιρεί όλους τους a_{ij}. Αρκεί να αποδείξουμε ότι $r \mid d$. Ταυτίζουμε το σώμα L με την εικόνα του ως υπόσωμα του $\mathbb{C}$. Κάθε εμφύτευση $\sigma : K \hookrightarrow \mathbb{C}$ του K επεκτείνεται μονοσήμαντα σε εμφύτευση $\sigma : KL \hookrightarrow \mathbb{C}$ του KL η οποία κρατάει όλα τα στοιχεία του L σταθερά. Κρατούμε τον ίδιο συμβολισμό για την εμφύτευση $\sigma : KL \hookrightarrow \mathbb{C}$. Επομένως

$$\sigma(\gamma) = \sum_{i,j} \frac{a_{ij}}{r} \sigma(\alpha_i) \beta_j.$$

Έστω

$$x_i := \sum_j \frac{a_{ij}}{r} \beta_j$$

και $\sigma_1, \sigma_2, \ldots, \sigma_m$ οι εμφυτεύσεις του K στο $\mathbb{C}$. Προκύπτει σύστημα m γραμμικών εξισώσεων της μορφής

$$\sum_i \sigma_k(\alpha_i) x_i = \sigma_k(\gamma), \qquad k = 1, 2, \ldots, m.$$

Σύμφωνα με τον κανόνα του Cramer έχουμε

$$\Delta x_i = \Delta_i$$

όπου $\Delta = \det(\sigma_j(\alpha_i))$ και το Δ_i μια ανάλογη ορίζουσα. Αλλά η διακρίνουσα του K, $D_K = \Delta^2$. Συνεπώς $D_K x_i = \Delta\Delta_i$. Τα Δ και Δ_i είναι εκ κατασκευής ακέραιοι αλγεβρικοί αριθμοί. Επομένως και τα $D_K x_i$ είναι ακέραιοι αλγεβρικοί. Αλλά τα

$$D_K x_i = \sum \frac{D_K a_{ij}}{r} \beta_j.$$

Το σύνολο $\{\beta_1, \beta_2, \ldots, \beta_n\}$ είναι βάση ακεραιότητας του L ως προς $\mathbb{Q}$. Αυτό σημαίνει ότι οι αριθμοί $D_K a_{ij}/r \in \mathbb{Z}$, δηλαδή $r \mid D_K a_{ij}$ για όλα τα i, j. Επειδή κανένας πρώτος παράγοντας του r δεν διαιρεί όλα τα a_{ij} έπεται ότι $r \mid D_K$. Ανάλογα αποδεικνύεται ότι $r \mid D_L$, οπότε $r|d$ και συνεπώς $\gamma \in \frac{1}{d} R_K R_L$. □

Πόρισμα IV.7.3. *Υποθέτουμε ότι* K, L *είναι δύο αλγεβρικά σώματα αριθμών για τα οποία ισχύουν*

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$$

και $(D_K, D_L) = 1$. *Τότε ισχύει* $R_{KL} = R_K R_L$.

Παράδειγμα IV.7.4. Έστω $\mathbb{Q}(\sqrt{5},\sqrt{6})$. Αν $K=\mathbb{Q}(\sqrt{5})$ και $L=\mathbb{Q}(\sqrt{6})$ έχουμε $KL=\mathbb{Q}(\sqrt{5},\sqrt{6})$ και

$$[KL:\mathbb{Q}]=[K:\mathbb{Q}][L:\mathbb{Q}]=4.$$

Επίσης $D_K=5$ και $D_L=24$ άρα $(D_K,D_L)=(5,24)=1$. Μια βάση ακεραιότητας του K είναι το σύνολο $\{1,\frac{1+\sqrt{5}}{2}\}$ και μια βάση ακεραιότητας του L είναι το συνόλο $\{1,\sqrt{6}\}$. Συνεπώς μια βάση ακεραιότητας του $\mathbb{Q}(\sqrt{5},\sqrt{6})$ είναι το σύνολο

$$\left\{1,\frac{1+\sqrt{5}}{2},\sqrt{6},\frac{\sqrt{6}+\sqrt{30}}{2}\right\}.$$

Παρατήρηση IV.7.5. Η υπόθεση ότι $(D_K,D_L)=1$ είναι αναγκαία. Πράγματι έστω $K=\mathbb{Q}(\sqrt{-2n})$ και $L=\mathbb{Q}(\sqrt{2n})$ όπου n ελεύθερος τετραγώνου περιττός φυσικός αριθμός $n>1$. Ισχύει $[KL:\mathbb{Q}]=4$, $R_K=\mathbb{Z}[\sqrt{-2n}]$, $R_L=\mathbb{Z}[\sqrt{2n}]$. Επομένως

$$R_KR_L=\{a_0+a_1\sqrt{2n}+a_2\sqrt{-2n}+a_32n\sqrt{-1}:a_i\in\mathbb{Z}\}.$$

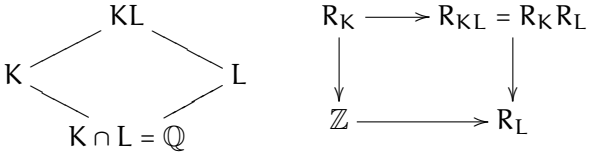
Όμως $\sqrt{-1}\notin R_KR_L$, αφού ο συντελεστής της $\sqrt{-1}$ είναι άρτιος. Όμως $\sqrt{-1}\in KL$ για $a_0=a_1=a_2=0$ και $a_3=\frac{1}{2n}$ και επειδή $\sqrt{-1}$ ρίζα του x^2+1 ακέραιος αλγεβρικός έχουμε ότι $\sqrt{-1}\in R_{KL}$ $R_KR_L\subsetneq R_{KL}$.

Πρόταση IV.7.6. *Έστω K,L αλγεβρικά σώματα αριθμών. Υποθέτουμε ότι*

$$[KL:\mathbb{Q}]=[K:\mathbb{Q}][L:\mathbb{Q}]$$

και ότι $d=ΜΚΔ(D_K,D_L)=1$. Η διακρίνουσα του σώματος KL είναι $D_{KL}=D_K^{[L:\mathbb{Q}]}D_L^{[K:\mathbb{Q}]}$.

Απόδειξη. Η βασική ιδέα της απόδειξης της πρότασης είναι ότι με βάση τις υποθέσεις το ίχνος $\mathrm{Tr}_{KL/L}|_K=\mathrm{Tr}_{K/\mathbb{Q}}$.



Η συνέχεια είναι ο υπολογισμός ιχνών κατά το σχήμα άνω δεξιά. □

Με βάση το θεώρημα IV.7.1 το πόρισμα IV.7.3 την πρόταση IV.7.6 και εφαρμόζοντας μαθηματική επαγωγή έχουμε το

Θεώρημα IV.7.7. *Έστω N φυσικός αριθμός $N>1$ και ζ_N μια πρωταρχική N-ρίζα της μονάδας. Μία βάση ακεραιότητας του κυκλοτομικού σώματος αριθμών $K=\mathbb{Q}(\zeta_N)$ είναι το σύνολο $\{1,\zeta_N,\zeta_N^2,\dots,\zeta_N^{\phi(N)}-1\}$. Η διακρίνουσα του σώματος K είναι*

$$D_K=(-1)^{\frac{\phi(N)}{2}}N^{\phi(N)}\left(\prod_{p|N}p^{\frac{\phi(N)}{p-1}}\right)^{-1}.$$

IV.8 Αλγόριθμος υπολογισμού βάσεων ακεραιότητας

Έστω K αλγεβρικό σώμα αριθμών, $[K:\mathbb{Q}]=n$ και $\{\omega_1,\omega_2,\dots,\omega_n\}$ μια βάση ακεραιότητας αυτού. Ως γνωστό ο R_K είναι μια ελεύθερη αβελιανή ομάδα τάξης n. Έστω τώρα $\{\alpha_1\,\alpha_2,\dots,\alpha_n\}$ μια βάση της επέκτασης $K/\mathbb{Q}$ με στοιχεία ακέραιους αλγεβρικούς αριθμούς. Η προσθετική ομάδα

$$H:=\mathbb{Z}\alpha_1+\mathbb{Z}\alpha_2+\cdots+\mathbb{Z}\alpha_n$$

είναι επίσης ελεύθερη αβελιανή ομάδα με τάξη n. Ισχύει

$$D_K(\alpha_1,\alpha_2,\dots,\alpha_n)=[R_K:H]^2D_K(\omega_1,\omega_2,\dots,\omega_n)=[R_K:H]^2D_K.$$

Πρόταση IV.8.1. *Αν* $H \neq R_K$, *τότε υπάρχει ακέραιος αλγεβρικός* θ *της μορφής*

$$\theta = \frac{m_1\omega_1 + \cdots + m_n\omega_n}{p},$$

$m_j \in \mathbb{Z}$ $j = 1, 2, \ldots, n$ *με* p *πρώτος όχι όλα τα* m_j *μηδέν και* $0 \leq m_j < p$, $j = 1, 2, \ldots, n$.

Απόδειξη. Η ομάδα R_K/H είναι πεπερασμένης τάξης. Από $R_K \neq H$ έπεται ότι υπάρχει πρώτος p που διαιρεί την τάξη της ομάδος, $p \mid [R_K : H]$ και συνεπώς $p^2 \mid D_K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Από το θεώρημα του Cauchy έπεται ότι υπάρχει στοιχείο $\theta \in R_K$ έτσι ώστε το σύμπλοκο $p\theta \in H$ και $\theta \notin H$. Έχουμε $p\theta = m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n$, δηλαδή

$$\theta = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{p},$$

$m_j \in \mathbb{Z}$ όχι όλοι μηδέν αφού $\theta \notin H$. Επειδή αν τροποποιήσουμε τους συντελεστές κατά πολλαπλάσια του p η κλάση του θ, $\theta + H$ δεν αλλάζει, μπορούμε να υποθέσουμε ότι $0 \leq m_j < p$ για $j = 1, 2, \ldots, n$. □

IV.8.1 Αλγόριθμος

Βήμα 1ο Επιλέγουμε $B = \{\omega_1, \ldots, \omega_n\}$ μια βάση της επέκτασης $K/\mathbb{Q}$, $[K : \mathbb{Q}] = n$ με στοιχεία ω_i ακέραιους αλγεβρικούς.
Βήμα 2ο Υπολογίζουμε τη διακρίνουσα $D_K(\omega_1, \ldots, \omega_n)$.
Βήμα 3ο Καταγράφουμε όλους τους πρώτους p για τους οποίους ισχύει $p^2 \mid D_K(\omega_1, \ldots, \omega_n)$.
Βήμα 4ο Για κάθε πρώτο p του βήματος 3 και κάθε στοιχείο της μορφής

$$\theta = \frac{m_1\omega_1 + \cdots + m_n\omega_n}{p}$$

$m_j \in \mathbb{Z}$ $0 \leq m_j < p$ όχι όλοι μηδέν και ελέγχουμε αν το $\theta \in R_K$.
Βήμα 5ο Αν βρούμε κάποιο τέτοιο θ στον R_K, τότε υπολογίζουμε μια βάση B' για την προσθετική αβελιανή ομάδα που παράγεται από το B και θ. Επιστρέφουμε στο βήμα 2 και αντικαθιστούμε τη βάση B με τη B'. Στην πραγματικότητα η καινούργια βάση έχει διακρίνουσα $D_K(B') = \frac{1}{p^2}D_K(B)$ συνεπώς πάμε κατ' ευθείαν στο βήμα 3.
Βήμα 6ο Αν δεν βρέθηκε τέτοιο θ, τότε το B είναι βάση ακεραιότητας του σώματος K.

Παράδειγμα IV.8.2. Έστω $f(X) = X^3 + 11X + 4 \in \mathbb{Z}[X]$. Το πολυώνυμο είναι ανάγωγο υπέρ του $\mathbb{Q}$. Έστω θ μια ρίζα αυτού. Επομένως $[K : \mathbb{Q}] = 3$ το $K = \mathbb{Q}(\theta)$ και $B = \{1, \theta, \theta^2\}$ είναι μια βάση της επέκτασης $K/\mathbb{Q}$. Η διακρίνουσα του θ είναι $D_K(\theta) = -1439 \cdot 2^2$, και 1439 είναι πρώτος.

Τον μοναδικό πρώτο που θα πρέπει να ελέγξουμε είναι ο $p = 2$. Επομένως είναι αναγκαίο να ελέγξουμε ποια από τα παρακάτω στοιχεία του σώματος K

$$\left\{\frac{1}{2}, \frac{\theta}{2}, \frac{\theta^2}{2}, \frac{1+\theta}{2}, \frac{1+\theta^2}{2}, \frac{\theta+\theta^2}{2}, \frac{1+\theta+\theta^2}{2}\right\}$$

είναι αλγεβρικοί ακέραιοι του K. Τα $1/2, \theta/2 \notin R_K$, έχουν norm που δεν είναι ακέραιος αριθμός. Το $\frac{1+\theta}{2} \notin R_K$, αφού το ίχνος $\mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1+\theta}{2}\right) = \frac{3}{2}$.

Έχουμε άλλους τέσσερις υποψήφιους για το θ. Εδώ υπολογίζουμε ένα κυβικό πολυώνυμο κάθε φορά το οποίο έχει ρίζα έναν αριθμό από τις υπόλοιπες δυνατότητες (το χαρακτηριστικό πολυώνυμο το οποίο είναι και το ελάχιστο πολυώνυμο του αριθμού).

Για παράδειγμα για $\alpha := \frac{\theta+\theta^2}{2}$, το χαρακτηριστικό πολυώνυμο είναι το $X^3 + 11X^2 + 36X + 4$. Συνεπώς το $\alpha = \frac{\theta+\theta^2}{2} \in R_K$.

Η υποομάδα του K η οποία παράγεται από το B και $\frac{\theta+\theta^2}{2}$ έχει βάση $\left\{1, \theta, \frac{\theta+\theta^2}{2}\right\}$ και περιέχει το $\mathbb{Z}[\theta]$ με δείκτη 2. Συνεπώς $D_K\left(1, \theta, \frac{\theta+\theta^2}{2}\right) = -1439$, που είναι ακέραιος ελεύθερος τετραγώνου. Επομένως το $B = \left\{1, \theta, \frac{\theta+\theta^2}{2}\right\}$ είναι μια βάση ακεραιότητας του K.

Παράδειγμα IV.8.3. Να βρεθεί ο δακτύλιος ακεραίων του σώματος $\mathbb{Q}(\sqrt[3]{5})$. Θεωρούμε τον δακτύλιο $\mathbb{Z}(\theta)$ για $\theta = \sqrt[3]{5}$ και υπολογίζουμε τη διακρίνουσα:

$$D_{K/\mathbb{Q}}(\theta) = -3^3 \cdot 5^2.$$

Ο δείκτης $[R_K : \mathbb{Z}[\theta]]$ είναι διαιρέτης του $3 \cdot 5$ και το πηλίκο είναι ισόμορφο με υποομάδα του $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Συνεπώς οι υποψήφιοι ακέραιοι αλγεβρικοί είναι της μορφής:

1. $\alpha = 1/3(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2)$ για $0 \leq \lambda_i \leq 2$
2. $\alpha = 1/5(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2)$ για $0 \leq \lambda_i \leq 4$.

Μπορούμε να ελέγξουμε τις πεπερασμένες παραπάνω περιπτώσεις μία προς μία αν είναι ακέραιοι αλγεβρικοί. Ας επικεντρωθούμε στη δεύτερη περίπτωση. Το ίχνος

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 3\lambda_1/5 \in \mathbb{Z}$$

συνεπώς $\lambda_1 \in 5\mathbb{Z}$. Αυτό σημαίνει ότι

$$\alpha' = 1/5(\lambda_2\theta + \lambda_3\theta^2)$$

θα πρέπει επίσης να είναι ακέραιος αλγεβρικός. Υπολογίζουμε ότι

$$N(\alpha') = N(\lambda_2\theta + \lambda_3\theta^2)/125 = (5\lambda_2^3 + 25\lambda_3^3)/125 = (\lambda_2^3 + 5\lambda_3^3)/25.$$

Είναι η τελευταία ποσότητα ακέραιος; Αυτό απαιτεί έναν πεπερασμένο υπολογισμό για όλα τα $0 \leq \lambda_2, \lambda_3 \leq 4$. Εναλλακτικά μπορούμε να επιχειρηματολογήσουμε ως εξής:. Αν $5 \mid \lambda_3$, τότε θα πρέπει $5 \mid \lambda_2$. Σε διαφορετική περίπτωση έχουμε

$$5 \equiv (-\lambda_2/\lambda_3)^3 \mod 25.$$

Δηλαδή το 5 είναι κυβικό υπόλοιπο modulo 25, δηλαδή $5 \equiv c^3 \mod 25$ το οποίο δίνει ότι $5 \mid c$ συνεπώς έχουμε $5 \equiv (5k)^3 \mod 25$ το οποίο έχει ως συνέπεια $5 \equiv 0 \mod 25$, άτοπο.

Για αποτελέσματα με χρήση ηλεκτρονικού υπολογιστή και χρήση των προγραμμάτων PARI και SAGE αντίστοιχα παραπέμπουμε στο [10] και [14].

IV.9 Ασκήσεις

1. Αν K αλγεβρικό σώμα αριθμών και $\alpha \in K$, να αποδειχθεί ότι για κάθε ακέραιο m ισχύει:
$$D_K(\alpha) = D_K(\alpha + m)$$
2. Αν $K = \mathbb{Q}(\zeta_p)$, $p \in \mathbb{P}$ να υπολογιστεί η διακρίνουσα $D_K(1 - \zeta_p)$.
3. Έστω $K = \mathbb{Q}(\theta)$, θ ακέραιος αλγεβρικός, ρίζα του αναγώγου υπέρ το $\mathbb{Q}$ πολυωνύμου
$$f(x) = x^n + ax = b,$$
$a, b \in \mathbb{Q}$, $n \geq 2$. Να υπολογιστεί η διακρίνουσα $D_K(\theta)$.
4. Έστω $f(x) = x^5 + ax + b$, $a, b \in \mathbb{Q}$ και $f(x)$ ανάγωγο υπέρ το $\mathbb{Q}$. Αν α είναι μία ρίζα του $f(x)$ να αποδειχτεί ότι
$$D_K(\alpha) = 4^4a^5 + 5^5b^4.$$
Υποθέτουμε ότι $\alpha^5 = \alpha + 1$. Να αποδεχθεί ότι $R_K = \mathbb{Z}[\alpha]$, όπου $K = \mathbb{Q}(\alpha)$.

5. Να αποδειχτεί ότι αν το α είναι ρίζα μονικού πολυωνύμου με συντελεστές ακέραιους αλγεβρικούς αριθμούς, τότε το α είναι ακέραιος αλγεβρικός αριθμός.

6. Έστω $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, με m και n ακέραιους ελευθέρους τετραγώνου $\neq \pm 1$, $m \neq n$. Να αποδειχτεί ότι ο $\alpha \in K$ είναι ακέραιος αλγεβρικός, τότε και μόνο τότε όταν η $N_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ και το ίχνος $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ είναι ακέραιοι αλγεβρικοί.

7. Αν $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, όπου m, n ακέραιοι ελεύθεροι τετραγώνου και πρώτοι μεταξύ τους. Να υπολογιστεί μία βάση ακεραιότητας του K όταν

   (α′) $m, n \equiv 1 \mod 4$ καθώς και όταν

   (β′) $m \equiv 1 \mod 4$ και $n \not\equiv 1 \mod 4$.

Σημείωση IV.9.1. Για τη γενική περίπτωση των διτετραγωνικών επεκτάσεων του $\mathbb{Q}$ παραπέμπουμε στην εργασία [16].

Σημείωση IV.9.2. Αργότερα θα αποδείξουμε ότι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του μέγιστου πραγματικού υποσώματος του $K = \mathbb{Q}(\zeta_p)$, το οποίο είναι το $K_+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ είναι ο $R_{K_+} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

Βιβλιογραφία

[1] Alaca, Ş. *p-integral bases of a cubic field*. *Proc. Amer. Math. Soc.* 126.7 (1998), pp. 1949–1953. ISSN: 0002-9939.

[2] Alaca, Ş. & Williams, K. S. *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, 2004, pp. xviii+428. ISBN: 0-521; 0-521-54011-9.

[3] Berwick, W. E. H. *Integral Bases*. Cambridge Tracts in Mathematics and Mathematical Physics, No. 22. Stechert-Hafner, Inc., New York, 1964, pp. v+95.

[4] Bosch, S. *Algebra*. Springer-Lehrbuch. Springer Berlin, 2013. ISBN: 9783662056493. URL: https://books.google.gr/books?id=4BiyBgAAQBAJ.

[5] Cohen, H. *A Course in Computational Algebraic Number Theory*. Vol. 138. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993, pp. xii+534. ISBN: 3-540-55640-0.

[6] Gaál, I. *Diophantine Equations and Power Integral Bases*. Theory and algorithms, Second edition of [MR1896601]. Birkhäuser/Springer, Cham, 2019, pp. xxii+326. ISBN: 978-3-030-23864-3; 978-3-030-23865-0.

[7] Hungerford, T. W. *Algebra*. Rinehart and Winston, Inc., New York: Holt, 1974, pp. xix+502.

[8] Llorente, P. & Nart, E. *Effective determination of the decomposition of the rational primes in a cubic field*. *Proc. Amer. Math. Soc.* 87.4 (1983), pp. 579–585. ISSN: 0002-9939.

[9] Marcus, D. A. *Algebraic Number Fields*. Universitext. 2nd edition of [MR0457396], With a foreword by Barry Mazur. Springer, 2018, pp. xviii+203. ISBN: 978-3-319-90232-6; 978-3-319-90233-3.

[10] Milne, J. S. *Algebraic Number Theory (v3.08)*. Available at www.jmilne.org/math/. 2020.

[11] Motoda, Y. *On Power Integral Bases for Certain Abelian Fields*. PhD thesis. 2011.

[12] Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*. 3rd edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004, pp. xii+708. ISBN: 3-540-21902-1.

[13] Pollack, P. *A Conversational Introduction to Algebraic Number Theory, Arithmetic beyond* $\mathbb{Z}$. Vol. 84. Student Mathematical Library. American Mathematical Society, Providence, RI, 2017, pp. ix + 316. ISBN: 978-1-4704-3653-7.

[14] Stein, W. *Algebraic Number Theory, a computational approach. Harvard. Massachusetts* (2012). URL: https://wstein.org/books/ant/ant.pdf.

[15] Stewart, I. & Tall, D. *Algebraic Number Theory and Fermat's Last Theorem*. 4th edition. CRC Press, Boca Raton, FL, 2016, pp. xix+322. ISBN: 978-1-4987-3839-2.

[16] Williams, K. S. *Integers of biquadratic fields. Canad. Math. Bull.* 13 (1970), pp. 519–526. ISSN: 0008-4395.

V

Norm ιδεωδών και το πεπερασμένο του αριθμού κλάσεων

Έστω $K = \mathbb{Q}(\theta)$ αλγεβρικό σώμα αριθμών, R_K ο δακτύλιος του Dedekind των ακεραίων αλγεβρικών αυτού. Στο κεφάλαιο αυτό θα ορίσουμε και θα μελετήσουμε την έννοια της norm των ιδεωδών του R_K. Είναι φυσικό η έννοια αυτή να είναι συμβατή με την έννοια στοιχείου του R_K και να έχει την πολλαπλασιαστική ιδιότητα.

Στη συνέχεια αποδεικνύουμε το πεπερασμένο του αριθμού κλάσεων ιδεωδών του K. Χρησιμοποιούμε το θεώρημα του Minkowski, το οποίο θα το αποδείξουμε αργότερα, και έτσι έχουμε ένα καλό άνω φράγμα αυτού.

V.1 Norm ιδεωδών αλγεβρικού σώματος αριθμών

Ορισμός V.1.1. Έστω A ένα ακέραιο ιδεώδες του R_K. Ο δακτύλιος R_K/A έχει πεπερασμένο πλήθος στοιχείων. Ορίζουμε *(απόλυτη) norm* του A τον φυσικό αριθμό $N_K(A) = \#R_K/A$.

Πριν προχωρήσουμε στη μελέτη της έννοιας της norm θα μελετήσουμε μερικές ιδιότητες των ιδεωδών του R_K.

Είναι προφανές ότι αν $a, b \in R_K$, τότε η ισοτιμία $ax \equiv b \mod A$ έχει λύση ακριβώς τότε όταν $b \in A + aR_K$. Έστω τώρα ένα πρώτο ιδεώδες P του R_K και $\alpha \in R_K - P$. Για κάθε φυσικό $n \in \mathbb{N}$ τα ιδεώδη αR_K και P^n είναι πρώτα μεταξύ τους και αφού είναι ακέραια ισχύει

$$(P^n, \alpha R_K) = P^n + \alpha R_K = R_K.$$

Επομένως για κάθε $n \in \mathbb{N}$ η ισοτιμία

$$\alpha x \equiv \beta \mod P^n$$

έχει λύση για κάθε $\beta \in R_K$.

Αν τώρα $P_1, \ldots, P_m$ πρώτα ιδεώδη του R_K διάφορα μεταξύ τους ανά δύο, τότε για κάθε m-άδα στοιχείων του R_K $\alpha_1, \ldots, \alpha_m$ και κάθε φυσικό αριθμό n το σύστημα

$$x \equiv \alpha_i \mod P_i^n, i = 1, \ldots, m$$

έχει λύση.

Πράγματι, διαλέγουμε $b_i \in (P_1P_2 \cdots P_{i-1}P_{i+1}P_m)^n - P_i$ για κάθε $i = 1, \ldots, m$ και έστω x_i η λύση της

$$b_i x_i \equiv \alpha_i \mod P^n.$$

Το στοιχείο $x = b_1x_1 + b_2x_2 + \cdots + b_mx_m$ είναι λύση του συστήματος.

Το γνωστό θεώρημα υπολοίπων του Κινέζου της στοιχειώδους θεωρίας αριθμών γενικεύεται και στα ιδεώδη.

Πρόταση V.1.2 (Θεώρημα υπολοίπων του Κινέζου)**.** *Έστω* $A_1, \dots, A_m$ *ακέραια ιδεώδη του* K *πρώτα μεταξύ τους ανά δύο και* $\alpha_1, \dots, \alpha_m$ *στοιχεία του* R_K*. Το σύστημα ισοτιμιών*

$$x \equiv \alpha_i \mod A_i, i = 1, 2, \dots, m$$

έχει λύση.

Απόδειξη. Παρατηρούμε ότι αν $A = \prod_{i=1}^{\ell} P_i^{\alpha_i(A)}$ είναι η ανάλυση ενός ακέραιου ιδεώδους A του K σε γινόμενο πρώτων ιδεωδών P_i, $i = 1, 2, \dots, \ell$ και $\alpha_i(A) \in \mathbb{N}$, η ισοτιμία

$$x \equiv \alpha \mod A$$

έχει λύση, τότε και μόνο τότε όταν το σύστημα

$$x \equiv \alpha \mod P_i^{\alpha_i(A)}, i = 1, 2, \dots, \ell$$

έχει λύση. Αφού τα A_i είναι πρώτα μεταξύ τους ανά δύο η παρατήρηση πριν την πρόταση V.1.2 οδηγεί στο ζητούμενο. □

Πρόταση V.1.3. *Έστω* A *ακέραιο ιδεώδες του* K *και*

$$A = \prod_{i=1}^{\ell} P_i^{\alpha_i(A)}$$

η ανάλυσή του σε γινόμενο πρώτων ιδεωδών. Τότε ισχύει

$$\frac{R_K}{A} \cong \bigoplus_{i=1}^{\ell} \frac{R_K}{P_i^{\alpha_i(A)}}.$$

Απόδειξη. Η συνάρτηση

$$\phi : R_K \ni x \mapsto \left(x \mod P_1^{\alpha_1(A)}, x \mod P_2^{\alpha_2(A)}, \dots, x \mod P_\ell^{\alpha_\ell(A)}\right) \in \bigoplus_{i=1}^{\ell} \frac{R}{P_i^{\alpha_i(A)}}.$$

είναι προφανώς ομομορφισμός δακτυλίων. Από την πρόταση V.1.2 προκύπτει ότι η συνάρτηση ϕ είναι επιμορφισμός. Επιπλέον $\ker\phi = \bigcap_{i=1}^{\ell} P_i^{\alpha_i(A)} = \prod_{i=1}^{\ell} P_i^{\alpha_i(A)} = A$. □

Πρόταση V.1.4. *Έστω* P *πρώτο ιδεώδες του* K *και* $n \in \mathbb{N}$*. Οι δακτύλιοι πηλίκων* R_K/P *και* P^n/P^{n+1} *είναι ισόμορφες σαν προσθετικές ομάδες.*

Απόδειξη. Έστω $\alpha \in P^n - P^{n+1}$. Θεωρούμε τη συνάρτηση

$$\phi : (R_K, +) \ni x \mapsto \alpha x \in (P^n, +).$$

Για κάθε $x \in P$ ισχύει $\phi(x) = \alpha x \in P^{n+1}$ δηλαδή $\phi(x) \subset P^{n+1}$. Συνεπώς η ϕ επάγει έναν ομομορφισμό ομάδων

$$\begin{aligned} \widetilde{\phi} : R_K/P &\to P^n/P^{n+1} \\ x + P &\mapsto \alpha x + P^{n+1}. \end{aligned}$$

Ο $\ker\widetilde{\phi} = \{x + P | \alpha x \in P^{n+1}\}$. Επειδή $\alpha \in P^n - P^{n+1}$ έχουμε ότι

$$\ker\widetilde{\phi} = \{x + P : x \in P\} = P.$$

Επομένως η $\widetilde{\phi}$ είναι μονομορφισμός ομάδων. Επιπλέον είναι και επιμορφισμός. Πράγματι, έστω

$$y + P^{n+1} \in P^n/P^{n+1}.$$

Η ισοτιμία

$$ax \equiv y \mod P^{n+1}$$

έχει λύση αφού το $a \in P^n \backslash P^{n+1}$ δηλαδή $aR_K + P^{n+1} = P^n$. Έστω x_0 μία λύση αυτής. Επομένως

$$\widetilde{\phi}(x_0 + P) = ax_0 + P^{n+1} = y + P^{n+1}.$$

Έχουμε λοιπόν ότι $\widetilde{\phi}$ είναι ισομορφισμός ομάδων και συνεπώς το ζητούμενο. □

Θεώρημα V.1.5. *Έστω A, B ακέραια ιδεώδη του K. Ισχύει ότι*

$$N_K(AB) = N_K(A)N_K(B).$$

Απόδειξη. Από την πρόταση V.1.4 έχουμε ότι ο δακτύλιος πηλίκων P^n/P^{n+1} έχει $\#R_K/P = N_K(P)$ το πλήθος στοιχεία. Αλλά

$$(\#R/P^{n+1})/(\#R/P^n) = \#P^n/P^{n+1}.$$

επομένως $N_K(P^{n+1}) = N_K(P^n)N_K(P)$ και επαγωγικά ως προς n, $N_K(P^n) = N_K(P)^n$ για κάθε $n \in \mathbb{N}$.

Έστω τώρα $A = \prod_{i=1}^{\ell} P_i^{\alpha_i(A)}$ και $B = \prod_{j=1}^{m} Q_j^{\beta_j(B)}$. Οι αναλύσεις των A, B σε γινόμενο πρώτων ιδεωδών. Από την πρόταση V.1.3 έχουμε ότι

$$N_K(A) = \prod_{i=1}^{\ell} N_K(P_i^{\alpha_i(A)}) \text{ και } N_K(B) = \prod_{j=1}^{m} N_K(Q_j^{\beta_j(B)})$$

οπότε

$$N_K(A)N_K(B) = \prod_{i=1}^{\ell} N_K(P_i)^{\alpha_i(A)} \prod_{j=1}^{m} N_K(Q_j^{\beta_j(B)}) = N_K(AB).$$

□

Η έννοια της norm επεκτείνεται και στα κλασματικά ιδεώδη με εντελώς φυσιολογικό τρόπο. Θα συμβολίζουμε με $\mathrm{Spec}R_K$ το σύνολο των πρώτων ιδεωδών του δακτυλίου R_K.

Ορισμός V.1.6. Έστω A κλασματικό ιδεώδες του K,

$$A = \prod_{P \in \mathrm{Spec}R_K} P^{\alpha_P(A)}, \alpha_P(A) \in \mathbb{Z}, \text{ σχεδόν όλα } 0.$$

Ορίζουμε ως norm του A:

$$N_K(A) = \prod_{P \in \mathrm{Spec}R_K} N_K(P)^{\alpha_P(A)}.$$

Παρατήρηση V.1.7. Είναι προφανές από τον ορισμό το Θεώρημα V.1.5 ισχύει και για κλασματικά ιδεώδη.

Πρόταση V.1.8. *Κάθε πρώτο ιδεώδες P του K έχει norm ίση προς τη δύναμη κάποιου πρώτου αριθμού.*

Απόδειξη. Έστω P ένα πρώτο ιδεώδες του R_K. Ο δακτύλιος R_K είναι δακτύλιος Dedekind. Συνεπώς το P είναι μέγιστο, συνεπώς το R_K/P είναι σώμα και μάλιστα πεπερασμένο άρα έχει p^f το πλήθος στοιχεία για κάποιο $f \in \mathbb{N}$. Συνεπώς, $N_K(P) = p^f$. □

Ορισμός V.1.9. Ο φυσικός αριθμός f λέγεται *βαθμός* του πρώτου ιδεώδους P.

Σημείωση V.1.10. Από τη θεωρία σωμάτων γνωρίζουμε ότι $f = [R_K/P : \mathbb{Z}/p\mathbb{Z}]$. Αν τώρα $\alpha \in R_K - \{0\}$ έχουμε ορίσει την $N_{K/\mathbb{Q}}(\alpha)$ και την $N_K(\alpha R_K)$. Οι δύο έννοιες θα πρέπει να είναι συμβατές μεταξύ τους. Βέβαια η norm ένος στοιχείου μπορεί να είναι και αρνητικός ακέραιος, ενώ η norm ιδεώδους είναι πάντα φυσικός αριθμός.

Θα αποδείξουμε ότι

Πρόταση V.1.11. *Έστω $\alpha \in R_K - \{0\}$, τότε*

$$N_K(\alpha R_K) = |N_{K/\mathbb{Q}}(\alpha)|.$$

Απόδειξη. Έστω $[K : \mathbb{Q}] = n$ και $\{\omega_1, \dots, \omega_n\}$ μια βάση ακεραιότητας του K. Δηλαδή

$$R_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$$

και $\alpha R_K = \mathbb{Z}\alpha\omega_1 \oplus \cdots \oplus \mathbb{Z}\alpha\omega_n$. Έχουμε

$$\alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = (\omega_1, \dots, \omega_n) A(\alpha),$$

όπου

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ji}\omega_j, A(\alpha) = (a_{ij}) \in M_n(\mathbb{Z}).$$

Οπότε λόγω του θεωρήματος IV.3.10 έχουμε:

$$N_K(\alpha R_K) = \#R_K/\alpha R_K = |\det A(\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|.$$

□

Παρατήρηση V.1.12. Τέλος παρατηρούμε ότι η norm κάθε ακέραιου ιδεώδους του K ανήκει στο ιδεώδες. Πράγματι, αν A ακέραιο ιδεώδες του R_K, τότε $N_K(A) = \#R_K/A$. Αυτό σημαίνει ότι για κάθε $\alpha \in R_K$ ισχύει $N_K(A) \cdot (\alpha + A) = 0 + A$. Άρα $N_K(A)\alpha \in A$ και για $\alpha = 1$ έχουμε $N_K(A) \in A$.

Ιδιαίτερα για κάθε πρώτο ιδεώδες P του K υπάρχει πρώτος $p \in P$, αφού $N_K(P) = p^f \in P$.

Αποδεικνύεται ότι αυτός είναι ο μοναδικός πρώτος που ανήκει στο πρώτο ιδεώδες P (άσκηση) και συνεπώς υπάρχουν άπειρα πρώτα ιδεώδη στο σώμα K.

Παράδειγμα V.1.13. Έστω $K = \mathbb{Q}(\sqrt{m})$, $m = 6 \equiv 2 \mod 4$. Επομένως $R_K = \mathbb{Z} + \mathbb{Z}\sqrt{6}$. Θεωρούμε το κλασματικό ιδεώδες $A = \mathbb{Z} + \mathbb{Z}\frac{\sqrt{6}}{2}$. Το A γράφεται $A = \frac{1}{2}I$, όπου $I = \langle 2, \sqrt{6}\rangle = 2\mathbb{Z} + \mathbb{Z}\sqrt{6}$. Το $I^2 = \langle 2, \sqrt{6}\rangle = \langle 4, 2\sqrt{6}, 6\rangle = \langle 2\rangle\langle 2, \sqrt{6}, 3\rangle = \langle 2\rangle$. Το τελευταίο ισχύει αφού $1 = 3 - 2 \in \langle 2, \sqrt{6}, 3\rangle$. Επομένως $N_K(I)^2 = N_K(I^2) = N_K(\langle 2\rangle) = |N_{K/\mathbb{Q}}(2)| = 4$ και καταλήγουμε ότι $N_K(I) = 2$. Τελικά $N_K(A) = 2/2^2 = 1/2$.

Παράδειγμα V.1.14. Έστω $K = \mathbb{Q}(\sqrt{-5})$, $m \equiv 3 \mod 4$, $R_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$, $A = \langle 2, 1 + \sqrt{-5}\rangle$, $A^2 = \langle 4, 2 + 2\sqrt{-5}, (1+\sqrt{-5})^2\rangle = \langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5}$. Το ιδεώδες περιέχει τη διαφορά $2+2\sqrt{-5}-(-4+2\sqrt{-5}) = 6$. Αφού περιέχει το 4 και το 6 περιέχει και τη διαφορά τους, δηλαδή το 2. Τώρα όλοι οι γεννήτορες του A^2 είναι πολλαπλάσια του 2. Συνεπώς, $A^2 = \langle 2\rangle$ και $N_K(A)^2 = N_K(A^2) = |N_{K/\mathbb{Q}}(2)| = 4$, οπότε $N_K(A) = 2$.

V.2 Το πεπερασμένο του αριθμού κλάσεων

Έστω K αλγεβρικό σώμα αριθμών και $[K : \mathbb{Q}] = n$, R_K είναι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών, I_R είναι ομάδα των κλασματικών ιδεωδών και $H_R = \{\alpha R_K : \alpha \in K^* - \{0\}\}$ η ομάδα των κύριων κλασματικών ιδεωδών του K.

Ορισμός V.2.1. Θα ονομάζουμε *ομάδα κλάσεων ιδεωδών* την ομάδα πηλίκο:

$$\mathfrak{K}_{R_K} = \frac{I_{R_K}}{H_{R_K}}.$$

Η τάξη της $\mathfrak{k}_{R_K}$ θα ονομάζεται *αριθμός κλάσεων* h_K του σώματος K.

Στόχος αυτής της παραγράφου είναι να αποδείξουμε το πεπερασμένο του αριθμού κλάσεων για κάθε αλγεβρικό σώμα αριθμών K. Πρώτα από όλα θα αποδείξουμε την

Πρόταση V.2.2. *Ο αριθμός κλάσεων ιδεωδών του K είναι $h_K = 1$, τότε και μόνο τότε όταν ο δακτύλιος των ακεραίων αλγεβρικών R_K είναι περιοχή μονοσήμαντης ανάλυσης.*

Απόδειξη. Αν $h_K = 1$, τότε R_K είναι περιοχή κυρίων ιδεωδών και συνεπώς δακτύλιος μονοσήμαντης ανάλυσης.

Αντιστρόφως έως ότι R_K περιοχή μονοσήμαντης ανάλυσης. Αφού κάθε ιδεώδες του R_K αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών αρκεί να αποδείξουμε ότι κάθε πρώτο ιδεώδες του R_K είναι κύριο ιδεώδες.

Έστω λοιπόν P πρώτο ιδεώδες του R_K. Ισχύει $P^2 \subsetneq P$, αλλιώς δεν θα είχαμε μονοσήμαντη ανάλυση. Έστω $\alpha \in P - P^2 \neq \varnothing$. Αυτό σημαίνει ότι

$$\alpha R_K \subset P \text{ και } \alpha R_K \nsubseteq P^2,$$

δηλαδή $P \mid \langle\alpha\rangle = \alpha R_K$ ενώ $P^2 \nmid \langle\alpha\rangle = \alpha R_K$. Το ιδεώδες αR_K αναλύεται σε γινόμενο πρώτων ιδεωδών.

$$\alpha R_K = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_r^{\alpha_r}, \alpha_i > 0.$$

Ένα από αυτά είναι το P. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $P = P_1$ άρα και $\alpha_1 = 1$. Ο δακτύλιος R_K είναι όμως περιοχή μονοσήμαντης ανάλυσης. Το $\alpha \neq 0$ και δεν είναι μονάδα του R_K αφού $\alpha \in P$. Επομένως το α αναλύεται σε γινόμενο αναγωγών στοιχείων:

$$\alpha \cong \pi_1^{\beta_1} \pi_2^{\beta_2} \cdots \pi_n^{\beta_n}, \beta_i \in \mathbb{N}.$$

Σε περιοχή μονοσήμαντης ανάλυσης τα πρώτα στοιχεία παράγουν τα πρώτα ιδεώδη. Επομένως τα $\pi_i R_K$ είναι πρώτα ιδεώδη του R_K. Συνπώς, το κύριο ιδεώδες αR_K αναλύεται σε γινόμενο πρώτων ιδεωδών και ως εξής

$$\alpha R_K = (\pi_1 R_K)^{\beta_1} (\pi_2 R_K)^{\beta_2} \cdots (\pi_n R_K)^{\beta_n} = P P^{\alpha_2} \cdots P_r^{\alpha_r}.$$

Λόγω του μονοσήμαντου της ανάλυσης σε γινόμενο πρώτων ιδεωδών έχουμε ότι υπάρχει $i \in \{1, 2, \ldots, n\}$ ώστε

$$P = \pi_i R_K$$

δηλαδή το τυχαίο P είναι κύριο ιδεώδες. □

Παρατήρηση V.2.3. Στην αλγεβρική θεωρία αριθμών οι έννοιες *περιοχή κυρίων ιδεωδών* και *περιοχή μονοσήμαντης ανάλυσης* ταυτίζονται. Αυτό φυσικά δεν ισχύει γενικά στην αντιμεταθετική άλγεβρα. Για παράδειγμα ο $\mathbb{Z}[x, y]$ είναι περιοχή μονοσήμαντης ανάλυσης αλλά όχι περιοχή κυρίων ιδεωδών.

Συνεχίζουμε με στόχο την απόδειξη του πεπερασμένου του αριθμού κλάσεων ιδεωδών. Αυτό θα γίνει σε τέσσερα βήματα. Μέχρι το τέλος αυτής της παραγράφου $\{\omega_1, \omega_2, \ldots, \omega_n\}$ θα είναι μια βάση ακεραιότητας της επέκτασης $K/\mathbb{Q}$.

Λήμμα V.2.4. *Υπάρχει μια σταθερά $C \in \mathbb{R}_+$, ώστε για κάθε n-αδα $(x_1, x_2, \ldots, x_n)$ ρητών αριθμών ισχύει*

$$|N_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_n\omega_n)| \leq C \left(\max_{i=1,\ldots,n} |x_i| \right)^n$$

Απόδειξη. Αν σ_i είναι οι n-εμφυτεύσεις του K στο $\mathbb{C}$ έχουμε:

$$|N_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_n\omega_n)| = \prod_{i=1}^{n}\left|\sum_{\nu=1}^{n} x_\nu\sigma_i(\omega_\nu)\right| \le \prod_{i=1}^{n}\sum_{\nu=1}^{n}|x_\nu||\sigma_i(\omega_\nu)|$$
$$= \left|\prod_{i=1}^{n}\sum_{\nu=1}^{n}\sigma_i(\omega_\nu)\right| \cdot \left(\max_{\nu=1,2,\ldots,n}|x_\nu|\right)^n.$$

Η σταθερά $C := |\prod_{i=1}^{n}\sum_{\nu=1}^{n}\sigma_i(\omega_\nu)|$. □

Για παράδειγμα για $K = \mathbb{Q}(i)$, $(\omega_1, \omega_2) = (1, i)$,

$$\sigma_1 = \mathrm{Id} : \left\{\begin{array}{c} 1 \mapsto 1 \\ i \mapsto i \end{array}\right\} \text{ και } \sigma_2 = \left\{\begin{array}{c} 1 \mapsto 1 \\ i \mapsto -i \end{array}\right\},$$

τότε

$$N(x_1 + x_2 i) = x_1^2 + x_2^2 \le 2\left(\max_{i=1,2}|x_i|\right)^2,$$

δηλαδή το $C = |(1+i)(1-i)| = 2$.

Λήμμα V.2.5 (Dirichlet pigeon principle). *Έστω C η σταθερά του λήμματος V.2.4 και A ένα ακέραιο ιδεώδες του R_K. Τότε υπάρχει $\alpha \in A - \{0\}$ ώστε*

$$|N_{K/\mathbb{Q}}(\alpha)| \le CN_K(A).$$

Απόδειξη. Θα εφαρμόσουμε το αξίωμα του περιστεριώνα του Dirichlet (pigeon hole principle). Θεωρούμε το σύνολο:

$$M = \left\{\xi : \xi = x_1\omega_1 + \cdots x_n\omega_n, x_i \in \mathbb{Z}, 1 \le x_i \le \sqrt[n]{N_K(A)} + 1\right\}$$

δηλαδή

$$\#M = \left(\sqrt[n]{N_K(A)} + 1\right)^n > \sqrt[n]{N_K(A)}^n = N_K(A) = \#R/A.$$

Άρα υπάρχουν τουλάχιστον δύο στοιχεία του M ξ, ξ', $\xi \ne \xi'$ ώστε $\xi \equiv \xi' \mod A$, συνεπώς $\xi - \xi' \in A$. Θέτουμε: $\alpha = \xi - \xi' \in A - \{0\}$. Ισχυριζόμαστε ότι αυτό το α πληροί τις απαιτήσεις του λήμματος.

Γράφουμε

$$\alpha = x_1\omega_1 + \cdots + x_n\omega_n : x_i \in \mathbb{Z}$$
$$\alpha = \xi - \xi', \xi, \xi' \in M \text{ συνεπώς } |x_i| \le \left(\sqrt[n]{N_K(A)} + 1\right) - 1 = \sqrt[n]{N_K(A)}.$$

οπότε από το λήμμα V.2.4 έπεται ότι

$$|N_{K/\mathbb{Q}}(\alpha)| \le C\left(\max_{i=1,\ldots,n}|x|_i\right)^n \le C\left(\sqrt[n]{N_K(A)}\right)^n = CN_K(A).$$

□

Λήμμα V.2.6. *Έστω C η σταθερά του λήμματος V.2.4. Σε κάθε κλάση $\mathfrak{k} \in \mathfrak{K}_K = I_{R_K}/H_{R_K}$ υπάρχει ένα ακέραιο ιδεώδες A με norm $N_K(A) \le C$.*

Απόδειξη. Επιλέγουμε ένα ιδεώδες $A' \in \mathfrak{k}^{-1}$ το οποίο χωρίς περιορισμό της γενικότητας το θεωρούμε ακέραιο. Πράγματι αν το A' ήταν κλασματικό, τότε εξ ορισμού υπάρχει $a \in R_K$ με $\langle a\rangle A' \subset R_K$ και τα ιδεώδη A', aA' ανήκουν στην ίδια κλάση ιδεωδών.

Το λήμμα V.2.5 εξασφαλίζει την ύπαρξη ενός $\beta \in A' - \{0\}$ ώστε

$$|N_{K/\mathbb{Q}}(\beta)| \le CN_K(A').$$

Το ιδεώδες $A = (A')^{-1}\beta R_K \in \mathfrak{k}$. Αρκεί να δείξουμε ακόμη ότι $A \subset R_K$ και ότι $N_K(A) \leq C$. Έχουμε $\beta \in A'$ συνεπώς $\beta R_K \subset A'$ και $(A')^{-1}\beta \subset A'(A')^{-1} = R_K$. Αυτό αποδεικνύει ότι A είναι ακέραιο. Από την άλλη

$$N_K(A) = \frac{N_K(\beta R_K)}{N_K(A')} = \frac{|N_{K/\mathbb{Q}}(\beta)|}{N_K(A')} \leq \frac{CN_K(A')}{N_K(A')} = C.$$

□

Λήμμα V.2.7. *Υπάρχουν μόνο πεπερασμένου πλήθους ακέραια ιδεώδη A με $N_K(A) \leq C$.*

Απόδειξη. Αρκεί να δείξουμε ότι για δοσμένο φυσικό αριθμό $m \in \mathbb{N}$ υπάρχουν μόνο πεπερασμένου πλήθους ακέραια ιδεώδη A του R_K με $N_K(A) = m$. Πράγματι,

$$m = N_K(A) = [R_K : A] \text{ συνεπώς } m(\alpha + A) = A \text{ για κάθε } \alpha \in R_K.$$

Δηλαδή $mR_K \subset A$ και αν θέσουμε $B := mR_KA^{-1} \subset AA^{-1} = R_K$, τότε

$$mR = A \cdot B \text{ με } B \text{ ακέραιο ιδεώδες του } R_K. \tag{V.1}$$

Έστω $mR_K = P_1^{m_1} \cdots P_r^{m_r}$ με $m_i \in \mathbb{N}$ για $i = 1, \ldots, r$. Από την εξίσωση (V.1) προκύπτει $A = P_1^{a_1} \cdots P_r^{a_r}$, $0 \leq a_i \leq m_i$, δηλαδή για τα a_i έχω πεπερασμένου πλήθος δυνατότητες και συνεπώς υπάρχουν πεπερασμένα το πλήθος ακέραια ιδεώδη με $N_K(A) = m$. □

Θεώρημα V.2.8. *Ο αριθμός κλάσεων κάθε αλγεβρικού σώματος αριθμών είναι πεπερασμένος.*

Απόδειξη. Η απόδειξη προκύπτει από τα λήμματα V.2.6 και V.2.7. Αν δεν ήταν πεπερασμένος, θα είχαμε αντίφαση. □

Πόρισμα V.2.9. *Για κάθε ακέραιο ιδεώδες A του K, υπάρχει φυσικός αριθμός ℓ, με $1 \leq \ell \leq h_K$, ώστε το ιδεώδες A^ℓ να είναι κύριο ιδεώδες.*

Απόδειξη. Θεωρούμε το σύνολο των ιδεωδών:

$$\mathcal{A} = \{A^i : 1 \leq i \leq h_k + 1\}.$$

Τουλάχιστον δύο από αυτά τα ιδεώδη ανήκουν στην ίδια κλάση. Έστω $A^i \cong A^j$ για $i < j$, συνεπώς υπάρχουν $a, b \in R$ με $aR_KA^i = bR_KA^j$. Έστω $\ell = j - i$ και $B = A^\ell$, θα δείξουμε ότι το B είναι κύριο ιδεώδες. Η σχέση

$$aR_KA^i = bR_KA^j$$

γράφεται

$$aR_KA^i = bR_KBA^i \text{ συνεπώς } (a/b)R_KA^i = BA^i \text{ και } B = a/bR_K,$$

δηλαδή κύριο ιδεώδες. □

Χρήσιμο είναι επίσης και το

Πόρισμα V.2.10. *Αν A ακέραιο ιδεώδες του αλγεβρικού σώματος αριθμών K, για το οποίο ισχύει $A^m = \langle a \rangle$, κύριο ιδεώδες του K και $(m, h_K) = 1$, τότε το A είναι κύριο ιδεώδες του K.*

Απόδειξη. Αφού $(m, h_K) = 1$, υπάρχουν ακέραιοι αριθμοί k, ℓ ώστε να ισχύει $mk + \ell h_k = 1$. Επομένως

$$A = A^1 = A^{mk+h_k\ell} = (A^m)^k(A^{h_K})^\ell.$$

Όμως $A^m = \langle \alpha \rangle$ κύριο ιδεώδες. Επίσης h_K είναι η τάξη της ομάδας κλάσεων ιδεωδών του K, για κάθε ιδεώδες A ισχύει $A^{h_K} = \langle \beta \rangle$, $\beta \in R_K$, κύριο ιδεώδες του K. Συνεπώς και το A είναι κύριο ιδεώδες του K. □

V.3 Αλγόριθμοι υπολογισμού

Η βασική ιδέα είναι να βρούμε όλα τα ακέραια ιδεώδη του K με norm $\leq C$, όπου C είναι η σταθερά του λήμματος V.2.4 και στη συνέχεια να ελέγξουμε σε πόσες διαφορετικές μεταξύ τους κλάσεις ανήκουν. Μάλιστα επειδή η norm είναι πολλαπλασιαστική αρκεί να το κάνουμε αυτό με όλα τα πρώτα ιδεώδη του K.

Είναι όμως πάρα πολύ δύσκολο να υπολογίσουμε την τιμή της σταθεράς C για το συγκεκριμένο σώμα K. Αυτό δεν είναι καθόλου εύκολο. Χρειαζόμαστε μια καλύτερη σταθερά η οποία να εξαρτάται από διάφορες παραμέτρους του σώματος K. Υπάρχει κάποια τέτοια σταθερά; Φυσικά και υπάρχει!

Πρόκειται για το θεώρημα του Minkowski. Για την απόδειξή του όμως χρειάζεται μια ξεχωριστή ιδέα. Το θεώρημα ανήκει σε έναν κλάδο της θεωρίας αριθμών που λέγεται «Γεωμετρία των Αριθμών». Εδώ θα αναφέρουμε το θεώρημα και τις συνέπειές του και θα το αποδείξουμε στην παράγραφο IX.1 του κεφαλαίου IX.

Αλλά ας πάρουμε τα πράγματα με τη σειρά. Έστω K ένα αλγεβρικό σώμα αριθμών, $K = \mathbb{Q}(\theta)$ και $[K : \mathbb{Q}] = n$. Υπάρχουν ακριβώς n-εμφυτεύσεις του σώματος K στο σώμα $\mathbb{C}$. Έστω $\theta^{(1)} = \theta, \theta^{(2)}, \ldots, \theta^{(n)}$ οι ρίζες του $\mathrm{Irr}(\theta, \mathbb{Q})$. Υπενθυμίζουμε ότι αν r_1 είναι το πλήθος των πραγματικών ριζών και $2r_2$ το πλήθος των μιγαδικών, τότε έχουμε ονομάσει ταυτότητα (signature) το $[r_1, r_2]$.

Ισχύει το

Θεώρημα V.3.1. *Έστω K αλγεβρικό σώμα αριθμών με ταυτότητα (signature) $[r_1, r_2]$. Τότε σε κάθε κλάση $\mathfrak{k} \in \mathfrak{K}_{R_K}$ υπάρχει ένα ακέραιο ιδεώδες $A \subset R_K$ με*

$$N_K(A) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_{K/\mathbb{Q}}|^{1/2} := M_K.$$

Σημείωση V.3.2. Στα 1936 ο Siegel απέδειξε ότι για μιγαδικά τετραγωνικά σώματα αριθμών $K = \mathbb{Q}(\sqrt{m})$, $m < 0$ ισχύει ότι

$$\forall \epsilon > 0, \exists C_\epsilon > 0 : h_K \geq C_\epsilon |D_{K/\mathbb{Q}}|^{1/2-\epsilon}.$$

Επομένως, όταν $|D_{K/\mathbb{Q}}| \to \infty$ έχουμε ότι $h_K \to \infty$.

Παρατήρηση V.3.3. Δεδομένης της μονοσήμαντης ανάλυσης στον δακτύλιο Dedekind R_K, αν $N_K(A) \leq M_K$, τότε για κάθε πρώτο ιδεώδες $P, P \mid A$ ισχύει $N_K(P) \leq M_K$. Επειδή δε $N_K(P) = p^f$, $p \in \mathbb{P}$, $f \in \mathbb{N}$, όλα τα πρώτα ιδεώδη που εμφανίζονται στην ανάλυση του A είναι αυτά των οποίων οι πρώτοι αριθμοί p με $A \cap \mathbb{Z} = p\mathbb{Z}$, για τους οποίους ισχύει $p \leq M_K$.

Συνεπώς, αν πάρουμε όλους τους πρώτους αριθμούς $p \leq M_K$ υπολογίζουμε τις αναλύσεις των ιδεωδών $\langle p \rangle = pR_K$ σε γινόμενο πρώτων ιδεωδών στον δακτύλιος R_K και σχηματίζουμε όλα τα δυνατά γινόμενα πρώτων ιδεωδών τα οποία ορίζουν ιδεώδη με norm $\leq M_K$, τότε είμαστε εξασφαλισμένοι ότι έχουμε τουλάχιστον έναν αντιπρόσωπο από κάθε κλάση. Με βάση τα παρακάτω καταλήγουμε στον ακόλουθο:

Αλγόριθμο

- Θεωρούμε το αλγεβρικό σώμα αριθμών $K = \mathbb{Q}(\theta)$
- Υπολογίζουμε τον βαθμό της επέκτασης $[K : \mathbb{Q}] = n$
- Υπολογίζουμε την ταυτότητα $[r_1, r_2]$ του K
- Υπολογίζουμε τη διακρίνουσα D_K του σώματος K
- Υπολογίζουμε τη σταθερά Minkowski

$$M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_K|^{1/2}.$$

- Θεωρούμε όλους τους πρώτους αριθμούς p με $p \le M_K$
- Για κάθε $p \in \mathbb{P}$, $p \le M_K$ παραγοντοποιούμε τα πρώτα ιδεώδη $\langle p \rangle$ στον R_K
- Υπολογίζουμε όλα τα γινόμενα πρώτων ιδεωδών του προηγούμενου βήματος για τα οποία η norm είναι $\le M_K$
- Καθορίζουμε όλους τους γεννήτορες των κλάσεων ιδεωδών στις οποίες ανήκουν τα ιδεώδη του προηγούμενου βήματος.

Παράδειγμα V.3.4. Έστω το σώμα $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{2}$. Ο δακτύλιος των ακεραίων αλγεβρικών είναι ο $\mathbb{Z}[\sqrt[3]{2}]$. Προφανώς το ανάγωγο $f(x) = \mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q})$ δίνεται από

$$f(x) = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}),$$

και $[K : \mathbb{Q}] = 3$ και $r_1 = r_2 = 1$. Η διακρίνουσα του σώματος K είναι $D_K = -2^2 \cdot 3^3$ και $n = 3$, δείτε το παράδειγμα IV.6.4.

Η σταθερά Minkowski είναι

$$M_k = \left(\frac{4}{\pi}\right)\frac{3!}{3^3}\sqrt{|D_K|} = \frac{4}{\pi}\frac{6}{3^3} \cdot 2 \cdot 3\sqrt{3} \sim 2,94.$$

Από το θεώρημα V.3.1 έπεται ότι για κάθε κλάση ιδεωδών $\mathfrak{k} \in \mathfrak{K}_R = I_R/H_R$ υπάρχει ένα ακέραιο ιδεώδες $A \in \mathfrak{k}$ με $N_K(A) < 3$. Η μόνη δυνατότητα που έχουμε είναι $N_K(A) = 2$. Προφανώς $N_K(A)$ είναι πρώτος αριθμός, άρα το A είναι πρώτο ιδεώδες, $A = P$.

Αν $N_K(P) = 2$, τότε $2 \in P$ και συνεπώς $P \mid 2R_K$. Με τη βοήθεια του νόμου ανάλυσης I.3.11 που θα αποδειχθεί στο επόμενο κεφάλαιο VI.5.9 έχουμε

$$x^3 - 2 \equiv x^3 \mod 2$$

συνεπώς $2R_K = (\theta R_K)^3$, όπου θR_K πρώτο ιδεώδες με norm $(\theta R_K) = 2$. Άρα $P = \omega R_K$ κύριο ιδεώδες και $h_K = 1$.

Αφού η τάξη της ομάδας $\mathfrak{K}_{R_K} = I_{R_K}/H_{R_K}$ είναι πεπερασμένη, $h_K < \infty$, για κάθε κλάση $\mathfrak{k} \in \mathfrak{K}_{R_K}$ και $\mathfrak{k}^{h_K} = H_{R_K}$. Αν $A \in \mathfrak{k}$, τότε $A^{h_K} \in \mathfrak{k}^{h_K} = H_R$. Συνεπώς, το ιδεώδες A^{h_k} είναι κύριο ιδεώδες.

V.4 Επίλυση της διοφαντικής εξίσωσης $2y^3 = x^2 + 5$

Ξαναμελετούμε την εξίσωση $2y^3 = x^2 + 5$ που λύσαμε, εν γνώσει μας, με λανθασμένο τρόπο, στην εισαγωγή. Θα αποδείξουμε ότι $(x, y) = (\pm 7, 3)$ είναι οι μοναδικές της λύσεις.

Υποθέτουμε ότι (x, y) είναι μια λύση αυτής

$$2y^3 = x^2 + 5.$$

Παραγοντοποιούμε το δεξιό μέλος στην ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$

$$2y^3 = (x + \sqrt{-5})(x - \sqrt{-5}).$$

Το $-5 \equiv 3 \mod 4$. Επομένως ο $\mathbb{Z}[\sqrt{-5}]$ είναι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του σώματος $K = \mathbb{Q}(\sqrt{-5})$. Επομένως ο $\mathbb{Z}[\sqrt{-5}]$ είναι περιοχή του Dedekind, δηλαδή έχουμε μονοσήμαντη ανάλυση σε γινόμενο πρώτων ιδεωδών. Η διακρίνουσα του σώματος είναι $D_K = -20$. Επομένως για $p = 2$ το σύμβολο του Kronecker $\left(\frac{-20}{2}\right) = 0$. Συνεπώς, $\langle 2 \rangle = 2\mathbb{Z}[\sqrt{-5}] = P_2^2$, P_2 πρώτο ιδεώδες.

Επίσης $\left(\frac{-20}{5}\right) = 0$, άρα και το $\langle 5 \rangle = 5\mathbb{Z}[\sqrt{-5}] = P_5^2$, όπου P_5 πρώτο ιδεώδες. Από τον νόμο ανάλυσης των Kummer-Dedekind το $f(x) = x^2 - 5$ και στον δακτύλιο $\mathbb{F}_2[x]$ έχουμε

$$\bar{f}[x] = x^2 - 1 \equiv (x + 1)^2 \mod 2.$$

Επομένως $P_2 = \langle 2, 1+\sqrt{-5}\rangle$. Ομοίως $\bar{f}(x) \equiv x^2 \mod 5$. Άρα $P_5 = \langle 5, \sqrt{-5}\rangle = \langle \sqrt{-5}\rangle$. Μπορούμε να εφαρμόσουμε τον αλγόριθμο και να αποδείξουμε ότι ο αριθμός κλάσεων ιδεωδών του $K = \mathbb{Q}(\sqrt{-5})$ είναι $h_K = 2$. Πράγματι, αν $K = \mathbb{Q}(\sqrt{-5})$, τότε ο δακτύλιος των ακεραίων $\mathbb{Z}(\sqrt{-5})$ δεν έχει μοναδική πραγματοποίηση και συνεπώς $h_K > 1$. Η διακρίνουσα $D_K = -20$ συνεπώς η σταθερά του Minkowski είναι

$$\left(\frac{2}{\pi}\right)\sqrt{|D_K|} = \frac{2\sqrt{20}}{\pi} < 2.85$$

Κάθε ιδεώδες είναι ισοδύναμο με ιδεώδες που να έχει norm μικρότερο της σταθεράς του Minkowski. Ένα ιδεώδες με norm 1 είναι όλος ο δακτύλιος. Ένα ιδεώδες A με norm 2 θα είναι ένας διαιρέτης του $2R_K$. Παρατηρούμε ότι $2R_K = P_2^2$ και έχει τάξη 2 στην ομάδα κλάσεων.

Ο μέγιστος κοινός διαιρέτης των ιδεωδών$\langle x+\sqrt{-5}\rangle$ και $\langle x-\sqrt{-5}\rangle$ είναι το ιδεώδες P_2. Πράγματι, αν

$$A = \langle x+\sqrt{-5}\rangle R_K + \langle x-\sqrt{-5}\rangle R_K,$$

τότε $2\sqrt{-5} \in A$ άρα $\langle 2\rangle\langle\sqrt{-5}\rangle \subset A$ οπότε $A \mid \langle 2\rangle\langle\sqrt{-5}\rangle = P_2^2P_5^2$. Αλλά $P_5 \nmid A$ καθώς και $P_2^2 \nmid A$, $A \neq R_K$. Συνεπώς $A = P_2$.

Επομένως η σχέση των ιδεωδών γράφεται

$$P_2^2\langle y\rangle^3 = (P_2B)(P_2\overline{B}),$$

όπου $B, \overline{B}$ ιδεώδη του R_K πρώτα μεταξύ τους. Από τη σχέση

$$\langle y\rangle^3 = B\overline{B},$$

επειδή ο R_K είναι δακτύλιος Dedekind, προκύπτει ότι υπάρχει ακέραιο ιδεώδες C του R, ώστε

$$B = C^3, \overline{B} = \overline{C}^3.$$

Το ιδεώδες

$$\langle 2\rangle\langle x+\sqrt{-5}\rangle = P_2^2P_2B = (P_2C)^3$$

είναι κύριο ιδεώδες του R_K. Συνεπώς, υπάρχει $\alpha \in R_K = \mathbb{Z}[\sqrt{-5}]$ για το οποίο ισχύει ότι

$$\langle 2\rangle(x+\sqrt{-5}) = \langle\alpha\rangle^3$$

δηλαδή

$$2(x+\sqrt{-5}) = \epsilon\alpha^3, \epsilon \in E(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}.$$

Τελικά

$$2(x+\sqrt{-5}) = \beta^3, \beta = a+b\sqrt{-5}, a, b \in \mathbb{Z}.$$

Επομένως έχουμε

$$2(x+\sqrt{-5}) = a(a^2-15b^2) + b(3a^2+5b^2)\sqrt{-5}.$$

Συνεπώς,

$$2x = a(a^2-15b^2), 2 = b(3a^2-5b^2).$$

Άρα $b \mid 2$, δηλαδή $b = \pm 1, \pm 2$. Από τις δυνατές τιμές του b μόνο η τιμή δηλαδή $b = -1$ δίνει ακέραιο $a = \pm 1$, και τελικά $x_0 = \pm 7$, $y_0 = 3$. Αυτές είναι και οι μοναδικές λύσεις της διοφαντικής εξίσωσης.

Σημείωση V.4.1. Εντελώς ανάλογα αποδεικνύεται ότι η εξίσωση του Fermat

$$x^p + y^p = z^p, p \text{ πρώτος } \neq 2$$

δεν έχει μη τετριμμένη λύση στην περίπτωση που το p είναι regular prime, δηλαδή στην περίπτωση που $p \nmid h_{\mathbb{Q}(\zeta_p)}$. Αυτό θα το εξετάσουμε αναλυτικά στο κεφάλαιο XI.

V.5 Ασκήσεις

1. Έστω K αλγεβρικό σώμα αριθμών R_K ο δακτύλιος των ακεραίων αλγεβρικών αυτού και P πρώτο ιδεώδες του R_K. Να αποδειχθεί ότι για κάθε $x \in R_K$ ισχύει:

$$x^{N_K(P)} \equiv x \mod P.$$

Επίσης να αποδειχθεί ότι η norm $N_K(P)$ είναι ο ελάχιστος φυσικός n για τον οποίο ισχύει

$$x^n \equiv x \mod P$$

για κάθε $x \in R_K$.

2. Για κάθε ιδεώδες A του R_K συμβολίζουμε το πλήθος των αντιστρέψιμων στοιχείων του δακτυλίου R/A με $\phi(A)$. Να αποδειχθεί ότι αν A, B δύο ιδεώδη του του R_K πρώτα μεταξύ τους

$$\phi(AB) = \phi(A)\phi(B).$$

Στη συνέχεια να αποδειχθεί ότι

$$\phi(A) = N_{K/\mathbb{Q}}(A) \prod_{\substack{P \in \mathrm{Spec} A \\ P|A}} \left(1 - N_{K/\mathbb{Q}}(P)^{-1}\right).$$

Τέλος να αποδειχθεί ότι για κάθε $x \in R_K$ για το οποίο το ιδεώδες xR_K είναι πρώτο προς το A ισχύει

$$x^{\phi(A)} \equiv x \mod A.$$

3. Έστω L αλγεβρικό σώμα αριθμών το οποίο περιέχει την Galois θήκη της επέκτασης $K/\mathbb{Q}$. Έστω $A \lhd R_K$ ιδεώδες. Αν το σ διατρέχει όλες τις εμφυτεύσεις του K στο $\mathbb{C}$ να αποδειχθεί ότι

$$\prod_\sigma \sigma(A) R_L = N_{K/\mathbb{Q}}(A) R_L.$$

4. Έστω K αλγεβρικό σώμα αριθμών και $A \lhd R_K$ ιδεώδες. Να αποδειχθεί ότι υπάρχει επέκταση L/K στην οποία το ιδεώδες AR_L να είναι κύριο ιδεώδες.

5. Να λυθεί η διοφαντική εξίσωση

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

6. Έστω d ακέραιος ελεύθερος τετραγώνου $d < 0$ και $d \equiv 2, 3 \mod 4$. Έστω h_K ο αριθμός κλάσεων του σώματος $K = \mathbb{Q}(\sqrt{d})$. Υποθέτουμε ότι $3 \nmid h_K$. Να αποδειχθεί ότι οι ακέραιες λύσεις της διοφαντικής εξίσωσης

$$y^2 = x^3 + d$$

είναι ακριβώς τα ζευγάρια $(x, y) = (A^2 - d, A(A^2 + 3d))$, όπου το A διατρέχει όλους τους ακεραίους για τους οποίους ισχύει $3A^2 \pm 1 = -d$.

7. Να λυθεί η διοφαντική εξίσωση

$$y^2 = x^3 + 13.$$

8. Να υπολογιστεί ο αριθμός κλάσεων του σώματος $K = \mathbb{Q}(\sqrt{-13})$ και στη συνέχεια να λυθεί η διοφαντική εξίσωση

$$2y^3 = x^2 + 73.$$

9. Να αποδειχθεί ότι το πλήθος των ακέραιων ιδεωδών που διαιρούν κάποιο ακέραιο ιδεώδες ενός αλγεβρικού σώματος αριθμών είναι πεπερασμένο.

10. Να αποδειχθεί ότι κάθε φυσικός αριθμός ανήκει σε πεπερασμένο πλήθος ακέραιων ιδεωδών ενός αλγεβρικού σώματος αριθμών.

11. Να αποδειχθεί ότι το πλήθος των ακεραίων ιδεωδών ενός αλγεβρικού σώματος αριθμών με δοσμένη norm είναι πεπερασμένο.

12. Αν υπάρχει στοιχείο $\alpha \in A$ ενός ακεραίου ιδεώδους αλγεβρικού σώματος αριθμών K, ώστε
$$|N_{K/\mathbb{Q}}(\alpha)| = N_K(A),$$
τότε να αποδειχθεί ότι ισχύει $A = \langle \alpha \rangle$.

13. Έστω K αλγεβρικό σώμα αριθμών. Να αποδείξετε ότι υπάρχει πεπερασμένη επέκταση αλγεβρικών σωμάτων αριθμών L/K με την ιδιότητα ότι όλα τα ιδεώδη AR_L να είναι κύρια ιδεώδη για κάθε ακέραιο ιδεώδες A του K.

14. Να υπολογίσετε τον αριθμό κλάσεων ιδεωδών του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{6})$.

15. Να υπολογίστε τον αριθμό κλάσεων ιδεωδών του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt[3]{3})$.

16. Να υπολογίστε τον αριθμό κλάσεων ιδεωδών του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{-6})$.

17. Να υπολογίστε τον αριθμό κλάσεων ιδεωδών του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\theta)$, όπου θ ρίζα του πολυωνύμου $x^5 - x^3 + 1$.

18. Να υπολογιστεί η αλγεβρική δομή της ομάδας κλάσεων ιδεωδών του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{-14})$.

19. Να υπολογιστεί η αλγεβρική δομή της ομάδας κλάσεων ιδεωδών του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{-26})$.

20. Να υπολογιστεί η αλγεβρική δομή της ομάδας κλάσεων ιδεωδών του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{-65})$.

21. Έστω k ακέραιος ώστε $k < -1$, k ελεύθερος τετραγώνου, $k \equiv 2, 3 \mod 4$ και $3 \nmid h_{\mathbb{Q}(\sqrt{k})}$. Αν υπάρχει ένας ακέραιος a, $k = 1 - 3a^2$, τότε οι μοναδικές λύσεις της διοφαντικής εξίσωσης $y^2 = x^3 + k$ είναι οι $x = 4a^2 - 1$, $y = \pm(3a - 8a^2)$.

Βιβλιογραφία

[1] Alaca, Ş. & Williams, K. S. *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, 2004, pp. xviii+428. ISBN: 0-521; 0-521-54011-9.

[2] Janusz, G. J. *Algebraic Number Fields*. 2nd edition. Vol. 7. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 1996, pp. x+276. ISBN: 0-8218-0429-4.

[3] Marcus, D. A. *Algebraic Number Fields*. Universitext. 2nd edition of [MR0457396], With a foreword by Barry Mazur. Springer, 2018, pp. xviii+203. ISBN: 978-3-319-90232-6; 978-3-319-90233-3.

[4] Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*. 3rd edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004, pp. xii+708. ISBN: 3-540-21902-1.

[5] Pollack, P. *A Conversational Introduction to Algebraic Number Theory, Arithmetic beyond* $\mathbb{Z}$. Vol. 84. Student Mathematical Library. American Mathematical Society, Providence, RI, 2017, pp. ix + 316. ISBN: 978-1-4704-3653-7.

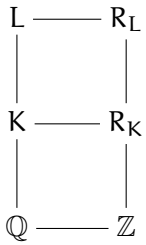
[6] Stewart, I. & Tall, D. *Algebraic Number Theory and Fermat's Last Theorem*. 4th edition. CRC Press, Boca Raton, FL, 2016, pp. xix+322. ISBN: 978-1-4987-3839-2.

VI

Νόμος ανάλυσης

VI.1 Εισαγωγή

Στο κεφάλαιο αυτό θα μελετήσουμε τον *νόμο ανάλυσης* στις σχετικές επεκτάσεις αλγεβρικών σωμάτων αριθμών L/K, όπου το K δεν είναι κατ' ανάγκη το σώμα των ρητών $\mathbb{Q}$. Έχουμε το ακόλουθο σχήμα:



Είναι γνωστό ότι, θεώρημα III.3.6, ο R_L είναι η ακεραία θήκη του R_K στο L και είναι δακτύλιος Dedekind. Αν $[K : Q] = n$, αποδείξαμε ότι ο R_K είναι ελεύθερο $\mathbb{Z}$-module βαθμού n, θεώρημα IV.4.2.

Τώρα ο R_L είναι και ένα R_K-module. Αφού και ο R_L είναι πεπερασμένα παραγόμενο $\mathbb{Z}$-module, έπεται ότι και ο R_L είναι ένα πεπερασμένα παραγόμενο R_K-module,

$$R_L = R_K\alpha_1 + R_K\alpha_2 + \cdots + R_K\alpha_r.$$

Επίσης είναι και *ελεύθερο στρέψεως* R_K-module, αφού είναι ελεύθερο στρέψεως ως $\mathbb{Z}$-module. Όμως ο R_K είναι δακτύλιος Dedekind, όχι πάντοτε περιοχή κυρίων ιδεωδών, και συνεπώς δεν μπορούμε να συμπεράνουμε ότι ο R_L είναι ελεύθερο R_K-module.

Για παράδειγμα κάθε κλασματικό ιδεώδες, ενός αλγεβρικού σώματος αριθμών K, είναι πεπερασμένα παραγόμενο αλλά είναι ελεύθερο ακριβώς τότε όταν το ιδεώδες είναι κύριο.

Επίσης η επέκταση $\mathbb{Q}(\sqrt{-14}, \sqrt{-7})/\mathbb{Q}(\sqrt{-14})$ δεν έχει βάση ακεραιότητας [8]. Ενώ η επέκταση $\mathbb{Q}(\sqrt{-14}, \sqrt{-7})/\mathbb{Q}(\sqrt{2})$ έχει βάση ακεραιότητας, αφού ο δακτύλιος των ακεραίων αλγεβρικών είναι ο $\mathbb{Z}[\sqrt{2}]$ και ως γνωστό είναι περιοχή κυρίων ιδεωδών. Βέβαια είναι δυνατόν ο R_L να είναι ελεύθερο R_K-module και σε περιπτώσεις που ο R_K δεν είναι κατ'ανάγκη περιοχή κυρίων ιδεωδών. Για παράδειγμα αν $K = \mathbb{Q}(\sqrt{-15})$ και $L = K(\sqrt{26}) = \mathbb{Q}(\sqrt{-15}, \sqrt{26})$ μπορεί να αποδειχθεί ότι το $R_L = R_K \oplus R_K\sqrt{26}$. Ο αριθμός κλάσεων του K είναι 2.

Τι γνωρίζουμε για τα πεπερασμένα παραγώμενα R-modules, όταν ο R είναι δακτύλιος του Dedekind;

Θεώρημα VI.1.1. *Έστω* R *δακτύλιος του Dedekind και* K *το σώμα πηλίκων αυτού.*

1. *Κάθε πεπερασμένα παραγόμενο και ελεύθερο στρέψης* R*-module* M *είναι ισόμορφο προς το ευθύ άθροισμα κλασματικών ιδεωδών του* K

$$M \cong A_1 \oplus A_2 \oplus \cdots \oplus A_m.$$

2. *Δύο πεπερασμένα παραγόμενα και ελεύθερα στρέψεως* R*-modules*

$$M \cong A_1 \oplus A_2 \oplus \cdots \oplus A_m \text{ και } N \cong B_1 \oplus B_2 \oplus \cdots \oplus B_n$$

είναι ισόμορφα τότε και μόνο τότε όταν $m = n$ *και* $\prod_{i=1}^{m} A_i \cong \prod_{i=1}^{m} B_i$ *modulo κύρια ιδεώδη.*

Επομένως

$$M \cong A_1 \oplus A_2 \oplus \cdots \oplus A_m \cong R \oplus R \oplus \cdots \oplus A_1 A_2 \cdots A_m.$$

Ορισμός VI.1.2. Έστω R-ακεραία περιοχή και M ένα R-module. Ο βαθμός του M ορίζεται ως η διάσταση του $K \otimes_R M$ ως K-διανυσματικός χώρος, όπου K το σώμα κλασμάτων του R.

Επομένως ο βαθμός του παραπάνω M είναι το m.

Παρατήρηση VI.1.3. Με βάση όλα τα παραπάνω προκύπτει ότι το σύνολο όλων των κλάσεων ισομορφίας πεπερασμένα παραγόμενων R-modules βαθμού ένα ταυτίζεται με την ομάδα κλάσεων του R.

Το αντίστοιχο του Elementarteilersatz για δακτυλίους Dedekind είναι το εξής:

Θεώρημα VI.1.4. *Έστω* R *μια περιοχή Dedekind και* M, N *πεπερασμένα παραγόμενα ελεύθερα στρέψεως* R*-modules με* $N \subset M$ *και* M, N *έχουν τον ίδιο βαθμό* m*. Υπάρχουν στοιχεία* $\alpha_1, \alpha_2, \ldots, \alpha_m \in M$ *και κλασματικά ιδεώδη* $A_1, A_2, \ldots, A_m$ *καθώς και ακέραια ιδεώδη* $B_1 \supset B_2 \supset \cdots \supset B_m$ *της* R *ώστε*

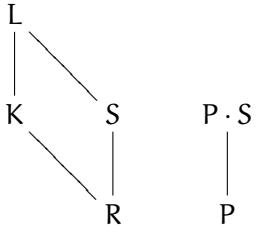
$$M = A_1\alpha_1 \oplus A_2\alpha_2 \oplus \cdots \oplus A_m\alpha_m, \qquad N = A_1B_1\alpha_1 \oplus A_2B_2\alpha_2 \oplus \cdots \oplus A_mB_m\alpha_m.$$

Τα ακέραια ιδεώδη $B_1, B_2, \ldots, B_m$ *ορίζονται μονοσήμαντα από το ζευγάρι των* R*-modules* $N \subset M$ *και λέγονται οι αναλλοίωτοι παράγοντες (invariant factors) του* N *στο* M.

[1], [10], [6], [11], [4].

VI.2 Νόμος ανάλυσης - το πρώτο θεώρημα

Στα επόμενα θα κρατήσουμε σταθερό τον παρακάτω συμβολισμό: K, L, M θα είναι αλγεβρικά σώματα αριθμών με $K \subset L \subset M$. Θα συμβολίζουμε τους αντίστοιχους δακτυλίους του Dedekind με $R \subset S \subset T$. Με P θα συμβολίζουμε ένα πρώτο ιδεώδες του R με Q ένα πρώτο ιδεώδες του S και U ένα πρώτο ιδεώδες του T. Θεωρούμε



Το γινόμενο PS είναι ένα ιδεώδες του S όχι κατ' ανάγκη πρώτο. Αφού ο S είναι δακτύλιος του Dedekind έχουμε μονοσήμαντη ανάλυση:

$$PS = Q_1^{e_1} \cdots Q_r^{e_r},$$

όπου $Q_1, \ldots, Q_r$ είναι πρώτα ιδεώδη του S

Πρόβλημα: Ποια ιδεώδη υπεισέρχονται στην ανάλυση του PS και με ποιους εκθέτες;

Πρόταση VI.2.1. *Ισχύουν οι ισοδύναμες μεταξύ τους παρακάτω προτάσεις:*

1. $Q \mid PS$ *δηλαδή υπάρχει ακέραιο ιδεώδες* Q' *του* S *ώστε* $PS = QQ'$.
2. $Q \supset PS$
3. $Q \supset P$
4. $Q \cap R = P$
5. $Q \cap K = P$

Απόδειξη. Προφανώς η πρώτη σχέση είναι ισοδύναμη με τη δεύτερη. Το ότι από τη δεύτερη έπεται η τρίτη είναι επίσης προφανές, αφού το P είναι ιδεώδες. Για να δείξουμε ότι η τρίτη συνεπάγεται την τέταρτη παρατηρούμε ότι $Q \supset P, R \supset P$ συνεπώς $Q \cap R \supset P$. Από την άλλη το $Q \cap R$ είναι ιδεώδες του R και μάλιστα διαφορετικό του R, γιατί διαφορετικά $1 \in Q$. Αφού P είναι μέγιστο, έχουμε $Q \cap R = P$.

Για να δείξουμε ότι η τέταρτη συνεπάγεται την πέμπτη παρατηρούμε ότι

$$Q \cap K = (Q \cap S) \cap K = Q \cap (S \cap K) = Q \cap R.$$

Τέλος για να δείξουμε ότι η πέμπτη συνεπάγεται τη δεύτερη παρατηρούμε ότι

$$Q \cap K = P \text{ συνεπώς } Q \supset P \text{ και } PS \subset Q.$$

□

Ορισμός VI.2.2. Αν ισχύει μία από τις παραπάνω σχέσεις (και συνεπώς και οι πέντε), τότε θα λέμε ότι ο Q *βρίσκεται πάνω από το* P και ότι το P *βρίσκεται κάτω από το* Q.

Πρόταση VI.2.3. *Έστω* P *πρώτο ιδεώδες του* K *και*

$$PS = Q_1^{e_1} \cdots Q_r^{e^r}$$

η ανάλυση του PS *σε γινόμενο πρώτων ιδεωδών του* S. *Τα πρώτα ιδεώδη* $Q_1, \ldots, Q_r$ *και μόνον αυτά βρίσκονται πάνω από το* P *στην επέκταση* L/K.

Απόδειξη. Έστω Q ένα πρώτο ιδεώδες του S πάνω από το P, συνεπώς $Q \supset PS = Q_1^{e_1} \cdots Q_r^{e_r}$, άρα υπάρχει $i = 1, \ldots, r$ ώστε $Q \mid Q_i$ συνεπώς $Q_i \subset Q$ και αφού Q_i μέγιστο $Q = Q_i$.

Επίσης αν $Q = Q_i$, τότε

$$Q \supset \prod_{i=1}^{r} Q_i^{e_i} = PS \supset P.$$

□

VI.3 Δείκτης διακλάδωσης, βαθμός αδρανείας και το πρώτο θεώρημα ανάλυσης

Ορισμός VI.3.1. Ο εκθέτης $e = e(Q/P)$ με τον οποίο εμφανίζεται το Q στην ανάλυση του PS σε γινόμενο πρώτων παραγόντων λέγεται *δείκτης διακλάδωσης* του Q υπεράνω του P. Θα λέμε ότι το Q *διακλαδίζεται* υπέρ το P αν και μόνο αν $e(Q/P) > 1$. Θα λέμε ότι το P διακλαδίζεται υπέρ το L αν υπάρχει πρώτος Q του S με $e(Q/P) > 1$.

Ο παραπάνω ορισμός έχει νόημα γιατί λόγω της πρότασης VI.2.1 υπάρχει ακριβώς ένα P που βρίσκεται κάτω από το Q.

Έστω τώρα ότι το Q βρίσκεται πάνω από το P. Θεωρούμε τη συνάρτηση

$$i : R/P \ni r + P \mapsto r + Q \in S/Q$$

η οποία είναι προφανώς μονομορφισμός σωμάτων. Πράγματι, αν $i(r_1 + P) = i(r_2 + P)$, τότε $r_1 + Q = r_2 + Q$ συνεπώς $r_1 - r_2 \in Q$. Άρα $r_1 - r_2 \in R \cap Q = P$, δηλαδή $r_1 + P = r_2 + P$.

Ταυτίζουμε λοιπόν τα σώματα R/P και $i(R/P) = (R + Q)/Q$, δηλαδή θεωρούμε το R/P ως υπόσωμα του S/Q.

Ορισμός VI.3.2. Έστω ότι Q βρίσκεται πάνω από το P. Τότε ο ακέραιος

$$f(Q/P) = [S/Q : R/P]$$

λέγεται *βαθμός αδρανείας* του Q υπέρ το P.

Πρόταση VI.3.3. *Αν ο Q βρίσκεται πάνω από το P, τότε ισχύει*

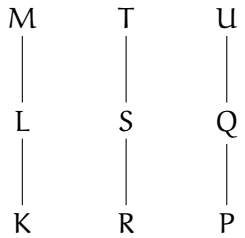
$$N_{L/\mathbb{Q}}(Q) = N_{K/\mathbb{Q}}(P)^{f(Q/P)}.$$

Απόδειξη. Ισχύει

$$N_{L/\mathbb{Q}}(Q) = \#S/Q \text{ και } N_{K/\mathbb{Q}}(P) = \#R/P$$

Το θεώρημα είναι απλή συνέπεια του ότι αν $F \subset F'$ είναι δύο πεπερασμένα σώματα και $[F' : F] = n$, τότε $\#F' = \#(F^n)$. □

Κατ' ευθείαν από τον ορισμό του δείκτη διακλαδώσεως και του βαθμού αδρανείας βγαίνει το συμπέρασμα ότι για τα διαδοχικά σώματα ισχύει



ισχύει

$$\begin{aligned} e(U/P) &= e(U/Q)e(Q/P) \\ f(U/P) &= f(U/Q)f(U/P). \end{aligned}$$

Θεώρημα VI.3.4 (Πρώτο θεώρημα ανάλυσης)**.** *Έστω $[L : K] = n$. Τότε ισχύει*

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_r f_r = \sum_{Q \supset P} e(Q/P) f(Q/P).$$

Απόδειξη. Έχουμε ότι

$$PS = Q_1^{e_1} \cdots Q_r^{e_r},$$

συνεπώς

$$N_{L/\mathbb{Q}}(PS) = N_{L/\mathbb{Q}}(Q_1)^{e_1} \cdots N_{L/\mathbb{Q}}(Q_r)^{e_r} = N_{K/\mathbb{Q}}(P)^{e_1 f_1 + \cdots + e_r f_r}.$$

Ισχυριζόμαστε ότι

$$N_{L/\mathbb{Q}}(PS) = N_{K/\mathbb{Q}}(P)^n$$

από το οποίο καταλήγουμε άμεσα στο ζητούμενο αφού

$$N_{K/\mathbb{Q}}(P) = \#R/P \geq 2,$$

οπότε οι εκθέτες θα είναι ίσοι.

Πράγματι γνωρίζουμε ότι $h_K < \infty$ συνεπώς $P^{h_K} = \lambda R$, $\lambda \in R$ συνεπώς $P^{h_K} S = \lambda S$ άρα

$$N_{L/\mathbb{Q}}(P^{h_K} S) = N_{L/\mathbb{Q}}(\lambda S) = |N_{L/\mathbb{Q}}(\lambda)|$$

$$= |N_{K/\mathbb{Q}}\left(N_{L/K}(\lambda)\right)| = |N_{K/\mathbb{Q}}(\lambda^n)| = |N_{K/\mathbb{Q}}(\lambda)|^n.$$

Δηλαδή

$$N_{L/\mathbb{Q}}(P^{h_K} S) = |N_{K/\mathbb{Q}}(\lambda)|^n = N_{K/\mathbb{Q}}(P)^{h_K n}$$

και τελικά

$$N_{L/\mathbb{Q}}(PS) = N_{K/\mathbb{Q}}(P)^n.$$

□

Εφαρμογή: $K = \mathbb{Q}$, $[L : Q] = 2$, p πρώτος αριθμός. Τότε $P = p\mathbb{Z}$ πρώτο ιδεώδες $\neq 0$ στο $\mathbb{Z} = R$. Τότε

$$PS = \begin{cases} Q, & f(Q/P) = 2, e(Q/P) = 1 \\ Q_1 Q_2 & f(Q_i/P) = 1, e(Q_i/P) = 1 \\ Q^2 & f(Q/P) = 1, e(Q/P) = 1 \end{cases}$$

VI.4 Νόμος ανάλυσης σε επεκτάσεις Galois

Έστω τώρα σ ένας K-αυτομορφισμός του σώματος L και Q πρώτο ιδεώδες του S που βρίσκεται πάνω από το πρώτο ιδεώδες P του R, τότε ισχύουν:

1. Το $\sigma(Q)$ είναι πρώτο ιδεώδες του S.
2. Το $\sigma(Q) \supset P$
3. $f(Q/P) = f(\sigma(Q)/P)$
4. $e(Q/P) = e(\sigma(Q)/P)$

Απόδειξη. Παρατηρούμε ότι το δεύτερο είναι προφανές, αφού $Q \supset P$ δίνει ότι $\sigma(Q) \supset \sigma(P) = P$.

Για το πρώτο: Ισχύει ότι $\sigma(S) = S$. Πράγματι $\sigma(s)$ είναι ακέραιο υπεράνω του R για κάθε $s \in S$, δηλαδή $\sigma(S) \subset S$. Επειδή η σ^{-1} είναι επίσης K-αυτομορφισμός του σώματος L οπότε $\sigma^{-1}(S) \subset S$ από όπου προκύπτει ότι $S \subset \sigma S$. Τώρα το $\sigma(Q)$ είναι προφανώς ιδεώδες του $\sigma(S) = S$, δηλαδή ισχύει η ισότητα. Επίσης είναι πρώτο ιδεώδες του S, διότι η συνάρτηση

$$\widehat{\sigma} : S/Q \to \sigma(S)/\sigma(Q) = S/\sigma(Q)$$

είναι ισομορφισμός και S/Q είναι ακέραια περιοχή.

Για το τρίτο: Τα πηλίκα S/Q και $S/\sigma(Q)$ είναι R/P-διανυσματικοί χώροι οι οποίοι είναι ισόμορφοι, άρα έχουν την ίδια διάσταση:

$$\dim_{R/P} S/Q = \dim_{R/P} S/\sigma(Q).$$

Συνεπώς

$$f(Q/P) = [S/Q : R/P] = [S/\sigma(Q) : R/P] = f(\sigma(Q)/P).$$

Τέλος για το τέταρτο έχουμε

$$PS = Q_1^{e_1} \cdots Q_r^{e^r} = \sigma(PS) = \sigma(Q_1)^{e_1} \cdots \sigma(Q_r)^{e_r}$$

και το ζητούμενο προκύπτει λόγω μοναδικής ανάλυσης σε γινόμενο πρώτων ιδεωδών. □

Θεώρημα VI.4.1. *Υποθέτουμε ότι η επέκταση* L/K *είναι επέκταση του Galois και έστω* $G = \mathrm{Gal}(L/K)$ *είναι η ομάδα Galois της επέκτασης αυτής. Αν*

$$PS = Q_1^{e_1} \cdots Q_r^{e_r}$$

η ανάλυση του PS *στον* S*, τότε η ομάδα* G *δρα μεταβατικά στο σύνολο* $\{Q_1, \ldots, Q_r\}$*, δηλαδή για κάθε ζευγάρι* Q_i, Q_j *υπάρχει* $\sigma \in G$ *ώστε* $\sigma(Q_i) = Q_j$.

Απόδειξη. Έστω ότι υπάρχει ένα Q_j ώστε $Q_j \notin \{\sigma(Q_i) : \sigma \in G\}$. Θεωρούμε το σύστημα:

$$\begin{aligned} x &\equiv 0 \mod Q_j \\ x &\equiv 1 \mod \sigma(Q_i) : \text{ για κάθε } \sigma \in G \end{aligned} \tag{VI.1}$$

και από την παραπάνω υπόθεση συμπεραίνουμε ότι για κάθε $\sigma \in G$ τα $Q_j, \sigma(Q_i)$ είναι πρώτα μεταξύ τους, οπότε από το θεώρημα υπολοίπων του Κινέζου έπεται ότι υπάρχει $s \in S$ λύση του συστήματος (VI.1). Επομένως

$$N_{L/K}(s) = \prod_{\sigma \in G} \sigma(s) \in K \cap S = R.$$

Ακόμη $s \in Q_j$ συνεπώς $N_{L/K}(s) \in Q_j$ και αφού $N_{L/K}(s) \in K$, έχουμε $N_{L/K}(s) \in Q_j \cap K = P$. Όμως $s \notin \sigma(Q_i)$ για κάθε $\sigma \in G$ συνεπώς $\sigma(s) \notin Q_i$ για κάθε $\sigma \in G$ δηλαδή $N_{L/K}(s) \notin Q_i \cap K = P$, άτοπο.

Πόρισμα VI.4.2. *Αν* L/K *επέκταση του Galois, τότε για κάθε πρώτο ιδεώδες* P *του* R *έχουμε την ανάλυση:*

$$PS = (Q_1 \cdots Q_r)^e$$

όπου $e = e(Q_i/P)$ *και* $f = f(Q_i/P)$ *για* $i = 1, \ldots, r$*. Επιπλέον* $n = efr$.

□

VI.5 Το δεύτερο θεμελιώδες θεώρημα ανάλυσης

Αυτό που λείπει από το πρώτο θεώρημα ανάλυσης είναι ότι δεν γνωρίζουμε ποια είναι τα ιδεώδη που εμφανίζονται στην ανάλυση του ιδεώδους PS.

Θα επιθυμούσαμε να έχουμε γεννήτορες των πρώτων ιδεωδών και φυσικά και τη (σχετική) norm της επέκτασης L/K την οποία θα ορίσουμε.

Έστω $\theta \in S$, $L = K(\theta)$, Όπως θα δούμε παρακάτω αν $S = R[\theta]$, τότε μπορούμε να δώσουμε απάντηση για όλα τα ιδεώδη του R. Όμως, όπως είδαμε στο παράδειγμα του Dedekind, αυτό δεν ήταν δυνατό για κανένα αλγεβρικό ακέραιο θ του σώματος K.

Επειδή είναι δύσκολο προς το παρόν να εργαστούμε με τον δακτύλιο του Dedekind S θα περιορισούμε στον δακτύλιο

$$S^* = R[\theta].$$

Προφανώς ο S^* είναι μια ακέραια περιοχή υποδακτύλιος του σώματος L με μοναδιαίο $1 \in R[\theta]$.

Ορισμός VI.5.1. Έστω L αλγεβρικό σώμα αριθμών και $\mathcal{O} \subset L$. Το $\mathcal{O}$ θα λέγεται *τάξη (order)* του L όταν

1. Το $\mathcal{O}$ είναι μια ελεύθερη αβελιανή ομάδα βαθμού n, όπου $n = [L : \mathbb{Q}]$,
$$\mathcal{O} = \mathbb{Z}\omega_1 \oplus \cdots \mathbb{Z}\omega_n,$$
2. $\mathcal{O}$ υποδακτύλιος του L με $1 \in \mathcal{O}$.

Πρόταση VI.5.2. *Αν $\mathcal{O}$ τάξη του σώματος L, ισχύουν:*

1. *$\mathcal{O} \subset S$, όπου S ο δακτύλιος των ακεραίων αλγεβρικών του L.*
2. *$[S : \mathcal{O}] = m < \infty$ (δείκτης πεπερασμένα παραγόμενης αβελιανής ομάδας ίδιου βαθμού (rank))*
3. *$mS \subset \mathcal{O}$*

Απόδειξη. 1. Έστω $s \in \mathcal{O} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \oplus \cdot \oplus \mathbb{Z}\omega_n$. Επομένως

$$s \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} \text{ και } A \in M_n(\mathbb{Z}).$$

Συνεπώς, $\det(s\mathbb{I}_n - A) = 0$, οπότε s ακέραιος αλγεβρικός, δηλαδή $s \in S$.

2. Είναι άμεση συνέπεια του Θεωρήματος IV.3.5.
3. Προφανές

□

Παρατήρηση VI.5.3. Το $S^* = R[\theta]$ είναι μία τάξη του L. Το ότι είναι ελεύθερη αβελιανή ομάδα αποδεικνύεται όπως και για τον S. Έχουμε τη γνωστή σχέση (εξίσωση III.5)

$$S \subset D^{-1}R[\theta], D := D_{L/K}(\theta)$$

συνεπώς

$$DS \subset R[\theta] \subset S,$$

όπου DS, S ελεύθερες αβελιανές ομάδες βαθμού (rank) n και το $\mathbb{Z}$ περιοχή κυρίων ιδεωδών, άρα και $R[\theta]$ ελεύθερη αβελιανή ομάδα βαθμού n.

Από τα παραπάνω είναι σαφές ότι και ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του L είναι επίσης μια τάξη αυτού. Επειδή όλες οι τάξεις περιέχονται στην S, ο S θα λέγεται *μέγιστη τάξη* του σώματος L.

Εργαζόμενοι όμως στην τάξη $R[\theta]$ έχουμε ξαναχάσει τον «παράδεισο» της μονοσήμαντης ανάλυσης ιδεωδών σε γινόμενο πρώτων ιδεωδών. Επειδή ο δακτύλιος $R[\theta]$ περιέχει μια $\mathbb{Q}$-βάση του σώματος L, έπεται ότι και ο $R[\theta]$ έχει ως σώμα πηλίκων το ίδιο με τον δακτύλιο των ακεραίων αλγεβρικών S.

Αν λοιπόν ισχύει $R[\theta] \subsetneq S$, τότε η τάξη $R[\theta]$ δεν είναι περιοχή του Dedekind, αφού δεν είναι ακέραια κλειστή. Για να πετύχουμε μονοσήμαντη ανάλυση σε γινόμενο πρώτων ιδεωδων, θα πρέπει να αποκλείσουμε κάποια, πεπερασμένου πλήθους, ιδεώδη. Είναι τα πρώτα ιδεώδη που διαιρούν τον *οδηγό* (conductor, Führer) $\mathcal{F}$ της τάξης.

Ορισμός VI.5.4. Αν S^* είναι μια τάξη του αλγεβρικού σώματος αριθμών L και S ο δακτύλιος των ακεραίων αλγεβρικών αριθμών, τότε οδηγός της τάξης S^* ορίζεται το σύνολο

$$\mathcal{F} = \mathcal{F}_{S/S^*} = \{\xi \in S^* : S\xi \subset S^*\}.$$

Ισχύουν

1. $\mathcal{F} = \mathcal{F}_{S/S^*} = \{\xi \in S^* : S\xi \subset S^*\}$ είναι ένα ιδεώδες του S.
2. $\mathcal{F}_{S/S^*} \supset \langle m\rangle = Sm$, όπου $m = [S : S^*]$, δηλαδή $\mathcal{F}_{S/S^*} \neq \langle 0\rangle$.

Είναι σαφές από τον ορισμό ότι $\mathcal{F} \subset S^*$, αφού $1 \in S$.

Παράδειγμα VI.5.5. Έστω $L = \mathbb{Q}(\sqrt{m})$, m, $m \in \mathbb{Z} - \{0\}$, m όχι τέλειο τετράγωνο

$$S = \mathbb{Z} + \mathbb{Z}\omega, \omega = \begin{cases} \sqrt{m} & \text{αν } m = 2, 3 \mod 4 \\ \frac{1+\sqrt{m}}{2} & \text{αν } m \equiv 1 \mod 4 \end{cases}$$

Έστω S^* μια τάξη του L. Αφού $1 \in S^*$ έχουμε ότι $\mathbb{Z} \subset S^*$. Η S^* είναι τώρα μια διδιάστατη ελεύθερη αβελιανή ομάδα και αφού $\mathbb{Z} \subset S^*$ είναι της μορφής

$$S^* = \mathbb{Z} + \mathbb{Z}\omega'$$

για κάποιο $\omega' \in S = \mathbb{Z} + \mathbb{Z}\omega$. Δηλαδή $\pm\omega' = a + f\omega$, $a \in \mathbb{Z}$, $f \in \mathbb{N} - \{0\}$. Άρα

$$S^* = \mathbb{Z} + \mathbb{Z}f\omega.$$

Επειδή δε για κάθε φυσικό αριθμό f το $\mathbb{Z} + \mathbb{Z}f\omega$ είναι μια τάξη του L, έπεται ότι για κάθε φυσικό αριθμό f έχουμε ακριβώς μία τάξη του L. Ο οδηγός της είναι το ιδεώδες του S, $Sf = \langle f\rangle$. Πολύ συχνά λέμε ότι ο οδηγός της τάξης S^* είναι f.

Πρόταση VI.5.6. *Έστω S^* μία τάξη του L με οδηγό $\mathcal{F} = \mathcal{F}_{S/S^*}$. Τότε τα σύνολα*

$$D_S(\mathcal{F}) = \{A : A \text{ακέραιο ιδεώδες του } S, A + \mathcal{F} = S\}$$

και

$$D_{S^*}(\mathcal{F}) = \{A^* : A^* \text{ακέραιο ιδεώδες του } S^*, A^* + \mathcal{F} = S^*\}$$

αποτελούν πολλαπλασιαστικές ημιομάδες στις οποίες ισχύει ο νόμος της διαγραφής.

Απόδειξη. Έστω $A, B \in D_S(\mathcal{F})$, δηλαδή $A + \mathcal{F} = S$ και $B + \mathcal{F} = S$ συνεπώς $AB + \mathcal{F} = S$, δηλαδή $A \cdot B \in D_S(\mathcal{F})$. Ομοίως αν $A^*, B^* \in D_{S^*}(\mathcal{F})$ έχουμε ότι $A^* \cdot B^* \in D_{S^*}(\mathcal{F})$. Δηλαδή $D_S(\mathcal{F})$ και $D_{S^*}(\mathcal{F})$ είναι πολλαπλασιαστικές ημιομάδες.

Τώρα στην $D_S(\mathcal{F})$ ισχύει ο νόμος της διαγραφής, διότι ισχύει στην ομάδα I_S όλων των ιδεωδών του L.

Το ότι το ίδιο ισχύει και στον $D_{S^*}(\mathcal{F})$ είναι άμεση συνέπεια του παρακάτω: □

Θεώρημα VI.5.7. *Έστω S^* μια τάξη του αλγεβρικού σώματος αριθμών L με οδηγό $\mathcal{F} = \mathcal{F}_{S/S^*}$. Τότε ισχύει*

1. *Η απεικόνιση $j : D_{S^*}(\mathcal{F}) \ni A^* \mapsto SA^* \in D_S(\mathcal{F})$ είναι ισομορφισμός ημιομάδων*
2. *Η αντίστροφη συνάρτηση j^{-1} είναι η $j^{-1} : D_S(\mathcal{F}) \ni A \mapsto A \cap S^* \in D_{S^*}(\mathcal{F})$.*
3. *Για κάθε $A \in D_S(\mathcal{F})$ με $A^* = A \cap S^*$ ισχύει $S/A \cong S^*/A^*$.*

Προτού αποδείξουμε το παραπάνω θεώρημα, διατυπώνουμε και αποδεικνύουμε το παρακάτω:

Πόρισμα VI.5.8. *Κάθε ιδεώδες $A^* \in D_{S^*}(\mathcal{F})$ έχει μονοσήμαντη ανάλυση σε γινόμενο μεγίστων ιδεωδών του $D_{S^*}(\mathcal{F})$.*

Απόδειξη. (του πορίσματος) Έστω $A^* \in D_{S^*}(\mathcal{F})$, τότε $j(A^*) = SA^* \in D_S(\mathcal{F})$. Το SA^* αναλύεται μονοσήμαντα σε γινόμενο μεγίστων ιδεωδών του S. Τα ιδεώδη αυτά περιέχουν το SA^* και επειδή το SA^* είναι πρώτο προς τον $\mathcal{F}$ και αυτά θα είναι πρώτα προς τον $\mathcal{F}$. Άρα

$$SA^* = Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}, Q_i + \mathcal{F} = S, i = 1, \ldots, r$$

Τώρα αφού λόγω του θεωρήματος VI.5.8 ο j είναι ισομορφισμός έχουμε ότι τα $j^{-1}(Q_i)$ είναι επίσης μέγιστα ιδεώδη του $D_{S^*}(\mathcal{F})$, δηλαδή

$$A^* = j^{-1}(Q_1)^{e_1}\cdots j^{-1}(Q_r)^{e_r}$$

□

Απόδειξη. (του Θεωρήματος VI.5.8) Στην απόδειξη θα χρησιμοποιήσουμε τα εξής:

(i) Έστω A, B, C υποομάδες μιας προσθετικής ομάδος $(G, +)$. Αν $A \leq C$, τότε $(A+B)\cap C = A+B\cap C$

(ii) Αν A, B ιδεώδη του S, $A + B = S$, τότε $A \cdot B = A \cap B$.

Ισχυριζόμαστε ότι

$$j(D_{S^*}(\mathcal{F})) \subset D_S(\mathcal{F}).$$

Πράγματι έστω $A^* \in D_{S^*}(\mathcal{F})$ συνεπώς $A^* + \mathcal{F} = S^*$, δηλαδή $SA^* + S\mathcal{F} = SS^*$. Όμως $SS^* = S$, διότι $1 \in S^*$ οπότε $SA^* + \mathcal{F} = S$ και επομένως $SA^* \in D_S(\mathcal{F})$.

Ο j είναι ομομορφισμός, δηλαδή

$$j(A^*B^*) = SA^*B^* = SA^*SB^* = j(A^*)j(B^*).$$

Ο j είναι μονομορφισμός. Πράγματι, έστω $A^* \in D_{S^*}(\mathcal{F})$. Ισχυριζόμαστε ότι $SA^* \cap S^* = A^*$. Αυτό προκύπτει ως εξής:

$$\begin{aligned} SA^* \cap S^* &= SA^* \cap (A^* + \mathcal{F}) = A^* + SA^* \cap \mathcal{F} \overset{(ii)}{=} A^* + \mathcal{F} \cdot SA^* = A^* + \mathcal{F}A^* \\ &= A^*(S^* + \mathcal{F}) = A^* \cap (S^* + \mathcal{F}) = A^*S^* \overset{1\in S^*}{=} A^* \end{aligned}$$

Ο j είναι επιμορφισμός. Πράγματι έστω $A \in D_S(\mathcal{F})$ συνεπώς $A + \mathcal{F} = S$ και

$$S^* \cap A + \mathcal{F} \overset{(i)}{=} (A + \mathcal{F}) \cap S^* = S \cap S^* = S^*$$

Αρκεί λοιπόν να δείξουμε ότι $A^* = S^* \cap A$ έχει την ιδιότητα $SA^* = A$.

$$\begin{aligned} SA^* &= S(S^* \cap A) = (A + \mathcal{F})(S^* \cap A) = A(S^* \cap A) + \mathcal{F}(S^* \cap A) \\ &\overset{(ii)}{=} A(S^* \cap A) + \mathcal{F} \cap S^* \cap A = A(S^* \cap A) + \mathcal{F} \cap A = \\ &\overset{(ii)}{=} A(S^* \cap A) + \mathcal{F}A = A(S^* \cap A + \mathcal{F}) = AS^* \overset{1\in S}{=} A. \end{aligned}$$

Δηλαδή αποδείξαμε τα (i) και (ii) του θεωρήματος. Για το τρίτο θεωρούμε τον κανονικό ομομορφισμό

$$\varphi : S^* \to S/A, s \mapsto s + A.$$

Προφανώς

$$\ker\varphi = \{s \in S^* : s \in A\} = S^* \cap A = A^*.$$

Επίσης ο φ είναι επιμορφισμός. Έστω τυχαίο $s+A \in S/A$, $s \in S$. Όμως $S = \mathcal{F}+A$ συνεπώς $S \subset S^*+A$, διότι $\mathcal{F} \subset S^*$. Γράφουμε τώρα $s = s^* + a$ με $s^* \in S^*$ και $a \in A$. Έχουμε

$$s + A = s^* + a + A = s^* + A = \varphi(s^*),$$

δηλαδή η φ είναι επί και $S^*/A^* \cong S/A$. □

Ο κύριος σκοπός της παρούσης παραγράφου είναι απόδειξη του

Θεώρημα VI.5.9 (2ο Θεμελιώδες Θεώρημα)**.** *Έστω* $K \subset L$ *αλγεβρικά σώματα αριθμών και* R, S *οι αντίστοιχοι δακτύλιοι των ακεραίων αλγεβρικών αριθμών,* $L = K(\theta)$ *με* $\theta \in S$ *και έστω* $\mathcal{F}$ *ο οδηγός της* $S/R[\theta]$*. Αφού* $\theta \in S$*,* $g(x) := \mathrm{Irr}(\theta, K) \in R[x]$*.*

Έστω P *πρώτο ιδεώδες του* R *με την ιδιότητα* $PS + \mathcal{F} = S$*, δηλαδή* $P \in D_S(\mathcal{F})$*. Την ανάλυση του* PS *σε γινόμενο πρώτων ιδεωδών τη βρίσκουμε ως εξής: Έστω*

$$\overline{g}(x) = \overline{g}_1(x)^{c_1} \cdots \overline{g}_t(x)^{c_t}$$

η ανάλυση του $g(x)$ *στον δακτύλιο* $\frac{R}{P}[x]$ *με* $g_i(x) \in R[X]$ *μονικά πολυώνυμα και* $\overline{g}_i(x)$ *ανάγωγα στον* $R/P[x]$*. Τότε*

1. *Τα πρώτα ιδεώδη* Q_i *του* S *που βρίσκονται πάνω από το* P *είναι τα*

   $$Q_i = PS + g_i(\theta)S, i = 1, \ldots, t$$

   Το πλήθος των ιδεωδών στην ανάλυση του PS *είναι* $r = t$*,* $f(Q_i/P) = \deg g_i(x)$ *και* $e_i(Q_i/P) = c_i$*, για* $i = 1, \ldots, t$*.*

2. $$PR[\theta] = P[\theta] = \left\{ \sum_{i=0}^{n-1} p_i \theta^i : p_i \in P \right\}$$

   και τα ιδεώδη $Q_i^* = j^{-1}(Q_i)$ *δίνονται από τη σχέση*

   $$Q_i^* = Q_i \cap R[\theta] = P[\theta] + g_i(\theta)R[\theta].$$

Σημείωση VI.5.10. Αν $f(x) = \sum_i a_i x^i \in R[x]$, τότε με

$$\overline{f(x)} = \sum_i \overline{a}_i x^i$$

συμβολίζουμε το πολυώνυμο στο $\frac{R}{P}[x]$ όπου $\overline{a}_i = a_i + P \in R/P$.

Στην ειδική περίπτωση που $S = R[\theta]$, τότε $\mathcal{F} = S$ και $PS + S = S$, δηλαδή η συνθήκη του θεωρήματος ισχύει για κάθε πρώτο ιδεώδες P του R.

Λήμμα VI.5.11. *Ικανές συνθήκες για να ισχύει* $PS + \mathcal{F} = S$*:*

1. *Αν* $P + Rm = R$ *όπου* $m = [S : R[\theta]]$*, τότε* $PS + \mathcal{F} = S$*.*
2. *Αν* $P \nmid D_{L/K}(\theta)$*, τότε* $PS + \mathcal{F} = S$*.*

Απόδειξη.

1. Ισχύει ότι $\mathcal{F} = \{\xi \in R[\theta] : S\xi \subset R[\theta]\}$. Επειδή δε $mS \subset R[\theta]$ όπου $m = [S : R[\theta]]$ άρα $m \in \mathcal{F}$ οπότε πολλαπλασιάζοντας τη σχέση $P + Rm = R$ με S έχουμε

   $$S = PS + Sm \subset PS + S\mathcal{F} = PS + \mathcal{F} \subset S$$

   συνεπώς $PS + \mathcal{F} = S$.

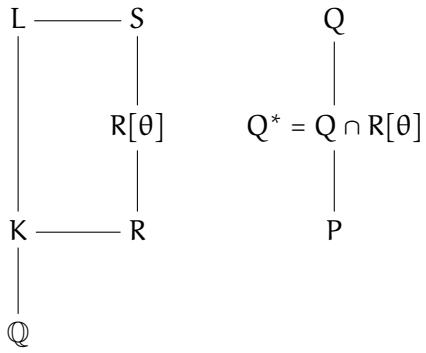
2. Ξαναθυμόμαστε ότι $S \subset \frac{1}{D_{L/K}(\theta)} R[\theta]$ συνεπώς $D_{L/K}(\theta)S \subset R[\theta]$ οπότε $D_{L/K}(\theta) \in \mathcal{F}$ άρα

   $$S = PS + SD_{L/k}(\theta) \subset PS + S\mathcal{F} = PS + \mathcal{F} \subset S,$$

   από όπου προκύπτει ότι $PS + \mathcal{F} = S$.

□

Απόδειξη. (του 2ου Θεμελιώδους θεωρήματος VI.5.9) Η απόδειξη είναι μακροσκελής. Η ιδέα πάντως είναι η εξής: Έστω P πρώτο ιδεώδες του R, $PS + \mathcal{F} = S$. Αντί να ψάξουμε να βρούμε τα ιδεώδη του S που βρίσκονται πάνω από το P, ψάχνουμε τα πρώτα ιδεώδη του $R[\theta]$ που βρίσκονται πάνω από το P και στη συνέχεια εφαρμόζουμε το θεώρημα VI.5.8.



Λήμμα VI.5.12. *Ισχύει*

$$R[\theta]/P[\theta] \cong \overline{R}[x]/\langle \overline{g}(x)\rangle,$$

όπου $\langle \overline{g}(x)\rangle = \overline{g}(x)\overline{R}[x]$.

Απόδειξη. Έστω

$$\rho : R[\theta] \to \frac{\overline{R}[x]}{\overline{g}(x)}$$

με

$$\rho(h(\theta)) = \overline{h}(x) + \langle \overline{g}(x)\rangle$$

για $h(x) \in R[\theta]$.

(i) Παρατηρούμε πρώτα ότι η ρ είναι καλά ορισμένος ομορφισμός δακτυλίων. Έστω $h(x), h'(x) \in R[x]$ ώστε $h(\theta) = h'(\theta)$ συνεπώς $f(\theta) = (h - h')(\theta) = 0$. Επειδή $g(x) = \mathrm{Irr}(\theta, K)$ θα πρέπει $g(x) \mid_{R[x]} f(x)$ και $\overline{g} \mid_{\overline{R}[x]} \overline{f}(x)$, δηλαδή $\overline{f}(x) \in \langle \overline{g}(x)\rangle$.

(ii) Επίσης παρατηρούμε ότι $\ker\rho = P[\theta]$. Έστω $h(\theta) \in \ker\rho$, $h(x) \in R[x]$ συνεπώς $\overline{h}[x] \in \langle \overline{g}(x)\rangle$ και $\overline{g}(x) \mid_{\overline{R}[x]} \overline{h}(x)$, δηλαδή υπάρχει $q(x) \in R[x]$ ώστε

$$\overline{h}(x) = \overline{g}(x)\overline{q}(x)$$

και κατά συνέπεια

$$h(x) = g(x)q(x) + r(x), \text{ όπου } r(x) \in P[x]$$

δηλαδή $h(\theta) = 0 + r(\theta) \in P[\theta]$.

Έστω τώρα $\xi \in P[\theta]$, συνεπώς $\xi = \sum_{i=1}^{n-1} p_i\theta^i$, $p_i \in P$. Θα πρέπει

$$\rho(\xi) = \sum_{i=1}^{n-1} \overline{p}_i x^i + \langle \overline{g}(x)\rangle = \langle \overline{g}(x)\rangle,$$

αφού $\overline{p}_i = \overline{0}$ στον $R/P = \overline{R}$.

Τέλος ο ρ είναι επιμορφισμός. Πράγματι, για κάθε

$$h(x) \in R[X] \text{ έχουμε } \overline{h}(x) + \langle \overline{g}(x)\rangle \in \frac{\overline{R}[x]}{\langle \overline{g}(x)\rangle},$$

και υπάρχει $h(\theta) \in R[\theta]$ με

$$\rho(h(\theta)) = \overline{h}(x) + \langle \overline{g}(x) \rangle.$$

□

Λήμμα VI.5.13. *Έστω* R *αντιμεταθετικός δακτύλιος με μοναδιαίο* $1 \in R$ *και* I *ιδεώδες του* R. *Θεωρούμε τα σύνολα*

$$K = \{A : A \lhd R, A \supset I\}$$

και

$$\Lambda = \{B : B \lhd R/I\}.$$

Υπάρχει μία αμφιμονοσήμαντη αντιστοιχία ανάμεσα στα σύνολα K *και* Λ

$$K \ni A \mapsto A + I \in \Lambda$$

η οποία διατηρεί τα μέγιστα και συνεπώς και τα πρώτα ιδεώδη (άσκηση).

Από τα τελευταία δύο λήμματα γίνεται φανερό, ότι για να βρούμε τα πρώτα ιδεώδη που βρίσκονται πάνω από το $P[\theta] = PR[\theta]$ στον $R[\theta]$, αρκεί να βρούμε όλα τα πρώτα ιδεώδη του $\overline{R}[x]/\langle \overline{g}(x) \rangle$.

Επιπλέον ο $\overline{R} = R/P$ είναι σώμα και συνεπώς ο $\overline{R}[x]$ είναι δακτύλιος κυρίων ιδεωδών και συνεπώς και ο $\overline{R}[x]/\langle \overline{g} \rangle$ είναι περιοχή κυρίων ιδεωδών.

Για δακτυλίους κυρίων ιδεωδών ισχύει

Λήμμα VI.5.14. *Έστω* $\widetilde{R}$ *ένας δακτύλιος κυρίων ιδεωδών, συνεπώς δακτύλιος μονοσήμαντης ανάλυσης. Έστω ότι το στοιχείο* $\alpha \in \widetilde{R} - \{0\}$ *έχει τη μονοσήμαντη ανάλυση*

$$\alpha \cong \pi_1^{c_1} \pi_2^{c_2} \cdots \pi_t^{c_t}$$

σε γινόμενο πρώτων (αναγώγων) στοιχείων του $\widetilde{R}$. *Τότε τα μόνα πρώτα ιδεώδη του* $\widetilde{R}$ *που βρίσκονται πάνω από το* $a\widetilde{R}$ *είναι τα* $\pi_i \widetilde{R}$ *και σύμφωνα με το λήμμα VI.5.13 στον δακτύλιο* $\widetilde{R}/a\widetilde{R}$ *τα μόνα πρώτα ιδεώδη είναι τα* $\pi_i \widetilde{R}/a\widetilde{R}$.

Απόδειξη. Προφανής, δες και V.2.2. □

Από το λήμμα VI.5.14 έπεται τώρα ότι $\langle \overline{g}_i(x) \rangle / \langle \overline{g}(x) \rangle$ είναι τα μόνα πρώτα ιδεώδη του $\overline{R}/\langle \overline{g}(x) \rangle$ οπότε αν

$$\overline{\rho} : \frac{R[\theta]}{P[\theta]} \to \frac{\overline{R}[x]}{\langle \overline{g}(x) \rangle}$$

με

$$\overline{\rho}(h(\theta) + P[\theta]) = \overline{h}(x) + \langle \overline{g}(x) \rangle,$$

είναι ο ισομορφισμός του λήμματος VI.5.12, έπεται ότι τα μόνα πρώτα ιδεώδη του $R[\theta]/P[\theta]$ είναι τα $\overline{\rho}^{-1}(\langle \overline{g}_i(x) \rangle / \langle \overline{g}(x) \rangle)$. Υπολογίζουμε ότι

$$\overline{\rho}^{-1}(\langle \overline{g}_i(x) \rangle / \langle \overline{g}(x) \rangle) = \frac{g_i(\theta)R[\theta] + P[\theta]}{P[\theta]}$$

και από το λήμμα VI.5.13 όλα τα πρώτα ιδεώδη του $R[\theta]$ που βρίσκονται πάνω από το $P[\theta] = PR[\theta]$ είναι τα $P[\theta] + g_i(\theta)R[\theta]$ για $i = 1, \ldots, t$.

Επειδή δε $PS + \mathcal{F} = S$, από το VI.5.8 έχουμε

1. Όλα τα πρώτα ιδεώδη του S που βρίσκονται πάνω από το PS είναι τα

$$Q_i = PS + g_i(\theta)S, i = 1, \ldots, t$$

2. $r = t$.

Απομένει να αποδειχτεί ακόμα ότι για $i = 1, \dots, t$

1. $f(Q_i/P) = \deg g_i(x) = \deg \overline{g}_i(x)$
2. $e(Q_i/P) = c_i$

Για την απόδειξη του πρώτου έχουμε

$$N_{K/\mathbb{Q}}(P)^{f(Q_i/P)} = (\#R/P)^{[S/Q_i:R/P]} = \#S/Q_i \overset{(VI.5.8)}{=} \#R[\theta]/Q_i^*$$

όπου $Q_i^* = Q_i \cap R[\theta]$ οπότε η τελευταία ποσότητα είναι ίση με

$$\#\frac{R[\theta]/P[\theta]}{Q_i^*/P[\theta]} \overset{(VI.5.12)}{=} \#\frac{\overline{R}[x]/\langle\overline{g}\rangle}{\langle\overline{g}_i(x)\rangle/\langle\overline{g}(x)\rangle},$$

διότι $Q_i^* = P[\theta] + g_i(\theta)R[\theta]$ οπότε η τελευταία ποσότητα υπολογίζεται σε

$$\#\frac{\overline{R}[x]}{\langle\overline{g}_i(x)\rangle} = \#\overline{R}[\theta_i],$$

όπου θ_i είναι μια ρίζα του $\overline{g}_i(x)$. Έτσι

$$\#\overline{R}[\theta_i] = (\#\overline{R})^{[\overline{R}(\theta_i):\overline{R}]} = N_{K/\mathbb{Q}}(P)^{\deg \overline{g}_i(x)}$$

και συνεπώς

$$f(Q_i/P) = \deg g_i(x) = \deg \overline{g}_i(x).$$

Για το δεύτερο αρχικά θα αποδείξουμε ότι

$$\prod_{i=1}^{r} Q_i^{c_i} \subset PS. \tag{VI.2}$$

Πράγματι

$$\prod_{i=1}^{r} Q_i^{c_i} = \prod_{i=1}^{r} (PS + g_i(\theta)S)^{c_i} \subset PS + g_1(\theta)^{c_1} \cdots g_r(\theta)^{c_r} S.$$

Αρκεί λοιπόν να δείξουμε ότι

$$g_1(\theta)^{c_1} \cdots g_r(\theta)^{c_r} \subset PS.$$

Παρατηρούμε ότι

$$\overline{g}(x) = \overline{g}_1(x)^{c_1} \cdots \overline{g}^{c_r}(x)$$

συνεπώς

$$g(\theta) = \left(g_1^{c_1} \cdots g_r^{c_r}\right)(\theta) \in P[\theta] \subset PS,$$

αφού $\theta \in S$. Από $g(\theta) = 0$ έχουμε ότι

$$g_1(\theta)^{c_1}(\theta) \cdots g_r^{c_r}(\theta) \in PS.$$

Λόγω του πρώτου τώρα έχουμε

$$PS = Q_1^{e_1} \cdots Q_r^{e_r},$$

όπου

$$e_i = e(Q_i/P). \tag{VI.3}$$

Από τις σχέσεις (VI.2) και (VI.3) έχουμε ότι $c_i \geq e_i$ για $i = 1, \dots, r$.

Από την άλλη μεριά

$$\begin{aligned}[L:K] = n &= \deg g(x) = \deg \overline{g}(x) = \sum_{i=1}^{r} \deg \overline{g_i}(x) c_i \\ &= \sum_{i=1}^{r} f(Q_i/P) c_i \leq \sum_{i=1}^{r} f(Q_i/P) e_i = n\end{aligned}$$

και τελικά καταλήγουμε στο ότι $c_i = e_i$ για $i = 1, \ldots, n$.

Η απόδειξη του θεμελιώδους θεωρήματος αυτής της παραγράφου έχει ολοκληρωθεί. □

Αποδεικνύουμε τώρα το ακόλουθο:

Θεώρημα VI.5.15. *Έστω* $L = K(\theta)$, $\theta \in S$. *Αν το πρώτο ιδεώδες* P *του* R *δεν διαιρεί τη διακρίνουσα* $D_{L/K}(\theta)$, *τότε το* P *δεν διακλαδίζεται στο σώμα* L. *Συνεπώς υπάρχουν το πολύ πεπερασμένου πλήθους πρώτα ιδεώδη του* R *τα οποία διακλαδίζονται στο* L.

Απόδειξη. Αρκεί να δείξουμε ότι αν $P \nmid D_{L/K}(\theta)$, τότε το $\overline{g}(x)$ έχει μόνο απλές ρίζες, όπου $g(x) = \mathrm{Irr}(\theta, K)$.

Έστω $\widetilde{K}$ ένα σώμα ανάλυσης του $g(x)$ υπεράνω του K. Έστω ακόμη $\widetilde{Q}$ ένα πρώτο ιδεώδες του $\widetilde{S}$ με $\widetilde{Q} \supset P$, όπου $\widetilde{S}$ ο δακτύλιος των ακεραίων αλγεβρικών του $\widetilde{K}$.

$$\begin{array}{ccccc} \widetilde{K} & - & \widetilde{S} & \longrightarrow & \widetilde{S}/\widetilde{Q} \\ | & & | & & | \\ L & - & S & \longrightarrow & S/Q \\ | & & | & & | \\ K & - & R & \longrightarrow & R/P \end{array}$$

Αν $\theta_1, \theta_2, \ldots, \theta_n \in \widetilde{S}$ είναι οι ρίζες του $g(x)$, τότε $\overline{\theta}_1, \ldots, \overline{\theta}_n$ ($\overline{\theta}_i \equiv \theta_i \mod \widetilde{Q}$) είναι οι ρίζες του $\overline{g}(x)$. Έστω ότι δεν είναι απλές, για παράδειγμα $\overline{\theta}_1 = \overline{\theta}_2$ συνεπώς $\theta_1 \equiv \theta_2 \mod \widetilde{Q}$, οπότε

$$\widetilde{Q} \mid \prod_{i<j} (\theta_i - \theta_j)^2$$

και αφού $D_{L/K}(\theta) = \prod_{i<j}(\theta_i - \theta_j)^2 \in \widetilde{Q} \cap K = P$, έχουμε ότι $P \mid D_{L/K}(\theta)$. □

Το παραπάνω θεώρημα μας υποδεικνύει πού πρέπει να ψάξουμε για να βρούμε πιθανά πρώτα ιδεώδη P του R τα οποία διακλαδίζονται στο σώμα L. Δεν μας λέει όμως ποια από αυτά που διαιρούν τη διακρίνουσα $D_{L/K}(\theta)$ διακλαδίζονται και ποια όχι. Περί αυτού θα μιλήσουμε στο επόμενο κεφάλαιο.

Θα διατυπώσουμε το 2ο θεώρημα ανάλυσης στην περίπτωση της απόλυτης επέκτασης $K/\mathbb{Q}$ ως ειδική περίπτωση.

Θεώρημα VI.5.16. *Έστω* K *αλγεβρικό σώμα αριθμών,* $[K:\mathbb{Q}]=n$, $K=\mathbb{Q}(\theta)$, $\theta\in R_K$. *Έστω* p *ένας πρώτος αριθμός* $p\nmid[R_K:\mathbb{Z}[\theta]]$ *και* $f(x)=\mathrm{Irr}(\theta,\mathbb{Q})$. *Αν*

$$\overline{f}(x)=\overline{f}_1(x)^{e_1}\overline{f}_2(x)^{e_2}\cdots\overline{f}_g(x)^{e_g}$$

η μονοσήμαντη ανάλυση του $\overline{f}(x)$ *σε γινόμενο αναγώγων πολυωνύμων στον δακτύλιο των πολυωνύμων* $\mathbb{F}_p[x]$, *τότε τα ιδεώδη του* K

$$P_i=\langle p,f_i(\theta)\rangle=pR_K+f_i(\theta)R_K,$$

$i=1,2,\ldots,g$ *είναι πρώτα ιδεώδη του* K *και ισχύει:*

$$\langle p\rangle=pR_K=P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}$$

και $N_{K/\mathbb{Q}}(P_i)=p^{f_i}$, *όπου* $f_i=\deg\overline{f}_i(x)$.

Παρατήρηση VI.5.17. Από τη σχέση

$$D_K(\theta)=[R_K:\mathbb{Z}[\theta]]^2\cdot D_K$$

προκύπτει αμέσως ότι αν $p^2\nmid D_K(\theta)$, τότε $p\nmid[R_K:\mathbb{Z}[\theta]]$.

Παράδειγμα VI.5.18. Θεωρούμε το κυβικό σώμα $K=\mathbb{Q}(\theta)$, θ ρίζα του κανονικού πολυωνύμου $f(x)=x^3-x+4$.

Το πολυώνυμο είναι ανάγωγο, η διακρίνουσά του είναι η $D_K(\theta)=-2^2\cdot 107$. Το $\frac{\theta+\theta^2}{2}$ είναι ακέραιος αλγεβρικός, αφού είναι ρίζα του πολυωνύμου $x^3-x^2+3x-2=0$ (άσκηση). Η διακρίνουσα του $\{1,\theta,\alpha=\frac{\theta+\theta^2}{2}\}$ είναι -107. Επειδή ο αριθμός είναι πρώτος το σύνολο $\{1,\theta,\frac{\theta+\theta^2}{2}\}$ είναι βάση ακεραιότητας του K. Από τη σχέση

$$D_K(\theta)=[R_K:\mathbb{Z}[\theta]]^2\cdot D_K$$

έπεται ότι ο δείκτης $[R_K:\mathbb{Z}[\theta]]=2$. Αυτό σημαίνει ότι δεν μπορούμε να εφαρμόσουμε το θεώρημα του Dedekind για τον αριθμό 2.

Η ιδέα είναι αν μπορούμε να αντικαταστήσουμε τον γεννήτορα θ του K από κάποιον άλλο. Θα αποδείξουμε ότι αυτό ισχύει για το $\alpha=\frac{\theta+\theta^2}{2}$. Πράγματι

$$\alpha^2=-2-\theta+\frac{\theta+\theta^2}{2}\Rightarrow\theta=-2+\alpha-\alpha^2.$$

Συνεπώς,

$$R_K=\mathbb{Z}\oplus\mathbb{Z}\theta\oplus\mathbb{Z}\frac{\theta+\theta^2}{2}=\mathbb{Z}\oplus\mathbb{Z}(-2+\alpha-\alpha^2)\oplus\mathbb{Z}\alpha=\mathbb{Z}\oplus\mathbb{Z}\alpha\oplus\mathbb{Z}\alpha^2.$$

Αυτό σημαίνει ότι και το σύνολο $\{1,\alpha,\alpha^2\}$ είναι βάση ακεραιότητας του $K=\mathbb{Q}(\alpha)$, δηλαδή $R_K=\mathbb{Z}[\alpha]$ και εδώ ο δείκτης είναι ένα. Συνεπώς μπορούμε να εφαρμόσουμε το θεώρημα του Dedekind και για $p=2$, αλλά θα χρησιμοποιήσουμε το πολυώνυμο

$$g(x)=x^3-x^2+3x-2.$$

Το

$$\overline{g}(x)\equiv x^3+x^2+x\equiv x(x^2+x+1)\mod 2$$

Συνεπώς σύμφωνα με το θεώρημα του Dedekind

$$\langle 2\rangle=2R_K=P\cdot Q,$$

όπου

$$P = \langle 2, \alpha \rangle = \langle 2, \frac{\theta + \theta^2}{2} \rangle, N_{K/\mathbb{Q}}(P) = 2$$

και

$$Q = \langle 2, 1 + \alpha + \alpha^2 \rangle = \langle 2, 1 - \theta^2 \rangle, N_{K/\mathbb{Q}}(Q) = 4.$$

Παρατήρηση VI.5.19. Αν στο παραπάνω παράδειγμα είχαμε εφαρμόσει (αφελώς) το θεώρημα για $p = 2$ και για το πολυώνυμο $f(x) = x^3 - x + 4$ θα είχαμε $\overline{f}(x) \equiv x(x+1)^2 \mod 2$ και θα είχαμε καταλήξει σε *λάθος* αποτέλεσμα. Το συμπέρασμα λοιπόν είναι ότι η υπόθεση

$$p \nmid [R_K : \mathbb{Z}[\theta]]$$

στο θεώρημα, είναι *ουσιαστική*.

Στη συνέχεια επεκτείνουμε το κριτήριο αναγωγησιμότητας του Eisenstein για πρώτα ιδεώδη. Έστω

$$f(x) = a_n X^n + a_{n-1} X^{n-1} + \cdots a_0 \in R_K[X]$$

όπου R_K ο δακτύλιος των ακεραίων αλγεβρικών αριθμών κάποιου αλγεβρικού σώματος αριθμών και υπάρχει ένα πρώτο ιδεώδες P του R_K για το οποίο ισχύουν $a_n \notin P$, $a_{n-1}, a_{n-2}, \ldots, a_0 \in P$ και $a_0 \notin P^2$, τότε το πολυώνυμο $f(X)$ θα λέγεται *τύπου Eisenstein* ως προς το P. Όπως, όταν $R_K = \mathbb{Z}$ έτσι και εδώ αποδεικνύεται ότι το $f(X)$ είναι ανάγωγο υπεράνω του σώματος K.

Θεώρημα VI.5.20. *Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών, $[L : K] = n$ και P ένα πρώτο ιδεώδες του R_K. Αν $\alpha \in R_L$ και $L = K(\alpha)$ και το $f(X) = \mathrm{Irr}(\alpha, K)$ είναι τύπου Eisenstein ως προς το P, τότε το P διακλαδίζεται πλήρως στην επέκταση L/K, δηλαδή το $PR_L = Q^n$ για κάποιο πρώτο ιδεώδες του R_L.*

Απόδειξη. Έστω Q ένα, οποιοδήποτε από τα πρώτα ιδεώδη του R_K που είναι πάνω από το P και έστω ότι $Q^e \parallel PR_L$. Είναι φανερό από το πρώτο θεώρημα ανάλυσης, ότι $e \leq n$. Αφού $\alpha^n \in PR_L$, αυτό από την ιδιότητα του πολυωνύμου $f(X) = \mathrm{Irr}(\alpha, K)$ ότι είναι τύπου Eisenstein ως προς το P έχουμε ότι $\alpha^n \in Q$ και αφού, Q πρώτο ιδεώδες, έπεται ότι $\alpha \in Q$.

Επίσης οι συντελεστές $a_0, a_1, \ldots, a_{n-1} \in Q^e$, αφού ανήκουν στο PR_L. Ας υποθέσουμε ότι $e \leq n-1$. Τότε το ιδεώδες Q^{1+e} θα διαιρεί το ιδεώδες που παράγεται από το στοιχείο a_0 του R_K, αφού

$$a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha).$$

Αυτό σημαίνει ότι το $P^2 \mid a_0$, το οποίο είναι άτοπο. □

Για εφαρμογές του προγράμματος PARI στον νόμο ανάλυσης παραπέμπουμε στο [9] [2] ή το πρόγραμμα SAGE στο [13].

VI.6 Εφαρμογή του νόμου Ανάλυσης στα τετραγωνικά, κυκλοτομικά σώματα και σε επεκτάσεις του Kummer

VI.6.1 Τετραγωνικά σώματα αριθμών

Υπενθυμίζουμε ότι $L = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z} - \{0\}$, m ελεύθερο τετραγώνου.

$$S = \mathbb{Z} + \mathbb{Z}\omega, \text{ όπου } \omega = \begin{cases} \sqrt{m} & \text{αν } m \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{m}}{2} & \text{αν } m \equiv 1 \mod 4 \end{cases}$$

Επίσης η διακρίνουσα υπολογίζεται:

$$D_L = \begin{cases} 4m & \text{αν } m \equiv 2, 3 \mod 4 \\ m & \text{αν } m \equiv 1 \mod 4 \end{cases}$$

Έχουμε $S^* = \mathbb{Z}[\sqrt{m}]$ και

$$\mathcal{F}_{S/S^*} = \begin{cases} S & \text{αν } m \equiv 2,3 \mod 4 \\ 2S & \text{αν } m \equiv 1 \mod 4 \end{cases}$$

Επιπλέον

$$2 = \sum_{i=1}^{r} e_i f_i \text{ συνεπώς } \left| \begin{array}{l} r = 2, e_1 = e_2 = f_1 = f_2 = 1 \\ r = 1, e = 2, f = 1 \\ r = 1, e = 1, f = 2 \end{array} \right.$$

Η $L/\mathbb{Q}$ είναι πάντα επέκταση του Galois, $G = \mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma\}$, $\sigma : \sqrt{m} \mapsto -\sqrt{m}$.

Παρατήρηση VI.6.1. Έστω $L = \mathbb{Q}(\sqrt{m})$ τετραγωνικό σώμα αριθμών. Για την ανάλυση του $p\mathbb{Z}$ (p πρώτος αριθμός) έχουμε τις παρακάτω δυνατότητες:

1. $pS = Q, f(Q/p\mathbb{Z}) = 2$, σε αυτή την περίπτωση λέμε ότι ο p *αδρανεί* στο L.
2. $pS = Q_1Q_2$, $Q_1 \neq Q_2$, $f(Q_i/p\mathbb{Z}) = 1$ σε αυτή την περίπτωση λέμε ότι ο p *αναλύεται* (πλήρως) στο L.
3. $pS = Q^2, f(Q/p\mathbb{Z}) = 1$, σε αυτή την περίπτωση ο p *διακλαδίζεται* (πλήρως) στο L.

Στη δεύτερη περίπτωση ισχύει επιπλέον ότι $\sigma Q_1 = Q_2$.

Για κάθε πρώτο αριθμό p θα συμβολίζουμε με $\left(\frac{D_L}{p}\right)$ το σύμβολο του Kronecker.

Θεώρημα VI.6.2 (Νόμος ανάλυσης στο $L = \mathbb{Q}(\sqrt{m})$)**.** *Έστω p πρώτος αριθμός. Τότε ισχύουν:*

- p *αδρανεί στο* L *αν και μόνο αν* $\left(\frac{D_L}{p}\right) = -1$.
- p *αναλύεται στο* L *αν και μόνο αν* $\left(\frac{D_L}{p}\right) = 1$.
- p *διακλαδίζεται στο* L *αν και μόνο αν* $\left(\frac{D_L}{p}\right) = 0$.

Απόδειξη. Έστω κατ' αρχήν $p \neq 2$, τότε $p\mathbb{Z} \nmid \mathcal{F}_{S/S^*}$, οπότε μπορούμε να εφαρμόσουμε το θεμελιώδες θεώρημα της προηγούμενης παραγράφου για $\theta = \sqrt{m}$, και

$$g(x) = x^2 - m,$$

$D_L = m$ ή $4m$, αφού $p \neq 2$ έχουμε $\left(\frac{D_L}{p}\right) = \left(\frac{m}{p}\right)$ οπότε

$$\left(\frac{D_L}{p}\right) = -1 \text{ αν και μόνο αν } \left(\frac{m}{p}\right) = -1 \text{ αν και μόνο αν } x^2 \equiv m \mod p \text{ δεν έχει λύση.}$$

Αυτό έχει ως συνέπεια ότι το $\overline{g}(x) = g(x) \mod p$ να παραμένει ανάγωγο στο $\mathbb{Z}/p\mathbb{Z}$ και το p αδρανεί στο L.

Αν τώρα

$$\left(\frac{D_L}{p}\right) = 1 \text{ αν και μόνο αν } \left(\frac{m}{p}\right) = 1 \text{ αν και μόνο αν } x^2 \equiv m \mod p \text{ έχει λύση,}$$

έστω $x_0 \in \mathbb{Z}$, $p \nmid x_0$ και

$$\overline{g}(x) = (x - x_0)(x + x_0) \text{ στο } \mathbb{Z}/p\mathbb{Z}[x]$$

όπου $-x_0 \neq x_0$ διότι $p \neq 2$ και σε αυτή την περίπτωση το p αναλύεται στο L.

Αν

$$\left(\frac{D_L}{p}\right) = 0 \text{ αν και μόνο αν } p \mid m,$$

συνεπώς

$$\overline{g}(x) = x^2 \mod p$$

και σε αυτή την περίπτωση το p διακλαδίζεται στο L.

Έστω τώρα $p = 2$. Αν $\left(\frac{D_L}{p}\right) = 0$, τότε $2 \mid D_L$ και αφού $D_L \equiv 0, 1 \mod 4$ έχουμε $4 \mid D_L$. Συνεπώς $S = \mathbb{Z}[\sqrt{m}]$,

$$g(x) = x^2 - m = (x - m)^2 \mod 2$$

και το 2 διακλαδίζεται στο L.

Αν πάλι $\left(\frac{D_L}{2}\right) = \pm 1$, τότε $2 \nmid D_L$, συνεπώς $D_L = m \equiv 1 \mod 4$. Θέτουμε $\theta = \frac{1+\sqrt{m}}{2}$ και $S = \mathbb{Z}[\theta]$, οπότε $\mathcal{F} = S$. Επομένως,

$$g(x) = \mathrm{Irr}(\theta, \mathbb{Q}) = x^2 - x + \frac{1-m}{4} \in \mathbb{Z}[x].$$

Αν $\left(\frac{D_L}{p}\right) = -1$, τότε $D_L = m \equiv 5 \mod 8$, συνεπώς $\frac{1-m}{4}$ περιττός και

$$\overline{g}(x) = (x^2 + x + 1) \mod 2.$$

Το $x^2 + x + 1$ είναι ανάγωγο στο $\mathbb{Z}/2\mathbb{Z}$ και το 2 αδρανεί στο L.

Τέλος αν $\left(\frac{D_L}{p}\right) = 1$, τότε $D_L = m = 1 \mod 8$, συνεπώς $\frac{1-m}{4}$ άρτιος και

$$\overline{g}(x) = (x^2 + x) = x(x + 1) \mod 2$$

και το 2 αναλύεται στο L και αντιστρόφως. □

Πόρισμα VI.6.3. *Έστω $L = \mathbb{Q}(\sqrt{m})$ τετραγωνικό σώμα αριθμών και p πρώτος αριθμός. Τα ιδεώδη που βρίσκονται πάνω από τον p έχουν τις εξής βάσεις:*

$$pS = Q_1 Q_2, Q_{1,2} = \begin{cases} \langle p, x_0 \pm \sqrt{m} \rangle & x_0 \in \mathbb{Z},\ \textit{λύση της } x_0^2 \equiv m \mod p, m \neq 1 \mod 4 \\ \langle p, \frac{x_0 \pm \sqrt{m}}{2} \rangle & x_0 \in \mathbb{Z}, 2 \nmid x_0, x_0^2 \equiv 0 \mod p, m \equiv 1 \mod 4 \end{cases}$$

$$pS = Q^2, Q = \begin{cases} \langle p, \sqrt{m} \rangle & m \not\equiv 1 \mod 4 \\ \langle p, \frac{m+\sqrt{m}}{2} \rangle & m \equiv 1 \mod 4 \end{cases}$$

Το θεώρημα VI.5.15 στα τετραγωνικά σώματα αριθμών διατυπώνεται ως εξής. Έστω $L = \mathbb{Q}(\sqrt{m})$. Έστω

$$\text{Αν } p \nmid D_{L/\mathbb{Q}}(\theta) = \begin{cases} m \\ 4m \end{cases}$$

τότε p δεν διακλαδίζεται στο L.

VI.6.2 Κυβικά σώματα αριθμών

Παράδειγμα VI.6.4. Έστω $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$. Ισχύει ότι $S = \mathbb{Z}[\sqrt[3]{2}]$, δείτε IV.6.4. Το ελάχιστο πολυώνυμο του $\alpha = \sqrt[3]{2}$ είναι το $g(x) = \mathrm{Irr}(\theta, \mathbb{Q}) = x^3 - 2$.

Έχουμε

$$g(X) \equiv x^3 \mod 2 \text{ συνεπώς } 2S = Q^3,$$

όπου

$$Q = 2S + \alpha S = \alpha S, N_L(Q) = 2.$$

Στην παραπάνω ισότητα έχουμε ότι $\langle 2 \rangle = \langle \alpha^3 \rangle$. Επίσης

$$g(x) = (x + 1)^3 \mod 3 \text{ συνεπώς } 3S = (Q')^3,$$

όπου

$$Q' = 3S + (\alpha+1)S = (\alpha+1)S, N_{L/\mathbb{Q}}(Q') = 3.$$

Στην παραπάνω ισότητα έχουμε $3 = (\alpha+1)^3 - 3\alpha(\alpha+1)$. Τέλος

$$g(x) = (x+2)(x^2+3x-1) \mod 5 \text{ συνεπώς } 5S = Q_1Q_2,$$

με

$$Q_1 = 5S + (\alpha+2)S, \quad Q_2 = 5S + (\alpha^2+3\alpha-1)S$$

και $N_{L/\mathbb{Q}}(Q_1) = 5$ και $N_{L/\mathbb{Q}}(Q_2) = 5^2$.

Παράδειγμα VI.6.5. Έστω $L = \mathbb{Q}(\theta)$, όπου θ ρίζα του $x^3+x^2-2x+8 = g(x)$. Έχουμε υπολογίσει ότι $D_{L/\mathbb{Q}}(\theta) = -4\cdot 503$ και $m_L = 2$, $D_L = -503$.

Επειδή $503 \nmid m(\theta) = 2$ μπορούμε να εφαρμόσουμε το θεμελιώδες θεώρημα αυτής της παραγράφου για τον πρώτο αριθμό 503.

Ισχύει

$$g(x) = (x-149)^2(x+299) \mod 503 \text{ συνεπώς } 503S = Q_1^2Q_2$$

όπου

$$Q_1 = 503S + (a-149)S, \quad Q_2 = 503S + (a+299)S$$

Έχουμε $Q_1 \neq Q_2$ και $f(Q_1/503\mathbb{Z}) = f(Q_2/503\mathbb{Z}) = 1$.

Στο παράδειγμά μας αυτό δεν μπορούμε να εφαρμόσουμε το «τέχνασμα» του παραδείγματος VI.5.18. Και αυτό επειδή ο R_K δεν είναι μονογενής (monogenic), αφού για κάθε $\alpha \in R_K, \alpha \neq 0$ ισχύει

$$D_K(\alpha) = 4D_K,$$

με δείκτη $[R_K : \mathbb{Z}(\alpha)] = 2$. Αυτό σημαίνει ότι δεν μπορούμε να εφαρμόσουμε το θεώρημα του Dedekind. Θα προσπαθήσουμε να υπολογίσουμε και την παραγοντοποίηση του $\langle 2\rangle = R_K 2$.

Ορισμός VI.6.6. Ένας πρώτος p *αναλύεται πλήρως* στο αλγεβρικό σώμα αριθμών K αν και μόνο αν το ιδεώδες $pR_K = P_1P_2\cdots P_t$, $P_t \neq P_j$, για $i \neq j$ και $t = [K:\mathbb{Q}] = n$.

Θα αποδείξουμε ότι ο 2 αναλύεται πλήρως στο $K = \mathbb{Q}(\theta)$,

$$2R_K = P_1P_2P_2,$$

$N_{K/\mathbb{Q}}(P_i) = 2$, $i = 1,2,3$. Για λόγους συντομίας, θα χρησιμοποιήσουμε το θεώρημα της Διακρίνουσας το οποίο έχουμε αναφέρει στην αρχή στο εισαγωγικό κεφάλαιο και θα αποδείξουμε στο κεφάλαιο X.

Το θεώρημα αυτό αναφέρει ότι ο πρώτος αριθμός p διακλαδίζεται στην επέκταση $K/\mathbb{Q}$ αν και μόνο αν $p \mid D_K$. Τη μία κατεύθυνση την έχουμε ήδη δει.

Στο παράδειγμά μας $D_K = -503$, $2 \nmid D_K$, συνεπώς ο 2 δεν διακλαδίζεται στο K. Για κάθε ακέραιο m θεωρούμε το ιδεώδες

$$A_m = \langle m - \theta\rangle$$

Η norm

$$N_{K/\mathbb{Q}}(A_m) = |N_{K/\mathbb{Q}}(m-\theta)| = |m-\theta|\cdot|m-\theta'|\cdot|m-\theta''| = |f(\theta)|,$$

όπου θ', θ'' είναι οι άλλες δύο ρίζες του $f(X)$. Επομένως $N_{K/\mathbb{Q}}(A_{-1}) = 10$, $N_{K/\mathbb{Q}}(A_{-2}) = 8$, $N_{K/\mathbb{Q}}(A_1) = 8$, $N_{K/\mathbb{Q}}(A_0) = 8$. Αφού οι norm είναι άρτιοι ακέραιοι, όλα αυτά τα ιδεώδη έχουν στην ανάλυσή τους πρώτα ιδεώδη που βρίσκονται πάνω από το 2. Τα ιδεώδη A_{-1} και A_{-2} είναι πρώτα μεταξύ τους αφού $(-1-\theta)-(-2-\theta) = 1$. Ομοίως και τα A_0 και A_1. Συνεπώς η ανάλυση του $2R_K$ περιέχει τουλάχιστον δύο πρώτους παράγοντες διαφορετικούς μεταξύ τους. Αν υποθέσουμε ότι υπάρχουν ακριβώς δύο παράγοντες, τότε έχουμε τις δυνατότητες:

(a) $\langle 2\rangle = P_1P_2$, με $N_{K/\mathbb{Q}}(P_1) = 2$ και $N_{K/\mathbb{Q}}(P_2) = 4$. Σ' αυτή την περίπτωση τα μόνα ιδεώδη με norm 8 είναι τα P_1^3 και P_1P_2. Αλλά τότε και τα δύο A_{-2} και A_{-1} έχουν κοινό παράγοντα, το P_1, άτοπο.

(b) $\langle 2\rangle = P_1P_2P_3$ με $N_{K/\mathbb{Q}}(P_i) = 2$ και $P_3 \in \{P_1, P_2\}$ αλλά τότε το $\langle 2\rangle$ θα διακλαδιζόταν, άτοπο.

Παρατήρηση VI.6.7. Αν είχαμε εφαρμόσει αφελώς το θεώρημα του Dedekind στο $f(X) \equiv X^2(X+1) \mod 2$, θα είχαμε καταλήξει στο *λάθος συμπέρασμα* ότι $\langle 2\rangle = P_2P_2'$. Με χρήση του Θεωρήματος του Hensel έχουμε ήδη αποδείξει ότι το 2 αναλύεται πλήρως στο K.

Η γνώση της ανάλυσης πρώτων ιδεωδών του $\mathbb{Z}$ στο αλγεβρικό σώμα αριθμών L είναι πολύ χρήσιμη στη λύση διοφαντικών εξισώσεων καθώς και στον προσδιορισμό του αριθμού κλάσεων h_L και της δομής της ομάδας κλάσεων του L, όπως έχουμε ήδη κάνει και στο προηγούμενο κεφάλαιο.

Παράδειγμα VI.6.8. Έστω $L = \mathbb{Q}(\sqrt[3]{7})$. Ισχύει ότι IV.6.4 $D_L = -3^3 7^2$, και ότι $S = \mathbb{Z}[\sqrt[3]{7}]$.

```
K.<y> = NumberField(x^3-7)
Number Field in y with defining polynomial x^3 - 7
K.discriminant().factor()
-3^3 * 7^2
K.integral_basis()
[1, y, y^2]
K.class_group()
Class group of order 3 with structure C3 of Number Field in y with defining
polynomial x^3 - 7
```

Αν

$$\alpha = x + y\sqrt[3]{7} + z\sqrt[3]{7^2} \in S,$$

υπολογίζουμε την norm

$$N_{L/\mathbb{Q}}(\alpha) = x^3 + 7y^3 + 7^2z^3 - 3 \cdot 7xyz. \tag{VI.4}$$

Γνωρίζουμε ότι σε κάθε κλάση της ομάδας κλάσεων ιδεωδών $\mathfrak{K}$ υπάρχει ένα ιδεώδες με norm μικρότερη ή ίση του $\frac{8}{3\pi}7\sqrt{3} < 21/2$.

Άρα θα πρέπει να ελέγξουμε ιδεώδη με norm μικρότερη ή ίση του 10. Έχουμε:

$$\begin{aligned}
g(x) &= x^3 - 7 \equiv x^3 + 1 = (x+1)(x^2 - x + 1) \mod 2\\
g(x) &= x^3 - 7 \equiv (x^3 - 1) = (x-1)^3 \mod 3\\
g(x) &= x^3 - 7 \equiv (x-3)(x^2 + 3x + 9) \mod 5\\
g(x) &= x^3 - 7 \equiv x^3 \mod 7
\end{aligned}$$

οπότε

$$\begin{aligned}
2S &= Q_2Q_2', N_{L/\mathbb{Q}}(Q_2) = 2, N_{L/\mathbb{Q}}(Q_2') = 4\\
3S &= Q_3^3, N_{L/\mathbb{Q}}(Q_3) = 3\\
5S &= Q_5Q_5', N_{L/\mathbb{Q}}(Q_5) = 5, N_{L/\mathbb{Q}}(Q_5') = 25\\
7S &= Q_7^3, N_{L/\mathbb{Q}}(Q_7) = 7
\end{aligned}$$

Για κάθε $x \in \mathbb{Z}$ έχουμε $x^3 \equiv 0, 1, -1 \mod 7$, οπότε $N_{L/\mathbb{Q}}(\alpha) = 0, 1, -1 \mod 7$ για κάθε $\alpha \in S$.

Από την παρατήρηση αυτή βγαίνει το συμπέρασμα ότι τα πρώτα ιδεώδη $Q_2, Q_2', Q_3, Q_5, Q_5'$ δεν είναι είναι κύρια, ενώ το Q_7 είναι κύριο αφού παράγεται από το $7^{1/3}$. Έστω X η κλάση των ιδεωδών που περιέχει το Q_3. Επειδή Q_3^3 είναι κύριο ιδεώδες, $X^3 = H$, όπου H είναι η κλάση των κυρίων ιδεωδών. Στην εξίσωση (VI.4) βάζουμε $x = -1, y = 1, z = 0$ και βρίσκουμε $N_{L/\mathbb{Q}}(\alpha) = 6$.

Βάζουμε $x = 2, y = 1, z = 0$ και βρίσκουμε $N_{L/\mathbb{Q}}(\alpha) = 15$. Υπάρχουν λοιπόν κύρια ιδεώδη των οποίων η norm είναι 6 ή 15. Αυτά θα πρέπει να είναι Q_2Q_3 και Q_3Q_5 αντίστοιχα. Δηλαδή

$$Q_2Q_3 = H \text{ συνεπώς } Q_2 \in X^{-1} = X^2.$$

Ομοίως

$$Q_5 \in X^2$$

και αφού Q_2Q_2' είναι κύριο ιδεώδες έχουμε $Q_2' \in X$. Ομοίως $Q_5' \in X$. Όλα τα ιδεώδη των αναλύσεων των πρώτων αριθμών $2, 3, 5, 7$ ανήκουν στην ομάδα που παράγεται από την κλάση X. Κάθε άλλο ιδεώδες με norm ≤ 10 είναι γινόμενο των παραπάνω πρώτων ιδεωδών και η ομάδα κλάσεων είναι τελικά ισόμορφη με την $\mathbb{Z}/3\mathbb{Z}$.

VI.6.3 Κυκλοτομικά σώματα Αριθμών

Έστω τώρα $\zeta_n = e^{2\pi i/n}$. Το n-στό κυκλοτομικό σώμα αριθμών είναι το σώμα $L = \mathbb{Q}(\zeta_n)$. Το L είναι το σώμα αναλύσεως του διαχωρισίμου πολυωνύμου $x^n - 1$ και συνεπώς $L/\mathbb{Q}$ είναι επέκταση Galois. Ο βαθμός της επέκτασης υπολογίζεται:

$$[L : \mathbb{Q}] = \varphi(n)$$

και το ανάγωγο πολυώνυμο είναι το

$$\Phi_n(X) = \mathrm{Irr}(\zeta_n, \mathbb{Q}) = \prod_{\substack{d=1 \\ (d,n)=1}}^{n-1} (x - \zeta_n^d) \in \mathbb{Z}[x].$$

Έστω

$$E(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^* = \{a \mod n, 1 \leq a \leq n, (a, n) = 1\}$$

η ομάδα των μονάδων του δακτυλίου $\mathbb{Z}/n\mathbb{Z}$. Θα αποδείξουμε ότι η ομάδα Galois $G = \mathrm{Gal}(L/\mathbb{Q})$ είναι ισόμορφη προς την $(\mathbb{Z}/n\mathbb{Z})^*$.

Πράγματι, αν $\sigma \in G$, τότε $\sigma(\zeta_n)$ θα είναι κατ' ανάγκη μια ρίζα του κυκλοτομικού πολυωνύμου $\Phi_n(x)$, δηλαδή υπάρχει $d \in \mathbb{Z}$, $1 \leq d \leq n$, $(d, n) = 1$, τέτοιο ώστε:

$$\sigma(\zeta_n) = \zeta_n^d.$$

Συμβολίζουμε αυτό το σ με σ_d και θεωρούμε τη συνάρτηση

$$f : \mathrm{Gal}(L/\mathbb{Q}) \ni \sigma_d \mapsto d \mod n \in (\mathbb{Z}/n\mathbb{Z})^*$$

η οποία είναι προφανώς ισομορφισμός ομάδων.

Ξαναθυμίζουμε ότι $D_{L/\mathbb{Q}}(\zeta_n) \mid n^{\varphi(n)}$ (Θεωρημα IV.7.7) οπότε το θεώρημα VI.5.15 δίνει:

Πρόταση VI.6.9. *Όλοι οι πρώτοι αριθμοί* p, $p \nmid n$ *δεν διακλαδίζονται στο σώμα* $L = \mathbb{Q}(\zeta_n)$.

Επειδή τώρα $L/\mathbb{Q}$ επέκταση του Galois, έχουμε $\varphi(m) = efr$ και αρκεί να υπολογίσουμε τα r, f.

Θεώρημα VI.6.10. *Έστω* p *πρώτος αριθμός* $p \nmid n$. *Τότε είναι* $e = 1$ *και* f *είναι ο ελάχιστος φυσικός αριθμός τέτοιος ώστε:*

$$p^f \equiv 1 \mod n$$

δηλαδή η τάξη του $p \mod n$.

Απόδειξη. Έστω Q κάποιο πρώτο ιδεώδες του S με $Q \supset p\mathbb{Z}$. Το f έχει οριστεί ως $f = [S/Q : \mathbb{Z}/p\mathbb{Z}]$. Το S/Q είναι ένα σώμα το οποίο είναι πεπερασμένη επέκταση του σώματος $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Από τη θεωρία των πεπερασμένων σωμάτων έπεται ότι η επέκταση $S/Q/\mathbb{Z}/p\mathbb{Z}$ είναι επέκταση του Galois και η ομάδα Galois της είναι κυκλική παραγόμενη από τον αυτομορφισμό του Frobenius

$$\sigma_p : S/Q \ni \overline{x} = x + Q \mapsto \overline{x}^p = x^p + Q \in S/Q.$$

Είναι σαφές ότι η τάξη του αυτομορφισμού σ_p είναι f, δηλαδή ο f είναι ο ελάχιστος φυσικός αριθμός για τον οποίο:

$$\sigma_p^f = \mathrm{Id}_{S/Q}.$$

Τώρα, ξαναθυμόμαστε ότι από την

$$1 + x + \cdots + x^{n-1} = \prod_{i=1}^{n-1} (x - \zeta_n^i)$$

για $x = 1$ προκύπτει

$$n = \prod_{i=1}^{n-1} (1 - \zeta_n^i), \qquad 1 \le i \le n-1,$$

δηλαδή

$$n + Q = \prod_{i=1}^{n-1} (1 - \zeta_n^i) + Q.$$

Επειδή $p \nmid n$ έχουμε

$$n + Q \neq Q \text{ συνεπώς } \prod_{i=1}^{n} (1 - \zeta_n^i) \notin Q$$

συνεπώς $1 - \zeta_n^i \notin Q$ για κάθε $1 \le i \le n-1$, δηλαδή

$$\zeta_n^i + Q \neq 1 + Q \text{ για κάθε } i = 1, \ldots, n-1$$

και συνεπώς

$$\zeta_n^i + Q \neq \zeta_n^j + Q \text{ για κάθε } 0 \le i, j \le n-1, i \neq j,$$

δηλαδή οι ρίζες της μονάδας ζ_n^i, $0 \le i \le n-1$ ανήκουν σε διαφορετικές μεταξύ τους κλάσεις modulo Q.

Επειδή $S = \mathbb{Z}[\zeta_n]$ έχουμε ότι $S/Q = \mathbb{F}_p[\overline{\zeta}_n]$, $\overline{\zeta}_n = \zeta_n + Q$. Άρα

$$\sigma_p^f = 1 \Leftrightarrow \sigma_p^f(\overline{\zeta}_n) = \overline{\zeta}_n \Leftrightarrow \overline{\zeta}_n^{p^f} = \overline{\zeta}_n \Leftrightarrow \overline{\zeta}_n^{p^f-1} = \overline{1} \Leftrightarrow \zeta_n^{p^f-1} \equiv 1 \mod Q.$$

Λόγω της παραπάνω παρατήρησης για τις κλάσεις των ριζών της μονάδας modulo Q η παραπάνω ισοδυναμία δίνει $p^f \equiv 1 \mod n$. Επειδή f είναι ο ελάχιστος φυσικός με την ιδιότητα $\sigma_p^f = 1$, έπεται, λόγω των ισοδυναμιών, ότι f είναι ο ελάχιστος φυσικός με την ιδιότητα $p^f \equiv 1 \mod n$. □

Παρατήρηση VI.6.11. Για κάθε πρώτο p, $p \nmid n$ έχουμε

$$pS = Q_1 Q_2 \ldots Q_r$$

και $N_{L/\mathbb{Q}}(Q_i) = p^f$, όπου f ο ελάχιστος φυσικός $p^f \equiv 1 \mod n$. Τέλος $r = \varphi(n)/f$. Παρατηρούμε ότι αν p πρώτος, $p \nmid n$ ο p αναλύεται πλήρως στο $L = \mathbb{Q}(\zeta_n)$ αν και μόνο αν $p \equiv 1 \mod n$.

Ορισμός VI.6.12. Αν $pS = Q^n$ όπου $n = [L : \mathbb{Q}]$, τότε λέμε ότι ο p είναι *πλήρως διακλαδιζόμενος* στο σώμα L.

Θεώρημα VI.6.13. *Έστω* p *πρώτος αριθμός,* $n = p^k$, $k \ge 1$, $L = \mathbb{Q}(\zeta_{p^k})$. *Τότε*

$$pS = Q^{\varphi(n)} = Q^{\varphi(p^k)}.$$

Απόδειξη. Έχουμε

$$\Phi_{p^k}(X) = \prod_{\substack{\nu \bmod p^k \\ (\nu,p)=1}} (X - \zeta_{p^k}^{\nu}) = \Phi_p(X^{p^{k-1}}).$$

Επίσης είναι γνωστό

$$\Phi_p(X) = X^{p-1} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}.$$

Συνδυάζοντας τα παραπάνω έχουμε:

$$p = \Phi_p(1) = \prod_{\substack{\nu \bmod p^k \\ (\nu,p)=1}} (1 - \zeta_{p^k}^{\nu})$$

και συνεπώς

$$pS = \prod_{\substack{\nu \bmod p^k \\ (\nu,p)=1}} (1 - \zeta_{p^k}^{\nu})S.$$

Επειδή το πλήθος των παραγόντων στο δεξιό μέλος είναι $\varphi(p^k)$ ίσο με τον βαθμό της επέκτασης, έχουμε ότι τα ιδεώδη $(1 - \zeta_{p^k}^{\nu})S$, $(\nu, p) = 1$ είναι πρώτα. Ισχυριζόμαστε ότι

$$(1 - \zeta_{p^k}^{\nu})S = (1 - \zeta_{p^k})S \text{ για κάθε } (\nu, p) = 1.$$

Αρκεί να δείξουμε ότι

$$1 - \zeta_{p^k}^{\nu} \text{ και } 1 - \zeta_{p^k}$$

είναι συνεταιρικά δηλαδή ότι

$$\frac{1 - \zeta_{p^k}^{\nu}}{1 - \zeta_{p^k}} \in S \text{ και } \frac{1 - \zeta_{p^k}}{1 - \zeta_{p^k}^{\nu}} \in S,$$

το πηλίκο είναι μονάδα του S. □

Το πρώτο είναι προφανές. Για το δεύτερο αφού $(\nu, p) = 1$ υπάρχει $\mu \in \mathbb{N}$ με $\nu\mu \equiv 1 \mod p^k$ οπότε

$$\frac{1 - \zeta_{p^k}}{1 - \zeta_{p^k}^{\nu}} = \frac{1 - \zeta_{p^k}^{\nu\mu}}{1 - \zeta_{p^k}^{\nu}} = 1 + \zeta_{p^k}^{\nu} + \cdots + \zeta_{p^k}^{\nu(\mu-1)} \in S.$$

Επομένως, αν $Q = (1 - \zeta_{p^k})S$ έχουμε $pS = \varphi(p^k)Q$.

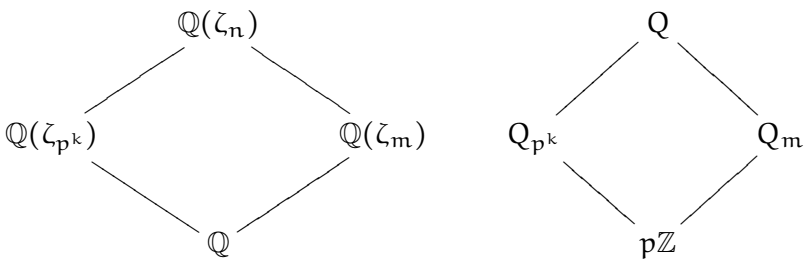
Εξετάζουμε τώρα τη γενική περίπτωση. Ισχύει το ακόλουθο:

Θεώρημα VI.6.14 (Νόμος αναλύσεως κυκλοτομικών σωμάτων)**.** *Έστω p πρώτος αριθμός, $n = p^k \cdot m$, $p \nmid m$, $k \geq 1$. Τότε το ιδεώδες pS αναλύεται στο σώμα $L = \mathbb{Q}(\zeta_n)$ ως εξής:*

$$pS = (Q_1 \cdots Q_r)^e$$

$N_{L/\mathbb{Q}}(Q_i) = p^f$, όπου $e = \varphi(p^k)$, f είναι η τάξη του p στην ομάδα $(\mathbb{Z}/n\mathbb{Z})^*$ και $r = \frac{\varphi(n)}{e \cdot f}$.

Απόδειξη. Έχουμε το παρακάτω σχεδιάγραμμα σωμάτων:



Από το θεώρημα VI.6.13 έχουμε ότι

$$\varphi(p^k) = e(Q_{p^k}/p\mathbb{Z}) \leq e(Q/p\mathbb{Z}) = e.$$

Από το θεώρημα VI.6.10 έχουμε ότι

$$f(Q_m/p\mathbb{Z}) = \text{τάξη του } p \mod m \leq f(Q/p\mathbb{Z}) = f.$$

Επίσης

$$\begin{aligned} r_m &= \#\{Q_m \supset p\mathbb{Z}, \text{ στο } \mathbb{Q}(\zeta_m)\} = \frac{\varphi(m)}{f(Q_m/p\mathbb{Z})} \leq \\ &\leq r = \#\{Q_m \supset p\mathbb{Z}, \text{ στο } \mathbb{Q}(\zeta_n)\}. \end{aligned}$$

Αρκεί να δείξουμε ότι σε κάθε μία από τις παραπάνω ανισότητες ισχύει η ισότητα. Έχουμε

$$\varphi(p^k)f(Q_m/p\mathbb{Z})r_m = \varphi(p^k)\varphi(m) = \varphi(p^k m) = \varphi(n),$$

και

$$\varphi(p^k) \leq e, f(Q_m/p\mathbb{Z}) \leq f, r_m \leq r$$
$$e \cdot f \cdot r = \varphi(n),$$

συνεπώς παντού ισχύουν οι ισότητες και συνεπώς το θεώρημα έχει αποδειχτεί. □

VI.6.4 Νόμος ανάλυσης στις επεκτάσεις Kummer

Αλγεβρική θεωρία

Έστω K ένα σώμα, $m \in \mathbb{N}$, και p η χαρακτηριστική του K. Υποθέτουμε ότι $p \nmid m$ και ότι το K περιέχει τις m-ρίζες της μονάδας.

Ορισμός VI.6.15. Έστω $L = K(\alpha)$, όπου $\alpha^m = a \in K^*$. Η επέκταση L/K, λέγεται επέκταση Kummer.

Παρατήρηση VI.6.16. Το σώμα L γράφεται $L = K(\sqrt[m]{a})$, και $\alpha = \sqrt[n]{a}$ είναι μια οποιαδήποτε ρίζα του πολυωνύμου $X^m - a$.

Αλγεβρικά θεωρήματα

1. Η επέκταση L/K είναι *κυκλική*. Αν $[L : K] = n$, τότε $n \mid m$ και ένας γεννήτορας αυτομορφισμός της ομάδας $\mathrm{Gal}(L/K)$ είναι ο
$$\sigma : \sqrt[m]{a} \longmapsto \zeta_n \sqrt[m]{a},$$
όπου ζ_n μια πρωταρχική n-στή ρίζα της μονάδας.
2. Κάθε κυκλική επέκταση L/K, βαθμού επέκτασης $[L : K] = n \mid m$ είναι μια επέκταση Kummer, $L = K(\sqrt[m]{a})$, $a \in K^*$.
3. Έστω L/K επέκταση Kummer, $[L : K] = n \mid m$. Τότε $L = K(\sqrt[n]{b})$, με $b \in K^*$.

Για αποδείξεις παραπέμπουμε στην πτυχιακή εργασία της Ανθής Ζερβού «Πολυώνυμα και Θεωρία Galois» [15].

Έστω τώρα K ένα αλγεβρικό σώμα αριθμών το οποίο περιέχει τις m-στές ρίζες της μονάδας. Από το 3. έπεται ότι, αν L/K επέκταση του Kummer, $[L : K] = n \mid m$ και $L = K(\sqrt[n]{b})$, $b \in K^*$. Ιδιαίτερα, ισχύει ότι υπάρχει $a \in R_K$:

$$L = K(\sqrt[n]{a}).$$

Αφού $b \in K^*$, γράφεται $b = u/v$, $u, v \in R_K$. Επομένως $b = uv^{n-1}/v^n$ συνεπώς $\sqrt[n]{b} = \sqrt[n]{a}/v$, όπου $a := uv^{n-1} \in R_K$ και $L = K(\sqrt[n]{a})$.

Από εδώ και κάτω, το K θα είναι αλγεβρικό σώμα αριθμών το οποίο περιέχει τις m-στές ρίζες της μονάδας.

Λήμμα VI.6.17. *Έστω* L/K *μια επέκταση Kummer,* $L = K(\sqrt[n]{a})$, $[L : K] = n \mid m$, P *ένα πρώτο ιδεώδες του* R_K*, για το οποίο το* a *είναι* P*-ακέραιο, δηλαδή* $\nu_P(a) \geq 0$*, τότε αν το* P *διακλαδίζεται στο* L*, τότε* $P \mid n$ *είτε* $P \mid a$.

Απόδειξη. Έστω $\langle a \rangle = A/B$, A, B ιδεώδη του R_K πρώτα μεταξύ τους δηλαδή $\text{Μ.Κ.Δ.}(A, B) = R_K$. Λόγω της υπόθεσης $\nu_P(a) \geq 0$, έπεται ότι $\nu_P(B) = 0$.

Έστω, η ανάλυση του B σε γινόμενο πρώτων ιδεωδών,

$$B = \prod_{i=1}^{s} P_i^{e_i}, e_i > 0 \text{ για } i = 1, 2, \ldots, s.$$

Θεωρούμε το σύστημα

$$\begin{aligned} X &\equiv 0 \mod P_i^{e_i}, i = 1, 2, \ldots, s \\ X &\equiv 1 \mod P \end{aligned}$$

Από το θεώρημα του Κινέζου, έχουμε ότι το σύστημα έχει λύση, έστω $\nu \in R_K$. Αυτό σημαίνει ότι $B \mid \nu$ ενώ $P \nmid \nu$. Έστω $a' = \nu^n a \in R_K$. Είναι φανερό ότι $L = K(\sqrt[n]{a'})$ και $\nu_P(a') = \nu_P(a)$. Επομένως, χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $a \in R_K$. Σύμφωνα με το 1. στη σελίδα 114 το $L = K(\alpha)$, $\alpha = \sqrt[n]{a} \in R_L$. Το πολυώνυμο $f(X) = X^n - a$, είναι ανάγωγο υπεράνω του K. Αφού $L = K(\alpha)$, έχουμε: Αν το P διακλαδίζεται στην επέκταση L/K έπεται ότι $P \mid D_{L/K}(\alpha)$. Η διακρίνουσα του α, υπολογίζεται

$$D_{L/K}(\alpha) = n^n a^{n-1}.$$

Επομένως, αν P διακλαδίζεται στο K, τότε $P \mid n$ είτε $P \mid a$. □

Το αντίστροφο είναι προφανές. Επομένως έχουμε το

Πόρισμα VI.6.18.

$$P \mid D_{L/K}(\alpha) \Leftrightarrow (P \mid n \text{ είτε } P \mid a)$$

Λήμμα VI.6.19. *Έστω* $L = K(\alpha)$, $\alpha^n = a \in K^*$, $[L : K] = n$ *και πρώτο ιδεώδες του* R_K, $P \nmid n$. *Τότε ισχύουν,*

(a) Αν $\nu_P(a) \equiv 0 \mod n$*, τότε το* P *δεν διακλαδίζεται στην* L/K.

(b) Αν $\nu_P(a) = 1$*, τότε το* P *διακλαδίζεται πλήρως στην* L/K*, δηλαδή* $P = Q^n$*,* Q *πρώτο ιδεώδες του* R_L *και* $Q = \langle P, \alpha \rangle$.

Απόδειξη. (a) Έστω $\nu_P(a) = \ell n$. Επιλέγουμε ένα $\pi \in P \backslash P^2$. Το $\nu_P(\pi) = 1$ και θεωρούμε το στοιχείο

$$a' := a\pi^{-n\ell}.$$

Επομένως, $L = K(\sqrt[n]{a'})$ και $\nu_P(a') = 0$. Συνεπώς $P \nmid n$ εξ υποθέσεως και $P \nmid a'$, άρα από το λήμμα VI.6.17, έπεται ότι το P δεν διακλαδίζεται στην επέκταση L/K.

(b) Το πολυώνυμο $f(x) = x^n - a \in K[x]$ είναι μονικό και έχει ως ρίζα του τον αριθμό $\alpha = \sqrt[n]{a}$. Επειδή $[L : K] = n$, έπεται ότι αυτό είναι το $\text{Irr}(\alpha, K)$. Λόγω της υπόθεσης ότι $\nu_P(a) = 1$, έπεται ότι το πολυώνυμο $f(x)$ είναι πολυώνυμο Eisenstein ως προς το πρώτο ιδεώδες P. Αυτό σημαίνει VI.5.20, X.3.42 το P αναλύεται πλήρως στην επέκταση L/K $PR_L = Q^n$, Q πρώτο του R_L και $Q = \langle P, \alpha \rangle = PR_L + \alpha R_L$.

□

Θεώρημα VI.6.20 (Νόμος ανάλυσης σε επεκτάσεις Kummer). *Έστω* $L = K(\sqrt[n]{a})$, $a \in R_K$, $[L:K] = n$ *και* P *πρώτο ιδεώδες του* K, $P \nmid n$.

(a) Ο δείκτης διακλάδωσης του P *στην επέκταση* L/K *είναι*

$$e_P(L/K) = \frac{n}{(v_P(a), n)}.$$

(b) Έστω $P \nmid a$. *Από το λήμμα VI.6.19 έπεται ότι το* P *δεν διακλαδίζεται στην επέκταση* L/K. *Ο βαθμός αδρανείας* f_P *του* P *στην επέκταση* L/K *είναι ο ελάχιστος φυσικός αριθμός* t *με την ιδιότητα*

$$a^t \equiv_n 1 \mod P,$$

δηλαδή

$$f_P = f_P(L/K) = \min\{t \in \mathbb{N} : a^t \equiv_n 1 \mod P\}.$$

Συνεπώς το P *αναλύεται στο* L *σε γινόμενο* n/f_P *πρώτων ιδεωδών του σώματος* L

Επεξηγήσεις:

1. Δεδομένου ότι η επέκταση L/K είναι επέκταση Galois, τόσο ο δείκτης διακλάδωσης, όσο και ο βαθμός αδρανείας εξαρτάται μόνο από το P. Νομιμοποιούνται επομένως οι συμβολισμοί $e_P(L/K)$ και $f_P(L/K)$.

2. Έστω R ακέραια περιοχή και P πρώτο ιδεώδες αυτής. Το υποσύνολο

$$R_P = \left\{ \frac{a}{b} : a \in R, b \in R \backslash P \right\}$$

του σώματος $\mathrm{Quot}(R)$ είναι *τοπικός δακτύλιος*, δηλαδή έχει μοναδικό πρώτο ιδεώδες το $R_P P$. Στον δακτύλιο R_P, ορίζεται η ισοτιμία

$$c \equiv_n c' \mod P, c, c' \in R_P$$

ακριβώς τότε όταν υπάρχει $x \in R_P$ για το οποίο ισχύει

$$c \equiv c' \cdot x^n \mod P.$$

Πρόκειται για την n-ισοτιμία modulo P. Επομένως, $c \equiv_n 1 \mod P$ αν και μόνο αν υπάρχει $x \in R_P$ τέτοιο ώστε $c = x^n \mod P$. Επίσης για $n = 2$ ισχύει

$$c \equiv_2 1 \mod P \Leftrightarrow (\text{το } c \text{ είναι τετραγωνικό υπόλοιπο mod} P).$$

Συνεπώς το a^t είναι n-στό υπόλοιπο modulo P αν και μόνο αν υπάρχει $z \in (R_K)_P$ για το οποίο ισχύει

$$a^t = z^n \mod (R_K)_P.$$

3. Αν $a \in R_K$, τότε ισχύει

$$a^t \equiv_n 1 \mod P(R_K)_P \Leftrightarrow a^t \equiv 1 \mod P.$$

Πράγματι, η κατεύθυνση "$\Leftarrow$" ισχύει αφού $R_K \subset (R_K)_P \cdot P$. Για την κατεύθυνση "$\Rightarrow$". Αν

$$a^t \equiv_n 1 \mod (R_K)_P \cdot P \Rightarrow a^t \equiv z^n \mod P \cdot (R_K)_P,$$

για κάποιο $z \in (R_K)_P$. Επιλέγουμε ένα $z' \in R_K$ για το οποίο ισχύει

$$z' \equiv z \mod P(R_K)_P.$$

Αυτό είναι δυνατό, αφού ισχύει

$$\frac{R_K}{P} \cong \frac{(R_K)_P}{P(R_K)_P}$$

Πόρισμα VI.6.21. *Υποθέτουμε ότι ισχύουν οι υποθέσεις του θεωρήματος* $(P \nmid n)$. *Ισχύουν*

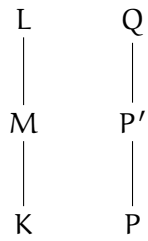
(a) Το P *δεν διακλαδίζεται στο* L *αν και μόνο αν* $\nu_P(a) \equiv 0 \mod n$.

(b) Το P *διακλαδίζεται πλήρως στο* L *αν και μόνο αν ο* $\nu_P(a)$ *είναι σχετικά πρώτος προς τον* n.

Απόδειξη. Άμεση συνέπεια του (a) του θεωρήματος □

Απόδειξη. (Του θεωρήματος)

Ο στόχος μας είναι να βρούμε ένα ενδιάμεσο σώμα M, έτσι ώστε το P να μην διακλαδίζεται στο M, $e(P'/P) = 1$ ενώ το P' να διακλαδίζεται πλήρως στο $e(Q/P') = n$.



Έστω $d := (\nu_P(a), n)$. Επομένως υπάρχουν ακέραιοι

$$\ell_0, m_0 \in \mathbb{Z} : d = \ell_0 \nu_P(a) + m_0 n.$$

Ψάχνουμε μια ανάλογη σχέση της μορφής

$$d = \ell \cdot \nu_P(a) + mn,$$

αλλά με $(\ell, n) = 1$. Αυτό δεν ισχύει πάντα. (Για παράδειγμα, το $2 = (4,6) = 2 \cdot 4 - 1 \cdot 6$, αλλά $2 = -4 + 6$).

Το

$$1 = \ell_0 \frac{\nu_P(a)}{d} + m_0 \frac{n}{d} = \ell_0 \cdot s + m_0 \cdot r.$$

Επομένως,

$$\ell \cdot \nu_P(a) + m \cdot n = d \Leftrightarrow 1 = \ell \cdot s + m \cdot r \Leftrightarrow (\ell_0 - \ell)s = (m - m_0)r$$

και $(s, r) = 1$. Άρα $s \mid (m - m_0)$ και $r \mid (\ell_0 - \ell)$. Συνεπώς

$$(\ell_0 - \ell)s = (m - m_0)r \Leftrightarrow \frac{\ell_0 - \ell}{r} = \frac{m - m_0}{s} \in \mathbb{Z}.$$

Το τελευταίο συνεπάγεται ότι υπάρχει $q \in \mathbb{Z}$ ώστε

$$\ell = \ell_0 - qr \text{ και } m = m_0 + qs.$$

Από τα παραπάνω συμπεραίνουμε ότι, κάθε $\ell \in \ell_0 + r\mathbb{Z}$ καθορίζει μια παράσταση της μορφής

$$d = \ell \cdot \nu_P(a) + m \cdot n.$$

Υπάρχουν ακέραιοι $\ell \in \ell_0 + r\mathbb{Z}$ με $(\ell, n) = 1$ αν και μόνο αν για κάθε πρώτο p, $p \mid n$, ισχύει $p \nmid \ell$.

Αν $p \mid n$ και $p \mid r$, τότε $p \nmid \ell$, αφού $(\ell, r) = 1$. Έστω λοιπόν $p_1, p_2, \ldots, p_s$ οι πρώτοι διαιρέτες του n οι οποίοι δεν διαιρούν το r. Τότε και ο $a = \prod_{i=1}^{s} p_i$ είναι πρώτος προς τον r, δηλαδή υπάρχει ένας $r' \in \mathbb{Z}$ για τον οποίο ισύει

$$rr' \equiv 1 \mod a$$

Αυτό σημαίνει ότι υπάρχει ένας ακέραιος q,

$$rq \equiv (\ell_0 - 1) \mod a$$

οπότε και το $\ell := \ell_0 - rq \equiv 1 \mod a$ και το $p_i \nmid \ell$, για κάθε $i = 1, 2, \ldots, s$, δηλαδή $(\ell, n) = 1$.

Έστω λοιπόν ότι $d = \ell \cdot \nu_P(a) + mn$, με $(\ell, n) = 1$. Θέτουμε $\beta := a^{\ell} \pi^{mn}$, όπου π ένα πρώτο στοιχείο του P, δηλαδή $\pi \in P \backslash P^2$. Ισχύει $L = K(\sqrt[n]{\beta})$. Λόγω της επιλογής του β, ισχύει

$$K(\sqrt[n]{\beta}) \subset L.$$

Το $(\ell, n) = 1$, συνεπώς υπάρχει $\ell' \in \mathbb{Z}$ ώστε $\ell \cdot \ell' \equiv 1 \mod n$ συνεπώς $\ell \cdot \ell' = 1 + qn$, $q \in \mathbb{Z}$. Επομένως

$$\beta^{\ell'} = a^{\ell\ell'}\pi^{mn\ell'} = aa^{qn}\pi^{mn\ell} \Rightarrow a = \beta^{\ell'}(a^{-q}\pi^{-m\ell})^n.$$

Το $a^{-q}\pi^{-m\ell} \in K$, και επειδή $(\ell', n) = 1$ έπεται ότι

$$L = K(\sqrt[n]{a}) \subset K(\sqrt[n]{\beta}),$$

δηλαδή η ισότητα.

Γράφουμε τώρα το $n = dr$, οπότε έχουμε το ακόλουθο σχήμα

$$\begin{array}{c} L = K(\sqrt[n]{\beta}) = M(\sqrt[r]{\beta_0}) \\ | \\ M = K(\sqrt[d]{\beta}) \\ | \\ K \end{array}$$

όπου το β_0 είναι μια d-στή ρίζα του β. Η επέκταση M/K, με $M = K(\sqrt[d]{\beta})$ είναι μια επέκταση Kummer βαθμού d και η L/M, με $L = M(\sqrt[r]{\beta_0})$ είναι επίσης μια Kummer επέκταση βαθμού r. Πράγματι, το K περιέχει τις n-ρίζες της μονάδας (αφού $n \mid m$), συνεπώς περιέχει και τις r-ρίζες της μονάδας καθώς και τις d-ρίζες της μονάδας.

$$dr = n = [L : K] = [L : M][M : K],$$

αλλά $[L : M] \le r$ και $[M : K] \le d$. Επομένως $[L : M] = r$ και $[M : K] = d$. Το $P \nmid n$, άρα $P \nmid d$,

$$\nu_P(\beta) = \ell\nu_P(a) + mn = d \equiv 0 \mod d$$

Επομένως, από το λήμμα VI.6.19, έπεται ότι ο P δεν διακλαδίζεται στο M.

Έστω Q ένα πρώτο ιδεώδες του M, $Q \mid P$. Το $P \nmid n$ συνεπώς $P \nmid r \Leftrightarrow p \nmid r$, όπου $p \in P$. Επομένως και το $Q \nmid r$, αφού $p \in Q$. Ο βαθμός της επέκτασης $[L : M] = r$,

$$\nu_Q(\beta_0) = \frac{1}{d}\nu_Q(\beta_0^d) = \frac{1}{d}\nu_Q(\beta) = \frac{1}{d}e(Q/P)\cdot\nu_P(\beta),$$

αλλά το Q είναι μη-διακλαδιζόμενο υπεράνω του P και επομένως $\nu_Q(\beta_0) = \frac{1}{d}\nu_P(\beta) = 1$. Από το λήμμα VI.6.19 πάλι συνεπάγεται ότι το Q είναι στο L πλήρως διακλαδιζόμενο. Επομένως,

$$e_{L/K}(P) = e_{L/M}(Qe_{M/K}(P)) = [L : M] = r = \frac{n}{d}.$$

Απόδειξη του (b)

Από την υπόθεση $P \nmid a$, έπεται ότι το P δεν εμφανίζεται στην ανάλυση του $\langle a\rangle = aR_L$ σε γινόμενο πρώτων ιδεωδών, δηλαδή ότι $\nu_P(a) = 0$. Συνεπώς το P δεν διακλαδίζεται στο L.

Το $a \in R_K$ και $\alpha \in L$, για το οποίο ισχύει $\alpha^n = a$. Επειδή $P \nmid a$ και $P \nmid n$ (γενική υπόθεση στο Θεώρημα), από το πόρισμα VI.6.18 έπεται ότι $P \nmid D_{L/K}(\alpha)$. Αυτό σημαίνει, κατά μείζονα λόγο, ότι $P \nmid [R_L : R_K[\alpha]]$ οπότε μπορούμε να εφαρμόσουμε τον νόμο ανάλυσης για το P. Το $\mathrm{Irr}(\alpha, K) = x^n - a$, αφού $[K(\alpha) : K] = [L : K] = n$. Το

$$X^n - \overline{a} = \prod_{i=1}^{g}\psi_i(x),$$

με $\psi_i(x) \in \frac{R_K}{P}[x]$ ανάγωγα και ανά δύο διαφορετικά. Επίσης, $\deg\psi_i = f_{L/K}(P) =: f$, για $i = 1, 2, \ldots, g$. Έστω Q ένα πρώτο ιδεώδες του L, $Q \mid P$. Αφού το $\alpha \in R_L$, έχουμε ότι $\overline{\alpha} \in R_L/Q$ και

είναι ρίζα του πολυωνύμου $x^n - \overline{a}$. Επομένως το $\overline{\alpha}$ είναι ρίζα ενός εκ των πολυωνύμων ψ_i. Το ψ_i όμως είναι ανάγωγο υπεράνω του $\frac{R_K}{P}[x]$, δηλαδή αν $\overline{K} := R_K/P$, $\overline{L} = R_L/Q$,

$$[\overline{K}(\overline{\alpha}) : \overline{K}] = \deg(\psi_i) = f = [\overline{L} : \overline{K}].$$

Επομένως $\overline{L} = \overline{K}(\overline{\alpha})$. Στη συνέχεια θα αποδείξουμε ότι η επέκταση $\overline{L}/\overline{K}$ είναι επέκταση Kummer. Πράγματι:

(i) $\overline{\alpha}^n = \overline{a} \in \overline{K}$.

(ii) Το $\overline{K}$ περιέχει τις n-ρίζες της μονάδας, αφού το $X^n - 1$ αναλύεται στο K πλήρως και έχει τις ρίζες του στο K. Επομένως το $X^n - \overline{1}$ αναλύεται πλήρως στον $\overline{K}[X]$.

(iii) Το $p = \mathrm{char}(\overline{K}) \nmid n$.

Από τα παραπάνω συνάγουμε ότι

$$[\overline{K}(\overline{\alpha}) : \overline{K}] = [\overline{K}(\sqrt[n]{\overline{a}}) : \overline{K}].$$

Αλλά από την αλγεβρική θεωρία των επεκτάσεων Kummer, ισχύει

$$[\overline{K}(\sqrt[n]{\overline{a}}) : \overline{K}] = \mathrm{ord}(\overline{a} \mod (\overline{K}^*)^n) = \min\{t \in \mathbb{N} : \overline{a}^t \in (\overline{K}^*)^n\}.$$

Τώρα,

$$\begin{aligned} \overline{a}^t \in (\overline{K}^*)^n &\Leftrightarrow (\text{Υπάρχει } \gamma \in \overline{K}^* : \overline{a}^t = \gamma^n) \\ &\overset{\nu_P(a)=0}{\Leftrightarrow} (\text{Υπάρχει } c \in R_K \text{ τέτοιο ώστε } a^t = c^n \mod P) \\ &\Leftrightarrow (\text{Το } a^t \text{ είναι } n\text{-στό υπόλοιπο modulo } P). \end{aligned}$$

Έστω τέλος a οποιοδήποτε στοιχείο του K, για το οποίο ισχύει $\nu_P(a) = 0$. Στην απόδειξη του λήμματος VI.6.17, έχουμε δείξει ότι υπάρχει $\nu \in R_K$ τέτοιο ώστε

$$\beta := a\nu^n \in R_K \text{ και } P \nmid \beta,$$

δηλαδή $\nu_P(\beta) = 0$. Το

$$f_{L/K}(P) = \min\{t \in \mathbb{N} : \beta^t \ \ n\text{-στό υπόλοιπο modulo } P\}.$$

Αλλά, το β^t είναι n-στό υπόλοιπο modulo P συνεπώς υπάρχει $c \in R_K$, για το οποίο ισχύει

$$a^t\nu^{nt} \equiv c^n \mod P.$$

Το $P \nmid \nu$, συνεπώς το ν είναι μονάδα του δακτυλίου $(R_K)_P$, δηλαδή

$$a^t \equiv \left(\frac{c}{\nu^t}\right)^n \mod (R_K)_P P.$$

□

VI.7 Ένα ενδιαφέρον παράδειγμα

Έστω $K = \mathbb{Q}(\alpha)$, όπου $\alpha = \sqrt[p]{2}$, $p \in \mathbb{P}$. Από το θεώρημα του Fermat γνωρίζουμε ότι ισχύει $2^p \equiv 2 \mod p$. Υποθέτουμε τώρα ότι για τον πρώτο αριθμό p ισχύει $2^p \not\equiv 2 \mod p^2$. Να αποδειχθεί ότι αν ένας πρώτος q διαιρεί τον δείκτη $[R_K : \mathbb{Z}[\alpha]]$, τότε θα διαιρεί και το γινόμενο $2p$. Στη συνέχεια να αποδειχτεί ότι το $2 \nmid [R_K : \mathbb{Z}[\alpha]]$ καθώς και ότι $p \nmid [R_K : \mathbb{Z}[\alpha]]$. Ισχύει ότι $R_K = \mathbb{Z}[\alpha]$.

Πράγματι, υπολογίζουμε τη διακρίνουσα του α:

$$D_K(\alpha) = (-1)^{\frac{p(p-1)}{2}} 2^{p-1} p^p,$$

και το πρώτο μέρος αφού μοναδικοί υποψήφιοι διαιρέτες του δείκτη είναι τα 2 και p. Το ανάγωγο πολυώνυμο $\mathrm{Irr}(\sqrt[p]{2}, \mathbb{Q}) = x^2 - 2$, και με χρήση του κριτηρίου Eisenstein έχουμε $2 \nmid [R_K : \mathbb{Z}[\alpha]]$. Θέτουμε $\beta = \alpha - 2$ οπότε η $\alpha^p = 2$ δίνει $(\beta + 2)^p = 2$, το οποίο αναπτύσσεται

$$\beta^p + \binom{p}{1}\beta^{p-1}2 + \binom{p}{2}\beta^{p-2}2^2 + \cdots + \binom{p}{p-1}\beta 2^{p-1} + 2^p.$$

Το β είναι ρίζα πολυωνύμου Eisenstein ως προς p και ως προς 2. Για τον πρώτο p χρειαζόμαστε το ότι $2^p - 2 \equiv 0 \mod p$ ενώ $2^p - 2 \not\equiv 0 \mod p^2$. Συνεπώς $p \nmid [R_K : \mathbb{Z}[\alpha]]$. Επομένως $R_K = \mathbb{Z}[\sqrt[p]{2}]$. Ισχύει και το αντίστροφο

Θα αποδείξουμε ότι $\langle p \rangle = P^2$, όπου $P = \langle p, \sqrt[p]{2} - 2 \rangle$. Στη συνέχεια θα αποδειξουμε ότι $\sqrt[p]{2} - 2 \notin P^2$. Συμπεράνετε ότι το $P^2 \nmid N_{K/\mathbb{Q}}(\sqrt[p]{2} - 2)$ και θα καταλήξουμε στο συμπέρασμα ότι $2^p \not\equiv 2 \mod p^2$.

Πράγματι, ισχύει ότι $K = \mathbb{Q}(\sqrt[p]{2}) = \mathbb{Q}(\sqrt[p]{2} - 2)$ και $\mathbb{Z}[\sqrt[p]{2}] = \mathbb{Z}[\sqrt[p]{2} - 2]$. Το $\beta = \sqrt[p]{2} - 2$ είναι ρίζα του πολυωνύμου

$$f(x) = x^p + \text{οροι με συντελεστή διαιρετό με } p$$

συνεπώς

$$\overline{f}(x) = x^p \mod p$$

και έτσι έχουμε το πρώτο. Από αυτό έχουμε $p \in P^2$ αφού $p \in P^p$, $p \geq 2$. Αν και το $\sqrt[p]{2} - 2 \in P^2$, τότε $P = \langle 2, \sqrt[p]{2} - 2 \rangle \subset P^2$ και συνεπώς $P = P^2$, άτοπο αφού P πρώτο ιδεώδες σε δακτύλιο Dedekind. Επομένως $\sqrt[p]{2} - 2 \notin P^2$. Από αυτό έχουμε ότι $P^2 \nmid \langle \sqrt[p]{2} - 2 \rangle$ συνεπώς $p^2 = N_{K/\mathbb{Q}}(P^2) \nmid N_{K/\mathbb{Q}}(\sqrt[p]{2} - 2) = 2^p - 2$.

Σημείωση VI.7.1. 1. Υπενθυμίζουμε το θεώρημα του A. Wieferich (1909) ότι αν η εξίσωση Fermat

$$X^p + Y^p = Z^p,$$

p πρώτος, $p \neq 2$ έχει μη τετριμμένη ακέραια λύση (x, y, z) ώστε $p \nmid xyz$, τότε $2^p \equiv 2 \mod p^2$.

2. Είναι γνωστό ότι για $p < 5 \cdot 10^{11}$ η ισοτιμία ισχύει μόνο για $p = 1093$ και $p = 3511$. Αυτό σημαίνει ότι ο δακτύλιος των ακεραίων αλγεβρικών του $\mathbb{Q}(\sqrt[p]{2})$ είναι ο $\mathbb{Z}[\sqrt[p]{2}]$ για όλους τους πρώτους $p < 1093$ αλλά όχι για το 1093.

3. Ο J.H. Silverman απέδειξε [12] ότι αν ισχύει η εικασία ABC, τότε υπάρχει άπειρο πλήθος πρώτων για τους οποίους ισχύει $2^p \not\equiv 2 \mod p^2$ (*Wieferich πρώτοι*).

4. Δεν είναι μέχρι σήμερα γνωστό αν υπάρχουν άπειροι πρώτοι για τους οποίους ισχύει $2^p \not\equiv 2 \mod p^2$.

5. Υπάρχει και η παρακάτω γενίκευση

Πρόταση VI.7.2. *Αν $n > 1$ και m ελεύθερος τετραγώνου για τον οποίο ισχύει*

$$m^p \not\equiv m \mod p^2$$

για όλους τους πρώτους p, $p \mid n$, τότε το σώμα $\mathbb{Q}(\sqrt[n]{m})$ είναι μονογενεϊκό (monogeneity), δηλαδή $R_K = \mathbb{Z}[\sqrt[n]{m}]$ [7], [5].

VI.8 Ασκήσεις

1. Θεωρούμε το σώμα $K = \mathbb{Q}(\sqrt[3]{2})$. Να υπολογιστεί η διακρίνουσα και να βρεθεί μια βάση ακεραιότητας αυτού. Έστω p πρώτος, $p \neq 2, 3$.
   (α') Να υπολογιστεί η ανάλυση του p στο K για $p = 5, 7, 11, 13$ και 31.
   (β') Γενικά αν $p \equiv 2 \mod 3$ να αποδειχθεί ότι $pR_K = P_1P_2$ με $f(P_1/p) = 1$ και $f(P_2/p) = 2$.
   (γ') Αν $p \equiv 1 \mod 3$, να αποδειχθεί ότι το p ή αναλύεται πλήρως $pR_K = P_1P_2P_3$, $N_{K/\mathbb{Q}}(P_i) = p$, $i = 1, 2, 3$ ή αδρανεί στο K, $pR_K = P$, $N_{K/\mathbb{Q}}(P) = p^3$. Υπόδειξη: θεώρημα 5.4.29 [14].
   (δ') Στην περίπτωση που $p \equiv 1 \mod 3$, πότε ισχύει η πλήρης ανάλυση και πότε η αδράνεια; (Ψάξτε το στη Βιβλιογραφία! Απάντηση στο μεθεπόμενο κεφάλαιο)
   (ε') Τέλος να υπολογισθεί η ανάλυση των $p = 2$ και $p = 3$ στο σώμα K.
2. Έστω $K = \mathbb{Q}(\sqrt[3]{10})$.
   (α') Να υπολογιστεί η διακρίνουσα και μια βάση ακεραιότητας του K.
   (β') Να υπολογιστεί η ανάλυση του $p = 7$
   (γ') Επίσης η ανάλυση του $p = 11$
   (δ') Το ίδιο για την ανάλυση του $p = 37$
   (ε') Το ίδιο για την ανάλυση του $p = 2, 3, 5$.
3. Να αποδειχθεί ότι κανένας πρώτος αριθμός p δεν αδρανεί, δηλαδή το pR_K παραμένει πρώτο ιδεώδες, στο σώμα $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
4. Να υπολογιστεί ο αριθμός κλάσεων του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{-21})$ καθώς και η δομή της ομάδας κλάσεων ιδεωδών αυτού.
5. Έστω α περιττός ακέραιος, $\alpha > 1$. Αν $d = 3^\alpha - x^2$ ελεύθερο τετραγώνου και x περιττός, $x^2 < 3^\alpha/2$. Να αποδειχθεί ότι το σώμα $\mathbb{Q}(\sqrt{-d})$ έχει στην ομάδα κλάσεών του ένα στοιχείο τάξης α.
6. Έστω $K = \mathbb{Q}(\zeta_8)$, όπου $\zeta_8 = e^{2\pi i/8}$. Να αποδειχθεί ότι κανένας πρώτος αριθμός p δεν αδρανεί στο K.
7. Έστω p περιττός πρώτος. Αν α είναι ένας ακέραιος ο οποίος δεν είναι p-στη δύναμη, τότε ο p διακλαδίζεται στο σώμα $K = \mathbb{Q}(\sqrt[p]{\alpha})$.

Βιβλιογραφία

[1] Bourbaki, N. *Commutative Algebra. Chapters 1-7*. Elements of Mathematics (Berlin). Translated from the French, Reprint of the 1972 edition. Berlin: Springer-Verlag, 1989, pp. xxiv+625. ISBN: 3-540-19371-5.

[2] Cohen, H. *A Course in Computational Algebraic Number Theory*. Vol. 138. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993, pp. xii+534. ISBN: 3-540-55640-0.

[3] Cox, D. A. *Primes of the Form x^2+ny^2, Fermat, class field theory, and complex multiplication*. 2nd edition. Pure and Applied Mathematics. John Wiley & Sons, Inc., 2013, pp. xviii+356. ISBN: 978-1-118-39018-4.

[4] Curtis, C. W. & Reiner, I. *Representation theory of finite groups and associative algebras*. Reprint of the 1962 original. AMS Chelsea Publishing, Providence, RI, 2006, pp. xiv+689. ISBN: 0-8218-4066-5.

[5] Fadil, L. E. *A note ON MONOGENEITY of pure number fields*. 2021. URL: arXiv:2106.00004.

[6] Fröhlich, A. & Taylor, J. M. *Algebraic number theory*. Vol. 27. Cambridge Studies in advanced mathematics. Cambridge: Cambridge University Press, 1993, pp. xiv+355. ISBN: 0-521-43834-9.

[7] Gassert, T. A. *A note on the monogeneity of power maps*. *Albanian J. Math.* 11.1 (2017), pp. 3–12.

[8] MacKenzie, R. & Scheuneman, J. *A number field without a relative integral basis*. *Amer. Math. Monthly* 78 (1971), pp. 882–883. ISSN: 0002-9890.

[9] Milne, J. S. *Algebraic Number Theory (v3.08)*. Available at www.jmilne.org/math/. 2020.

[10] Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*. 3rd edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004, pp. xii+708. ISBN: 3-540-21902-1.

[11] Ribenboim, P. *Classical Theory of Algebraic Numbers*. Universitext. Springer-Verlag, New York, 2001, pp. xxiv+681. ISBN: 0-387-95070-2.

[12] Silverman, J. H. *Wieferich's criterion and the* abc*-conjecture*. *J. Number Theory* 30.2 (1988), pp. 226–237. ISSN: 0022-314X.

[13] Stein, W. *Algebraic Number Theory, a computational approach*. *Harvard. Massachusetts* (2012). URL: https://wstein.org/books/ant/ant.pdf.

[14] Αντωνιάδης, I. A. & Κοντογεώργης, Α. *Θεωρία Αριθμών και Εφαρμογές*. Κάλλιπος, 2015, pp. ix+315. ISBN: 978-618-82124-5-9. URL: https://eclass.uoa.gr/modules/document/file.php/MATH443/NumberTheoryNov2016.pdf.

[15] Ζερβού, Α. *Πολυώνυμα και Θεωρία Galois*. MA thesis. Πανεπιστήμιο Κρήτης, 2015.

VII

Θεωρία (διακλάδωσης) του Hilbert

VII.1 Εισαγωγή

Στο κεφάλαιο αυτό θα ασχοληθούμε με τη θεωρία διακλάδωσης του Hilbert. Πρόκειται για το αριθμητικό ανάλογο της Θεωρίας Galois. Όπως η αλγεβρική δομή μιας επέκτασης Galois L/K απεικονίζεται στην ομάδα Galois $\mathrm{Gal}(L/K)$ της επέκτασης αυτής, έτσι και η αριθμητική δομή, δηλαδή η γέννεση κάθε πρώτου ιδεώδους Q του σώματος από το πρώτο ιδεώδες $P = K \cap Q$ του K, σχετίζεται με τις ιδιότητες της ομάδας Galois $\mathrm{Gal}(L/K)$.

Εδώ αναφερόμαστε σε επεκτάσεις αλγεβρικών σωμάτων αριθμών. Έτσι αν $L = K(\theta)$, $\theta \in R_K$ η επέκταση L/K είναι Galois τότε και μόνο τότε, όταν όλες οι ρίζες του ανάγωγου πολυωνύμου $f(x) = \mathrm{Irr}(\theta, K)$ ανήκουν στο L.

Γενικά μπορούμε να ορίσουμε την Galois θήκη μιας επέκτασης L/K αλγεβρικών σωμάτων αριθμών. Ορίζεται ως το ελάχιστο σώμα K^{gc} που περιέχει το L και η επέκταση K^{gc}/K είναι επέκταση Galois. Αν $L = K(\theta)$, τότε η Galois θήκη της L/K είναι το σώμα K^{gc} το οποίο παράγεται από το K με επισύναψη όλων των ριζών του ανάγωγου πολυωνύμου $f(x) = \mathrm{Irr}(\theta, K)$. Πόσο μεγάλη μπορεί να είναι η επέκταση K^{gc}/K σε σχέση με την επέκταση L/K; Γνωρίζουμε ότι η ομάδα $\mathrm{Gal}(K^{gc}/K)$ εμφυτεύεται στην ομάδα μεταθέσεων των K-συζυγών στοιχείων του θ. Επομένως, αν $L = [K(\theta) : K] = n$, τότε η ομάδα Galois

$$\mathrm{Gal}(K^{gc}/K) \hookrightarrow S_n.$$

Η τάξη της S_n είναι $|S_n| = n!$, συνεπώς $[K^{gc} : K] \mid n!$. Για παράδειγμα, αν $[L : K] = 2$, τότε $[K^{gc} : K] \mid 2! = 2$, οπότε $K^{gc} = L$ δηλαδή η L/K είναι πάντοτε αβελιανή.

Αν $[L : K] = 3$, τότε η Galois θήκη της L/K, είναι μια τετραγωνική επέκταση του L με Galois θήκη K^{gc} ώστε

$$\mathrm{Gal}(K^{gc}/K) \cong S_3$$

ή $K^{gc} = L$, οπότε L/K Galois, κυκλική βαθμού 3.

Επειδή γνωρίζουμε ότι η Galois θήκη για $n = 3$ προκύπτει από επισύναψη στο L της τετραγωνικής ρίζας της διακρίνουσας $D_{L/K}(\theta)$, έπεται ότι η L/K είναι Galois ακριβώς τότε όταν η διακρίνουσα είναι τέλειο τετράγωνο στο K.

Στη συνέχεια θα μελετήσουμε τη δράση της $\mathrm{Gal}(L/K)$ στο σύνολο των πρώτων ιδεωδών του L που εμφανίζονται στην ανάλυση ενός πρώτου ιδεώδους P του L στην επέκταση L/K. Βέβαια η ομάδα Galois $\mathrm{Gal}(L/K)$ δρα και σε άλλα σύνολα του σώματος όπως:

- Ο δακτύλιος των ακεραίων αλγεβρικών R_L
- Η ομάδα των μονάδων $E(R_L)$
- Η ομάδα των κλάσεων ιδεωδών του L, $\mathfrak{K}_L = I_L/H_L$.

VII.2 Ομάδα ανάλυσης, αδράνειας

Στην παράγραφο αυτή υποθέτουμε ότι η επέκταση L/K των αλγεβρικών σωμάτων αριθμών $K \subset L$ είναι επέκταση του Galois και έστω $G = \mathrm{Gal}(L/K)$.

Έχουμε το σχήμα

$$\begin{array}{ccc} L & \text{——} & S \\ | & & | \\ | & & | \\ K & \text{——} & R \end{array} \qquad \begin{array}{c} Q \\ | \\ | \\ P \end{array}$$

Γνωρίζουμε ήδη ότι

$$PS = (Q_1 \cdots Q_r)^e, \quad N_{L/\mathbb{Q}}(Q_i) = N_{K/\mathbb{Q}}(P)^f \text{ και } efr = n.$$

Επειδή η G δρα μεταβατικά στο σύνολο των πρώτων ιδεωδών που επεκτείνουν το P, μπορούμε ακόμα να γράψουμε

$$PS = \prod_{\sigma \in G}{}' \sigma(Q)^e,$$

όπου το σ διατρέχει τα στοιχεία της G που δίνουν διαφορετικές μεταξύ τους εικόνες.

Το πρόβλημα τώρα είναι ποια είναι αυτά τα σ. Απάντηση σε αυτό το πρόβλημα, έδωσε αναπτύσσοντας μια ολόκληρη θεωρία, ο Γερμανός Μαθηματικός David Hilbert.

Ορισμός VII.2.1. Έστω $[L : K] = n$ και $Q \in \{Q_1, Q_2, \ldots, Q_r\}$. Τα υποσύνολα της G

$$\begin{aligned} G_Z = G_Z(Q/P) &= \{\sigma \in G : \sigma(Q) = Q\} \\ G_T = G_T(Q/P) &= \{\sigma \in G : \sigma(\alpha) \equiv \alpha \mod Q, \text{ για κάθε } \alpha \in S\} \\ G_{\Delta_i} = G_{\Delta_i}(Q/P) &= \{\sigma \in G : \sigma(\alpha) \equiv \alpha \mod Q^{i+1} \text{ για κάθε } \alpha \in S\}, \end{aligned}$$

οι οποίες προφανώς αποτελούν υποομάδες της G. Οι παραπάνω ομάδες λέγονται ομάδα ανάλυσης του Q υπεράνω του P, ομάδα αδράνειας του Q υπεράνω του P και ομάδα διακλάδωσης τάξεως i του Q υπεράνω του P. Τα αντίστοιχα μέσω της θεωρίας του Galois σώματα θα λέγονται:

$$\begin{aligned} K_Z = K_Z(Q/P) &\quad \textit{σώμα ανάλυσης του } Q \text{ υπεράνω του } P \\ K_T = K_T(Q/P) &\quad \textit{σώμα αδράνειας του } Q \text{ υπεράνω του } P \\ K_{\Delta_i} = K_{\Delta_i} &\quad \textit{σώμα διακλάδωσης τάξεως } i \text{ του } Q \text{ υπεράνω του } P \end{aligned}$$

Παρατήρηση VII.2.2. Η ομάδα αδράνειας είναι ομάδα διακλάδωσης τάξεως 0. Για λόγους ομοιομορφίας η ομάδα ανάλυσης συμβολίζεται και ως $G_{-1}(Q/P)$. Αν $\alpha \in Q$ και $\sigma \in G_T$ τότε $\sigma\alpha - \alpha \in Q$ και αφού $\alpha \in Q$ τότε και το $\sigma\alpha \in Q$. Άρα $\alpha \in \sigma^{-1}Q$, δηλαδή $Q \subset \sigma^{-1}Q$ και $\sigma Q \subset Q$. Γράφοντας την τελευταία σχέση για το σ^{-1} έχουμε

$$\sigma^{-1}(Q) \subset Q \Rightarrow Q \subset \sigma(Q),$$

δηλαδή $\sigma(Q) = Q$ και επομένως $\sigma \in G_Z$. Ώστε $G_Z \geq G_T$. Έχουμε λοιπόν την ακολουθία ομάδων:

$$G \geq G_Z \geq G_T \geq G_{\Delta_1} \geq G_{\Delta_2} \geq \cdots$$

και λόγω θεωρίας του Galois

$$K \leq K_Z \leq K_T \leq K_{\Delta_1} \leq K_{\Delta_2} \leq \cdots$$

για τα αντίστοιχα σώματα.

Το Q είναι πρώτο ιδεώδες του S αλλά και το $\sigma(Q)$ είναι επίσης πρώτο ιδεώδες του S και είναι σαφές ότι $\sigma(Q) \supset P$. Στο ερώτημα πώς σχετίζονται μεταξύ τους οι ομάδες του Hilbert (ανάλυσης, αδράνειας, διακλαδώσεως) μας απαντά η επόμενη απλή

Πρόταση VII.2.3. *Ισχύουν*

1. $G_Z(\sigma(Q)/P) = \sigma G_Z(Q/P)\sigma^{-1}$
2. $G_T(\sigma(Q)/P) = \sigma G_T(Q/P)\sigma^{-1}$
3. $G_{\Delta_i}(\sigma(Q)/P) = \sigma G_{\Delta_i}(Q/P)\sigma^{-1}$

Λόγω θεωρίας του Galois, ισχύει εντελώς ανάλογη πρόταση για τα αντίστοιχα σώματα.

Απόδειξη. Για το πρώτο: Έστω $\tau \in G_Z(\sigma(Q)/P)$ συνεπώς

$$\tau\sigma(Q) = \sigma(Q) \Rightarrow \sigma^{-1}\tau\sigma(Q) = Q \Rightarrow \sigma^{-1}\tau\sigma \in G_Z(Q/P)$$

δηλαδή

$$G_Z(\sigma(Q)/P) \subset \sigma G_Z(Q/P)\sigma^{-1}.$$

Έστω τώρα $\rho \in G_Z(Q/P)$ συνεπώς $\rho(Q) = Q$, οπότε

$$\sigma\rho\sigma^{-1}(\sigma Q) = \sigma\rho(Q) = \sigma(Q)$$

και τελικά

$$\sigma\rho\sigma^{-1} \in G_Z(\sigma(Q)/P) \text{ δηλαδή } \sigma G_Z(Q/P)\sigma^{-1} \subset G_Z(\sigma(Q)/P).$$

Συνεπώς ισχύει η (1). Εντελώς όμοια αποδεικνύονται και η (2) και (3). □

Πρόταση VII.2.4. *Ισχύουν*

$$G_T \lhd G_Z \text{ και } G_{\Delta_i} \lhd G_Z \text{ για κάθε } i \in \mathbb{N}.$$

Επομένως οι επεκτάσεις K_{Δ_i}/K_Z και K_T/K_Z είναι επεκτάσεις του Galois.

Απόδειξη. Έστω $\sigma \in G_Z$ και $\tau \in G_T$ συνεπώς

$$\tau(\alpha) \equiv \alpha \mod Q \text{ για κάθε } \alpha \in S. \tag{VII.1}$$

Όταν το α διατρέχει όλα τα στοιχεία του S, το ίδιο κάνει και το $\sigma(\alpha)$ καθώς και το $\sigma^{-1}(\alpha)$. Εφαρμόζοντας την ισοτιμία (VII.1) για $\sigma^{-1}(\alpha)$ για κάθε $\alpha \in S$ έχουμε:

$$\tau(\sigma^{-1}(\alpha)) \equiv \sigma^{-1}(\alpha) \mod Q \text{ για κάθε } \alpha \in S$$

δηλαδή

$$\sigma\tau\sigma^{-1}(\alpha) \equiv \alpha \mod Q$$

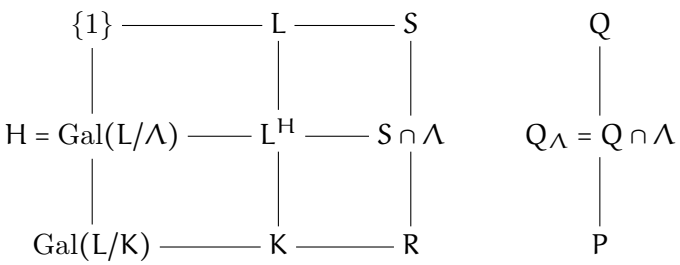
και συνεπώς $\sigma\tau\sigma^{-1} \in G_T$, άρα $\sigma G_T\sigma^{-1} \subset G_T$. Γράφουμε την τελευταία σχέση για σ^{-1} στη θέση του σ και έχουμε:

$$\sigma^{-1}G_T\sigma \subset G_T \Rightarrow G_T \subset \sigma G_T\sigma^{-1}.$$

Επομένως $\sigma G_T\sigma^{-1} = G_T$ για κάθε $\sigma \in G_Z$, επομένως $G_T \lhd G_Z$.

Ομοίως και για τις ομάδες διακλάδωσης. □

Έστω τώρα κάποιο ενδιάμεσο σώμα Λ



Έχουμε

$$\begin{aligned} G_Z(Q/Q_\Lambda) &= \{\sigma \in H : \sigma(Q) = Q\} \\ &= \{\sigma \in \mathrm{Gal}(L/K) : \sigma(Q) = Q \text{ και } \sigma|_\Lambda = \mathrm{Id}_\Lambda\} \\ &= H \cap G_Z(Q/P). \end{aligned}$$

Ανάλογα ισχύουν και για τις άλλες ομάδες του Hilbert.

Έστω τώρα $[G : G_Z] = g$ και

$$G = \bigcup_{i=1}^{g} \sigma_i G_Z$$

η ανάλυση της G σε αριστερές πλευρικές ομάδες της G_Z. Προφανώς $\sigma_i(Q) \neq \sigma_j(Q)$ για κάθε $i \neq j$, $i, j \in \{1, 2, \ldots, g\}$, διότι αν

$$\sigma_i(Q) = \sigma_j(Q) \text{ τότε } \sigma_j^{-1}\sigma_i(Q) = Q$$

και συνεπώς $\sigma_j^{-1}\sigma_i \in G_Z$, άρα $\sigma_i G_Z = \sigma_j G_Z$, οπότε και $i = j$.

Από την άλλη μεριά για τυχαίο $\sigma \in G$ υπάρχει $i \in \{1, 2, \ldots, r\}$ ώστε $\sigma = \sigma_i\tau$, $\tau \in G_Z$, συνεπώς $\sigma(Q) = \sigma_i\tau(Q) = \sigma_i(Q)$. Αποδείξαμε δηλαδή την

Πρόταση VII.2.5. *Ο δείκτης* $[G : G_Z] = r$ *και*

$$PS = (\sigma_1(Q)\sigma_2(Q)\cdots\sigma_r(Q))^e,$$

$$N_{L/\mathbb{Q}}(Q) = N_{K/\mathbb{Q}}(P)^{f(Q/P)}, \quad efr = n, \quad [G_Z : 1] = ef$$

και λόγω της θεωρίας Galois για τα αντίστοιχα σώματα έχουμε

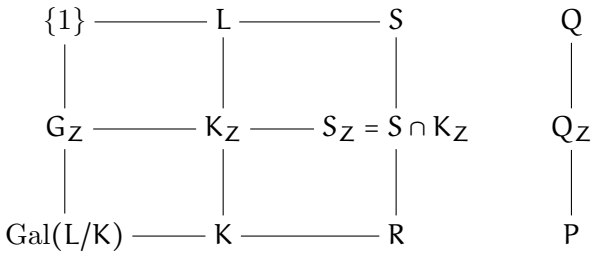
$$[K_Z : K] = r, [L : K_Z] = ef.$$

Σημείωση VII.2.6. Η πρόταση VII.2.5 δεν είναι τίποτε περισσότερο από το θεώρημα τροχιάς σταθεροποιητή της θεωρίας ομάδων.

Θεωρούμε τώρα την επέκταση του Galois L/K_Z. Ποια είναι η ομάδα ανάλυσης της επέκτασης αυτής; Έχουμε $G_Z(Q/Q_Z) = \mathrm{Gal}(L/K_Z) \cap G_Z(Q/P)$. Αλλά προηγούμενη πρόταση $\mathrm{GaL}(L/K_Z) = G_Z(Q/P)$ συνεπώς $G_Z(Q/Q_Z) = G_Z(Q/P) \cap G_Z(Q/P) = G_Z(Q/P)$, δηλαδή η αρχική ομάδα ανάλυσης της επέκτασης L/K, οπότε και το σώμα ανάλυσης

$$K_Z(Q/Q_Z) = K_Z(Q/P) = K_Z$$

Έχουμε το παρακάτω σχήμα:



Σύμφωνα με την τελευταία πρόταση το $Q_Z S_Z$ έχει ως μόνο πρώτο παράγοντα το Q, διότι $r = [K_Z : K_Z] = 1$, και συνεπώς

$$Q_Z S_Z = Q^{e'}$$

με $e' = e(Q/Q_Z) \leq e = e(Q/P)$. Από την άλλη μεριά έστω $f' = f(Q/Q_Z) \leq f(Q/P)$. Η G_Z τώρα θεωρούμενη σαν ομάδα ανάλυσης της επέκτασης L/K και της επέκτασης L/K_Z από την άλλη δίνει, λόγω της πρότασης VII.2.5, $[G_Z : 1] = e \cdot f = e' \cdot f'$. Άρα κατ' ανάγκη $e' = e$ και $f' = f$.

Όπως έχει αναφερθεί και πιο μπροστά, τα S/Q και R/P είναι δύο πεπερασμένα σώματα και το R/P περιέχεται ισόμορφα στο S/Q και επιπλέον $f = [S/Q : R/P]$ είναι ο βαθμός αδράνειας.

Από τη θεωρία των πεπερασμένων σωμάτων γνωρίζουμε ότι η επέκταση $(S/Q)/(R/P)$ είναι επέκταση του Galois και μάλιστα κυκλική βαθμού f.

Στη συνέχεια θα εξετάσουμε τι σχέση έχουν οι ομάδες

$$\overline{G} = \mathrm{Gal}\big((S/Q)/(R/P)\big), \qquad G_Z \text{ και } G_T.$$

Έστω

$$\pi : S \ni s \mapsto s + Q \in S/Q$$

ο κανονικός ομομορφισμός του S στο S/Q και έστω $\sigma \in G_Z$, δηλαδή $\sigma(Q) = Q$. Προφανώς αν $s \in S$ και $\sigma \in G$ τότε $\sigma(s) \in S$, συνεπώς $\sigma(S) \subset S$ και εφαρμόζοντας και στα δύο μέλη την σ^{-1} έχουμε $\sigma^{-1}S \subset S$, δηλαδή $\sigma(S) = S$.

Ορίζουμε τώρα για κάθε $\sigma \in G_Z$ μια συνάρτηση

$$\overline{\sigma} : S/Q \ni s + Q \mapsto \sigma(s) + Q \in S/Q.$$

Ο $\overline{\sigma}$ είναι αυτομορφισμός του σώματος S/Q και $\ker\overline{\sigma} = Q$ το μηδενικό στοιχείο του S/Q, ενώ ο $\overline{\sigma}$ είναι και επί αφού $\sigma(S) = S$.

Επίσης ο $\overline{\sigma}$ αφήνει τα στοιχεία του R/P σταθερά. Πράγματι

$$\mathrm{rest}(\overline{\sigma}) : R/P \ni a + P \mapsto a + P \in R/P.$$

Επομένως ο $\overline{\sigma}$ είναι ένας R/P-αυτομορφισμός του σώματος S/Q, δηλαδή $\overline{\sigma} \in \overline{G}$. Θεωρούμε τώρα τη συνάρτηση:

$$\phi : G_Z \ni \sigma \longmapsto \overline{\sigma} \in \overline{G}.$$

Ο ϕ είναι ομομορφισμός ομάδων. Επίσης

$$\begin{aligned}
\ker\phi &= \{\sigma \in G_Z : \overline{\sigma} = \mathrm{Id}_{\overline{L}}\} \\
&= \{\sigma \in G_Z : \overline{\sigma}(a + Q) = a + Q \text{ για κάθε } a \in S\} \\
&= \{\sigma \in G_Z : \sigma(a) + Q = a + Q \text{ για κάθε } a \in S\} \\
&= \{\sigma \in G_Z : \sigma(a) \equiv a \mod Q \text{ για κάθε } a \in S\} = G_T
\end{aligned}$$

η ομάδα αδράνειας του Q. Ο ϕ είναι επίσης επιμορφισμός ομάδων κάτι που είναι λίγο πιο πολύπλοκο.

Θεώρημα VII.2.7. *Ισχύει:*

$$G_Z/G_T \cong \overline{G},$$

δηλαδή η ομάδα πηλίκο G_Z/G_T είναι κυκλική τάξεως f. Συνεπώς λόγω της θεωρίας Galois η επέκταση K_T/K_Z είναι κυκλική επέκταση $[K_T : K_Z] = f$, $[L : K_T] = e = |G_T|$.

Απόδειξη. Το μόνο που χρειάζεται να αποδείξουμε είναι ότι η συνάρτηση ϕ είναι επί. Από τη θεωρία πεπερασμένων σωμάτων γνωρίζουμε ότι η επέκταση $(S/Q)/(R/P)$ είναι απλή. Συμβολίζουμε με $\overline{L} = S/Q$ και $\overline{K} = R/P$ και έστω $\theta \in S$ με $\pi(\theta) = \overline{\theta} = \theta + Q$ να παράγει την επέκταση $\overline{L}/\overline{K}$, δηλαδή $\overline{L} = \overline{K}(\overline{\theta})$.

Έστω $\widehat{\sigma} \in \overline{G}$ και έστω $g(X) = \mathrm{Irr}(\theta, K_Z)$. Αφού $\theta \in S$ το $g(X) \in S_Z[X]$ όπου $S_Z = S \cap K_Z$. Η επέκταση L/K_Z είναι επέκταση του Galois με ομάδα την ομάδα ανάλυσης G_Z οπότε αν

$$g(X) = \sum_{i=0}^{m} \beta_i X^i = \prod_{i=1}^{m} (X - \theta^{(i)})$$

με $\beta_i \in K_Z$ έπεται ότι όλες οι ρίζες $\theta^{(i)}$ του $g(X)$ ανήκουν στο L. Από την άλλη:

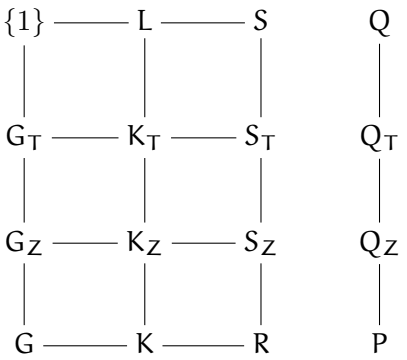
$$\overline{g}(X) = \sum_{i=1}^{m} \overline{\beta}_i X^i = \prod_{i=1}^{m} (X - \overline{\theta}^{(i)}), \quad \overline{\theta} = \overline{\theta}_1$$

και $\overline{\beta}_i \equiv \beta_i \mod Q_Z$ με $Q_Z = K_Z \cap Q$, δηλαδή $\overline{\beta}_i \in S_Z/Q_Z = R/P = \overline{K}$. Εδώ χρησιμοποιούμε το γεγονός ότι $[S_Z/Q_Z : R/P] = 1$. Έστω $\overline{f}(x) = \mathrm{Irr}(\overline{\theta}, \overline{K})$. Επειδή $\overline{g}(\overline{\theta}) = 0$ έχουμε ότι $\overline{f}(x) \mid_{\overline{K}[x]} \overline{g}(x)$. Τώρα $\widehat{\sigma} \in \mathrm{Gal}(\overline{L}/\overline{K})$ και συνεπώς $\widehat{\sigma}(\overline{\theta})$ είναι μιά άλλη ρίζα του $\overline{f}(x)$ και επειδή $\overline{f}(x) \mid \overline{g}(x)$ υπάρχει ℓ ώστε $\widehat{\sigma}(\overline{\theta}) = \overline{\theta}^{(\ell)}$. Το $\theta^{(\ell)}$ είναι ρίζα του $g(x) \in K_Z[x]$, συνεπώς υπάρχει $\sigma \in G_Z = \mathrm{Gal}(L/K_Z)$ ώστε $\sigma(\theta) = \theta^{(\ell)}$. Άρα $\overline{\sigma}(\overline{\theta}) = \overline{\theta}^{(\ell)} = \widehat{\sigma}(\overline{\theta})$, με $\overline{\sigma}, \widehat{\sigma} \in \overline{G}$. Επειδή δε $\overline{L} = \overline{K}(\overline{\theta})$ έχουμε ότι $\widehat{\sigma} = \overline{\sigma}$ και συνεπώς η ϕ είναι επί. □

Το προηγούμενο θεώρημα εκφράζεται και ως εξής: Η ακολουθία

$$1 \to G_T \hookrightarrow G_Z \to \overline{G} \to 1$$

είναι ακριβής. Το σχήμα μας τώρα είναι:



βαθμός επέκτασης	δείκτης διακλάδωσης	βαθμός αδράνειας
e	e	1
f	1	f
r	1	1

Πόρισμα VII.2.8. *Τα παρακάτω είναι ισοδύναμα:*

1. *Το* P *δεν διακλαδίζεται στο* L*, δηλαδή* $e = e(Q/P) = 1$ *για κάθε* $Q \mid P$.
2. *Η ομάδα* $G_T(Q/P) = \{1\}$ *για κάποιο και συνεπώς για όλα τα* $Q \mid P$.
3. *Η συνάρτηση* $\phi : G_Z \to \overline{G}$ *είναι ισομορφισμός ομάδων για ένα και συνεπώς για κάθε* $Q \mid P$.

Απόδειξη. Προφανής. □

Παρατήρηση VII.2.9. Η ομάδα ανάλυσης $G_Z(Q/P)$ δεν είναι, εν γένει, κανονική υποομάδα της ομάδας Galois $\mathrm{Gal}(L/K)$. Επομένως αυτό που γνωρίζουμε είναι ότι

$$PS_Z = \prod_{i=1}^{r} Q_i^{e_i}, \text{ με } Q_1 = Q_Z \text{ και } e(Q_Z/P) = f(Q_Z/P) = 1,$$

κάτι που δεν ισχύει εν γένει, για τα υπόλοιπα πρώτα ιδεώδη Q_i του ιδεώδους PS_Z, δηλαδή το ιδεώδες PS_Z δεν αναλύεται, εν γένει, πλήρως στο σώμα K_Z.

Αυτό φυσικά ισχύει όταν η ομάδα $G_Z(Q/P)$ είναι κανονική υποομάδα της $G = \mathrm{Gal}(L/K)$. Τότε

$$PS_Z = \prod \sigma_i(Q_Z),$$

όπου το σ_i διατρέχει ένα πλήρες σύστημα αντιπροσώπων των κλάσεων G/G_Z. Ιδιαίτερα ισχύει όταν η ομάδα G είναι αβελιανή.

Πόρισμα VII.2.10. *Έστω ότι* $G_Z \lhd G$. *Τότε το* P *αναλύεται σε γινόμενο* r *πρώτων ιδεωδών στο* K_Z. *Αν πάλι* $G_T \lhd G$ *τότε κάθε ένα από τα παραπάνω πρώτα ιδεώδη αδρανεί στο* K_T *και στη συνέχεια κάθε πρώτο ιδεώδες γίνεται* e*-στη δύναμη ενός πρώτου ιδεώδους του* L.

Απόδειξη. Έχουμε ότι $G_Z \lhd G$ συνεπώς η επέκταση K_Z/K είναι επέκταση του Galois. Αφού $r = [K_Z : K]$ και όλα τα πρώτα ιδεώδη του K_Z που βρίσκονται πάνω από το P έχουν τον ίδιο βαθμό αδράνειας και τον ίδιο δείκτη διακλάδωσης έχουμε ότι $f(Q_Z/P) = e(Q_Z/P) = 1$, συνεπώς

$$PS_Z = Q_{Z_1} Q_{Z_2} \cdots Q_{Z_r}.$$

Επειδή δε το πλήθος των πρώτων ιδεωδών του L που βρίσκονται πάνω από το P είναι επίσης r το ίδιο θα συμβαίνει και για το πλήθος των πρώτων ιδεωδών του K_Z πάνω από το P.

Αν τώρα $G_T \lhd G$, τότε η επέκταση K_T/K είναι επέκταση του Galois συνεπώς $e(Q_T/P) = e(Q_T/Q_Z) = 1$ για κάθε πρώτο $Q_T \mid Q_Z$, συνεπώς $Q_Z S_T = Q_T$ με $f(Q_T/Q_Z) = f = [K_T : K_Z]$. Επομένως

$$PS_T = Q_{T_1} Q_{T_2} \cdots Q_{T_r},$$

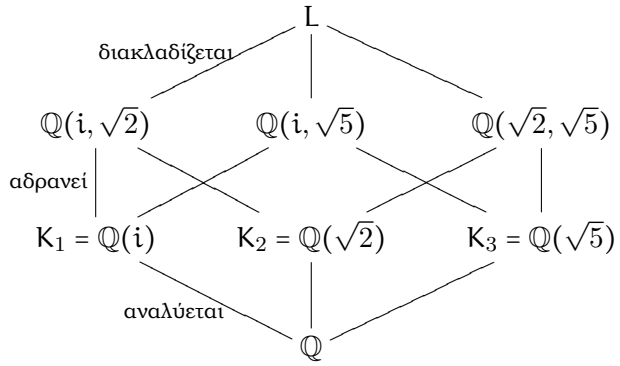
οπότε $e(Q/Q_T) = e$ διότι $erf = n$ για κάθε πρώτο Q του L που διαιρεί το S. □

Σημείωση VII.2.11. Οι υποθέσεις του τελευταίου πορίσματος πληρούνται αν για παράδειγμα η G είναι αβελιανή ομάδα.

Παράδειγμα VII.2.12. Θεωρούμε την επέκταση Galois $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{5})/\mathbb{Q}$ με ομάδα Galois την αβελιανή ομάδα

$$\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

η οποία έχει τα παρακάτω ενδιάμεσα υποσώματα:



Θεωρούμε τους δακτύλιους ακεραίων αλγεβρικών S_i του K_i. Έχουμε

$$5S_1 = P_1 P_2, \qquad 5S_2 = Q_2, \qquad 5S_3 = Q_3^2$$

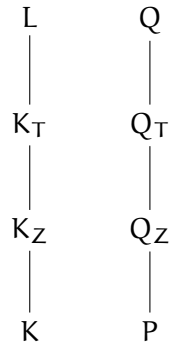
συνεπώς $2 \mid r$, $2 \mid e$, $2 \mid f$.Επειδή δε $erf = 8 = n$, έχουμε $r = 2$, $e = 2$, $f = 2$. Δηλαδή

$$PS = (Q_1 Q_2)^2, \qquad e(Q_i/P) = f(Q_i/P) = 2, i = 1, 2.$$

Καταλήγουμε ότι $K_Z = K_1 = \mathbb{Q}(i)$ και $K_T = \mathbb{Q}(i, \sqrt{2})$.

Τέλος θα προσπαθήσουμε να χαρακτηρίσουμε τα σώματα K_Z και K_T με τρόπο εντελώς διάφορο

του ορισμού τους. Έχουμε τον πύργο σωμάτων:



Θεώρημα VII.2.13. *Το* K_Z *είναι το μέγιστο υπόσωμα του* L *που περιέχει το* K*, ώστε το πρώτο ιδεώδες* P *που βρίσκεται κάτω από το* Q *να έχει* $f(Q_Z/P) = e(Q_Z/P) = 1$.
Το K_T *είναι το μέγιστο υπόσωμα του* L *που περιέχει το* K *με την ιδιότητα* $e(Q_T/P) = 1$.

Απόδειξη. Έστω Λ σώμα με $K \subset \Lambda \subset L$ και $P \subset Q_\Lambda = Q \cap S_\Lambda \subset Q$ τα αντίστοιχα ιδεώδη. Υποθέτουμε ότι $f(Q_\Lambda/P) = e(Q_\Lambda/P) = 1$. Αρκεί να δείξουμε ότι $\Lambda \subset K_Z$. Έστω πάλι Λ' σώμα $K \subset L' \subset L$ και $P \subset Q_{\Lambda'} = Q \cap S_{\Lambda'} \subset Q$ με $e(Q_{\Lambda'}/P) = 1$. Αρκεί να δείξουμε ότι $\Lambda' \subset K_T$.

Από τη σχέση

$$f = f(Q/P) = f(Q/Q_\Lambda)f(Q_\Lambda/P)$$

και την αντίστοιχη για το $e := e(Q/P)$ έπεται ότι $f(Q/Q_\Lambda) = f$ και $e(Q/Q_\Lambda) = e$. Αντίστοιχα $e(Q/Q_{\Lambda'}) = e$. Θεωρούμε τώρα τις επεκτάσεις L/Λ και L/Λ' και έστω

$$G'_Z = G_Z(Q/Q_\Lambda) \text{ και } G'_T = G_T(Q/Q_{\Lambda'}).$$

Έχουμε ήδη δείξει ότι

$$[G'_Z : 1] = f(Q/Q_\Lambda)e(Q/Q_\Lambda) = fe = [G_Z : 1]$$

και

$$[G'_T : 1] = f(Q/Q_{\Lambda'}) = f = [G_T : 1].$$

Από την άλλη μεριά γνωρίζουμε όμως ότι:

$$G'_Z = G_Z \cap \mathrm{Gal}(L/\Lambda) \text{ και } G'_T = G_T \cap \mathrm{Gal}(L/\Lambda')$$

συνεπώς

$$G'_Z \subset G_Z \text{ και } G'_T \subset G_T$$

οπότε αφού έχουν την ίδια τάξη $G_Z = G'_Z$ και $G_T = G'_T$, δηλαδή

$$G_Z = G_Z \cap \mathrm{Gal}(L/\Lambda) \text{ και } G_T = G_T \cap \mathrm{Gal}(L/\Lambda')$$

συνεπώς

$$\mathrm{Gal}(L/\Lambda) \geq G_Z \text{ και } \mathrm{Gal}(L/\Lambda') \geq G_T$$

άρα $K_Z \supset \Lambda$ και $K_T \supset \Lambda'$. □

Ας υποθέσουμε τώρα ότι η επέκταση L/K είναι αβελιανή. Σε αυτή την περίπτωση ισχύει προφανώς

$$K_Z = K_Z(Q/P) = K_Z(\sigma(Q)/P) \text{ για κάθε } \sigma \in \mathrm{Gal}(L/K)$$

και ομοίως όλα τα συζυγή πρώτα ιδεώδη Q του L $Q|P$ έχουν το ίδιο σώμα αδράνειας. Ώστε:

Πόρισμα VII.2.14. *Έστω* L/K *αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών. Τότε*

1. *Το σώμα ανάλυσης* K_Z *είναι το μέγιστο υπόσωμα του* L *που περιέχει το* K*, στο οποίο το πρώτο ιδεώδες* P *αναλύεται πλήρως στο σώμα* L*, δηλαδή είναι γινόμενο ιδεωδών βαθμού αδράνειας και δείκτη διακλάδωσης ίσων με ένα.*
2. *Το σώμα αδράνειας είναι το μέγιστο υπόσωμα του* L *που περιέχει το* K *και στο οποίο το πρώτο ιδεώδες* P *δεν διακλαδίζεται.*

VII.3 Ομάδες Διακλάδωσης

Περνούμε τώρα στις ομάδες διακλάδωσης. Το πρόβλημα είναι αν η ακολουθία είναι άπειρη, για παράδειγμα μετά από πεπερασμένο πλήθος βημάτων, όλες οι ομάδες διακλάδωσης είναι μεταξύ τους ίσες ή μετά από πεπερασμένο πλήθος βημάτων καταλήγουμε στην $G_{\Delta_i} = \{1\}$. Θα αποδείξουμε ότι ισχύει το δεύτερο.

Πρόταση VII.3.1. *Υπάρχει* i *ώστε* $G_{\Delta_i} = \{1\}$.

Απόδειξη. Έστω ότι δεν ισχύει η πρόταση, δηλαδή $G_{\Delta_i} \supsetneq \{1\}$ για κάθε φυσικό αριθμό $i \in \mathbb{N}$. Αυτό έχει ως συνέπεια ότι υπάρχει $\sigma \in \cap_{i=1}^{\infty} G_{\Delta_i} - \{1\}$. Δηλαδή για κάθε $i \in \mathbb{N}$ και $\alpha \in S$ ισχύει

$$\sigma(\alpha) \equiv \alpha \mod Q^{i+1}.$$

Επειδή $\sigma \neq 1$ υπάρχει $\alpha \in S$ με

$$\sigma(\alpha) \neq \alpha$$

οπότε

$$0 \neq \sigma(\alpha) - \alpha \in Q^{i+1}$$

για κάθε $i \in \mathbb{N}$, δηλαδή $Q^{i+1} \mid (\sigma(\alpha) - \alpha)S$ για κάθε φυσικό αριθμό, άτοπο. □

Ορισμός VII.3.2. Έστω i_0 ο ελάχιστος φυσικός ώστε $G_{\Delta_{i_0}} \neq \{1\}$ ενώ $G_{\Delta_{i_0+1}} = \{1\}$. Τότε ο αριθμός i_0 θα λέγεται αριθμός διακλάδωσης.

Αν $i_0 = 0$, τότε λέμε ότι έχουμε την περίπτωση της μη-υψηλότερης διακλάδωσης.

Παρατήρηση VII.3.3. Με χρήση της πρότασης V.1.4 αποδείξαμε στο θεώρημα V.1.5, ότι για κάθε αλγεβρικό σώμα αριθμών K με δακτύλιο των ακεραίων αλγεβρικών R_K, P ένα πρώτο ιδεώδες του K και n οποιοδήποτε φυσικό αριθμό n ισχύει

$$N_{K/\mathbb{Q}}(P^n) = \#R_K/P^n = N_{K/\mathbb{Q}}(P)^n = (\#R_K/P)^n.$$

Με τη βοήθεια αυτής της παρατήρησης θα αποδείξουμε την

Πρόταση VII.3.4. *Έστω* K *ένα αλγεβρικό σώμα αριθμών,* R_K *ο δακτύλιος των ακεραίων αλγεβρικών του* K*,* P *ένα πρώτο ιδεώδες αυτού και* $n \in \mathbb{N}$*,* $n \geq 1$*. Έστω* Σ_P *ένα πλήρες σύστημα αντιπροσώπων του* R_K *modulo* P *και* π *ένα πρώτο στοιχείο του* P*, δηλαδή* $\pi \in P \backslash P^2$*. Το σύνολο*

$$\mathcal{A} := \{a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} : a_i \in \Sigma_P, i = 0, 1, \ldots, n-1\}$$

αποτελεί ένα πλήρες σύστημα αντιπροσώπων του R_K *modulo* P^n*.*

Απόδειξη. Επαγωγικά ως προς n.

Για $n = 1$ προφανώς ισχύει.

Υποθέτουμε ότι ισχύει για $n-1$. Πρώτα θα δείξουμε ότι αν δύο στοιχεία της μορφής $\alpha = a_0 + a_1\pi$ και $\alpha' = a_0' + a_1'\pi$ είναι διαφορετικά μεταξύ τους, τότε

$$\alpha - \alpha' \notin P^n.$$

Πράγματι, αν $\alpha - \alpha' = (a_0 - a_0') + (a_1 - a_1')\pi \in P^n$, τότε

$$a_0 - a_0' = -(a_1 - a_1')\pi + (\alpha - \alpha') \in P.$$

Επομένως $a_0 = a_0'$, οπότε και $(a_1 - a_1')\pi \in P^n$. Αλλά $\pi \in P - P^2$, σημαίνει ότι $R_K\pi = P \cdot A$ με $P \nmid A$. Επίσης, η σχέση $(a_1 - a_1')\pi \in P^n$ συνεπάγεται

$$P^n \cdot A' = R_K(a_1 - a_1')R_K\pi = R_K(a_1 - a_1')P \cdot A,$$

δηλαδή $P^{n-1} \mid R_K(a_1 - a_1')A$ και επειδή $P \nmid A$ έπεται ότι $P^{n-1} \mid R_K(a_1 - a_1')$. Συνεπώς $a_1 - a_1' \in P^{n-1}$ και, λόγω της υπόθεσης της μαθηματικής επαγωγής, ισχύει $a_1 = a_1'$. □

Έστω τώρα L/K επέκταση Galois αλγεβρικών σωμάτων αριθμών, Q ένα πρώτο ιδεώδες του L και π ένα πρώτο στοιχείο του Q, $\pi \in Q\backslash Q^2$. Γνωρίζουμε ήδη ότι η n-στή ομάδα ανάλυσης ορίζεται ως εξής:

$$G_{\Delta_n} = G_{\Delta_n}(Q/P) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \mod Q^{n+1} \text{ για κάθε } \alpha \in S\}.$$

Εμείς έχουμε αποδείξει ότι $G_{\Delta_n}(Q/P) \subset G_T(Q/P)$ για κάθε $n \geq 1$. Επομένως μπορούμε να γράψουμε

$$G_{\Delta_n} = G_{\Delta_n}(Q/P) = \{\sigma \in G_T(Q/P) : \sigma(\alpha) \equiv \alpha \mod Q^{n+1} \text{ για κάθε } \alpha \in S\}.$$

Αφού $\pi \in Q \subset S$, έπεται ότι για κάθε $\sigma \in G_{\Delta_n}$, ισχύει $\sigma(\pi) \equiv \pi \mod Q^{n+1}$.

Αντίστροφα, έστω $\sigma \in G_T(Q/P)$ για το οποίο ισχύει $\sigma(\pi) \equiv \pi \mod Q^{n+1}$. Κάθε στοιχείο $\alpha \in S$, σύμφωνα με την προηγούμενη πρόταση, γράφεται μονοσήμαντα στη μορφή

$$\alpha \equiv a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n \mod Q^{n+1},$$

όπου τα $a_i \in \Sigma_Q$, $i = 0, 1, 2, \ldots, n$ ή ισοδύναμα οι αριθμοί αυτοί αποτελούν πλήρες σύστημα αντιπροσώπων των στοιχείων του δακτυλίου S/Q.

Τα a_i ανήκουν στο Σ_Q ένα σταθερό, πλήρες σύνολο των κλάσεων υπολοίπων modulo Q. Επειδή όμως το πρώτο ιδεώδες $Q_T = Q \cap K_T$ έχει τον ίδιο βαθμό με το πρώτο ιδεώδες Q του S, έπεται ότι $S/Q = R_T/Q_T$. Αυτό σημαίνει ότι μπορούμε το σύνολο Σ_Q να το επιλέξουμε από στοιχεία του R_T. Επομένως κάθε $\alpha \in S$, πρώτο προς το Q, γράφεται μονοσήμαντα στη μορφή:

$$\alpha = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n \mod Q^{n+1}$$

με $a_i \in R_T \subset K_T$, δηλαδή για κάθε $\sigma \in G_T(Q/P)$ ισχύει $\sigma(a_i) = a_i$. Άρα,

$$\begin{aligned} \sigma(\alpha) &= a_0 + a_1\sigma(\pi) + \cdots + a_n\sigma(\pi^n) \\ &\equiv a_0 + a_1\pi + \cdots + a_n\pi^n \\ &\equiv \alpha \mod Q^{n+1}, \text{ για κάθε } \alpha \in S. \end{aligned}$$

Αυτό σημαίνει ότι $\sigma \in G_{\Delta_n}(Q/P)$. Αποδείξαμε λοιπόν ότι

$$G_{\Delta_n}(Q/P) = \{\sigma \in G_T(Q/P) : \sigma(\pi) \equiv \pi \mod Q^{n+1}\}$$

Αν $\sigma \in G_T(Q/P)$, τότε αφού $\pi \in Q\backslash Q^2$ και $\sigma(\pi) \in Q\backslash Q^2$. Αυτό σημαίνει ότι

$$\sigma(\pi) \equiv a_\sigma \cdot \pi \mod Q^2,$$

με a_σ πρώτο προς το Q, $a_\sigma \in \Sigma_Q$ ($a_\sigma \notin Q$). Όπως παραπάνω, το Σ_Q έχει επιλεγεί με στοιχεία του K_T. Στη συνέχεια ορίζουμε την ακόλουθη συνάρτηση:

$$\phi : G_T(Q/P) \ni \sigma \longmapsto \alpha_\sigma \in (S/Q)^* = S/Q\backslash\{0+Q\}.$$

Η απεικόνιση ϕ είναι επιμορφισμός ομάδων. Πράγματι, αν $\tau \in G_T(Q/P)$ με $\phi(\tau) = \alpha_\tau$, έχουμε

$$(\tau\sigma)(\pi) = \tau(\sigma(\pi)) \equiv \tau(\alpha_\sigma\pi) \equiv \alpha_\sigma\tau(\pi) \equiv \alpha_s(\alpha_\tau\pi) = (\alpha_s\alpha_\tau)\pi \mod Q^2.$$

Ο πυρήνας της ϕ είναι:

$$\begin{aligned}\ker\phi &= \{\sigma \in G_T(Q/P) : \alpha_\sigma \equiv 1 \mod Q\}\\ &= \{\sigma \in G_T(Q/P) : \sigma(\pi) \equiv \pi \mod Q^2\} = G_{\Delta_1}(Q/P).\end{aligned}$$

Επομένως η ομάδα πηλίκο

$$\frac{G_T(Q/P)}{G_{\Delta_1}(Q/P)}$$

εμφυτεύεται μέσα στην $(S/Q)^*$, οπότε και η τάξη $|\frac{G_T(Q/P)}{G_{\Delta_1}(Q/P)}|$ διαιρεί την τάξη της $(S/Q)^*$ η οποία είναι $N_{L/\mathbb{Q}}(Q)-1$. Επειδή η $(S/Q)^*$ είναι κυκλική, έπεται ότι και η ομάδα πηλίκο είναι κυκλική. Επίσης επειδή η norm $N_{L/\mathbb{Q}}(Q)$ είναι δύναμη του πρώτου αριθμού p, έπεται ότι το p δεν διαιρεί την τάξη της ομάδας πηλίκο $\frac{G_T}{G_{\Delta_1}}$.

Μέχρι στιγμής, αποδείξαμε το

Θεώρημα VII.3.5. *Η ομάδα G_T/G_{Δ_1} είναι κυκλική τάξης e_0 με $p \nmid e_0$, $p\mathbb{Z} = Q \cap \mathbb{Z}$. Επίσης $e_0 \mid N_{L/\mathbb{Q}}(Q) - 1$.*

Επιπλέον ισχύει και $e = e_0 \cdot p^r$, για κάποιο εκθέτη r, αλλά αυτό θα το αποδείξουμε στη συνέχεια μετά την απόδειξη του επόμενου θεωρήματος.

Σειρά έχει η μελέτη των επόμενων ομάδων διακλαδώσεως. Έχουμε ήδη δει ότι η

$$G_{\Delta_n}(Q/P) = \{\sigma \in G_T(Q/P) : \sigma(\pi) \equiv \pi \mod Q^{n+1}\}.$$

Επομένως

$$\sigma(p) \equiv \pi + y_\sigma\pi^{n+1} \mod Q^{n+2}$$

με y_σ ορισμένο modulo Q και επιλεγμένο από το K_T. Στη συνέχεια ορίζουμε τη συνάρτηση

$$\psi : G_{\Delta_n}(Q/T) \ni \sigma \longmapsto y_\sigma \in S/Q.$$

Σημείωση VII.3.6. Εδώ το y_σ όχι, κατ' ανάγκη πρώτο προς το Q. Δεξιά η ομάδα S/Q είναι προσθετική.

Η ψ είναι ομομορφισμός ομάδων. Αν $\psi(\tau) = y_\tau$, έχουμε

$$\begin{aligned}(\tau\sigma)(\pi) &\equiv \tau(\sigma(\pi)) \equiv \tau(\pi + y_\sigma\pi^{n+1}) \equiv \tau(\pi) + y_\sigma\tau(\pi^{n+1})\\ &\equiv (\pi + y_\tau\pi^{n+1}) + y_\sigma(\pi + y_\tau\pi^{n+1})^{n_1}\\ &\equiv \pi + (y_\sigma + y_\tau)\pi^{n+1} \mod Q^{n+2}\end{aligned}$$

Υπολογίζουμε τον πυρήνα της ψ

$$\begin{aligned}\ker\psi &= \{\sigma \in G_{\Delta_n}(Q/P) : y_\sigma \equiv 0 \mod Q\}\\ &= \{\sigma \in G_{\Delta_n}(Q/P) : \sigma(\pi) \equiv \pi + 0\pi^{n+1} \mod Q^{n+2}\}\\ &= \{\sigma \in G_{\Delta_n}(Q/P) : \sigma(\pi) \equiv \pi \mod Q^{n+2}\}\\ &= G_{\Delta_{n+1}}(Q/P)\end{aligned}$$

Επομένως η ομάδα πηλίκο $G_{\Delta_n}(Q/P)/G_{\Delta_{n+1}}$ είναι ισόμορφη προς μια υποομάδα της αβελιανής προσθετικής ομάδας S/Q, η οποία έχει τάξη $N_{L/\mathbb{Q}}(Q) = p^{f(Q/p\mathbb{Z})}$. Για κάθε $\alpha \in S$ ισχύει ότι $p\alpha \equiv 0 \mod Q$. Συνεπώς είναι μια στοιχειώδης αβελιανή p-ομάδα, δηλαδή του τύπου $(p, p, \ldots, p)$, ισόμορφη με την

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

Αποδείξαμε, επομένως το

Θεώρημα VII.3.7. *Η ομάδα πηλίκο $G_{\Delta_n}(Q/P)/G_{\Delta_{n+1}(Q/P)}$ είναι μια στοιχειώδης αβελιανή p-ομάδα, δηλαδή του τύπου $(p, \ldots, p)$. Η τάξη της είναι $\leq N_{L/\mathbb{Q}}(Q)$.*

Από τα παραπάνω συνάγουμε ότι η ομάδα G_T έχει την ακόλουθη ακολουθία κανονικών υποομάδων

$$G_T \geq G_{\Delta_1} \geq G_{\Delta_2} \geq \ldots \geq G_{\Delta_n} = \{1\}$$

με G_T/G_{Δ_1} κυκλική με τάξη πρώτη προς το p και $G_{\Delta_i}/G_{\Delta_{i+1}}$ p-ομάδα. Ισχύει

$$|G_T| = [G_T : G_{\Delta_1}][G_{\Delta_1} : \{1\}] = e_0 p^r,$$

για κάποιο r, δηλαδή αυτό που είχαμε αφήσει αναπόδεικτο στο αμέσως προηγούμενο θεώρημα.

Ορισμός VII.3.8. Αν το σώμα $\overline{k} = R_K/P$ έχει χαρακτηριστική p και $[L : K_T] = e$ με $p \nmid e$, τότε $|G_{\Delta_1}(Q/P)| = 1$ και συνεπώς όλα τα σώματα διακλαδώσεων ταυτίζονται με το L. Δεν υπάρχει λοιπόν υψηλότερη διακλάδωση και, σ' αυτή την περίπτωση θα λέμε ότι ο το P *διακλαδίζεται ομαλά (tamely)* στην επέκταση L/K.

Αν το $p \mid e$, τότε θα λέμε ότι το P *διακλαδίζεται αγρίως (wildly)* στην L/K.

Πόρισμα VII.3.9. *Αν Q είναι ένα πρώτο ιδεώδες του S και $Q \cap R_K = P$, τότε η ομάδα ανάλυσης $G_Z(Q/P)$ είναι επιλύσιμη.*

Απόδειξη. Έχουμε $G_Z(Q/P) \geq G_T(Q/P) \geq \{1\}$. Η $G_T(Q/P)$ είναι επιλύσιμη και η $G_Z(Q/P)/G_T(Q/P)$ είναι κυκλική, συνεπώς $G_Z(Q/P)$ επιλύσιμη. □

Στη συνέχεια θα μελετήσουμε τα πρώτα ιδεώδη $Q_{\Delta_i} = Q \cap K_{\Delta_i}$ των σωμάτων διακλάδωσης. Έχουμε αποδείξει ήδη ότι το $Q_T = Q \cap K_T$ είναι πλήρως διακλαδιζόμενο στο L. Είναι αυτονόητο ότι αυτό ισχύει και για τα ενδιάμεσα σώματα. Επομένως, $Q_T = Q_{\Delta_1}^{e_0}$ και $Q_{\Delta_i} = Q_{\Delta_{i+1}}^{p_i^{r_i - r_{i+1}}}$ οπότε και $Q_{\Delta_i} = Q^{p_i^r}$.

Στο τέλος θα συνοψίσουμε μερικές οριακές, αλλά ενδιαφέρουσες περιπτώσεις της θεωρίας. Για λόγους ευκολίας θα αλλάξουμε, για λίγο, τον συμβολισμό. Θα συμβολίζουμε τα σώματα $K_{-1} = K_Z$, $K_0 = K_T$ και $K_{\Delta_n} = K_n$, που αντιστοιχούν στις ομάδες Galois.

1. Πάνω από το P, στο σώμα L υπάρχει ακριβώς ένα πρώτο ιδεώδες Q αν και μόνο αν η ομάδα $G = \mathrm{Gal}(L/K) := G_{-1}$. Αυτό επειδή το πλήθος των διαφορετικών παραγόντων του PS είναι όσο ο δείκτης $[G : G_{-1}]$.
2. Το P αναλύεται πλήρως στο σώμα $L \Leftrightarrow K_{-1} = L$ και το $G_{-1} = \{\mathrm{Id}_L\}$.
3. Το P διακλαδίζεται πλήρως στο $L \Leftrightarrow K_0 = K$ αν και μόνο αν $G_0 = G$.
4. Το πρώτο ιδεώδες Q του L, $Q \mid P$ είναι μη-διακλαδιζόμενο αν και μόνο αν $G_0 = \{\mathrm{Id}_L\}$. Εάν τώρα K' είναι ένα ενδιάμεσο σώμα της επέκτασης L/K και $G' = \mathrm{Gal}(L/K')$ η αλυσίδα των ομάδων της θεωρίας του Hilbert για το Q υπεράνω του πρώτου ιδεώδους $P' = Q \cap K'$ του K', έστω G'_n, τότε ισχύει
$$G'_n = G' \cap G_n \qquad n \geq -1.$$
Αυτό το αποδείξαμε μόνο για την ομάδα ανάλυσης και αδράνειας, αλλά ισχύει και για τις ομάδες διακλαδώσεων.

5. Ισχύει $K_{-1} \subset K'$, δηλαδή το P' αναλύεται σε ένα ακριβώς ιδεώδες στο L, αν και μόνο αν υπάρχει $t \in \mathbb{N}$, $P'S = Q^t$. Πράγματι $K_{-1} \subset K'$ αν και μόνο αν $G' \subset G_{-1}$. Αλλά

$$G'_{-1} = G' \cap G_{-1} = G',$$

δηλαδή $K_{-1} \subset K'$ αν και μόνο αν $G' = G'_{-1}$.

6. Το $K' \supset K_0$ αν και μόνο αν $P'S = Q^t$ και $f(P'/P) = f(Q/P)$. Πράγματι, λόγω της πολλαπλασιαστικότητας του βαθμού αδράνειας, έχουμε

$$f(Q/P) = f(Q/P')f(P'/P),$$

συνεπώς $f(Q/P') = 1$. Επομένως, $f(Q/P') = 1$ και $P'S = Q^t$ σημαίνουν ότι το $P'S$ αναλύεται πλήρως στο L και συνεπώς $G' = G'_0$.

7. Το $K' \subset K_0$ αν και μόνο αν $G_0 \subset G'$. Επειδή $G'_0 = G' \cap G_0 = G_0$, επομένως $K' \subset K_0$ αν και μόνο αν $e(Q/P') = e(Q/P)$.

8. $p \nmid e(P'/P)$ αν και μόνο αν $K' \subset K_1$. Πράγματι $K' \subset K_1$ αν και μόνο αν $G_1 \subset G'$. Αλλά $G'_1 = G' \cap G_1 = G_1$ και αυτό σημαίνει ότι $e(Q/P')$ είναι ένα πολλαπλάσιο της τάξης της G_1. Το τελευταίο δίνει την ισοδυναμία με το $p \nmid e(P'/P)$.

VII.4 Ασκήσεις

1. Έστω L/K μία επέκταση Galois αλγεβρικών σωμάτων αριθμών με $[L : K] = 6$. Υποθέτουμε ότι για κάποιο πρώτο ιδεώδες P του K ισχύει

$$PR_L = Q^2, Q \text{ πρώτο ιδεώδες του } L$$

Να αποδειχθεί ότι η επέκταση L/K είναι κατ' ανάγκη κυκλική.

2. Έστω L_1 και L_2 πεπερασμένες επεκτάσεις του αλγεβρικού σώματος αριθμών K και P ένα πρώτο ιδεώδες του K. Να αποδειχθεί ότι το P δεν διακλαδίζεται στις επεκτάσεις L_1/K και L_2/K τότε και μόνο τότε όταν αυτό δεν διακλαδίζεται στην επέκταση L_1L_2/K.

3. Αντικαταστήστε την έκφραση «δεν διακλαδίζεται» στην άσκηση 2 με την «αναλύεται πλήρως» και αποδείξτε το ανάλογο της 2.

4. Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών και M η Galois θήκη της L/K. Να αποδείξετε ότι το πρώτο ιδεώδες P του K δεν διακλαδίζεται στην επέκταση L/K τότε και μόνο τότε όταν δεν διακλαδίζεται στην επέκταση M/K

5. Αποδείξτε το ανάλογο αντικαθιστώντας το «δεν διακλαδίζεται» με το «αναλύεται πλήρως».

6. Έστω d_1, d_2 ακέραιοι, ελεύθεροι τετραγώνου διαφορετικοί μεταξύ τους και

$$d_i \equiv 1 \mod 3, \qquad i = 1, 2$$

Θεωρούμε το σώμα $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Να αποδείξετε ότι ο δακτύλιος των ακεραίων αλγεβρικών του K δεν είναι μονογενής. Για παράδειγμα $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$.

7. Έστω L/K μια επιλύσιμη επέκταση αλγεβρικών σωμάτων αριθμών, βαθμού δύναμης πρώτου αριθμού, $[L : K] = p^\ell$. Αν ένα πρώτο ιδεώδες P, δεν διακλαδίζεται στο L και στην ανάλυση του PR_L σε γινόμενο πρώτων ιδεωδών, εμφανίζονται δύο πρώτα ιδεώδη του L, Q_1, Q_2 με $f(Q_1/P) = f(Q_2/P) = 1$, τότε το P αναλύεται πλήρως στο σώμα L.

Υπόδειξη: Θεώρημα της Θεωρίας Ομάδων. Αν G είναι μια μεταβατική επιλύσιμη ομάδα μεταθέσεων τάξεως δύναμης πρώτου αριθμού p, τότε δεν υπάρχει μετάθεση $\sigma \in G$, $\sigma \neq 1$ η οποία να κρατάει σταθερά δύο διαφορετικά ψηφία.

8. Έστω L/K Galois επέκταση αλγεβρικών σωμάτων αριθμών $G = \mathrm{Gal}(L/K)$ και P πρώτο ιδεώδες του K.
   (α′) Αν το P αδρανεί στην επέκταση L/K, τότε η ομάδα G είναι κυκλική.
   (β′) Έστω ότι το P διακλαδίζεται πλήρως σε κάθε ενδιάμεσο σώμα $K \subsetneq M \subsetneq L$ αλλά όχι στο L. Να αποδειχθεί ότι δεν υπάρχει ενδιάμεσο σώμα και συνεπώς η ομάδα G είναι κυκλική πεπερασμένης τάξης.
   (γ′) Υποθέτουμε ότι σε κάθε ενδιάμεσο σώμα υπάρχει ακριβώς ένα πρώτο ιδεώδες Q πρώτο $Q \mid P$, αλλά στο L αυτό δεν ισχύει. Να αποδειχθεί ότι η G είναι κυκλική πεπερασμένης τάξης.
9. Αν $K/\mathbb{Q}$ επέκταση Galois και $G = \mathrm{Gal}(K/\mathbb{Q})$ να αποδειχθεί ότι η ομάδα G παράγεται από τις ομάδες αδράνειας όλων των πρώτων ιδεωδών του σώματος K.

Βιβλιογραφία

[1] Cox, D. A. *Primes of the Form x^2+ny^2, Fermat, class field theory, and complex multiplication*. 2nd edition. Pure and Applied Mathematics. John Wiley & Sons, Inc., 2013, pp. xviii+356. ISBN: 978-1-118-39018-4.

[2] Hasse, H. *Vorlesungen über Klassenkörpertheorie*. Thesaurus Mathematicae, Band 6. Physica-Verlag, Würzburg, 1967, pp. iii+275.

[3] Leutbecher, A. *Zahlentheorie: Eine Einführung in die Algebra*. Springer-Lehrbuch. Springer, Berlin, 2013. ISBN: 9783642614057. URL: `https://books.google.gr/books?id=PG2nBgAAQBAJ`.

[4] Marcus, D. A. *Algebraic Number Fields*. Universitext. 2nd edition of [MR0457396], With a foreword by Barry Mazur. Springer, 2018, pp. xviii+203. ISBN: 978-3-319-90232-6; 978-3-319-90233-3.

[5] Neukirch, J. *Algebraische Zahlentheorie*. German. Springer-Verlag Berlin, 1992.

[6] Ribenboim, P. *Classical Theory of Algebraic Numbers*. Universitext. Springer-Verlag, New York, 2001, pp. xxiv+681. ISBN: 0-387-95070-2.

[7] Λάκκης, Κ. *Θεωρία Αριθμών*. Εκδ. Ζήτη, 1990.

VIII

Νόμοι Αντιστροφής

VIII.1 Εισαγωγή

Ο νόμος αντιστροφής του Gauss αποτελεί ένα από τα πιο σημαντικά θεωρήματα της Θεωρίας Αριθμών. Η διαδρομή από τις πρώτες σχετικές διατυπώσεις του Euler, τα ενδιάμεσα αποτελέσματα των Lagrange και Legendre μέχρι την πρώτη πλήρη απόδειξη του Gauss στις 8 Απριλίου του 1796, κράτησε περίπου 60 χρόνια, [9].

Είναι το κλειδί της μελέτης της θεωρίας των τετραγωνικών υπολοίπων (ισοτιμιών δευτέρου βαθμού). Στο έργο του "Disquisitiones Arithmeticae" μάλιστα ο Gauss γράφει (από μετάφραση στην αγγλική):

"Since almost everything that can be said about quadratic residues depends on this theorem, the term fundamental theorem which will use from now on should be acceptable" [2].

Εντελώς φυσικό ήταν η εύρεση και ανάπτυξη αντίστοιχης θεωρίας ενός κυβικού, διτετραγωνικού κ.λπ. νόμου αντιστροφής.

Παράλληλα προς την προσπάθεια και τη διαδικασία της απόδειξης της εικασίας του Fermat, η προσπάθεια εύρεσης, διατύπωσης και απόδειξης ενός γενικού νόμου αντιστροφής υπήρξε η κινητήρια ώθηση της τεράστιας ανάπτυξης που γνώρισε η Θεωρία Αριθμών από τα τέλη του 18ου αιώνα μέχρι σήμερα. Η έννοια έχει διάφορες όψεις. Μια από αυτές θα παρουσιάσουμε εδώ.

VIII.2 Ο τετραγωνικός νόμος αντιστροφής

Στην παράγραφο αυτή θα μετασχηματίσουμε τον τετραγωνικό νόμο αντιστροφής κατά τέτοιο τρόπο που να ταιριάζει στην προσπάθεια γενίκευσής του στη συνέχεια.

Έστω $K = \mathbb{Q}(\sqrt{q})$, όπου q πρώτος, $f(x) = \mathrm{Irr}(\sqrt{q}, \mathbb{Q}) = x^2 - q$ και p πρώτος αριθμός. Σύμφωνα με τον νόμο ανάλυσης η «συμπεριφορά» του πολυωνύμου

$$f_p(x) \equiv f(x) \mod p$$

μας δίνει την ανάλυση του pR_K σε γινόμενο πρώτων ιδεωδών του K και αυτή πάλι με τη σειρά της χαρακτηρίζεται μέσω του συμβόλου του Kronecker $\left(\frac{D_K}{p}\right)$, όπου D_K η διακρίνουσα του σώματος K, δηλαδή $D_K = q$ ή $D_K = 4q$. Αν $p \mid D_K$ έχουμε αμέσως $\left(\frac{D_K}{p}\right) = 0$ και $pR = Q^2$. Πώς θα ξεχωρίσουμε όμως πότε $\left(\frac{D_K}{p}\right) = 1$ και πότε $\left(\frac{D_K}{p}\right) = -1$;

Για $p \nmid D_K$, $p \neq 2$ έχουμε

$$\left(\frac{D_K}{p}\right) = \left(\frac{q}{p}\right)$$

όπου το τελευταίο είναι το σύμβολο του Legendre. Το $\left(\frac{q}{p}\right)$ δεν είναι εύκολο να υπολογιστεί μέσω του ορισμού του. Αλλά και εύκολο να ήταν, αν μας έδιναν έναν άλλο πρώτο, έστω p', για να υπολογίσουμε το $\left(\frac{q}{p'}\right)$ θα έπρεπε να ξαναεφαρμόσουμε την ίδια «διαδικασία» για το p' και μια και υπάρχουν άπειροι πρώτοι για να βρούμε την ανάλυση όλων των πρώτων θα χρειαζόμασταν άπειρο χρόνο.

Το ερώτημα λοιπόν είναι αν υπάρχει καλύτερη περιγραφή. Η απάντηση είναι προφανώς ναι αν αντί του $\left(\frac{q}{p}\right)$ είχαμε $\left(\frac{p}{q}\right)$. Τότε, επειδή η τιμή του $\left(\frac{p}{q}\right)$ εξαρτάται όχι από το p αλλά από την κλάση $p \mod q$ στην οποία το p ανήκει, θα χρειαζόμασταν λοιπόν πεπερασμένο πλήθος υπολογισμών μόνο $q-1$ σύμβολα του Legendre.

Γεννιέται λοιπόν φυσιολογικά το ερώτημα. Μήπως υπάρχει κάποια σχέση ανάμεσα στα $\left(\frac{q}{p}\right)$ και $\left(\frac{p}{q}\right)$;

Η απάντηση είναι ναι και είναι προϊόν της ιδιοφυίας του Gauss και λέγεται τετραγωνικός νόμος αντιστροφής.

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right), \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

όπου p, q είναι περιττοί πρώτοι, $p \neq q$.

Ο ίδιος ο Gauss, έδωσε κατά τη διάρκεια της ζωής του 7 αποδείξεις του τετραγωνικού νόμου αντιστροφής ενώ σήμερα είναι πάνω από 200[1].

Μια ισοδύναμη έκφραση του νόμου αντιστροφής είναι

1. Αν $q \equiv 1 \mod 4$ τότε $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$
2. Αν $q \equiv 3 \mod 4$ τότε $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{αν } p \equiv 1 \mod 4 \\ -\left(\frac{p}{q}\right) & \text{αν } p \equiv 3 \mod 4 \end{cases}$

Έστω

$$\mathrm{Spl}(f(x)) = \{p \in \mathbb{P} : \left(\frac{q}{p}\right) = 1\}.$$

Αν για παράδειγμα $q = 17$ τότε

$$\left(\frac{17}{p}\right) = \left(\frac{p}{17}\right) = 1 \text{ αν και μόνο αν } p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \mod 17$$

Δηλαδή $p \in \mathrm{Spl}(x^2 - 17)$ αν και μόνο αν $p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \mod 17$.

Έστω πάλι $q = 11 \equiv 3 \mod 4$ συνεπώς $\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{11}\right)$.

Επομένως $\left(\frac{11}{p}\right) = 1$ αν και μόνο αν $p \equiv 1 \mod 4$ και $\left(\frac{p}{11}\right) = 1$ ή αν $p \equiv 3 \mod 4$ και $\left(\frac{p}{11}\right) = -1$ οπότε το πρόσημο του $\left(\frac{11}{p}\right)$ εξαρτάται από την κλάση του p modulo 44. Έχουμε λοιπόν:

$$p \in \mathrm{Spl}(x^2 - 11) \text{ αν και μόνο αν } p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \mod 44$$

Εντελώς όμοια αποδεικνύεται ότι οι παρατηρήσεις στα παραπάνω παραδείγματα ισχύουν γενικά. Έχουμε δηλαδή το

Θεώρημα VIII.2.1 (Τετραγωνικός νόμος αντιστροφής)**.** *Έστω q περιττός πρώτος. Τότε το $\mathrm{Spl}(x^2-q)$ ορίζεται μέσω ισοτιμιών modulo q αν $q \equiv 1 \mod 4$ και μέσω ισοτιμιών $\mod 4q$ αν $q \equiv 3 \mod 4$.*

Πριν προχωρήσουμε θα δώσουμε μια απόδειξη του τετραγωνικού νόμου αντιστροφής με χρήση του κυκλοτομικού νόμου ανάλυσης της οποίας η αρχική ιδέα οφείλεται στον Kronecker.

[1] http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

Ξαναθυμίζουμε ότι εξ ορισμού για $a \in \mathbb{Z}$, p πρώτο, $p \neq 2$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{όταν η } x^2 \equiv a \mod p \text{ έχει λύση} \\ -1 & \text{όταν η } x^2 \equiv a \mod p \text{ δεν έχει λύση} \\ 0 & \text{όταν } p \mid a \end{cases}$$

ενώ

$$\left(\frac{a}{2}\right) = \begin{cases} (-1)^{\frac{a^2-1}{8}}, & \text{όταν } 2 \nmid a \\ 0, & \text{όταν } 2 \mid a \end{cases}$$

1. Επίσης το σύμβολο του Kronecker είναι πολλαπλασιαστικός χαρακτήρας: Για κάθε $a, b \in \mathbb{Z}$ και p πρώτο, $p \nmid ab$ έχουμε $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
2. Το κριτήριο του Euler: για $p \neq 2$, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$.

Λήμμα VIII.2.2. *Έστω p πρώτος, $p \neq 2$. Τότε το $\mathbb{Q}(\zeta_p)$ έχει ακριβώς ένα τετραγωνικό υπόσωμα, το $K_2 = \mathbb{Q}(\sqrt{p^*})$, με $p^* = (-1)^{\frac{p-1}{2}} p$.*

Απόδειξη. Η ομάδα $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^*$ είναι κυκλική τάξεως $p - 1 \equiv 0 \mod 2$. Συνεπώς υπάρχει ακριβώς μία υποομάδα της G τάξης $\frac{p-1}{2}$, δηλαδή ένα υπόσωμα του $\mathbb{Q}(\zeta_p)$, το K_2 ώστε $[K_2; \mathbb{Q}] = 2$.

Απομένει να δείξουμε ότι $K_2 = \mathbb{Q}(\sqrt{p^*})$. Αρκεί να δείξουμε ότι ο p είναι ο μοναδικός πρώτος που διαιρεί τη διακρίνουσα του K_2, διότι τότε

$$D_{K_2} = \pm p$$

και επειδή $D_{K_2} \equiv 0, 1 \mod 4$ έχουμε $D_{K_2} = (-1)^{\frac{p-1}{2}} p$ έχουμε ότι $K_2 = \mathbb{Q}(\sqrt{D_{K_2}}) = \mathbb{Q}(\sqrt{p^*})$.

Έστω λοιπόν q πρώτος, σύμφωνα με το θεώρημα της διακρίνουσας ο $q \mid D_{K_2}$ ο q διακλαδίζεται στο σώμα $K_2 \subset \mathbb{Q}(\zeta_p)$, συνεπώς ο q διακλαδίζεται στο $\mathbb{Q}(\zeta_p)$ και $q \mid p$, συνεπώς $q = p$. □

Λήμμα VIII.2.3. *Έστω p, q πρώτοι αριθμοί, $p \neq q$, $p \neq 2$ (επιτρέπουμε στο q να είναι και 2). Έστω*

$$qS = Q_1 \cdots Q_r$$

η ανάλυση του q στο $\mathbb{Q}(\zeta_p)$. Τότε ισχύει $\left(\frac{q}{p}\right) = 1$ αν και μόνο αν $2 \mid r$.

Λήμμα VIII.2.4. *Έχουμε τις ίδιες ακριβώς υποθέσεις όπως και στο λήμμα VIII.2.3. Τότε*

$$\left(\frac{p^*}{q}\right) = 1 \text{ αν και μόνο αν } 2 \mid r.$$

Απόδειξη. (του τετραγωνικού νόμου αντιστροφής) Από τα λήματα VIII.2.3 και VIII.2.4 προκύπτει ότι

$$\left(\frac{q}{p}\right) = 1 \text{ αν και μόνο αν } \left(\frac{p^*}{q}\right) = 1$$

επομένως

$$\left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right) = 1$$

για όλους τους πρώτους αριθμούς p, q, $p \neq 2 \neq q$. Ισχύει

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right),$$

δηλαδή

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}.$$

□

Σημείωση VIII.2.5. • Το ότι ο $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$ φαίνεται καλύτερα από τη γνωστή σχέση των αθροισμάτων Gauss:

$$\pm\sqrt{p^*} = \sum_{x \bmod p} \left(\frac{x}{p}\right)\zeta_p^x$$

• Όμοια αποδεικνύεται και το $\left(\frac{2}{p}\right) = \left(\frac{p}{2}\right) = (-1)^{\frac{p^2-1}{8}}$ για πρώτο $p \neq 2$.

Απόδειξη. (του λήμματος VIII.2.3) Έστω ότι $\mathbb{F}_p^* = \langle\overline{x}_0\rangle$, $\overline{x}_0 \equiv x_0 \mod p$ και έστω U_p η μοναδική υποομάδα της κυκλικής ομάδας $\mathbb{F}_p^*$ τάξεως $\frac{p-1}{2}$ η οποία είναι προφανώς η $U_p = \langle\overline{x}_0^2\rangle$. Έχουμε

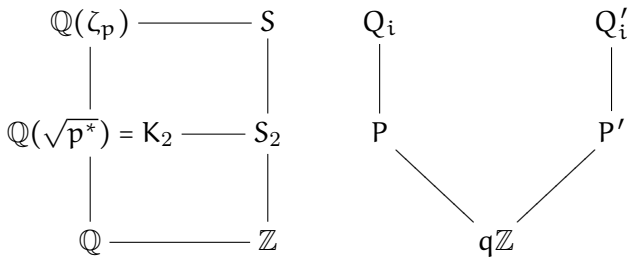
$$\left(\frac{q}{p}\right) = 1 \Leftrightarrow x^2 \equiv q \mod p \text{ έχει λύση } \Leftrightarrow q \mod p \in U_p \Leftrightarrow \operatorname{ord}(q \mod p) \mid \frac{p-1}{2}.$$

Η τάξη όμως της κλάσης $q \mod p$ είναι ο βαθμός αδράνειας του q στο $\mathbb{Q}(\zeta_p)$, δηλαδή

$$\left(\frac{q}{p}\right) = 1 \Leftrightarrow f \mid \frac{p-1}{2}$$

και επειδή $fr = p - 1$ το παραπάνω συμβαίνει αν και μόνο αν $2 \mid r$. □

Απόδειξη. (Του λήμματος VIII.2.4) Έστω ότι $\left(\frac{p^*}{q}\right) = 1$ συνεπώς το q αναλύεται πλήρως στο K_2, δηλαδή $qS_2 = PP'$ με $P \neq P'$.



Επειδή $q \nmid p$ έχουμε $e(Q_i/P) = e(Q_i'/P) = 1$ από τον νόμο ανάλυσης κυκλοτομικών σωμάτων, δηλαδή $PS = Q_1Q_2\cdots Q_k$ και $P'S = Q_1'Q_2'\cdots Q_{k'}'$. Συνεπώς

$$qS = qS_2S = Q_1Q_2\cdots Q_k \cdot Q_1'Q_2'\cdots Q_{k'}'.$$

Θα δείξουμε ότι $k = k'$ οπότε θα έχουμε το ζητούμενο, δηλαδή

$$r = 2k \equiv 0 \bmod 2 \Rightarrow 2 \mid r.$$

Η επέκταση $K_2/\mathbb{Q}$ είναι επέκταση του Galois, συνεπώς υπάρχει $\sigma \in \mathrm{Gal}(K_2/\mathbb{Q})$ με $\sigma(P) = P'$. Έστω $\widehat{\sigma} \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ μια επέκταση του σ, $\widehat{\sigma}(P) = P'$. Έχουμε

$$\widehat{\sigma}(Q_1)\cdots\widehat{\sigma}(Q_k) = \widehat{\sigma}(Q_1\cdots Q_k) = \widehat{\sigma}(PS) = P'S = Q_1'\cdots Q_{k'}'.$$

Το μονοσήμαντο της ανάλυσης σε πρώτα ιδεώδη στον S δίνει $k = k'$.

Αντιστρόφως, υποθέτουμε ότι $2 \mid r$. Ισχυριζόμαστε ότι το q αναλύεται πλήρως στο K_2, δηλαδή ότι $\left(\frac{p^*}{q}\right) = 1$. Την ανάλυση

$$qS = Q_1\cdots Q_r$$

τη γράφουμε ως

$$qS = \left(\prod_{\substack{\sigma \in G \\ \sigma \mod G_Z}} \sigma(Q) \right),$$

όπου $Q = Q_1$ και $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ και G_Z είναι η ομάδα ανάλυσης του Q. Θεωρούμε την $G_2 = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_2)$. Ισχύει $[G : G_2] = [K_2 : \mathbb{Q}] = 2$. Λόγω της υπόθεσης $2 \mid r$ έχουμε $[G : G_Z] = r \equiv 0 \mod 2$ και κατά συνέπεια $\#G_Z \mid \#G_2$ και αφού η G είναι κυκλική τάξης $p-1$ έχει μοναδική υποομάδα για κάθε διαιρέτη του $p-1$ συνεπώς $G_Z \leq G_2$.

Γράφουμε τώρα $G = G_2 \sqcup \tau G_2$ συνεπώς

$$\begin{aligned} qS &= \left(\prod_{\substack{\sigma \in G \\ \sigma \mod G_Z}} \sigma(Q) \right) \\ &= \left(\prod_{\substack{\sigma \in G_2 \\ \sigma \mod G_Z}} \sigma(Q) \right) \tau \left(\prod_{\substack{\sigma \in G_2 \\ \sigma \mod G_Z}} \sigma(Q) \right) \end{aligned} \tag{VIII.1}$$

Έστω $P = Q \cap K_2$,

$$PS = \left(\prod_{\substack{\sigma \in G_2 \\ \sigma \mod G'_Z}} \sigma(Q) \right)^{e_2}$$

όπου

$$G'_Z = \{\sigma \in G_2 : \sigma(Q) = Q\}$$

η ομάδα ανάλυσης του Q στην επέκταση $\mathbb{Q}(\zeta_p)/K_2$. Έχουμε $e_2 = 1$, διότι $q \nmid p$ και το q δεν διακλαδίζεται και συνεπώς το ίδιο ισχύει για το P.

Προφανώς $G'_Z = G_2 \cap G_Z = G_Z$ διότι $G_Z \leq G_2$, άρα

$$PS = \left(\prod_{\substack{\sigma \in G_2 \\ \sigma \mod G_Z}} \sigma(Q) \right). \tag{VIII.2}$$

Από τις (VIII.1) και (VIII.2) έχουμε ότι το q δεν αδρανεί στο K_2 διότι διαφορετικά $qS_2 = P$ συνεπώς $qS = PS$, δηλαδή οι αναλύσεις στα (VIII.1) και (VIII.2) θα έπρεπε να είναι ίσες, άτοπο.

Το $q \neq p$ συνεπώς το q δεν διακλαδίζεται στο K_2 και επομένως το q αναλύεται στο K_2 και $\left(\frac{p^*}{q}\right) = 1$. □

Βέβαια η απόδειξη φαίνεται σαν να «ξύνουμε το αριστερό αυτί με το δεξί χέρι και μάλιστα φέρνοντάς το πίσω από το κεφάλι!»,

It may be thought that this proof, pretty as it is, is much more complicated than the previous proof and so does not add much. This is not the case, because the ideas involved provide the key to studying higher reciprocity laws, [6, σελ. 200].

VIII.3 Διτετραγωνικός και κυβικός νόμος αντιστροφής

Ο Gauss προσπάθησε, μετά τον τετραγωνικό νόμο αντιστροφής, να αποδείξει τον διτετραγωνικό νόμο αντιστροφής. Διατύπωσε τον νόμο, αλλά δεν κατάφερε να τον αποδείξει. Διαπίστωσε πάντως ότι ο κατάλληλος δακτύλιος στον οποίο πρέπει να εργαστεί δεν είναι πλέον ο δακτύλιος των ακεραίων, αλλά ο δακτύλιος $\mathbb{Z}[i]$, ο δακτύλιος του Gauss, όπως ονομάζεται σήμερα.

Στην αριθμητική του δακτυλίου $\mathbb{Z}[i]$ αναφερόμαστε στο Παράρτημα. Έστω π ένα ανάγωγο (πρώτο) στοιχείο του $\mathbb{Z}[i]$ και $\alpha \in \mathbb{Z}[i]$ τέτοιο ώστε $\pi \nmid \alpha$. Τότε το θεώρημα του Fermat, για $K = \mathbb{Q}(i)$ μας δίνει

$$\alpha^{N_{K/\mathbb{Q}}(\pi)-1} \equiv 1 \mod \pi.$$

Στη συνέχεια θα ορίσουμε το διτετραγωνικό σύμβολο του Legendre $\left(\frac{\alpha}{\pi}\right)_4$ ή $\chi_\pi(\alpha)$.

Πρόταση VIII.3.1. *Αν $\pi \nmid \alpha$ και $\langle\pi\rangle \neq \langle 1+i\rangle$ τότε υπάρχει ένας μοναδικός ακέραιος j, $0 \leq j \leq 3$, για τον οποίο ισχύει*

$$\alpha^{\frac{N_{K/\mathbb{Q}}(\pi)-1}{4}} \equiv i^j \mod \pi$$

Απόδειξη. Λόγω της υπόθεσης $\langle\pi\rangle \neq \langle 1+i\rangle$ έπεται ότι οι αριθμοί $1, -1, i, -i$ ανήκουν σε διαφορετικές κλάσεις modulo π. Όλες είναι λύσεις της ισοτιμίας $x^4 \equiv 1 \mod \pi$. Αλλά η κλάση υπολοίπων του $\alpha^{\frac{N_{K/\mathbb{Q}}(\pi)-1}{4}}$ είναι επίσης μια λύση της $x^4 \equiv 1 \mod \pi$. □

Ορισμός VIII.3.2. Έστω π ανάγωγο στοιχείο του $\mathbb{Z}[i]$ $N_{K/\mathbb{Q}}(\pi) \neq 2$. Για κάθε $\alpha \in \mathbb{Z}[i]$, $\pi \nmid \alpha$ ο διτετραγωνικός χαρακτήρας του α ορίζεται ως εξής:

$$\chi_\pi(\alpha) = i^j$$

όπου το j καθορίζεται από την προηγούμενη πρόταση. Αν $\pi \mid \alpha$, τότε $\chi_\pi(\alpha) = 0$

Ισχύουν οι παρακάτω ιδιότητες, [6, prop. 9.8.3]

1. Αν $\pi \nmid \alpha$, τότε

$$\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_4 = 1 \Leftrightarrow \text{ η } x^2 \equiv \alpha \mod \pi \text{ είναι επιλύσιμη στον δακτύλιο } \mathbb{Z}[i]$$

2.

$$\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta)$$

3. Αν $\alpha \equiv \beta \mod \pi$, τότε $\chi_\pi(\alpha) \equiv \chi_\pi(\beta)$

Προκειμένου να ξεχωρίσουμε ένα στοιχείο από το συνεταιρικό του, ορίζουμε ένα ανάγωγο στοιχείο π του $\mathbb{Z}[i]$ να λέγεται primary όταν $\pi \equiv 1 \mod (2+2i)$. Αποδεικνύεται ότι αν π ανάγωγο του $\mathbb{Z}[i]$ ώστε $\pi \nmid (1+i)$, τότε υπάρχει μοναδική μονάδα ϵ του $\mathbb{Z}[i]$ ώστε $\epsilon\pi$ να είναι primary, [6, σελ. 121, lemma 7].

Ο νόμος διτετραγωνικής αντιστροφής διατυπώνεται ως εξής:

Θεώρημα VIII.3.3. *Αν π και θ δύο primary ανάγωγα (πρώτα) στοιχεία του $\mathbb{Z}[i]$, τότε*

$$\left(\frac{\theta}{\pi}\right)_4 = \left(\frac{\pi}{\theta}\right)_4 (-1)^{\frac{N_{K/\mathbb{Q}}(\theta)-1}{4}\frac{N_{K/\mathbb{Q}}(\pi)-1}{4}}.$$

Όπως, στον τετραγωνικό νόμο αντιστροφής έχουμε και τους συμπληρωματικούς νόμους

$$\left(\frac{i}{\pi}\right)_4 = i^{-\frac{(a-1)}{2}} \text{ και}$$
$$\left(\frac{1+i}{\pi}\right)_4 = i^{\left(\frac{a-b-1-b^2)}{4}\right.}.$$

δείτε [6, Παρ. 9.9 σελ. 123, Ασκήσεις 32-37, σελ. 176].

Θεώρημα VIII.3.4.

(i) Αν $\pi = a + bi$ *ένα primary ανάγωγο στοιχείο του* $\mathbb{Z}[i]$*, τότε*

$$\left(\frac{2}{\pi}\right)_4 = i^{\frac{a\cdot b}{2}}$$

(ii) Αν p *πρώτος αριθμός, τότε ο* $p = x^2 + 64y^2, x, y \in \mathbb{Z}$ *αν και μόνο αν* $p \equiv 1 \mod 4$ *και το* 2 *είναι διτετραγωνικό υπόλοιπο modulo* p*.*

Απόδειξη. Σε πρώτο βήμα αποδεικνύουμε ότι (i)⇒(ii)

Έστω λοιπόν p πρώτος (ακέραιος) αριθμός και $p \equiv 1 \mod 4$. Γράφουμε το $p = a^2 + b^2 = \pi\overline{\pi}$, όπου π primary πρώτος του $\mathbb{Z}[i]$. Ο π είναι primary, άρα $\pi \equiv 1 \mod (2+2i)$. Συνεπώς ο

$$\frac{\pi - 1}{2+2i} \in \mathbb{Z}[i] \Rightarrow \frac{[(a-1)+bi]}{2+2i} \in \mathbb{Z}[i]$$

που σημαίνει ότι

$$\frac{a-1+b}{4} + \frac{b-a+1}{4}i \in \mathbb{Z}[i].$$

Επομένως $a + b \equiv 1 \mod 4$ και $a - b \equiv 1 \mod 4$, συνεπώς $2a \equiv 2 \mod 4$ από όπου έχουμε

$$a \equiv 1 \mod 2 \text{ και } 2b \equiv 0 \mod 4, \text{ δηλαδή } b \equiv 0 \mod 2.$$

Επειδή $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$ η (i) μας δίνει ότι ο 2 είναι διτετραγωνικό υπόλοιπο modulo p αν και μόνο αν $i^{\frac{a\cdot b}{2}} = 1$ αν και μόνο αν $8 \mid b$.

Τώρα $p \equiv 1 \mod 4$ αν και μόνο αν $p = a^2 + b^2$, $a, b \in Z$, $(p \neq 2)$ και $8 \mid b$ αν και μόνο αν $p = x^2 + 64y^2$, $x, y \in \mathbb{Z}$. Αποδείξαμε το (ii), υπό την προϋπόθεση ότι ισχύει το (i). Την απόδειξή του (i) την αφήνουμε ως άσκηση. □

Ανάλογα εργαζόμαστε και για την εύρεση και διατύπωση ενός κυβικού νόμου αντιστροφής. Εδώ ο δακτύλιος στον οποίο εργαζόμαστε είναι ο $\mathbb{Z}[\omega]$, όπου ω μια κυβική πρωταρχική 3-ρίζα της μονάδας. Περιγράφουμε εν συντομία τη διαδικασία. Ο δακτύλιος $\mathbb{Z}[\omega]$ είναι περιοχή κυρίων ιδεωδών. Οι μονάδες του είναι $E(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}$. Ο νόμος ανάλυσης στο $K = \mathbb{Q}(\omega)$ διατυπώνεται ως εξής: Έστω p ένας πρώτος αριθμός.

1. Αν $p = 3$, τότε το $1 - \omega$ είναι ανάγωγο (πρώτο) στοιχείο του $\mathbb{Z}[\omega]$ και ισχύει $3 = -\omega^2(1-\omega)^2$.
2. Αν $p \equiv 1 \mod 3$, τότε υπάρχει μοναδικός πρώτος $\pi \in \mathbb{Z}[\omega]$, ώστε $p = \pi\overline{\pi}$ και $\pi \nmid \overline{\pi}$ στον $\mathbb{Z}[\omega]$.
3. Αν $p \equiv 2 \mod 3$, τότε ο p παραμένει πρώτος στον δακτύλιο $\mathbb{Z}[\omega]$ και συνεταιρικός προς έναν από τους παραπάνω πρώτους.

Από το θεώρημα του Fermat προκύπτει ότι: Αν π πρώτος του $\mathbb{Z}[\omega]$, $\alpha \in \mathbb{Z}[\omega]$ και $\pi \nmid \alpha$, τότε

$$\alpha^{N_{K/\mathbb{Q}}(\pi)-1} \equiv 1 \mod \pi$$

Έστω τώρα ένας πρώτος που δεν διαιρεί το 3, δηλάδή π όχι συνεταιρικός του $1 - \omega$. Οι κλάσεις του $1, \omega, \omega^2$ είναι διαφορετικές modulo π. Αφού $\{1, \omega, \omega^2\}$ κυκλική ομάδα έπεται ότι

$$3 \mid \left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^* = N_{K/\mathbb{Q}}(\pi) - 1.$$

Από τα παραπάνω προκύπτει ότι αν $x := \alpha^{\frac{N_{K/\mathbb{Q}}(\pi)-1}{3}}$, τότε $x^3 \equiv 1 \mod \pi$. Αλλά

$$x^3 - 1 \equiv (x-1)(x-\omega)(x-\omega^2) \mod \pi,$$

οπότε, αφού ο π είναι πρώτος έχουμε ότι ο π θα πρέπει να διαιρεί έναν από τους τρεις παράγοντες του αριστερού μέλους. Επομένως,

$$\alpha^{\frac{N_{K/\mathbb{Q}}(\pi)-1}{3}} \equiv 1, \omega, \omega^2 \mod \pi$$

και επειδή τα $1, \omega, \omega^2$ δεν είναι μεταξύ τους ισότιμα modulo π μπορούμε να ορίσουμε το κυβικό σύμβολο αντιστροφής (κυβικό χαρακτήρα).

Ορισμός VIII.3.5. Έστω π πρώτος του $\mathbb{Z}[\omega]$, όχι συνεταιρικός προς τον $1-\omega$ και $\pi \nmid \alpha$. Το κυβικό σύμβολο αντιστροφής ορίζεται ως η μοναδική κυβική ρίζα της μονάδας για την οποία ισχύει

$$\alpha^{\frac{N_{K/\mathbb{Q}}(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \mod \pi$$

Αν $\pi \mid \alpha$, τότε ορίζουμε $\left(\frac{\alpha}{\pi}\right)_3 = 0$.

Ανάλογες προς το διτετραγωνικό σύμβολο αντιστροφής ισχύουν οι ιδιότητες, [6, Prop. 9.3.3]

1. Αν $\pi \nmid \alpha$, τότε

$$\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3 = 1 \Leftrightarrow \left(\text{ όταν η ισοτιμία } x^3 \equiv \alpha \mod \pi \text{ είναι επιλύσιμη στον } \mathbb{Z}[\omega]\right),$$

δηλαδή ακριβώς όταν το α είναι κυβικό υπόλοιπο modulo π.

2.

$$\chi_\pi(\alpha\beta) = \left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 = \chi_\pi(\alpha)\chi_\pi(\beta)$$

3. Αν $\alpha \equiv \beta \mod \pi$, τότε $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

Προκειμένου να διατυπώσουμε τον κυβικό νόμο αντιστροφής, χρειαζόμαστε και πάλι την έννοια του primary πρώτου στοιχείου του $\mathbb{Z}[\omega]$.

Ορισμός VIII.3.6. Ένα πρώτο στοιχείο π του $\mathbb{Z}[\omega]$ θα λέγεται primary όταν $\pi \equiv 2 \mod 3$. Αν το $\pi = q$, ένας ρητός πρώτος, τότε γνωρίζουμε ότι $q \equiv 2 \mod 3$. Συνεπώς δεν έχουμε κάτι καινούργιο. Αν $\pi = a + b\omega$ πρώτος (μιγαδικός) αριθμός, τότε π primary σημαίνει $a \equiv 2 \mod 3$ και $b \equiv 0 \mod 3$. Και εδώ ισχύει αυτό που θέλουμε, δηλαδή αν $N_{K/\mathbb{Q}}(\pi) = p \equiv 1 \mod 3$, τότε από τους 6 συνεταιρικούς κάθε στοιχείου ακριβώς ένας είναι primary, [6, σελ. 113].

Ακολουθεί ο νόμος της κυβικής αντιστροφής:

Θεώρημα VIII.3.7. *Έστω* π *και* θ *δύο primary πρώτοι του* $\mathbb{Z}[\omega]$*, όχι συνεταιρικοί ως προς το* $(1-\omega)$*, δηλαδή* $N_{K/\mathbb{Q}}(\pi) \neq 3$ *και* $N_{K/\mathbb{Q}}(\theta) \neq 3$ *και για τους οποίους ισχύει*

$$N_{K/\mathbb{Q}}(\pi) \neq N_{K/\mathbb{Q}}(\theta).$$

Ισχύει

$$\chi_\pi(\theta) = \left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3 = \chi_\theta(\pi).$$

Έχουμε και τους αντίστοιχους συμπληρωματικούς τύπους για το $\left(\frac{\omega}{\pi}\right)_3$ *και* $\left(\frac{1-\omega}{\pi}\right)_3$*. Έστω* π *πρώτος όχι συνεταιρικός προς τον* $(1-\omega)$*. Αν* $\pi = q$ *πρώτος ακέραιος, τότε* $q \equiv 2 \mod 3$*. Τον γράφουμε στη μορφή* $q = 3m-1$*. Αν* $\pi = a+b\omega$*, primary (μιγαδικός) πρώτος, τότε γράφουμε* $a = 3m-1$*. Υπό τις παραπάνω προϋποθέσεις ισχύει*

$$\chi_\pi(1-\omega) = \left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}.$$

Αν γράψουμε τον $\pi \equiv 2 \mod 3$ *στη μορφή* $\pi = -1+3m+3n\omega$*, τότε*

$$\chi_\pi(\omega) = \left(\frac{\omega}{\pi}\right)_3 = \omega^{m+n},$$

δείτε [6, Th. 1, 1', σελ. 114].

Στη συνέχεια θα εξετάσουμε την περίπτωση των κυβικών υπολοίπων ως προς πρώτους ακέραιους αριθμούς. Το πρόβλημα είναι το εξής: Αν p πρώτος αριθμός, πότε έχει η ισοτιμία $x^3 \equiv a \mod p$, $a \in \mathbb{Z}$ μία ακέραια λύση; Αν $p = 3$, αυτό ισχύει πάντοτε, αφού για κάθε ακέραιο a ισχύει $a^3 \equiv a \mod 3$. Αν $p \equiv 2 \mod 3$, η συνάρτηση

$$\phi : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \ni a \mod p \longmapsto a^3 \mod p \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$$

επάγει έναν αυτομορφισμό της ομάδας $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, αφού $3 \nmid (p-1)$. Συνεπώς, αν $p \equiv 2 \mod 3$, και πάλι η ισοτιμία έχει πάντοτε λύση. Έστω λοιπόν τώρα $p \equiv 1 \mod 3$, οπότε

$$p = \pi\overline{\pi}, \qquad \pi, \overline{\pi} \text{ πρώτοι του } \mathbb{Z}[\omega].$$

Επομένως $f(\pi/p) = 1$, δηλαδή

$$\frac{Z[\omega]}{\pi\mathbb{Z}[\omega]} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

Αν τώρα $p \nmid a$ έχουμε

$$(x^3 \equiv a \mod \pi \text{ είναι επιλύσιμη στο } \mathbb{Z}) \Leftrightarrow (x^3 \equiv a \mod \pi) \text{ είναι επιλύσιμη στο } \mathbb{Z}[\omega]) \Leftrightarrow \left(\frac{a}{\pi}\right)_3 = 1.$$

Παρατήρηση VIII.3.8. Η ομάδα $(\mathbb{Z}/p\mathbb{Z})^*$ διασπάται σε τρία μέρη ίσου πλήθους εκ των οποίων το ένα είναι τα κυβικά υπόλοιπα και τα άλλα δύο μη-κυβικά υπόλοιπα.

Στη συνέχεια θα αποδείξουμε το

Θεώρημα VIII.3.9. *Έστω* p *ένας πρώτος αριθμός. Ο* $p = x^2+27y^2$*,* $x, y \in \mathbb{Z}$ *τότε και μόνο τότε όταν* $p \equiv 1 \mod 3$ *και το* 2 *είναι κυβικό υπόλοιπο modulo* p*.*

Απόδειξη. Έστω $p = x^2 + 27y^2$. Αυτό αμέσως συνεπάγεται ότι $p \equiv x^2 \equiv 1 \mod 3$. Αρκεί λοιπόν να αποδείξουμε ότι το 2 είναι κυβικό υπόλοιπο modulo p. Το

$$p = x^2 + 27y^2 = (x + 3\sqrt{-3}y)(x - 3\sqrt{-3}y) = \pi\overline{\pi},$$

όπου $\pi = x + 3\sqrt{-3}y$. Αυτή είναι η ανάλυση του p σε γινόμενο πρώτων στον $\mathbb{Z}[\omega]$.

Επομένως, από τα παραπάνω έχουμε ότι το 2 είναι κυβικό υπόλοιπο modulo p, τότε και μόνο τότε όταν $\left(\frac{2}{\pi}\right)_3 = 1$. Αλλά το π είναι primary (γιατί;) καθώς επίσης και το 2. Επομένως ο κυβικός νόμος αντιστροφής μας δίνει

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3.$$

Αρκεί να αποδείξουμε ότι $\left(\frac{\pi}{2}\right)_3 = 1$. Αλλά $N_{K/\mathbb{Q}}(2) - 1 = 4 - 1 = 3$, οπότε η ισοτιμία

$$\alpha^{\frac{N_{K/\mathbb{Q}}(\pi)}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \mod \pi$$

γράφεται $\left(\frac{\pi}{2}\right)_3 \equiv \pi \mod 2$. Θα πρέπει λοιπόν να αποδείξουμε ότι $\pi \equiv 1 \mod 2$. Το $\pi = x + 3\sqrt{-3}y$. Το $\sqrt{-3} = 1 + 2\omega$. Συνεπώς $\pi = x + 3y + 6y\omega$ συνεπώς $\pi = x + 3y \equiv x + y \mod 2$. Αλλά τα x και y πρέπει να είναι ετερότυποι, αφού $p = x^2 + 27y^2$ οπότε $x + y \equiv 1 \mod 2$.

Αντίστροφα, υποθέτουμε ότι $p \equiv 1 \mod 3$ και ότι το 2 είναι κυβικό υπόλοιπο modulo p. Γράφουμε το $p = \pi \cdot \overline{\pi}$, και χωρίς βλάβη της γενικότητας υποθέτουμε ότι π είναι ένας primary πρώτος. Αυτό σημαίνει ότι $\pi = a + 3b\omega$ και $a \equiv 2 \mod 3$. Επομένως,

$$4p = 4\pi\overline{\pi} = 4(a + 3b\omega)(a + 3b\omega^2) = 4(a^2 - 4ab + 9b^2) = (2a - 3b)^2 + 27b^2.$$

Τώρα θα πρέπει να αποδείξουμε ότι το b είναι άρτιος. Θα χρησιμοποιήσουμε τη δεύτερη υπόθεση ότι το 2 είναι τετραγωνικό υπόλοιπο modulo p. Και πάλι από την ισοδυναμία πριν τη διατύπωση του θεωρήματος, έχουμε $\left(\frac{2}{\pi}\right)_3 = 1$ και από τον κυβικό νόμο αντιστροφής έχουμε $\left(\frac{\pi}{2}\right)_3 = 1$. Από την ισοτιμία $\left(\frac{\pi}{2}\right)_3 \equiv \pi \mod 2$ έπεται ότι $\pi \equiv 1 \mod 2$ συνεπώς $a + 3b\omega \equiv 1 \mod 2$ άρα $3b\omega = 2\lambda\omega$ οπότε $2 \mid 3b$ και καταλήγουμε στο $2 \mid b$. □

Παρατήρηση VIII.3.10. Τα δύο τελευταία θεωρήματα των δύο υποπαραγράφων ήταν εικασίες του Euler, από το 1748-1750.

Παρατήρηση VIII.3.11. Όπως ήδη παρατηρήσατε, για λόγους οικονομίας χρόνου χρησιμοποιήσαμε δύο εξαιρετικά βιβλία. Αμφότερα περιέχουν και εκτεταμένες ιστορικές αναφορές, [1, παρ. 4 C, σελ. 83-89] και [6, κεφ. 9ο, σελ. 133-134]. Θεωρούμε χρέος μας να σας συστήσουμε να τα μελετήσετε.

Παρατήρηση VIII.3.12. Φυσικά είναι δυνατό να ορίσουμε το n-στό σύμβολο του Legendre, για κάθε φυσικό αριθμό n. Παρατηρούμε ότι το διτετραγωνικό σύμβολο ορίστηκε στον δακτύλιο των ακεραίων αλγεβρικών $\mathbb{Z}[i]$ του σώματος $\mathbb{Q}(i)$, ο οποίος περιέχει τις 4-ρίζες της μονάδας. Επίσης το κυβικό σύμβολο ορίστηκε στον δακτύλιο ακεραίων αλγεβρικών $\mathbb{Z}[\omega]$ του $K = \mathbb{Q}(\omega)$, ο οποίος περιέχει τις 3-ρίζες της μονάδας.

Για το n-στό σύμβολο θα πρέπει να το ορίσουμε ως προς κάποιο αλγεβρικό σώμα αριθμών του οποίου ο δακτύλιος περιέχει μια πρωταρχική, και συνεπώς όλες, τις n-στες ρίζες της μονάδας και φυσικά έχουμε αντίστοιχο νόμο αντιστροφής.

VIII.4 Το σύμβολο του Frobenius

Προτού προχωρήσουμε, παρατηρούμε ότι ο νόμος ανάλυσης των κυκλοτομικών πολυωνύμων δίνει αμέσως:

$$\mathrm{Spl}(\Phi_n(x)) = \{p \in \mathbb{P} : p \equiv 1 \mod n\},$$

τον οποίο και θα ονομάζουμε και κυκλοτομικό νόμο αντιστροφής. Αυτό που παρατηρούμε είναι ότι και ο κυκλοτομικός νόμος αντιστροφής ορίζεται μέσω ισοτιμιών.

VIII.4.1 Το 9ο πρόβλημα του Hilbert

Το 9ο πρόβλημα του Hilbert (πρόκειται για μια σειρά προβλημάτων που έθεσε ο Hilbert, σαν τα βασικά προβλήματα των Μαθηματικών που μπαίνουν άλυτα στο κατώφλι του 20ού αιώνα. Η διάλεξη δόθηκε στο Παγκόσμιο Συνέδριο των Μαθηματικών στα 1900, στο Παρίσι) ασχολείται με την εύρεση του «πιο» γενικού νόμου αντιστροφής σε κάθε αλγεβρικό σώμα αριθμών. Η λύση του προβλήματος προέκυψε μέσω της class field theory για όλες τις αβελιανές επεκτάσεις τόσο απόλυτες $L/\mathbb{Q}$) όσο και σχετικές (L/K, K αλγεβρικό σώμα αριθμών) από τον Artin. Για μη αβελιανές επεκτάσεις Galois το γενικό πρόβλημα είναι ανοιχτό. Υπάρχουν σχετικές εικασίες (πρόγραμμα Langlands).

Όπως ακριβώς αποδεικνύεται ότι η επέκταση $F/\mathbb{F}_p$ πεπερασμένων σωμάτων είναι κυκλική επέκταση του Galois και παράγεται από τον αυτομορφισμό $\sigma : F \ni x \mapsto x^p \in F$, εντελώς όμοια αποδεικνύεται ότι και η επέκταση $\mathbb{F}_{q^n}/\mathbb{F}_q$, με $q = p^s$, p πρώτος είναι κυκλική επέκταση του Galois και παράγεται από τον αυτομορφισμό

$$\sigma : \mathbb{F}_{q^n} \ni x \mapsto x^q \in \mathbb{F}_{q^n}$$

καλούμενο και αυτομορφισμό του Frobenius.

Έστω λοιπόν L/K επέκταση του Galois αλγεβρικών σωμάτων αριθμών P πρώτο ιδεώδες του R και Q πρώτο ιδεώδες του S $P \mid Q$.

$$\begin{array}{ccc} L & \text{——} & S \\ | & & | \\ | & & | \\ K & \text{——} & R \end{array} \qquad \begin{array}{c} Q \\ | \\ | \\ P \end{array}$$

Η ομάδα $\overline{G} = \mathrm{Gal}(\frac{S/Q}{R/P})$ είναι κυκλική τάξεως $f = [S/Q : R/P]$ και παράγεται από τον αυτομορφισμό του Frobenius:

$$\overline{\sigma} : S/Q \ni \overline{s} = s + Q \mapsto \overline{s}^{N_{K/\mathbb{Q}}(P)} = s^{N_{K/\mathbb{Q}}(P)} + Q \in S/Q.$$

Επειδή $G_Z(Q/P)/G_T(Q/P) \cong \overline{G}$ (Θεώρημα VII.2.8 σελ. 128) υπάρχει $\sigma \in G_Z(Q/P)$ ώστε

$$\sigma(s) = s^{N_{K/\mathbb{Q}}(P)} \mod Q \text{ για κάθε } s \in S \tag{VIII.3}$$

Αν ο Q δεν διακλαδίζεται στην L/K ή, όπερ το αυτό, μιας και η επέκταση είναι επέκταση του Galois, αν το πρώτο ιδεώδες P δεν διακλαδίζεται στην επέκταση L/K, τότε ως γνωστό $G_T(Q/P) = \{1\}$ συνεπώς $G_Z(Q/P) \cong \overline{G}$, δηλαδή υπάρχει ακριβώς ένας K-αυτομορφισμός του L με την ιδιότητα (VIII.3) ο ο οποίος θα λέγεται σύμβολο του Frobenius και θα συμβολίζεται με $\left[\frac{L/K}{P}\right]$.

Παράδειγμα VIII.4.1. Έστω $L = \mathbb{Q}(\zeta_n)$, $K = \mathbb{Q}$, p πρώτος, $p \nmid n$ και Q πρώτο ιδεώδες του L με $Q \mid p\mathbb{Z}$. Τότε

$$\left[\frac{L/K}{Q}\right] = \sigma_p : \zeta_n \mapsto \zeta_n^p.$$

Αρκεί να αποδείξουμε ότι

$$\sigma_p(\alpha) \equiv \alpha^p \mod Q \text{ για κάθε } \alpha \in S.$$

Ισχυριζόμαστε ότι για $M = n^{\phi(n)}$ ισχύει $M \cdot S \subset \mathbb{Z}[\zeta_n]$. Αν ισχύει αυτό έχουμε τελειώσει διότι για κάθε $s \in S$ γράφουμε

$$Ms = \sum_i x_i \zeta^i, \qquad x_i \in \mathbb{Z}$$

και συνεπώς

$$\begin{aligned} \sigma_p(Ms) &= \sum_i x_i \zeta_n^{ip} \equiv \sum_i x_i^p \zeta_n^{ip} \mod pS \\ &\equiv \left(\sum_i x_i \zeta_n^i\right)^p \mod pS \\ &\equiv (Ms)^p \mod Q. \end{aligned}$$

Επίσης, $M \in \mathbb{N}$ και $p \nmid n$ συνεπώς $M^p \equiv M \mod Q$ και $M(\sigma_p(s) - s^p) \equiv 0 \mod Q$. Αφού $p \nmid n$ έχουμε $M \notin Q$ οπότε $\sigma_p(s) \equiv s^p \mod Q$.

Απομένει η απόδειξη του ισχυρισμού. Έχουμε ήδη δείξει πιο μπροστά ότι

$$\frac{1}{D_{L/\mathbb{Q}(\zeta_n)}}\mathbb{Z}[\zeta_n] \supset S \supset \mathbb{Z}[\zeta_n]$$

και ότι $D_{L/\mathbb{Q}(\zeta_n)} \mid n^{\phi(n)}$, συνεπώς

$$\frac{1}{M}\mathbb{Z}[\zeta_n] \supset \frac{1}{D_{L/\mathbb{Q}(\zeta_n)}}\mathbb{Z}[\zeta_n] \supset S$$

οπότε $MS \subset \mathbb{Z}[\zeta_n]$.

Πρόταση VIII.4.2. *Αν L/K επέκταση αλγεβρικών σωμάτων αριθμών, P ένα πρώτο ιδεώδες του R, Q ένα πρώτο ιδεώδες του S, $P \mid Q$ και το P δεν διακλαδίζεται στην L/K, τότε για κάθε $\sigma \in \mathrm{Gal}(L/K)$ ισχύει*

$$\left[\frac{L/K}{\sigma(Q)}\right] = \sigma\left[\frac{L/K}{Q}\right]\sigma^{-1}.$$

Απόδειξη. Κάθε στοιχείο $s \in S$ μπορεί να γραφεί ως $\sigma^{-1}(s')$ με $s' \in S$, οπότε

$$\left[\frac{L/K}{Q}\right]\sigma^{-1}(s') = \left[\frac{L/K}{Q}\right]s \equiv \left(\sigma^{-1}(s')\right)^{N_{K/\mathbb{Q}}(P)} \equiv \sigma^{-1}\left((s')^{N_{K/\mathbb{Q}}(P)}\right) \mod Q$$

Συνεπώς

$$\sigma\left[\frac{L/K}{Q}\right]\sigma^{-1}(s') = (s')^{N_{K/\mathbb{Q}}(P)} \mod \sigma(Q), \text{ για κάθε } s' \in S$$

Η μοναδικότητα του συμβόλου του Frobenius μας δίνει την ζητούμενη της πρότασης ισότητα. □

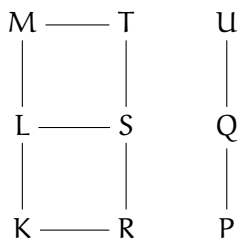
Θεωρούμε τώρα την ιδιαίτερα ενδιαφέρουσα περίπτωση L/K αβελιανή επέκταση. Αν P πρώτο ιδεώδες του K μη διακλαδιζόμενο στην επέκταση L/K, τότε για όλα τα πρώτα ιδεώδη του Q του L με $Q \mid P$, λόγω της πρότασης VIII.4.2 τα σύμβολα του Frobenius συμπίπτουν. Σ' αυτή την περίπτωση το σύμβολο του Frobenius εξαρτάται μόνο από το P, λέγεται σύμβολο του Artin και συμβολίζεται $\left(\frac{L/K}{P}\right)$. Οι πιο πολλές από τις παρακάτω ιδιότητες ισχύουν και για το σύμβολο του Frobenius, αλλά εμείς περιοριζόμαστε πλεον μόνο στην περίπτωση του συμβόλου του Artin.

Σημείωση VIII.4.3. Το σύμβολο του Artin στα κυκλοτομικά σώματα αριθμών επεκτείνεται πολλαπλασιαστικά για κάθε $a \in \mathbb{Z}$ $(a, n) = 1$ μέσω της $\zeta_n \mapsto \zeta_n^a$.

Επειδή το σύμβολο του Artin $\left(\frac{L/K}{P}\right)$ παράγει την ομάδα ανάλυσης, έπεται ότι η τάξη του είναι $f = f(Q/P)$. Ιδιαίτερα:

$$\left(\frac{L/K}{P}\right) = 1 \Leftrightarrow G_Z(Q/P) = \{\mathrm{Id}_L\} \Leftrightarrow P \text{ αναλύεται πλήρως στο } L.$$

Έστω M/K αβελιανή και P μη διακλαδιζόμενο στην M/K. Θεωρούμε μια ενδιάμεση επέκταση $K \subset L \subset M$. Η M/L είναι πάντα επέκταση του Galois, αβελιανή και το πρώτο ιδεώδες $Q = U \cap S$ είναι μη-διακλαδιζόμενο στην M/L.



Πρόταση VIII.4.4. *Τα δύο σύμβολα του Artin, ως προς τις δύο επεκτάσεις συνδέονται μεταξύ τους*

$$\left(\frac{M/K}{P}\right)^{f(Q/P)} = \left(\frac{M/L}{Q}\right)$$

Απόδειξη. Προφανώς $N_{L/\mathbb{Q}}(Q) = N_{K/\mathbb{Q}}(P)^{f(Q/P)}$, διότι $\#S/Q = (\#R/P)^{f(Q/P)}$. Επίσης, εξ ορισμού του συμβόλου του Artin, έχουμε

$$\left(\frac{M/K}{Q}\right) x \equiv x^{N_{K/\mathbb{Q}}(P)} \mod U \text{ για κάθε } x \in T$$

και

$$\left(\frac{M/L}{Q}\right) x \equiv x^{N_{L/\mathbb{Q}}(Q)} \mod U \text{ για κάθε } x \in T$$

Δηλαδή

$$\left(\frac{M/L}{Q}\right) x \equiv x^{N_{K/\mathbb{Q}}(P)^{f(Q/P)}} \mod U \text{ για κάθε } x \in T$$

ή

$$\left(\frac{M/K}{P}\right) x \equiv \left(x^{N_{K/\mathbb{Q}}(P)} \mod U\right)^{f(Q/P)} \text{ για κάθε } x \in T$$

και συνεπώς

$$\left(\frac{M/L}{Q}\right) = \left(\frac{M/K}{P}\right)^{f(Q/P)}.$$

□

Έχουμε ήδη υποθέσει ότι M/K είναι αβελιανή, επομένως και η επέκταση L/K είναι αβελιανή.

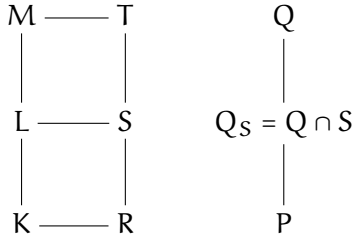
Άρα αν το πρώτο ιδεώδες P του K δεν διακλαδίζεται στο M, τότε δεν θα διακλαδίζεται και στο L, οπότε ορίζονται τα σύμβολα του Artin $\left(\frac{M/K}{P}\right)$ και $\left(\frac{L/K}{P}\right)$. Το ερώτημα είναι ποια σχέση έχουν μεταξύ τους.

Πρόταση VIII.4.5. *Ισχύει το παρακάτω*

$$\mathrm{rest}_L\left(\frac{M/K}{P}\right) = \left(\frac{L/K}{P}\right).$$

Απόδειξη. Αν $\sigma \in G = \mathrm{Gal}(M/K)$ και $\sigma' = \mathrm{res}_L \sigma$ ο περιορισμός του σ στο L, τότε αφού L/K επέκταση του Galois $\sigma' \in \mathrm{Gal}(L/K)$.

Αν τώρα $\sigma \in G_Z(Q/P)$ ισοδύναμα $\sigma(Q) = Q$, οπότε $\sigma'(Q) \cap \sigma'(S) = Q \cap S = Q_S$, δηλαδή $\sigma' = \mathrm{rest}_L \sigma \in G_Z(Q_S/P)$.



Τέλος από τη σχέση

$$\sigma(x) \equiv x^{N_{K/\mathbb{Q}}(P)} \mod Q \text{ για κάθε } x \in T$$

έπεται ότι

$$\sigma'(x) \equiv x^{N_{K/\mathbb{Q}}(P)} \mod Q \text{ για κάθε } x \in S$$

και επειδή $\sigma'(x) - x^{N_{K/\mathbb{Q}}(P)} \in S$ συνεπάγεται $\sigma'(x) - x^{N_{K/\mathbb{Q}}(P)} \in S \cap Q = Q_S$ έχουμε και

$$\sigma'(x) \equiv x^{N_{K/\mathbb{Q}}(P)} \mod Q_S.$$

Αποδείξαμε λοιπόν ότι αν $\sigma = \left(\frac{M/K}{P}\right)$, τότε $\sigma' = \mathrm{rest}_L \sigma = \left(\frac{L/K}{P}\right)$, δηλαδή

$$\mathrm{rest}_L \left(\frac{M/K}{P}\right) = \left(\frac{L/K}{P}\right).$$

□

Αν τώρα θυμηθούμε από την άλγεβρα ότι

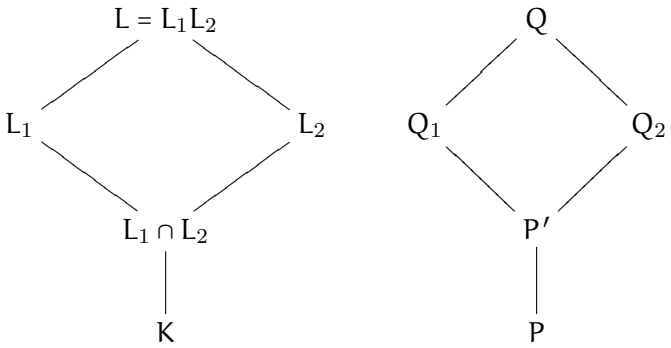
$$\mathrm{Gal}(L/K) = G/H, \text{ όπου } G = \mathrm{Gal}(M/K), H = \mathrm{Gal}(M/L)$$

έχουμε ότι

Πόρισμα VIII.4.6.

$$(P \textit{ αναλύεται πλήρως στο } L) \Leftrightarrow \left(\frac{L/K}{P}\right) \in H$$

Έστω τώρα L_i/K, $i = 1, 2$ αβελιανές επεκτάσεις του K και P πρώτο ιδεώδες του K το οποίο δεν διακλαδίζεται στις επεκτάσεις L_i/K (τα L_i θεωρούνται υποσώματα κάποιου σώματος). Σχηματίζουμε τη σύνθεση των σωμάτων L_1 και L_2, L_1L_2.



Είναι γνωστό ότι και η επέκταση L/K είναι αβελιανή και μάλιστα η απεικόνιση

$$\mathrm{Gal}(L/K) \ni \sigma \mapsto (\sigma_1, \sigma_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

είναι μονομορφισμός ομάδων. Στο παραπάνω έχουμε $\sigma_1 = \mathrm{rest}_{L_1}\sigma$, $\sigma_2 = \mathrm{rest}_{L_2}\sigma$. Επιπλέον αν $L_1 \cap L_2 = K$, τότε είναι ισομορφισμός.

Ταυτίζουμε πρότυπα και εικόνες και έτσι θεωρούμε την $\mathrm{Gal}(L/K)$ ως υποομάδα του ευθέως γινομένου $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$. Έστω Q πρώτο ιδεώδες του L $Q \mid P$ και $Q_i = Q \cap L_i$. Επειδή το P δεν διακλαδίζεται στο L_i, $i = 1, 2$ έχουμε ότι $L_i \subset K_T(Q/P)$ και $L = L_1L_2 \subset K_T(Q/P)$, δηλαδή $L = K_T(Q/P)$ δηλαδή το P δεν διακλαδίζεται στην L/K και επομένως ορίζεται στο σύμβολο του Artin $\left(\frac{L/K}{P}\right)$.

Σημείωση VIII.4.7. Το αντίστροφο είναι προφανές. Έστω $\sigma = \left(\frac{L/K}{P}\right) = (\sigma_1, \sigma_2)$. Έχουμε ήδη αποδείξει ότι

$$\sigma_1 = \mathrm{rest}_{L_1}\sigma = \left(\frac{L_1/K}{P}\right), \sigma_2 = \mathrm{rest}_{L_1}\sigma = \left(\frac{L_2/K}{P}\right),$$

οπότε προκύπτει αμέσως ότι

$$\left(\frac{L/K}{P}\right) = \left(\left(\frac{L_1/K}{P}\right), \left(\frac{L_2/K}{P}\right)\right)$$

Άμεσο συμπέρασμα της παραπάνω σχέσης είναι

Πρόταση VIII.4.8.

(P *αναλύεται πλήρως στο* $L = L_1L_2$) $\Leftrightarrow$ (P *αναλύεται πλήρως στο* L_1 *και στο* L_2)

VIII.5 Ο νόμος αντιστροφής του Artin

Στην παράγραφο αυτή θα διατυπώσουμε τον νόμο αντιστροφής του Artin για αβελιανές επεκτάσεις του $\mathbb{Q}$.

Θα χρειαστούμε ένα πολύ σημαντικό

Θεώρημα VIII.5.1 (Kronecker-Weber)**.** *Αν* L *ένα αλγεβρικό σώμα αριθμών, αβελιανή επέκταση του* $\mathbb{Q}$*, τότε αυτό είναι υπόσωμα κάποιου κυκλοτομικού σώματος, δηλαδή υπάρχει ένας φυσικός αριθμός* m *ώστε* $L \subset \mathbb{Q}(\zeta_m)$*, όπου* ζ_m *μία πρωταρχική* m*-ρίζα της μονάδας.*

Το θεώρημα αυτό θα το αποδείξουμε σε επόμενο κεφάλαιο. Κάθε τέτοιο m θα λέγεται ένα modul ορισμού του L (defining modulus).

Ορισμός VIII.5.2. Οδηγός (conductor, Führer) του L λέγεται ο ελάχιστος φυσικός f_L για τον οποίο ισχύει $L \subset \mathbb{Q}(\zeta_{f_L})$.

Υπάρχει πράγματι έλαχιστος, αφού ισχύει (άσκηση)

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)}).$$

Επομένως

$$L \subset \mathbb{Q}(\zeta_m) \Leftrightarrow f_L \mid m.$$

Παράδειγμα VIII.5.3. Έστω $K = \mathbb{Q}(\sqrt{m})$, το m ελεύθερο τετραγώνου, ένα τετραγωνικό σώμα αριθμών. Τότε [7, σελ. 198]

$$f_K = \begin{cases} |m| & \text{αν } m \equiv 1 \mod 4 \\ 4|m| & \text{αν } m \equiv 2,3 \mod 4 \end{cases}$$

Έχουμε ήδη αποδείξει ότι $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Έστω $H_{L,m}$ η υποομάδα της G που αντιστοιχεί στο σώμα L.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_m) & \text{———} & \{1\} \\ | & & | \\ L & \text{———} & H = H_{L,m} \\ | & & | \\ \mathbb{Q} & \text{———} & G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \end{array}$$

Για κάθε $a \in \mathbb{Z}$, $(a,m) = 1$ το σύμβολο του Artin για την κυκλοτομική επέκταση $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ θα συμβολίζεται με σ_a:

$$\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{a\mathbb{Z}}\right) = \sigma_a : \zeta_m \mapsto \zeta_m^a.$$

Από την άλλη

$$H_{L,m} = \{a \mod m : (a,m) = 1, \mathrm{rest}_L \sigma_a = \mathrm{Id}_L\}.$$

Έχουμε ήδη δείξει ότι το σύμβολο του Artin για κάθε μη-διακλαδιζόμενο πρώτο p στο $\mathbb{Q}(\zeta_m)$, δηλαδή $p \nmid m$ για την επέκταση $L/\mathbb{Q}$ δίνεται από τη σχέση:

$$\left(\frac{L/\mathbb{Q}}{p\mathbb{Z}}\right) = \mathrm{rest}_L \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p\mathbb{Z}}\right) = \mathrm{rest}_L(\zeta_m \mapsto \zeta_m^p).$$

VIII.5.1 Νόμος Αντιστροφής του Artin

Για κάθε πρώτο p, $p \nmid m$, η παρακάτω ακολουθία είναι ακριβής:

$$1 \to H_{L,m} \hookrightarrow \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \xrightarrow{\left(\frac{L/\mathbb{Q}}{p\mathbb{Z}}\right)} \mathrm{Gal}(L/\mathbb{Q}) \to 1$$

Δηλαδή το σύμβολο του Artin επάγει έναν ισομορφισμό

$$\frac{(\mathbb{Z}/m\mathbb{Z})^*}{H_{L,m}} \cong \mathrm{Gal}(L/\mathbb{Q}).$$

Ο νόμος ανάλυσης παίρνει τώρα τη μορφή:

Θεώρημα VIII.5.4 (Νόμος ανάλυσης σε αβελιανές επεκτάσεις του $\mathbb{Q}$)**.** *Έστω $L/\mathbb{Q}$ αβελιανή επέκταση, αλγεβρικών σωμάτων αριθμών και m κάποιο defining modulus του σώματος L. Για κάθε $p \nmid m$ η τάξη του συμπλόκου $\overline{p}H$ στην G/H είναι ίση με τον βαθμό f του p στο L. Με $\overline{p}$ συμβολίζουμε την κλάση $p \mod m$.*

Απόδειξη. Αφού $L/\mathbb{Q}$ είναι επέκταση του Galois έχουμε

$$pS = Q_1 \cdots Q_r = \prod_{\sigma \mod G_Z(Q_1/p\mathbb{Z})} \sigma(Q_1)$$

συνεπώς

$$r = [\mathrm{Gal}(L/\mathbb{Q}) : G_Z(Q_1/p\mathbb{Z})]$$

και, αφού $e = 1$ έχουμε $rf = [L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})|$. Άρα

$$f = \#G_Z(Q_1/p\mathbb{Z}).$$

Επίσης, αφού δεν έχουμε διακλάδωση, $G_T(Q_1/p\mathbb{Z}) = \{\mathrm{Id}_L\}$, οπότε

$$G_Z(Q_1/p\mathbb{Z}) \cong \mathrm{Gal}\left(\frac{S/Q_1}{\mathbb{Z}/p\mathbb{Z}}\right)$$

και συνεπώς η $G_Z(Q_1/p\mathbb{Z})$ παράγεται από το σύμβολο του Artin $\left(\frac{L/\mathbb{Q}}{p\mathbb{Z}}\right)$,

$$G_Z(Q_1/p\mathbb{Z}) = \left\langle \left(\frac{L/\mathbb{Q}}{p\mathbb{Z}}\right) \right\rangle.$$

Δηλαδή το f είναι η τάξη του συμβόλου του Artin.

Αν τώρα Q πρώτο ιδεώδες του $\mathbb{Q}(\zeta_m)$ ώστε $Q \mid Q_1 \mid p$, τότε έχουμε ήδη δείξει ότι

$$\left(\frac{L/\mathbb{Q}}{p\mathbb{Z}}\right) = \mathrm{rest}_L \sigma_p,$$

οπότε το f είναι η τάξη του $\mathrm{rest}_L \sigma_p$. Αλλά

$$(\mathrm{rest}_L \sigma_p)^\ell = \mathrm{Id}_L \Leftrightarrow \mathrm{rest}_L(\sigma_p^\ell) = \mathrm{Id}_L \Leftrightarrow \mathrm{rest}_L(\sigma_{p^\ell}) = \mathrm{Id}_L \Leftrightarrow p^\ell \mod m \in H \Leftrightarrow \overline{p}^\ell H = H.$$

Και τελικά έχουμε ότι f είναι η τάξη $\overline{p}H$ στην G/H. □

Έστω τώρα $\mathfrak{m} = \mathfrak{f}_L$, $L/\mathbb{Q}$ αβελιανή, $p \nmid \mathfrak{m}$ και

$$\mathrm{Spl}(L/\mathbb{Q}) := \{p \text{ πρώτος} : p\mathbb{Z} \text{ αναλύεται πλήρως στο } L\}.$$

Λόγω της γνωστής ήδη σχέσεως

$$e \cdot f \cdot g = [L : \mathbb{Q}],$$

έχουμε ότι

$$p \in \mathrm{Spl}(L/\mathbb{Q}) \Leftrightarrow (e = 1 \text{ και } f = 1) \Leftrightarrow (p \nmid \mathfrak{f}_L \text{ και } \overline{p} \in H).$$

Στην τελευταία σχέση χρησιμοποιήσαμε το θεώρημα οδηγού διακλαδώσεως το οποίο αναφέρει ότι

$$(p \mid \mathfrak{f}_L) \Leftrightarrow (p \text{ διακλαδίζεται στο } L).$$

Έστω ότι η H περιέχει τις κλάσεις

$$H = \{\overline{a}_1, \ldots, \overline{a}_s\}, \;\; a_i \in \mathbb{Z}, \overline{a}_i \equiv a_i \mod \mathfrak{f}_L, (a_i, \mathfrak{f}_L) = 1.$$

Το σύμβολο του Artin για a_i είναι

$$\left(\frac{L/\mathbb{Q}}{a_i\mathbb{Z}}\right) : \zeta_{\mathfrak{f}_L} \mapsto \zeta_{\mathfrak{f}_L}^{a_i}.$$

Επομένως

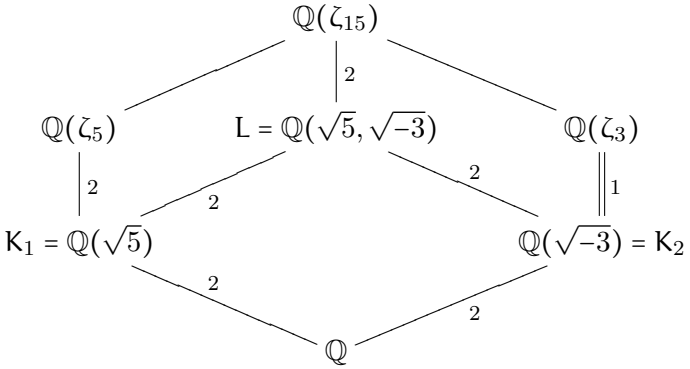
$$(p \nmid \mathfrak{f}_L \text{ και } \overline{p} \in H) \Leftrightarrow (\overline{p} = \overline{a}_i \text{για κάποιο } i).$$

Ώστε

$$(p \in \mathrm{Spl}(L/\mathbb{Q})) \Leftrightarrow (p \equiv a_i \mod \mathfrak{f}_L \text{ για κάποια } a_i),$$

δηλαδή και πάλι το σύνολο $\mathrm{Spl}(L/\mathbb{Q})$ χαρακτηρίζεται μέσω ισοτιμιών.

Παράδειγμα VIII.5.5. Έστω $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$. Έχουμε $K_1 = \mathbb{Q}(\sqrt{5})$, $5 \equiv 1 \mod 4$ άρα $\mathfrak{f}_{K_1} = 5$ και $\mathbb{Q}(\zeta_5) \supset \mathbb{Q}(\sqrt{5})$. Επίσης $K_2 = \mathbb{Q}(\sqrt{-3})$, $-3 \equiv 1 \mod 4$ και $\mathfrak{f}_{K_2} = 3$ και $\mathbb{Q}(\zeta_3) \supset \mathbb{Q}(\sqrt{-3})$.



Έχουμε $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \langle\overline{3}\rangle$. Επίσης $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^* = \{\overline{1}, \overline{2}\} = \langle\overline{2}\rangle$. Επειδή $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ έχουμε ότι $\mathbb{Q}(\zeta_3) = K_2$ και $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}(\sqrt{3})) = \langle\overline{1}\rangle$.

Γνωρίζουμε ότι

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) = \langle 3 \mod 5\rangle \times \langle 2 \mod 3\rangle.$$

Επίσης $[\mathbb{Q}(\zeta_5) : \mathbb{Q}(\sqrt{5})] = 2$ συνεπώς $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})) = \langle\overline{4}\rangle$. Έστω $H = \mathrm{Gal}(\mathbb{Q}(\zeta_{15})/L)$. Η απεικόνιση

$$H \ni \sigma \mapsto \mathrm{rest}_{\mathbb{Q}(\zeta_5)}\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$$

είναι ισομορφισμός. Άρα

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/L) \cong \langle 4 \mod 5\rangle \times \langle 1 \mod 3\rangle.$$

Επομένως

$$H = \mathrm{Gal}(\mathbb{Q}(\zeta_{15})/L) = \langle 4 \mod 15 \rangle = \{4 \mod 15, 1 \mod 15\}.$$

Συμπέρασμα:

$$p \in \mathrm{Spl}(L/\mathbb{Q}) \Leftrightarrow (p \equiv 1, 4 \mod 15).$$

Σημείωση VIII.5.6. Ισχύουν $f_L = 3 \cdot 5$ και $|D_{L/\mathbb{Q}}| = 3^2 \cdot 5^2$.

Στη συνέχεια θα αποδείξουμε ότι το σύμβολο του Artin αποτελεί γενίκευση του συμβόλου του Legendre. Έστω $L = \mathbb{Q}(\sqrt{m})$, $G = \{1, \sigma\} \cong \{\pm 1\}$, μέσω της $1 \mapsto 1$ και $\sigma \mapsto -1$.

Έστω p περιττός πρώτος, $p \nmid f_L$. Ο τετραγωνικός νόμος αντιστροφής δίνει

$$\left(\frac{m}{p}\right) = 1 \Leftrightarrow p \in \mathrm{Spl}(L/\mathbb{Q}).$$

Από την άλλη μεριά:

$$p \in \mathrm{Spl}(L/\mathbb{Q}) \Leftrightarrow (e = 1 \text{ και } f = 1) \Leftrightarrow (p \nmid f_L \text{ και } \overline{p}H = H) \Leftrightarrow \overline{p} \in H \Leftrightarrow \left(\frac{L/\mathbb{Q}}{p\mathbb{Z}}\right) = 1$$

Δηλαδή

$$\left(\frac{m}{p}\right) = 1 \Leftrightarrow \left(\frac{L/\mathbb{Q}}{p\mathbb{Z}}\right) = 1.$$

Θα αποδείξουμε ακόμη ότι ο τετραγωνικός νόμος αντιστροφής είναι συνέπεια του νόμου αντιστροφής του Artin. Ο τετραγωνικός νόμος αντιστροφής σε μία από τις ισοδύναμες μορφές του (βλ. πχ. H. Hasse, *Vorlesungen über Zahlentheorie*, Springer [3]) είναι:

Έστω p, q περιττοί πρώτοι, $a \in \mathbb{Z}, p \nmid a, q \nmid a$ και $p \equiv q \mod 4a$. Τότε

$$(x^2 \equiv a \mod p \text{ έχει λύση }) \Leftrightarrow (x^2 \equiv a \mod q \text{ έχει λύση}).$$

Πράγματι οι παρακάτω σχέσεις είναι ισοδύναμες:

$$x^2 \equiv a \mod p \text{ έχει λύση,}$$

$$x^2 \equiv m \mod p \text{ έχει λύση, όπου } a = r^2 \cdot m, r \nmid m \text{ και ελευθερο τετραγώνου}$$

$$\left(\frac{d}{p}\right) = 1$$

$$p \in \mathrm{Spl}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$$

$$\left(\frac{L/\mathbb{Q}}{p\mathbb{Z}}\right) = 1$$

αφού $p \equiv q \mod 4a$ συνεπώς $p \equiv q \mod 4m$ ισοδύναμα $p \equiv q \mod f_L$

$$\left(\frac{L/\mathbb{Q}}{q\mathbb{Z}}\right) = 1$$

$$\left(\frac{a}{q}\right) = 1$$

$$x^2 \equiv a \mod q \text{ έχει λύση.}$$

Στη συνέχεια θα αποδείξουμε ότι και ο κυβικός νόμος αντιστροφής είναι ειδική περίπτωση του νόμου αντιστροφής του Artin.

Έστω τώρα $K = \mathbb{Q}(\sqrt{-3})$ και $L = K(\sqrt[3]{2})$. Ο δακτύλιος των ακεραίων αλγεβρικών του K είναι ο $R_K = \mathbb{Z}[\omega]$, ο οποίος είναι περιοχή κυρίων ιδεωδών. Συνεπώς κάθε πρώτο ιδεώδες αυτού είναι της μορφής $P = \pi\mathbb{Z}[\omega]$, όπου π είναι κάποιο πρώτο στοιχείο του $\mathbb{Z}[\omega]$. Η επέκταση L/K είναι μια Kummer επέκταση.

Συνεπώς αν ο $\pi \nmid 6 = 2 \cdot 3$, τότε ο π δεν διακλαδίζεται στο L. Η ομάδα $\mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$, είναι αβελιανή (μάλιστα κυκλική), συνεπώς ορίζεται το σύμβολο του Artin για το π. Για να καθορίσουμε ποιος αυτομορφισμός είναι θα πρέπει να υπολογίσουμε τη δράση του στην $\sqrt[3]{2}$. Πράγματι, θα αποδείξουμε ότι

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) = \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2}.$$

Επομένως θα έχουμε ότι το σύμβολο του Artin γενικεύει και το κυβικό σύμβολο υπολοίπων.

Έστω λοιπόν τώρα, Q ένα πρώτο ιδεώδες του L, $Q \mid \langle\pi\rangle$. Επομένως,

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) \equiv \left(\sqrt[3]{2}\right)^{N_{K/\mathbb{Q}}(\pi)} \equiv 2^{\frac{N_{K/\mathbb{Q}}(\pi)-1}{3}} \sqrt[3]{2} \mod Q.$$

Όμως, γνωρίζουμε ότι

$$2^{\frac{N_{K/\mathbb{Q}}(\pi)-1}{3}} \equiv \left(\frac{2}{\pi}\right)_3 \mod \pi.$$

Αλλά το $Q \mid \langle\pi\rangle$, δηλαδή το $\pi \in Q$. Μπορούμε επομένως να γράψουμε ότι

$$2^{\frac{N_{K/\mathbb{Q}}(\pi)-1}{3}} \equiv \left(\frac{2}{\pi}\right)_3 \mod Q.$$

Συνεπώς έχουμε

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) \equiv \left(\frac{2}{\pi}\right)_3 \mod Q.$$

Αλλά το $\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2})$ είναι ίσο με το γινόμενο της $\sqrt[3]{2}$ επί μια κυβική ρίζα της μονάδας. Οι κυβικές ρίζες της μονάδας ανήκουν σε διαφορετικές κλάσεις modulo Q (όπως ακριβώς κάναμε στα κυκλοτομικά σώματα). Το ίδιο κάνει και το κυβικό σύμβολο. Επομένως,

$$\left(\frac{L/K}{\pi}\right) = \left(\frac{2}{\pi}\right)_3.$$

Παρατήρηση VIII.5.7. Ανάλογα αποδεικνύεται ότι το σύμβολο του Artin γενικεύει και το n-στό σύμβολο του Legendre.

Παρατήρηση VIII.5.8. Το σύμβολο του Artin, ορίστηκε μόνο για μη-διακλαδιζόμενα πρώτα ιδεώδη.

Παρατήρηση VIII.5.9. Ο ορισμός του συμβόλου του Artin για τη σχετική επέκταση L/K είναι ακριβώς ο ίδιος.

VIII.6 Νόμος αντιστροφής σε μη-αβελιανές επεκτάσεις του $\mathbb{Q}$

Για να έχουμε τώρα μια πλήρη θεωρία και στην περίπτωση που το βασικό μας σώμα είναι ένα αλγεβρικό σώμα αριθμών $K \neq \mathbb{Q}$ θα πρέπει να λύσουμε τα επί μέρους προβλήματα:

1. Το m θα πρέπει να αντικατασταθεί με κάτι γενικότερο
2. Θα πρέπει να γενικεύσουμε την έννοια της ισοτιμίας
3. Η ομάδα $(\mathbb{Z}/m\mathbb{Z})^*$ θα πρέπει να παραχωρήσει τη θέση της σε κάτι γενικότερο

4. Θα πρέπει να βρούμε έννοιες ανάλογες με τον «οδηγό» και του «defining modulus» ενός σώματος L/K
5. Θα πρέπει να αντικατασταθεί το $\mathbb{Q}(\zeta_m)$ με κάτι γενικότερο

Το δυσκολότερο από όλα είναι ίσως το τελευταίο μιας και το θεώρημα των Kronecker-Weber δεν ισχύει για κάθε αλγεβρικό σώμα αριθμών K. Απάντηση σε όλα τα προηγούμενα προβλήματα όταν η L/K είναι αβελιανή επέκταση, έδωσε η θεωρία κλάσεων σωμάτων (class field theory).

Τι γίνεται όμως από εκεί και πέρα;

Ο νόμος αντιστροφής του Artin σε επεκτάσεις L/K μπορεί να πάρει και τη μορφή

$$\mathrm{Spl}(L/K) \text{ χαρακτηρίζεται μέσω ισοδυναμιών } \Leftrightarrow \text{ η επέκταση } L/K \text{ είναι αβελιανή.}$$

Αλλά αν η επέκταση L/K είναι Galois αλλά όχι αβελιανή;

Όπως μόλις έχουμε αναφέρει υπάρχουν γενικές εικασίες, στις οποίες δεν επιθυμούμε να επεκταθούμε. Απλά ας αναφέρουμε το παράδειγμα της επέκτασης $L/\mathbb{Q}$, όπου $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Η επέκταση είναι Galois με ομάδα Galois ισόμορφη προς την S_3, η οποία δεν είναι αβελιανή. Πώς θα μπορούσαμε να χαρακτηρίσουμε το σύνολο $\mathrm{Spl}(L/\mathbb{Q})$;

Το έχουμε ήδη κάνει:

$$\begin{aligned}\mathrm{Spl}(L/\mathbb{Q}) &= \{p \in \mathbb{P} : p \equiv 1 \mod 3, p = x^2 + 27y^2, x, y \in \mathbb{Z}\} \\ &= \{p \in \mathbb{P} : p \equiv 1 \mod 3, \left(\frac{2}{\pi}\right)_3 = 1, \text{ για } p = \pi\overline{\pi}\}.\end{aligned}$$

Παρατηρούμε ότι ο χαρακτηρισμός δεν δίνεται μέσω ισοτιμιών πλέον.

Υπάρχει και άλλος χαρακτηρισμός του συνόλου $\mathrm{Spl}(L/\mathbb{Q})$. Αυτός είναι

$$\mathrm{Spl}(L/\mathbb{Q}) = \{p \in \mathbb{P} : p \equiv 1 \mod 3 \text{ και } a(p) = 2\},$$

όπου $a(p)$ είναι ο p-στός συντελεστής του αναπτύγματος

$$\eta(6z)\eta(18z) = \sum a(n)q^n, q = e^{2\pi i z}, \mathrm{Im}(z) > 0$$

και $\eta(z)$ είναι η συνάρτηση του Dedekind η οποία ορίζεται ως:

$$\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 - q^n),, q = e^{2\pi i z}, \mathrm{Im}(z) > 0.$$

Το τι σχέση έχει η αριθμητική της επέκτασης $L/\mathbb{Q}$ με τη συνάρτηση $\eta(z)$ είναι μια άλλη ιστορία, δείτε [5].

Το πρόβλημα λοιπόν είναι να χαρακτηριστούν οι επεκτάσεις του Galois L/K. Χρήσιμα εργαλεία για την ανάπτυξη αυτού του κλάδου της Θεωρίας των Αριθμών αποδείχτηκαν η θεωρία των modular Μορφών (συναρτήσεων με μεγάλη αριθμητική σημασία) και η θεωρία των L-σειρών και θεωρία αναπαραστάσεων ομάδων (η «Φιλοσοφία του Langlands»).

VIII.6.1 Νόμος ανάλυσης σε μη-Galois επεκτάσεις

Θα κλείσουμε την παράγραφο με έναν νόμο ανάλυσης σε μη Galois επεκτάσεις. Ο λόγος που αναφέρεται στο παρόν κεφάλαιο και όχι στο προηγούμενο είναι η χρήση του αυτομορφισμού του Frobenius.

Έστω L/K μια Galois επέκταση $G = \mathrm{Gal}(L/K)$ και E ενδιάμεσο σώμα $K \subset E \subset L$. Η επέκταση E/K δεν είναι κατ' ανάγκη Galois. Έστω $H = \mathrm{Gal}(L/E)$ και έστω

$$G = H\sigma_1 \dot\cup H\sigma_2 \dot\cup \cdots \dot\cup H\sigma_k$$

η ανάλυση της G σε σύμπλοκα ως προς την H. Αν $\sigma \in G$, τότε το σ όταν δράσει από τα δεξιά στα σύμπλοκα τα μεταθέτει

$$\sigma : \{H\sigma_1, H\sigma_2, \dots, H\sigma_k\} \to \{H\sigma_1\sigma, H\sigma_2\sigma, \dots, H\sigma_k\sigma\} = \{H\sigma_1, H\sigma_2, \dots, H\sigma_k\}.$$

Ως ένας κύκλος μήκους t ορίζεται η ακολουθία $H\sigma_i, H\sigma_i\sigma, \dots, H\sigma_i\sigma^{t-1}$ από διακεκριμένα μεταξύ τους σύμπλοκα και $H\sigma_i\sigma^i = H\sigma_i$. Πρόκειται για τη συνηθισμένη έννοια του κύκλου στις μεταθέσεις.

Το σύνολο λοιπόν όλων των συμπλόκων της G ως προς H διαμερίζεται σε ξένους μεταξύ τους κύκλους της σ.

Θεώρημα VIII.6.1. *Έστω τα αλγεβρικά σώματα αριθμών* $K \subset E \subset L$ *με* L/K *Galois,* Q *ένα πρώτο ιδεώδες του* L *και* $P = K \cap Q$. *Υποθέτουμε ότι το* Q *δεν διακλαδίζεται στην επέκταση* L/K. *Έστω* $\sigma := \left[\frac{L/K}{Q}\right]$. *Υποθέτουμε ότι το* σ *δρα στο σύνολο των δεξιών συμπλόκων της* $G = \mathrm{Gal}(L/K)$ *ως προς την υποομάδα* $H = \mathrm{Gal}(L/E)$ *και αναλύεται σε κύκλους μήκους* $t_1, t_2, \dots, t_s$.

Τότε το pR_E *αναλύεται σε γινόμενο* s *διαφορετικών μεταξύ τους πρώτων ιδεωδών του* E *με βαθμούς αδρανείας* $t_1, t_2, \dots, t_s$ *αντίστοιχα.*

Απόδειξη. Έστω ότι το σύμπλοκο Ht ανήκει σε έναν κύκλο του σ μήκους t. Έστω $P_0 = \tau(Q) \cap E$. Προφανώς το P_0 είναι ένα πρώτο ιδεώδες του E, $P_0 \mid P$. Ο βαθμός αδρανείας $f(P_0/P) = f$ του P_0 μπορεί να υπολογιστεί ως εξής: Ο βαθμός αδρανείας $f(\tau(Q)/P_0)$ είναι ίσος προς την τάξη της ομάδας αναλύσεως:

$$G_Z(\tau(Q)/P_0) = H \cap G_Z(\tau(Q)/P) = H \cap \tau G_Z(Q/P)\tau^{-1}.$$

Ο αυτομορφισμός του Frobenius $\sigma = \left[\frac{L/K}{Q}\right]$ είναι γεννήτορας της ομάδας αναλύσεως $G_Z(\tau(Q)/P) = \langle\sigma\rangle$.

Αν t ο ελάχιστος θετικός ακέραιος για τον οποίο ισχύει $Ht = Ht\sigma^t$, τότε έχουμε (άσκηση)

$$H \cap \langle\tau\sigma\tau^{-1}\rangle = \langle\tau\sigma^t\tau^{-1}\rangle.$$

Αυτό σημαίνει ότι

$$G_Z(\tau(Q)/P_0) = \langle\tau\sigma^t\tau^{-1}\rangle.$$

Επομένως,

$$f(P_0/P) = \frac{f(Q/P)}{f(Q/P_0)} = \frac{|G_Z(Q/P)|}{|G_Z(\tau(Q)/P_0)|} = \frac{|\langle\sigma\rangle|}{|\langle\tau\sigma^t\tau^{-1}\rangle|} = t.$$

Έτσι, ένας κύκλος μήκους t αντιστοιχεί σε ένα πρώτο ιδεώδες P_0 του E, $P_0 \mid P$ με βαθμό αδρανείας $f(P_0/P) = t$. Θα αποδείξουμε ότι η απεικόνιση αυτή είναι ένα προς ένα. Έστω λοιπόν Ht και Hρ δύο σύμπλοκα της G ως προς την H για τα οποία ισχύει

$$P_0 = E \cap \tau(Q) = E \cap \rho(Q).$$

Τα $\tau(Q)$ και $\rho(Q)$ είναι πρώτα ιδεώδη του L, $\tau(Q) \mid P_0$ και $\rho(Q) \mid P_0$. Αφού η ομάδα Galois $H = \mathrm{Gal}(L/E)$ δρα μεταβατικά στα πρώτα ιδεώδη του L που εμφανίζονται στην ανάλυση του P_0R_L θα υπάρχει ένα $\phi \in H$ για το οποίο θα ισχύει $\phi(\rho(Q)) = \tau(Q)$. Αυτό σημαίνει ότι $\tau^{-1}\phi\rho(Q) = Q$, δηλαδή $\tau^{-1}\phi\rho \in G_Z(Q/P) = \langle\sigma\rangle$, οπότε $\phi\rho = \tau\sigma^i$ για κάποιο i. Επομένως, $Ht\sigma^i = H\phi\rho = H\rho$, αφού $\phi \in H$. Άρα τα Ht και Hρ είναι δύο σύμπλοκα της G στην H τα οποία ανήκουν στον ίδιο κύκλο του σ.

Αρκεί, τέλος να αποδείξουμε ότι η παραπάνω απεικόνιση είναι και επί, δηλαδή ότι κάθε πρώτο ιδεώδες P_E του E προκύπτει σύμφωνα με την παραπάνω διαδικασία. Κάθε ένας από τους s κύκλους αντιστοιχεί σε κάποιο πρώτο ιδεώδες P_i του E με βαθμό αδρανείας $f(P_i/P) = t_i$. Αλλά το άθροισμα $\sum t_i = [G : H] = [E : K]$. Το άθροισμα $\sum f(P_i/P) = \sum t_i = [E : K]$, αυτό σημαίνει ότι όλα τα πρώτα ιδεώδη P του E έχουν μετρήσει, δηλαδή το $P_E = P_i$, για κάποιο i. □

Πόρισμα VIII.6.2. *Το πλήθος των πρώτων ιδεωδών* P_i *του* E *για τα οποία ισχύει* $f(P_i/P) = 1$ *είναι ίσο προς το πλήθος των συμπλόκων* $H\sigma_i$ *για τα οποία ισχύει* $\sigma_i G_Z(Q/P)\sigma_i^{-1} \subset H$.

Σημείωση VIII.6.3. Το θεώρημα είναι το 2.7 του Janusz [7] και χρησιμοποιείται στην απόδειξη του θεωρήματος πυκνότητας πρώτων του Frobenius.

VIII.7 Ασκήσεις

1. Έστω $\alpha = a + ib \in \mathbb{Z}[i], \alpha \notin E(\mathbb{Z}[i])$. Το α θα λέγεται primary, αν $\alpha \equiv 1 \mod (1+i)^3$. Να αποδειχθεί ότι αν το α είναι primary, τότε
$$a \equiv 1 \mod 4 \text{ και } b = 0 \mod 4$$
$$\text{ή } a \equiv 3 \mod 4 \text{ και } b \equiv 2 \mod 4$$
2. Έστω $\alpha \in \mathbb{Z}[i], \alpha \notin E(\mathbb{Z}[i])$ και $(1+i) \nmid \alpha$. Να αποδειχθεί ότι υπάρχει μοναδική μονάδα $\epsilon \in E(\mathbb{Z}[i])$ ώστε το $\epsilon\alpha$ να είναι primary.
3. Κάθε primary στοιχείο του $\mathbb{Z}[i]$ μπορεί να γραφεί ως γινόμενο από πρώτα primary στοιχεία.
4. Αν $\pi = a + bi$ είναι ένα πρώτο primary στοιχείο του $\mathbb{Z}[i]$, να αποδειχθεί ότι
$$\left(\frac{2}{\pi}\right)_4 = i^{a\cdot b/2}.$$
5. Αν $m, n \in \mathbb{N}$, να αποδειχθεί ότι
$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(n,m)}).$$
Αν $L/\mathbb{Q}$ αβελιανή, τότε υπάρχει ένας ελάχιστος φυσικός ώστε $L \subset \mathbb{Q}(\zeta_{f_L})$. Επίσης να αποδειχτεί ότι $L \subset \mathbb{Q}(\zeta_m) \Leftrightarrow f_L \mid m$.
6. Να βρεθούν τα τετραγωνικά υποσώματα που περιέχονται στο σώμα $\mathbb{Q}(\zeta_8)$.
7. Να αποδειχθεί ότι ο οδηγός ενός τετραγωνικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{D_K})$ είναι $f_K = |D_k|$.
8. Ποιος είναι ο οδηγός ένος κυκλοτομικού σώματος αριθμών; Ποιος είναι ο οδηγός του μέγιστου πραγματικού υποσώματος αυτού;
9. Έστω f και g δύο ανάγωγα πολυώνυμα του δακτυλίου $\mathbb{Z}[x]$ και K_f, K_g τα αντίστοιχα σώματα ανάλυσης των πολυωνύμων αυτών. Αν $K_f \subset K_g$ να αποδειχθεί ότι
$$\mathrm{Spl}(K_g/\mathbb{Q}) \overset{*}{\subset} \mathrm{Spl}(K_f/\mathbb{Q}),$$
όπου το $*$ σημαίνει «εκτός από πεπερασμένο πλήθος πρώτων».
Σημείωση: Ισχύει και το αντίστροφο αλλά χρειαζόμαστε αποτελέσματα που δεν έχουμε διδαχτεί. Άρα
$$K_f = K_g \Leftrightarrow \mathrm{Spl}(K_g/\mathbb{Q}) \overset{*}{=} \mathrm{Spl}(K_f/\mathbb{Q}),$$
δηλαδή το σύνολο $\mathrm{Spl}(K/\mathbb{Q})$ μιας επέκτασης Galois καθορίζει πλήρως το σώμα.
10. Έστω $K = \mathbb{Q}(\sqrt[4]{m})$, $m \in \mathbb{Z}$ ελεύθερος τετραγώνου και $L = \mathbb{Q}(\sqrt[4]{m}, i)$ η κανονική θήκη της $K/\mathbb{Q}$.
(α′) Να αποδειχθεί ότι ο βαθμός της επέκτασης $K/\mathbb{Q}$ είναι 4.
(β′) Θέτουμε $\alpha = \sqrt[4]{m}$, οπότε οι ρίζες του πολυωνύμου είναι $\alpha, i\alpha, -\alpha, -i\alpha$ και τις συμβολίζουμε με $1, 2, 3, 4$. Επομένως η ομάδα Galois $\mathrm{Gal}(L/\mathbb{Q})$ μπορεί να παρασταθεί με μεταθέσεις του $\{\}1, 2, 3, 4\}$. Να αποδειχθεί ότι
$$\mathrm{Gal}(L/K) = \{1, \tau, \sigma, \tau\sigma, \sigma^2, \tau\sigma^2, \sigma^3, \tau\sigma^3\},$$
όπου $\sigma = (1, 2, 3, 4)$ και $\tau = (2, 4)$.

(γ′) Αν p περιττός πρώτος, $p \nmid m$, τότε ο p δεν διακλαδίζεται στο L.

(δ′) Για p όπως στο 10γ′, έστω Q πρώτο ιδεώδες του L, $Q \mid p\mathbb{Z}$. Υποθέτουμε ότι $\left[\frac{L/\mathbb{Q}}{Q}\right] = \tau$. Να αποδειχθεί ότι το $p\mathbb{Z}$ αναλύεται σε γινόμενο τριών πρώτων ιδεωδών του K.

(ε′) Να καθοριστεί πώς αναλύεται το $p\mathbb{Z}$ στο K, για κάθε δυνατότητα του $\left[\frac{L/\mathbb{Q}}{Q}\right]$.

Βιβλιογραφία

[1] Cox, D. A. *Primes of the Form x^2+ny^2, Fermat, class field theory, and complex multiplication*. 2nd edition. Pure and Applied Mathematics. John Wiley & Sons, Inc., 2013, pp. xviii+356. ISBN: 978-1-118-39018-4.

[2] Gauss, C. F. *Disquisitiones Arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966, pp. xx+472.

[3] Hasse, H. *Vorlesungen über Zahlentheorie*. Zweite neubearbeitete Auflage. Die Grundlehren der Mathematischen Wissenschaften, Band 59. Springer-Verlag, Berlin, 1964, pp. xv+504.

[4] Hasse, H. *Zahlentheorie*. Dritte berichtigte Auflage. Akademie-Verlag, Berlin, 1969, pp. xvi+611.

[5] Hiramatsu, T. & Saito, S. *An Introduction to non-abelian Class Field Theory*. Vol. 13. Series on Number Theory and its Applications. Automorphic forms of weight 1 and 2-dimensional Galois representations. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2017, pp. xii+175. ISBN: 978-981-3142-26-8.

[6] Ireland, K. & Rosen, M. *A classical Introduction to Modern Number Theory*. Second. Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, New York, 1990, pp. xiv+389. ISBN: 0-387-97329-X.

[7] Janusz, G. J. *Algebraic number fields*. Second. Vol. 7. Graduate Studies in Mathematics. Providence, RI: American Mathematical Society, 1996, pp. x+276. ISBN: 0-8218-0429-4.

[8] Marcus, D. A. *Algebraic Number Fields*. Universitext. 2nd edition of [MR0457396], With a foreword by Barry Mazur. Springer, 2018, pp. xviii+203. ISBN: 978-3-319-90232-6; 978-3-319-90233-3.

[9] Weil, A. *Number Theory, An approach through history from Hammurapi to Legendre, Reprint of the 1984 edition*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007, pp. xxii+377. ISBN: 978-0-8176-4565-6; 0-8176-4565-9.

IX

Το θεώρημα Minkowski και το Θεώρημα μονάδων του Dirichlet

IX.1 Το θεώρημα Minkowski και εφαρμογές

IX.1.1 Εισαγωγή

Το πεπερασμένο του αριθμού κλάσεων ιδεωδών αποδείχθηκε από τον L. Kronecker στη δεκαετία του 1880. Προς το τέλος του δεκάτου ενάτου αιώνα ο H. Minkowski είχε την επαναστατική για την εποχή ιδέα να εισαγάγει γεωμετρικές μεθόδους στη θεωρία Αριθμών. Η μέθοδος αυτή ονομάζεται «γεωμετρία των αριθμών». Έτσι προέκυψε η σταθερά Minkowski M_k η οποία είναι πολύ καλύτερη από τη σταθέρα C του Kronecker που είδαμε στο κεφάλαιο V. Η θεώρηση του Minkowski είχε και άλλες, εξαιρετικές εφαρμογές, όπως θα δούμε παρακάτω, στη θεωρία αριθμών. Στην εποχή μας η γεωμετρία των αριθμών αποτελεί έναν ξεχωριστό κλάδο της αριθμητικής, [4].

IX.1.2 Διακριτές υποομάδες του $\mathbb{R}^n$

Ορισμός IX.1.1. Μια υποομάδα H του $\mathbb{R}^n$ θα λέγεται διακριτή όταν για κάθε συμπαγές (κλειστό και φραγμένο) υποσύνολο $K \subset \mathbb{R}^n$ η τομή $H \cap K$ είναι πεπερασμένο σύνολο.

Πρόταση IX.1.2. *Έστω* H *διακριτή υποομάδα του* $\mathbb{R}^n$. *Υπάρχουν* $\alpha_1, \alpha_2, \ldots, \alpha_r \in H$ *τα οποία παράγουν την* H *υπεράνω του* $\mathbb{Z}$ *και είναι γραμμικά ανεξάρτητα υπέρ το* $\mathbb{R}$.

Παρατήρηση IX.1.3. Η H είναι ελεύθερο $\mathbb{Z}$-module βαθμού $r \leq n$, αλλά με γραμμικά ανεξάρτητα υπέρ το $\mathbb{R}$ στοιχεία της βάσης.

Απόδειξη. Θεωρούμε το σύνολο $\{\alpha_1, \alpha_2, \ldots, \alpha_r\} \subset H$ το οποίο είναι $\mathbb{R}$-γραμμικά ανεξάρτητο για r το μέγιστο δυνατό. Ορίζουμε το σύνολο

$$P = \left\{ \sum_{i=1}^{r} \ell_i \alpha_i : 0 \leq \ell_i \leq 1 \right\}.$$

Αφού η H είναι διακριτή ομάδα και το P είναι συμπαγές έπεται ότι η τομή $H \cap P$ είναι πεπερασμένη. θα αποδείξουμε ότι

1. Κάθε $x \in H$ γράφεται στη μορφή

$$x = \sum_{i=1}^{r} \ell_i \alpha_i, \text{ με } \ell_i \in \mathbb{Q}$$

2. Η H παράγεται πάνω από το $\mathbb{Z}$ από το πεπερασμένο σύνολο $H \cap P$.

Έστω $x \in H$. Το σύνολο $\{\alpha_1, \alpha_2, \dots, \alpha_r, x\}$ είναι $\mathbb{R}$-γραμμικά εξαρτημένο, αφού το r είναι μέγιστο. Επομένως,

$$x = \sum_{i=1}^{r} \ell_i \alpha_i, \ell_i \in \mathbb{R}$$

Ορίζουμε

$$x_j := jx - \sum_{i=1}^{r} [j\ell_i]\alpha_i, j \in \mathbb{Z}.$$

Για κάθε $j \in \mathbb{Z}$, το $x_j \in H \cap P$ το οποίο όπως είπαμε, είναι πεπερασμένο, ενώ τα j είναι άπειρα. Άρα υπάρχουν $j, k \in \mathbb{Z}$, $j \neq k$ ώστε $x_j = x_k$. Συνεπώς

$$\sum_{i=1}^{r} (j\ell_i - [j\ell_i])\alpha_i = \sum_{i=1}^{r} (k\ell_i - [k\ell_i])\alpha_i$$

οπότε για κάθε $i = 1, 2, \dots, r$ ισχύει

$$j\ell_i - [j\ell_i] = k\ell_i - [\kappa\ell_i] \Rightarrow \ell_i = \frac{1}{j-\kappa}([j\ell_i] - [\kappa\ell_i]) \in \mathbb{Q}.$$

Αποδείξαμε ότι το $\mathbb{Z}$-module H παράγεται από πεπερασμένο σύνολο και είναι γραμμικοί συνδυασμοί των στοιχείων α_i με συντελεστές ρητούς αριθμούς, δηλαδή το (1).

Για το (2). Το $x_1 = x - \sum_{i=1}^{r} [\ell_i]\alpha_i$ συνεπώς $x = x_1 + \sum_{i=1}^{r} [\ell_i]\alpha_i$. Το $x_1 \in H \cap P$. Το $\alpha_i \in H$, αλλά και στο P (για $\ell_i = 1$ και $\ell_j = 0$, για κάθε $i \neq j$). Επομένως, κάθε $x \in H$ γράφεται ως γραμμικός συνδυασμός στοιχείων του $H \cap P$ με συντελεστές ακέραιους. Επειδή το $H \cap P$ είναι πεπερασμένο έπεται ότι το H είναι ένα $\mathbb{Z}$-module πεπερασμένα παραγόμενο, δηλαδή ισχύει και το (2).

Έστω d το ελάχιστο κοινό πολλαπλάσιο των παρονομαστών των ℓ_i. Προφανώς $dH \subset \sum_{i=1}^{r} \mathbb{Z}\alpha_i$. Σύμφωνα με το θεώρημα IV.3.5 υπάρχει μια βάση $\{\omega_1, \omega_2, \dots, \omega_r\}$ του $\mathbb{Z}$-module $\sum_{i=1}^{r} \mathbb{Z}\alpha_i$ και ακέραιοι αριθμοί $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r$ ώστε το διατεταγμένο σύνολο $(\varepsilon_1\omega_1, \varepsilon_2\omega_2, \dots, \varepsilon_r\omega_r)$ να παράγει το $\mathbb{Z}$-module dH.

Έστω

$$\varepsilon_i\omega_i = dh_i, h_i \in H$$

Για κάθε $x \in H$ έχουμε

$$dx = \sum_{i=1}^{r} m_i\varepsilon_i\omega_i = \sum_{i=1}^{r} m_i dh_i,$$

Δηλαδή

$$x = \sum_{i=1}^{r} m_i h_i \text{ με } m_i \in \mathbb{Z} \text{ για } i = 1, 2, \dots, r$$

Μένει να δείξουμε ότι το σύνολο $\{h_i\}_{i=1}^{r}$ είναι βάση του $\sum_{i=1}^{r} \mathbb{Z}\alpha_i$. Σύμφωνα με το θεώρημα IV.3.4 υπάρχει unimodular πίνακας $A \in M_r(\mathbb{Z})$ με $\det(A) = \pm 1$ ώστε να ισχύει

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_r \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{pmatrix}$$

Επομένως, το $\{\omega_1, \omega_2, \dots, \omega_r\}$ είναι ένα $\mathbb{R}$-γραμμικά ανεξάρτητο σύνολο και συνεπώς το σύνολο $\{h_1, h_2, \dots, h_r\}$ είναι $\mathbb{R}$-γραμμικά ανεξάρτητο.

Το $\mathbb{Z}$-module dH έχει τον ίδιο βαθμό με το H. Επειδή $H \supset \sum_{i=1}^{r} \mathbb{Z}\alpha_i$, έπεται ότι ο βαθμός του dH μεγαλύτερος ή ίσος. Επομένως ο βαθμός του $dH = r$ και συνεπώς όλα τα ε_i, $i = 1, 2, \dots, r$ είναι $\varepsilon_i \neq 0$, δηλαδή το $\{\varepsilon_1\omega_1, \varepsilon_2\omega_2, \dots, \varepsilon_r\omega_r\}$ είναι μια βάση του $\mathbb{Z}$-module dH και το σύνολο είναι $\mathbb{R}$-γραμμικά ανεξάρτητο. □

Ορισμός IX.1.4. Αν L διακριτή υποομάδα του $\mathbb{R}^n$ με βαθμό $r = n$, τότε αυτή λέγεται δικτυωτό (lattice) του $\mathbb{R}^n$.

Σημείωση IX.1.5. Μερικοί συγγραφείς ταυτίζουν την έννοια της διακριτής υποομάδας του $\mathbb{R}^n$ με την έννοια του δικτυωτού. Τότε στην περίπτωση του ορισμού μας, όπου επιπλέον έχουμε $r = n$, το δικτυωτό λέγεται πλήρες [15, σελ. 73].

Ορισμός IX.1.6. Έστω L ένα δικτυωτό του $\mathbb{R}^n$ και $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ μια $\mathbb{Z}$-βάση αυτού. Το σύνολο

$$P_B = \left\{ x \in \mathbb{R}^n : x = \sum_{i=1}^{n} \beta_i \alpha_i, 0 \leq \beta_i < 1, i = 1, 2, \ldots, r \right\}$$

λέγεται θεμελιώδες παραλληλεπίπεδο του L.

Είναι φανερό ότι για κάθε $x \in \mathbb{R}^n$ υπάρχει μοναδικό $y \in P_B$ τέτοιο ώστε $x - y \in L$. Πράγματι, αν $x = \sum_{i=1}^{n} \beta_i \alpha_i$ και $y := \sum_{i=1}^{n} (\beta_i - [\beta_i])\alpha_i$, τότε $y \in P_B$ και $x - y = \sum_{i=1}^{n} [\beta_i]\alpha_i \in L$. Αν υπήρχε και $y_1 = \sum_{i=1}^{n} \gamma_i \alpha_i \in P_B$ ώστε $x - y_1 \in L$, τότε θα είχαμε $y - y_1 = \sum_{i=1}^{n} (\beta_i - [\beta_i] - \gamma_i)\alpha_i \in L$, δηλαδή ότι $\beta_i - [\beta_i] - \gamma_i \in \mathbb{Z}$, $\beta_i - [\beta_i] \in [0, 1)$, $\gamma_i \in [0, 1)$, οπότε $\gamma_i = \beta_i - [\beta_i]$. Αυτό μπορούμε να το εκφράσουμε και ως εξής:

$$\mathbb{R}^n = \bigsqcup_{x \in L} (x + P_B).$$

Ορισμός IX.1.7. Έστω S ένα υποσύνολο του $\mathbb{R}^n$. Το S θα λέγεται κυρτό όταν για οποιαδήποτε $x, y \in S$, όλα τα σημεία του ευθύγραμμου τμήματος που συνδέει τα x, y ανήκουν στο S. Ισοδύναμα, αν $x, y \in S$, τότε για κάθε $\lambda \in R$ $\lambda \in [0, 1]$ και το $\lambda x + (1 - \lambda)y \in S$.

Επίσης το σύνολο S θα λέγεται συμμετρικό όταν είναι συμμετρικό ως προς την αρχή των αξόνων. Ισοδύναμα το S είναι συμμετρικό αν για κάθε $x \in S$ και το $-x \in S$.

Θα χρειαστούμε μερικές ιδιότητες του όγκου (μέτρου) των κυρτών συνόλων. Για τον δικό μας σκοπό αυτό που πρέπει να γνωρίζουμε είναι ότι κάθε κυρτό σύνολο είναι μετρήσιμο, δηλαδή έχει έναν καλά ορισμένο όγκο[1]. Απλά αναφέρουμε μερικές χρήσιμες ιδιότητες. Υπάρχει μια μεγάλη κλάση M φραγμένων συνόλων του $\mathbb{R}^n$ τα οποία λέγονται *Lebesgue μετρήσιμα*, στα οποία περιέχονται όλα τα κυρτά σύνολα ώστε:

- Αν $A \in M$, τότε ο όγκος $\mathrm{Vol}(A)$ είναι καλά ορισμένος.
- Αν το A είναι κυρτό, τότε ο όγκος του συμπίπτει με τον όγκο, όπως ορίζεται στο ολοκλήρωμα του Riemann.
- Αν το A είναι πεπερασμένη ή πιο γενικά αριθμήσιμη, ξένη ένωση μετρήσιμων συνόλων A_i, τότε και το A είναι μετρήσιμο και μάλιστα ισχύει

$$\mathrm{Vol}(A) = \sum \mathrm{Vol}(A_i).$$

- Αν A, B είναι μετρήσιμα και $A \subset B$, τότε $\mathrm{Vol}(A) \leq \mathrm{Vol}(B)$.
- Αν $A \subset \mathbb{R}^n$ μετρήσιμο και $x \in \mathbb{R}^n$, τότε και το $x + A$ είναι μετρήσιμο και $\mathrm{Vol}(A) = \mathrm{Vol}(x + A)$.
- Έστω $S \subset \mathbb{R}^n$, $\alpha \in \mathbb{R}$, $\alpha > 0$ $\alpha S = \{\alpha x : x \in S\}$ και S μετρήσιμο, τότε και το αS είναι μετρήσιμο και $\mathrm{Vol}(\alpha S) = \alpha^n \mathrm{Vol}(S)$.

Έστω $S \subset \mathbb{R}^n$ ένα φραγμένο μετρήσιμο σύνολο. Η απεικόνιση

$$T : S \longrightarrow \mathbb{R}^n$$

θα λέγεται *τμηματικά διατηρούσα του όγκο (piecewise volume preserving)* αν το S μπορεί να γραφεί ως μια πεπερασμένη ξένη ένωση μετρήσιμων υποσυνόλων S_i για τα οποία ισχύει

$$\mathrm{Vol}(T(S_i)) = \mathrm{Vol}(S_i) \text{ για κάθε } i.$$

[1] https://math.stackexchange.com/questions/207609/the-measurability-of-convex-sets

Παρατήρηση IX.1.8. Έστω $S \subset \mathbb{R}^n$ ένα φραγμένο μετρήσιμο σύνολο και T μια τμηματικά διατηρούσα τον όγκο συνάρτηση. Αν $\mathrm{Vol}(S) > \mathrm{Vol}(T(S))$, τότε η T δεν είναι 1-1 (injective).

Πράγματι, αν η T ήταν 1-1 και

$$T(S) = \bigcup\!\!\!\cdot\, T(S_i),$$

τότε

$$\mathrm{Vol}(T(S)) = \sum \mathrm{Vol}(T(S_i)) = \sum \mathrm{Vol}(S_i) = \mathrm{Vol}(S),$$

άτοπο. Η παρατήρηση είναι το γεωμετρικό ανάλογο του αξιώματος του Dirichlet.

Πρόταση IX.1.9. *Ο όγκος του θεμελιώδους παραλληλεπιπέδου P_B, δεν εξαρτάται από τη βάση.*

Απόδειξη. Έστω $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Ο όγκος

$$\mathrm{Vol}(P_B) = |\det(\alpha_1, \alpha_2, \ldots, \alpha_n)|.$$

Έστω $B' = \{\alpha_1', \alpha_2', \ldots, \alpha_n'\}$ μια άλλη βάση, έχουμε

$$\mathrm{Vol}(P_{B'}) = |\det(\alpha_1', \alpha_2', \ldots, \alpha_n')|.$$

Όμως οι δύο βάσεις συνδέονται

$$\begin{pmatrix} \alpha_1' \\ \alpha_2' \\ \vdots \\ \alpha_n' \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}, \qquad A \in M_n(\mathbb{Z}), \text{ και } \det(A) = \pm 1.$$

Επομένως, $\mathrm{Vol}(P_{B'}) = |\det(A)| \cdot (P_B) = \mathrm{Vol}(P_B)$. □

Ορισμός IX.1.10. Θα συμβολίζουμε με $\mathrm{Vol}(L)$ των όγκο του θεμελιώδους παραλληλεπιπέδου οποιασδήποτε βάσης του L.

IX.1.3 Το θεώρημα του Minkowski

Θεώρημα IX.1.11. *Έστω L ένα δικτυωτό, $L \subset \mathbb{R}^n$ και $S \subset \mathbb{R}^n$ μετρήσιμο με $\mathrm{Vol}(S) > \mathrm{Vol}(L)$. Υπάρχουν $x, y \in S$, $x \neq y$ με $x - y \in L$.*

Απόδειξη. Αρκεί να δείξουμε ότι υπάρχουν $\ell, \ell' \in L, \ell \neq \ell'$ ώστε $(\ell + S) \cap (\ell' + S) \neq \varnothing$. Πράγματι, έστω $z \in (\ell + S) \cap (\ell' + S)$ δηλαδή $z = \ell + x = \ell' + y$, $x, y \in S \Rightarrow \ell' - \ell = x - y \in L$ και $x \neq y$. Έστω $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ μια βάση του L και P_B το αντίστοιχο θεμελιώδες παραλληλεπίπεδο του L. Αφού $\mathbb{R}^n = \sqcup_{x \in L}(x + P_B)$, το S γράφεται ως ξένη ένωση υποσυνόλων του τύπου

$$S_x := S \cap (x + P_B), \qquad S = \bigcup_{x \in L}\!\!\!\cdot\, S_x.$$

Άρα, $\mathrm{Vol}(S) = \sum_{x \in L} \mathrm{Vol}(S_x)$. Ο όγκος όμως διατηρείται κατά τη μεταφορα. Επομένως

$$\mathrm{Vol}(S \cap (x + P_B)) = \mathrm{Vol}((-x + S) \cap B).$$

Τα σύνολα όμως $\{(-x + s) \cap P_B : x \in L\}$ δεν μπορούν όλα να είναι ανά δύο ξένα μεταξύ τους αφού αλλιώς

$$\begin{aligned} \mathrm{Vol}(P_B) &\geq \sum_{x \in P_B} \mathrm{Vol}((x + S) \cap P_B) \\ &= \sum_{x \in P_B} \mathrm{Vol}(S \cap (-x + P_B)) \\ &= \mathrm{Vol}\Big(\sqcup (S \cap (-x + P_B)) \Big) \\ &= \mathrm{Vol}(S), \end{aligned}$$

άτοπο. □

Πόρισμα IX.1.12. *Έστω* L *δικτυωτό στον* $\mathbb{R}^n$ *και* S *υποσύνολο του* $\mathbb{R}^n$*, συμμετρικό και κυρτό. Υποθέτουμε ότι*

(a) $\mathrm{Vol}(S) > 2^n \mathrm{Vol}(L)$ *ή*

(b) $\mathrm{Vol}(S) \geq 2^n \mathrm{Vol}(L)$ *και* S *συμπαγές*

Τότε $S \cap (L \backslash \{0\}) \neq \varnothing$.

Απόδειξη. (a) Έστω $S' = \frac{1}{2}S = \{\frac{1}{2}s : s \in S\}$. Ο όγκος του S',

$$\mathrm{Vol}(S') = \frac{1}{2^n}\mathrm{Vol}(S) > \mathrm{Vol}(L).$$

Επομένως από το θεώρημα έπεται ότι υπάρχουν $x, y \in S$, $x \neq y$ και $z := \frac{1}{2}x - \frac{1}{2}y \in L$. Τώρα, $y \in S$ και αφού S συμμετρικό και $-y \in S$ και αφού το S κυρτό έχουμε $z = \frac{x-y}{2} \in S$. Τελικά το $z \in S \cap L$.

(b) Το S είναι συμπαγές άρα κλειστό και φραγμένο. θα χρησιμοποιήσουμε την κλειστότητα. Θεωρούμε τα σύνολα:

$$(1+\varepsilon)S : 0 < \varepsilon < 1.$$

Το $(1+\varepsilon)S \supset S$, αφού το S κυρτό. Αφού $\varepsilon > 0$,

$$\mathrm{Vol}\big((1+\varepsilon)S\big) = (1+\varepsilon)^n \mathrm{Vol}(S) > 2^n \mathrm{Vol}(L).$$

Αφού το S είναι κυρτό έπεται ότι και το $(1+\varepsilon)S$ κυρτό και αφού το S συμμετρικό συνεπάγεται ότι και το $(1+\varepsilon)S$ συμμετρικό. Τα σύνολα αυτά είναι όλα συμπαγή, για κάθε $\varepsilon > 0$. Συνεπώς από το (a) που μόλις αποδείξαμε έχουμε

$$(L\backslash\{0\}) \cap (1+\varepsilon)S \neq \varnothing,$$

και αυτό για κάθε $\varepsilon > 0$. Στην πραγματικότητα είναι πεπερασμένα αφού είναι και διακριτά λόγω του εγκλεισμού τους στο L. Αν πάρουμε $\varepsilon = \frac{1}{\kappa}$, $\kappa \in \mathbb{N}$, τότε η

$$C_\kappa = (L\backslash\{0\}) \cap (1+\frac{1}{\kappa})S$$

είναι φθίνουσα ακολουθία συμπαγών συνόλων και συνεπώς

$$\bigcap_{\kappa=1}^{\infty} C_\kappa \neq \varnothing.$$

Έστω $x \in \bigcap_{\kappa=1}^{\infty} C_\kappa$, τότε το $x = (1+1/\kappa)s_\kappa$, $s_\kappa \in S$. Από τη συμπάγεια του S έπεται ότι $x \in S$ (εδώ έχουμε $x \in (1+\varepsilon)S, \forall \varepsilon > 0$). Το $x \in L\backslash\{0\}$. Συνεπώς $S \cap (L\backslash\{0\}) \neq \varnothing$.

□

Παρατήρηση IX.1.13. Η υπόθεση ότι το S στο (b) είναι συμπαγές είναι ουσιαστική. Αντιπαράδειγμα: Έστω $L = \mathbb{Z}^n$ και

$$S = \left\{ \sum_{i=1}^{n} \ell_i e_i : -1 < \ell_i < 1 \right\},$$

και e_i η συνηθισμένη βάση του $\mathbb{R}^n$. Έχουμε $\mathrm{Vol}(S) = 2^n = 2^n \mathrm{Vol}(\mathbb{Z}^n)$. Το S δεν είναι συμπαγές, είναι κυρτό, είναι συμμετρικό αλλά δεν έχει μη μηδενικό σημείο με ακέραιες συντεταγμένες.

IX.1.4 Η κανονική εμφύτευση ενός αλγεβρικού σώματος αριθμών

Είναι καιρός να θεωρήσουμε όλες τις εμφυτεύσεις ενός αλγεβρικού σώματος αριθμών K στο $\mathbb{C}$ και να προσπαθήσουμε να εξαγάγουμε συμπεράσματα σχετικά με την αριθμητική του K.

Έστω λοιπόν ότι $[K:\mathbb{Q}] = n = r_1 + 2r_2$, με ταυτότητα $[r_1, r_2]$. Αν $\sigma_1, \sigma_2, \dots, \sigma_{r_1}$ είναι οι πραγματικές εμφυτεύσεις του K και $\sigma_j, \overline{\sigma}_j$ είναι τα ζευγάρια των μιγαδικών εμφυτεύσεων για $r_1 + 1 \le j \le r_1 + r_2$, τότε η απεικόνιση

$$\begin{aligned} \sigma_K : K &\hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\mapsto \sigma_K(x) = \left(\sigma_1(x), \sigma_2(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \sigma_{r_1+2}(x), \dots, \sigma_{r_1+r_2}(x)\right) \end{aligned}$$

θα λέγεται κανονική εμφύτευση του K στο $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Η απεικόνιση σ_K είναι ένας μονομορφισμός δακτυλίων. Ταυτίζουμε το $\mathbb{C}$ με το $\mathbb{R} \oplus i\mathbb{R} \cong \mathbb{R}^2$ και έτσι έχουμε την κανονική εμφύτευση του K

$$\begin{aligned} \sigma_K : K &\hookrightarrow \mathbb{R}^n \\ x &\mapsto \sigma(x) = \left(\sigma_1(x), \dots, \sigma_{r_1}(x), \mathrm{Re}(\sigma_{r_1+1}(x)), \mathrm{Im}(\sigma_{r_1+1}(x)), \dots, \mathrm{Re}(\sigma_{r_1+r_2}(x)), \mathrm{Im}(\sigma_{r_1+r_2}(x))\right) \end{aligned}$$

Πρόταση IX.1.14. *Έστω M ένα ελεύθερο $\mathbb{Z}$-module του K βαθμού $n = [K:\mathbb{Q}]$ και έστω μια βάση αυτού $\{x_i : i = 1, 2, \dots, n\}$. Η εικόνα $\sigma_K(M)$ είναι ένα δικτυωτό του $\mathbb{R}^n$ και ο όγκος του είναι*

$$\mathrm{Vol}(\sigma_K(M)) = \frac{1}{2^{r_2}} \left|\det\left(\sigma_j(x_i)\right)_{1 \le i,j \le n}\right|.$$

Απόδειξη. Κάθε βάση του $\mathbb{Z}$-module M είναι κατ' ανάγκη μία $\mathbb{Q}$-βάση του K. Αφού τα x_i, $i = 1, 2, \dots, n$ παράγουν το M τα $\sigma(x_i)$ παράγουν το $\sigma_K(M)$. Θα αποδείξουμε ότι το $\sigma_K(M)$ είναι ένα δικτυωτό του $\mathbb{R}^n$, δηλαδή ότι τα $\{\sigma_\kappa(x_i)\}_{1 \le i \le n}$ είναι $\mathbb{R}$-γραμμικά ανεξάρτητο σύνολο του $\mathbb{R}^n$. Αρκεί, ως γνωστό, να δείξουμε ότι ο πίνακας

$$M = \begin{pmatrix} \sigma_\kappa(x_1) \\ \sigma_\kappa(x_2) \\ \vdots \\ \sigma_\kappa(x_n) \end{pmatrix}$$

έχει ορίζουσα διάφορη του μηδενός. Αυτό θα το πετύχουμε εργαζόμενοι με πράξεις στηλών. Θα υπολογίσουμε την $|\det(M)|$. Θεωρούμε τον πίνακα M ως έναν $n \times n$ πίνακα με στοιχεία στο $\mathbb{C}$. Αυτό επειδή είναι ανάγκη να κάνουμε πράξεις στηλών με μιγαδικούς αριθμούς. Ο πίνακάς μας είναι

$$M = \begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_{r_1}(x_1) & \mathrm{Re}\sigma_{r_1+1}(x_1) & \mathrm{Im}\sigma_{r_1+1}(x_1) & \dots & \mathrm{Re}\sigma_{r_1+r_2}(x_1) & \mathrm{Im}\sigma_{r_1+r_2}(x_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(x_n) & \dots & \sigma_{r_1}(x_n) & \mathrm{Re}\sigma_{r_1+1}(x_n) & \mathrm{Im}\sigma_{r_1+1}(x_n) & \dots & \mathrm{Re}\sigma_{r_1+r_2}(x_n) & \mathrm{Im}\sigma_{r_1+r_2}(x_n) \end{pmatrix}$$

Θεωρούμε τα ζευγάρια των $2r_2$-στηλών στα δεξιά του πίνακα $\mathrm{Re}\sigma_j$ και $\mathrm{Im}\sigma_j$ ($r_1 + 1 \le j \le r_1 + r_2$). Πολλαπλασιάζουμε τις στήλες $\mathrm{Im}\sigma_j$ με $-i$ και τις αφαιρούμε από τις αντίστοιχες $\mathrm{Re}\sigma_j$. Αυτό προφανώς δεν αλλάζει την τιμή $|\det(M)|$. Στη συνέχεια τις στήλες $-i\mathrm{Im}\sigma_j$ τις πολλαπλασιάζουμε με 2. Αυτό σημαίνει ότι η ορίζουσα του M πολλαπλασιάζεται με το 2^{r_2}. Προσθέτουμε τώρα την j στήλη ή οποία έχει ήδη γίνει σ_j στη στήλη $-2i\mathrm{Im}\sigma_j$. Συνεπώς ο πίνακας M έχει γίνει

$$M' = \begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_{r_1}(x_1) & \sigma_{r_1+1}(x_1) & \overline{\sigma}_{r_1+1}(x_1) & \dots & \sigma_{r_1+r_2}(x_1) & \overline{\sigma}_{r_1+r_2}(x_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(x_n) & \dots & \sigma_{r_1}(x_n) & \sigma_{r_1+1}(x_n) & \overline{\sigma}_{r_1+1}(x_n) & \dots & \sigma_{r_1+r_2}(x_n) & \overline{\sigma}_{r_1+r_2}(x_n) \end{pmatrix}$$

δηλαδή ο πίνακας είναι ο $(\sigma(x_i))_{\sigma, 1 \le i \le n}$ όπου το $i = 1, 2, \dots, n$ και το σ διατρέχει όλες τις εμφυτεύσεις του K. Αφού τα $\{x_i : 1 \le i \le n\}$ είναι μια $\mathbb{Q}$-βάση του K έπεται ότι $\det(M') = \det(\sigma(x_i))_{\sigma, 1 \le i \le n} \neq$

0. Συνεπώς και $|\det(M)| = \frac{1}{2^{r_2}}|\det(M')| \neq 0$. Αυτό σημαίνει ότι το $\sigma_K(M)$ είναι ένα δικτυωτό του $\mathbb{R}^n$ και ο όγκος του είναι

$$\mathrm{Vol}(\sigma_K(M)) = |\det(M)| = \frac{1}{2^{r_2}}|\det \sigma_j(x_i)|_{1\le i,j\le n}.$$

□

Πρόταση IX.1.15. *Έστω K αλγεβρικό σώμα αριθμών, R_K ο δακτύλιος των ακεραίων αλγεβρικών αριθμών και A ένα ακέραιο ιδεώδες του K. Το $\sigma_K(R_K)$ και $\sigma_K(A)$ είναι δικτυωτά. Επιπλέον ισχύει*

$$\mathrm{Vol}(\sigma_K(R_K)) = \frac{1}{2^{r_2}}|D_{K/\mathbb{Q}}|^{1/2}$$
$$\mathrm{Vol}(\sigma_K(A)) = \frac{1}{2^{r_2}}|D_{K/\mathbb{Q}}|^{1/2}N_{K/\mathbb{Q}}(A)$$

Απόδειξη. Και ο δακτύλιος R_K και το ιδεώδες A είναι $\mathbb{Z}$-modules βαθμού n συνεπώς (πρόταση IX.1.14) τα $\sigma_K(R_K)$ και $\sigma_K(A)$ είναι δικτυωτά του $\mathbb{R}^n$, όπου $[K:\mathbb{Q}] = n$.

Έστω $\{\omega_1, \omega_1, \dots, \omega_n\}$ μια βάση ακεραιότητας του K.

$$\mathrm{Vol}(\sigma_K(R_K)) = \frac{1}{2^{r_2}}|\det(\sigma_j(\omega_i))_{1\le i,j\le n}| = \frac{1}{2^{r_2}}|D_{K/\mathbb{Q}}|^{1/2}.$$

Ως γνωστό, υπάρχουν $\varepsilon_i \in \mathbb{Z}$, $i = 1, 2, \dots, n$ ώστε το σύνολο $\{\varepsilon_i\omega_i : i = 1, 2, \dots, n\}$ να είναι $\mathbb{Z}$-βάση του ιδεώδους A. Σύμφωνα και πάλι με την πρόταση IX.1.14 ισχύει

$$\begin{aligned}\mathrm{Vol}(\sigma_K(A)) &= \frac{1}{2^{r_2}}|\det(\sigma_j(\varepsilon_i\omega_i))_{1\le i,j\le n}| \\ &= \frac{1}{2^{r_2}}|\det(\sigma_j(\omega_i))_{1\le i,j\le n}| \cdot |\varepsilon_1\varepsilon_2\cdots\varepsilon_n| \\ &= \frac{1}{2^{r_2}}|D_{K/\mathbb{Q}}|^{1/2}N_{K/\mathbb{Q}}(A).\end{aligned}$$

□

IX.1.5 Εφαρμογές στη διακρίνουσα

Έστω K αλγεβρικό σώμα αριθμών $[K:\mathbb{Q}] = n = r_1 + 2r_2$ με ταυτότητα $[r_1, r_2]$. Στην προηγούμενη παράγραφο αναφερθήκαμε στη συνάρτηση

$$\sigma_K : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

Μπορούμε να ορίσουμε την έννοια της norm στοιχείων του $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2}$:

$$N(a_1, a_2, \dots, a_{r_1}, x_1, y_1, x_2, y_2, \dots, x_{r_2}, y_{r_2}) = a_1a_1\cdots a_{r_1}(x_1^2 + y_1^2)(x_2^2 + y_2^2)\cdots(x_{r_2}^2 + y_{r_2}^2).$$

Ο ορισμός είναι συμβατός με την norm στοιχείου αλγεβρικού σώματος αριθμών. Πράγματι, αν $\alpha \in K$, τότε

$$N_{K/\mathbb{Q}}(\alpha) = N(\sigma_K(\alpha)).$$

Επίσης

$$N_{K/\mathbb{Q}}(\alpha\beta) = N(\sigma_K(\alpha))N(\sigma_K(\beta)).$$

Έτσι μπορούμε να μεταφέρουμε την norm του δακτυλίου R_K και των ακέραιων ιδεωδών στην norm των αντίστοιχων δικτυωτών.

Για την εφαρμογή του θεωρήματος του Minkowski στα ιδεώδη του K, θα πρέπει να βρούμε ένα συμμετρικό, κυρτό και συμπαγές σύνολο S το οποίο να περιέχεται στο σύνολο $\{x \in \mathbb{R}^n : N(x) \le 1\}$. Αν το βρούμε αυτό μπορούμε να εφαρμόσουμε το θεώρημα Minkowski στην ομογενή επέκταση του S, $\{tS : t > 0\}$.

Πρόταση IX.1.16. *Έστω S ένα σύνολο, όπως παραπάνω. Για κάθε ιδεώδες A του K υπάρχει ένα στοιχείο $\alpha \in A$ $(\alpha \neq 0)$, ώστε*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{2^n 2^{-r_2}\sqrt{|D_{K/\mathbb{Q}}|}}{\mathrm{Vol}(S)} N_{K/\mathbb{Q}}(A).$$

Απόδειξη. Το σύνολο tS για $t > 0$ είναι φραγμένο, συμμετρικό κυρτό με όγκο $t^n \mathrm{Vol}(S)$ και, από τη σχέση

$$N(tx) = t^n N(x), \text{ έπεται ότι } tS \subset \{x \in \mathbb{R}^n : N(x) \leq t^n\}.$$

Επιλέγουμε τώρα το t ώστε

$$t^n \mathrm{Vol}(S) = 2^n \cdot \mathrm{Vol}(\sigma_K(A)).$$

Σύμφωνα με το θεώρημα του **Minkowski** το tS περιέχει ένα μη-μηδενικό στοιχείο στο δικτυωτό $\sigma_K(A)$. Αυτό σημαίνει ότι υπάρχει ένα στοιχείο $\alpha \in A$ ώστε $N(\sigma_K(\alpha)) \leq t^n$. Επειδή ο όγκος του $\sigma_K(A)$ είναι

$$\mathrm{Vol}(\sigma_K(A)) = \frac{1}{2^r}|D_{K/\mathbb{Q}}|^{1/2} N_{K/\mathbb{Q}}(A)$$

αυτό μας δίνει το επιθυμητό άνω φράγμα του $|N_{K/\mathbb{Q}}(\alpha)|$. □

Είναι πάρα πολύ ωραίο ότι υπάρχει ένα τέτοιο S. Ας πάρουμε για S να είναι μια αρκετά μικρή μπάλα με κέντρο την αρχή των αξόνων στο $\mathbb{R}^n$. Αυτό μας δίνει μια νέα απόδειξη του πεπερασμένου του αριθμού κλάσεων ιδεωδών.

Αλλά για τις εφαρμογές θα επιθυμούσαμε να έχουμε ένα σύνολο S με όγκο όσο πιο πολύ μεγάλο γίνεται.

Ως πρώτο υποψήφιο σύνολο θα ήταν ίσως το

$$H = \{x = (a_1, a_2, \ldots, a_{r_1}, x_1, y_1, \ldots, x_{r_2}, y_{r_2}) \in \mathbb{R}^n : |a_1 a_2 \cdots a_{r_1}(x_1^2 + y_1^2)\cdots(x_{r_2}^2 + y_{r_2}^2)| \leq 1\}.$$

Δυστυχώς όμως αυτό το σύνολο δεν είναι, εν γένει, ούτε φραγμένο ούτε κυρτό. Ας πάρουμε για παράδειγμα $r_1 = 2, r_2 = 0$ και

$$H = \{(a, b) \in \mathbb{R}^2 : |ab| \leq 1\}.$$

Αυτή είναι η περιοχή που φράσσεται από τις υπερβολές $xy = 1$ και $xy = -1$ και δεν είναι ούτε φραγμένο ούτε κυρτό σύνολο. Όμως στο H περιέχεται το σύνολο

$$B := \{(a, b) \in \mathbb{R}^2 : |a| + |b| \leq 2\}$$

το οποίο είναι και φραγμένο και κυρτό! Το $B \subset H$. Πράγματι, ο γεωμετρικός μέσος δύο πραγματικών αριθμών είναι μικρότερος ή ίσος του αριθμητικού μέσου. Συνεπώς για $(a, b) \in B$ ισχύει

$$|ab| \leq \frac{(|a| + |b|)^2}{4} \leq \frac{4}{4} = 1.$$

Μπορούμε να γενικεύσουμε την ιδέα και να ορίσουμε στον χώρο $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ για το

$$x = (x_1, x_2, \ldots, x_{r_1}, z_{r_1+1}, z_{r_2+2}, \ldots, z_{r_1+r_2})$$

την norm

$$||x|| = \sum_{i=1}^{r_1} |x_i| + 2 \sum_{i=r_1+1}^{r_1+r_2} |z_i|$$

Για κάθε t θετικό πραγματικό αριθμό ορίζουμε το σύνολο

$$S(t) = \{x \in V : ||x|| \leq t\}. \tag{IX.1}$$

Προφανώς το $S(t)$ είναι συμμετρικό και συμπαγές. Είναι επίσης κυρτό σύνολο (άσκηση). Θα αποδείξουμε ότι

$$\mathrm{Vol}(S(t)) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$$

Απόδειξη. Το $S(t)$ είναι συμμετρικό ως προς τον πραγματικό άξονα. Επομένως

$$\mathrm{Vol}(S(t)) = 2^{r_1}\mathrm{Vol}(S_1(t)),$$

όπου

$$S_1(t) = \{x \in V : ||x|| \leq t \text{ και } x_1, x_2, \ldots, x_{r_1} \geq 0\}.$$

Αντικαθιστούμε τις μιγαδικές μεταβλητές με πολικές συντεταγμένες:

$$z_j = x_j + iy_j = \frac{1}{2}\rho_j(\cos\theta_j + i\sin\theta_j), j = r_1+1, r_1+2, \ldots, r_1+r_2.$$

Αν το $z = U(\rho,\theta) + iV(\rho,\theta) = \frac{1}{2}\rho\big(\cos(\theta) + i\sin(\theta)\big)$, τότε η Ιακωβιανή είναι

$$J := \det\begin{pmatrix} \frac{\partial U}{\partial \rho} & \frac{\partial V}{\partial \rho} \\ \frac{\partial U}{\partial \theta} & \frac{\partial V}{\partial \theta} \end{pmatrix}$$

Επομένως η Ιακωβιανή για κάθε μεταβλητή $z_{r_1+1}, \ldots, z_{r_1+r_2}$ είναι $\rho_j/4$, $j = r_1+1, r_1+2, \ldots, r_1+r_2$. Αν λοιπόν ολοκληρώσουμε ως προς τα θ_j, $0 \leq \theta_j \leq 2\pi$ έχουμε

$$\mathrm{Vol}(S(t)) = 2^{r_1}4^{-r_2}(2\pi)^{r_2}\int_{T(t)} dx_1 dx_2 dx_{r_1}\rho_{r_1+1}\rho_{r_2+2}\cdots\rho_{r_1+r_2}d\rho_{r_1+1}d\rho_{r_2+2}\cdots d\rho_{r_1+r_2}$$

και

$$T(t) = \left\{(x,\rho) \in \mathbb{R}^{r_1+r_2} : x_i \geq 0, \rho_i \geq 0 \text{ και } \sum_{i=1}^{r_1} x_i + \sum_{i=r_1+1}^{r_1+r_2}\rho_i < t\right\}.$$

Αν στο επόμενο λήμμα, θέσουμε $m = r_1+r_2$, $a_i = 0$ για $1 \leq i \leq r_1$ και $a_1 = 1, r_1+1 \leq i \leq m$ προκύπτει

$$\mathrm{Vol}(S(t)) = 2^{r_1}\frac{(2\pi)^{r_2}}{4^{r_2}}\frac{t^n}{n!}.$$

□

Λήμμα IX.1.17. *Για $a_i > 0$, $a_i \in \mathbb{R}$, $i = 1, 2, \ldots, m$ έστω το ολοκλήρωμα*

$$I(a_1, a_2, \ldots, a_m, t) = \int_{T(t)} x_1^{a_1}x_2^{a_2}\cdots x_m^{a_m}dx_1dx_2\cdots dx_m$$

όπου

$$T(t) = \{x \in \mathbb{R}^m | x_i \geq 0, \sum_{i=1}^{m} x_i < t\}.$$

Τότε

$$I(a_1, a_2, \ldots, a_m, t) = t^{\sum_{i=1}^m a_i + m}\frac{\Gamma(a_1+1)\Gamma(a_2+1)\cdots\Gamma(a_m+1)}{G(a_1+a_2+\cdots+a_m+m+1)}$$

Σημείωση IX.1.18. Η Γ-συνάρτηση ορίζεται ως

$$\Gamma(x) = \int_{0^+}^{\infty} e^{-t}t^{x-1}dt, \text{ για κάθε } x > 0.$$

Μάλιστα, αν n μη-αρνητικός ακέραιος, τότε

$$\Gamma(n) = (n-1)!$$

Επίσης ισχύει

$$\int_0^1 x^{m-1}(1-x)^{n-1}dx = B(m,n) = \frac{\Gamma(m)\Gamma(n)}{\Gamma(n+m)}.$$

Απόδειξη. (του λήμματος) Αν κάνουμε αλλαγή μεταβλητής $x_i' = tx_i$ στο I έχουμε

$$I(a_1, a_2, \dots, a_m; t) = t^{\sum_{i=1}^{r_1} a_i + m} I(a_1, a_2, \dots, a_m, 1).$$

Επομένως, αρκεί να αποδείξουμε τον τύπο για $t = 1$. Θα εφαρμόσουμε επαγωγή ως προς m. Για $m = 1$,

$$I(a_1, 1) = \int_0^1 x_1^{a_1} dx_1 = \frac{1}{a_1 + 1} = \frac{\Gamma(a_1 + 1)}{\Gamma(a_2 + 1)}.$$

Έστω

$$T'(x_m) := \left\{ x \in \mathbb{R}^{m-1} : x_i \geq 0 \text{ και } \sum_{i=1}^{m-1} x_i \leq 1 - x_m \right\}$$

Επομένως,

$$\begin{aligned} I(a_1, a_2, \dots, a_m, 1) &= \int_{T(t)} x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} dx_1 dx_2 \cdots dx_m \\ &= \int_0^1 x_m^{a_m} \left(\int_{T'(x)} x_1^{a_1} \cdots x_{m-1}^{a_{m-1}} dx_1 dx_2 \cdots dx_{m-1} \right) dx_m \\ &= \int_0^1 x_m^{a_m} I(a_1, a_2, \dots, a_{m-1}; 1 - x_m) dx_m \\ &= I(a_1, a_2, \dots, a_{m-1}; 1) \frac{\Gamma(a_m + 1)\Gamma(a_1 + a_2 + \cdots + a_{m-1} + m)}{\Gamma(\alpha_1 + \alpha_2 + \cdots + a_m + m + 1)}. \end{aligned}$$

□

Επομένως για $t = n$ έχουμε το

Λήμμα IX.1.19. *Ο όγκος του συνόλου $S(n)$ είναι*

$$\mathrm{Vol}(S(n)) = \frac{n^n}{n!} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2}.$$

Σημείωση IX.1.20. Η απόδειξη αυτή είναι του E. Artin. Μπορείτε να δείτε και τις σημειώσεις του Milne. Όλες οι αποδείξεις χρησιμοποιούν επαγωγή. Ο ενδιαφερόμενος αναγνώστης παραπέμπεται στο [20].

Θεώρημα IX.1.21. *Έστω K ένα αλγεβρικό σώμα αριθμών $[K : \mathbb{Q}] = n$. Για κάθε κλάση ιδεωδών του K υπάρχει ένα τουλάχιστο ιδεώδες με norm μικρότερη της σταθεράς Minkowski*

$$M_K := \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|D_{K/\mathbb{Q}}|}.$$

Απόδειξη. Υπολογίζουμε τη σταθερά της προηγούμενης πρότασης αντικαθιστώντας το $\mathrm{Vol}(S)$ με το λήμμα και έχουμε

$$\frac{2^n 2^{-r_2} \sqrt{|D_{K/\mathbb{Q}}|}}{\frac{n^n}{n!} 2^{r_1} \left(\frac{\pi}{2}\right)} = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|D_{K/\mathbb{Q}}|}.$$

Έστω A' ένα ιδεώδες της δοσμένης κλάσης. Αν το πολλαπλασιάσουμε με κατάλληλο κύριο ιδεώδες, μπορούμε να υποθέσουμε ότι το $A = (A')^{-1}$ είναι ένα ακέραιο ιδεώδες. Έστω $\alpha \in A (\alpha \neq 0)$ για το οποίο ισχύει η πρόταση IX.1.16. Έχουμε

$$|N_{K/\mathbb{Q}}(\alpha)| N_{K/\mathbb{Q}}((A')^{-1})| \leq M_K.$$

Αλλά $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\langle \alpha \rangle)$, οπότε έχουμε

$$N_{K/\mathbb{Q}}(\langle a \rangle A) \leq M_K.$$

Το ιδεώδες $\langle \alpha \rangle A$ είναι ένα ακέραιο ιδεώδες που ανήκει στην ίδια κλάση με το A'. □

Παρατήρηση IX.1.22. Έχουμε εφαρμόσει το θεώρημα σε προηγούμενο κεφάλαιο και έχουμε δει ότι το φράγμα του Minkowski είναι πολύ καλύτερο του φράγματος του Kronecker. Ας το υπενθυμίσουμε με ένα απλό παράδειγμα: για $K = \mathbb{Q}(\sqrt{-5})$ έπρεπε να ελέγξουμε τους πρώτους $2, 3, 5, 7$, ενώ με το φράγμα του Minkowski μόνο του 2.

Το Θεώρημα του Minkowski έχει και εξαιρετικές εφαρμογές πέρα από τον υπολογισμό των κλάσεων.

Πόρισμα IX.1.23. *Αν* K *αλγεβρικό σώμα αριθμών* $[K : \mathbb{Q}] = n \geq 2$*, τότε*

$$|D_{K/\mathbb{Q}}| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

Επίσης η ποσότητα $n/\log|D_{K/\mathbb{Q}}|$ *φράσσεται από μία σταθερά ανεξάρτητη του* K.

Απόδειξη. Αφού, εξ ορισμού, η norm κάθε ιδεώδους του A είναι $N_{K/\mathbb{Q}}(A) \geq 1$, από το θεώρημα προκύπτει ότι

$$1 \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|D_{K/\mathbb{Q}}|^{1/2}.$$

Επομένως $|D_{K/\mathbb{Q}}| \geq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2}$. Αλλά $\pi/4 < 1$ και $2r_2 \leq n$. Επομένως

$$|D_{K/\mathbb{Q}}| \geq \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{(n!)^2} =: a_n.$$

Για $n = 2$ $a_2 = \pi^2/4$ και

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} = \frac{\pi}{4}(1 + 2 + \text{ θετικούς όρους })$$

Επομένως

$$\frac{a_{n+1}}{a_n} \geq \frac{3\pi}{4},$$

οπότε για $n \geq 2$,

$$a_n \geq \left(\frac{3\pi}{4}\right)^{n-2} \cdot a_2 = \left(\frac{3\pi}{4}\right)^{n-2} \frac{\pi^4}{4} = \left(\frac{3\pi}{4}\right)^{n-1} \frac{\pi}{3}.$$

Έτσι έχουμε το ακόλουθο κάτω φράγμα της διακρίνουσας του K

$$|D_{K/\mathbb{Q}}| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

Λογαριθμίζοντας έχουμε

$$\log|D_{K/\mathbb{Q}}| \geq \log\frac{\pi}{3} + (n-1)\log\frac{3\pi}{4} \geq (n-1)\log(\frac{3\pi}{4})$$

και

$$\frac{\log|D_{K/\mathbb{Q}}|}{n} \geq \frac{n-1}{n}\log\frac{3\pi}{4} \overset{n\geq 2}{\geq} \frac{1}{2}\log\frac{3\pi}{4}.$$

Τελικά

$$\frac{n}{\log|D_{K/\mathbb{Q}}|} \leq \frac{2}{\log 3\pi/4} = C,$$

σταθερά ανεξάρτητη του σώματος □

Άμεση συνέπεια του πορίσματος είναι το

Θεώρημα IX.1.24 (Hermite-Minkowski). *Για κάθε αλγεβρικό σώμα αριθμών* $K \neq \mathbb{Q}$, *ισχύει* $|D_{K/\mathbb{Q}}| > 1$.

Απόδειξη. Προφανώς $\frac{3\pi}{4} > 1$ και $\pi/3 > 1$ Άρα

$$|D_{K/\mathbb{Q}}| > 1.$$

□

Το θεώρημα αυτό συνδυαζόμενο με το θεώρημα της διακρίνουσας, το οποίο θα αποδείξουμε στο επόμενο κεφάλαιο: «Οι πρώτοι αριθμοί που διακλαδίζονται στο K είναι αυτοί που διαιρούν τη διακρίνουσα» μας δίνει

Πόρισμα IX.1.25. *Σε κάθε επέκταση αλγεβρικών σωμάτων αριθμών* $K/\mathbb{Q}$, $K \neq \mathbb{Q}$ *υπάρχει ένας τουλάχιστον διακλαδιζόμενος πρώτος.*

Άλλη μια σημαντική συνέπεια του Θεωρήματος του Minkowski είναι το

Θεώρημα IX.1.26 (Hermite). *Για κάθε ακέραιο* d *υπάρχουν το πολύ πεπερασμένου πλήθους αλγεβρικά σώματα αριθμών* K *με διακρίνουσα* $D_{K/\mathbb{Q}} = d$.

Απόδειξη. Θα αποδείξουμε ότι αν K αλγεβρικό σώμα αριθμών με $D_{K/\mathbb{Q}} = d$, τότε αν $K = \mathbb{Q}(\alpha)$, το α έχει πεπερασμένου πλήθους δυνατότητες. Από το πόρισμα IX.1.23 έχουμε ότι $n/\log(|d|) \leq C$, δηλαδή το n είναι φραγμένο. Συνεπώς, αρκεί να αποδείξουμε ότι υπάρχουν πεπερασμένου πλήθους αλγεβρικά σώματα αριθμών K με διακρίνουσα $D_{K/\mathbb{Q}}$ και σταθερό βαθμό επέκτασης $[K : \mathbb{Q}] = n = r_1 + 2r_2$. Θεωρούμε το σύνολο S ορισμένο με δύο τρόπους:
(a)-τρόπος Αν $r_1 > 0$, τότε

$$S = \left\{ a_1, a_2, \ldots, a_{r_1}, z_1, z_2, \ldots, Z_{r_2} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : \begin{array}{l} |a_1| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d|^{1/2}, \\ |a_i| \leq 1/2, 2 \leq i \leq r_1, \text{ και } |z_j| \leq 1/2, 1 \leq j \leq r_2. \end{array} \right\}$$

(b)-τρόπος Αν $r_1 = 0$, τότε

$$S = \left\{ (z_1, z_2, \ldots, z_{r_2}) \in \mathbb{C} : |z_1 - \bar{z}_2| \leq 2^n \left(\frac{\pi}{2}\right)^{1-r_2} |d|^{1/2}, |z_1 + \bar{z}_1| \leq 1/2, |z_j| \leq 1/2, 2 \leq j \leq r_2 \right\}$$

Το σύνολο S είναι συμπαγές κυρτό και συμμετρικό ως προς την αρχή των συντεταγμένων και έχει όγκο (άσκηση, πρόκειται για γινόμενο μήκους διαστημάτων, κυκλικών δίσκων και ενός τετραγώνου)

$$\mathrm{Vol}(S) = 2^{n-r_2}|d|^{1/2} = 2^n \left(\frac{1}{2^{r_2}}|D_K|^{1/2}\right) = 2^n \mathrm{Vol}(R_K).$$

Από το θεώρημα του Minkowski, προκύπτει ότι υπάρχει $\alpha \in R_K \backslash \{0\}$ ώστε $\sigma_K(x) \in S$. Θα αποδείξουμε ότι $K = \mathbb{Q}(\alpha)$.

Στην (a)-περίπτωση, $\alpha \in R_K$ συνεπώς

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \in \mathbb{N}$$

και για κάθε $i = 2, 3, \ldots, n$ $|\sigma_i(\alpha)| \leq 1/2$. Κατ' ανάγκη λοιπόν $|\sigma_1(\alpha)| \geq 1$. Αυτό σημαίνει ότι $\sigma_1(\alpha) \neq \sigma_i(\alpha)$, για $i = 2, 3, \ldots, n$. Οι ρίζες του χαρακτηριστικού πολυωνύμου του α είναι $\sigma_i(\alpha)$, $i = 1, 2, \ldots, n$ και το χαρακτηριστικό πολυώνυμο του α είναι ως γνωστό μια δύναμη του αναγώγου. Επειδή η ρίζα $\sigma_1(\alpha)$ είναι απλή έπεται ότι το χαρακτηριστικό πολυώνυμο συμπίπτει με το $\mathrm{Irr}(\alpha, \mathbb{Q})$, συνεπώς $K = \mathbb{Q}(\alpha)$.

Ανάλογα, στην περίπτωση (b) από το ίδιο επιχείρημα έχουμε $|\sigma_1(\alpha)| = \overline{|\sigma_1(\alpha)|} \geq 1$ και για όλα τα σ_j, $j \neq 1$ και $\sigma_j \neq \sigma_1$ και $\sigma_j \neq \bar{\sigma}_1$. Τώρα από την $|z_1 + \bar{z}_1| \leq 1/2$ αν $\bar{\sigma}_1(\alpha) = \sigma_1(a)$ και $\sigma_1(\alpha) \in \mathbb{R}$

θα είχαμε $|\sigma_1(\alpha)| \leq 1/4$, άτοπο αφού $|\sigma_1(\alpha)| \geq 1$. Επομένως και $\sigma_1(\alpha) \neq \overline{\sigma}_1(\alpha)$ και όπως και στην περίπτωση (a) είναι γεννήτορας του K, $K = \mathbb{Q}(\alpha)$. Από τον ορισμό του S έπεται ότι όλες οι τιμές $\sigma_i(\alpha)$ είναι φραγμένες. Το ίδιο και οι συντελεστές του ανάγωγου πολυωνύμου $\mathrm{Irr}(\alpha, \mathbb{Q})$ ως συμμετρικά πολυώνυμα των $\sigma_i(\alpha)$. Αλλά το $\mathrm{Irr}(\alpha, \mathbb{Q})$ είναι μονικό με συντελεστές στο $\mathbb{Z}$. Ο βαθμός του ανάγωγου πολυωνύμου και οι συντελεστές του είναι φραγμένοι, άρα υπάρχουν πεπερασμένου πλήθους δυνατότητες για το ανάγωγο πολυώνυμο $\mathrm{Irr}(\alpha, \mathbb{Q})$ και συνεπώς πεπερασμένου πλήθους δυνατότητες για το $\alpha \in \mathbb{C}$. Αφού $K = \mathbb{Q}(\alpha)$ υπάρχουν και πεπερασμένου πλήθους σώματα K. □

Παρατήρηση IX.1.27. Αν χρησιμοποιήσουμε τον τύπο του Stirling

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^e e^{\theta/12n}, 0 < \theta < 1,$$

τότε παίρνουμε το φράγμα

$$|D_{K/\mathbb{Q}}| \geq \left(\frac{\pi}{4}\right)^{2r_2} \frac{1}{2\pi n} e^{2n - \frac{1}{6n}}$$

Παρατήρηση IX.1.28. Για πάρα πολύ καιρό το φράγμα του Minkowski ήταν το καλύτερο γνωστό σχετικό φράγμα. Στα μέσα της δεκαετίας του '70 ο Stark ανακάλυψε μια νέα αναλυτική μέθοδο η οποία αναπτύχθηκε περαιτέρω από τους Odlyzko, Serre, Poitou και άλλους.

Αν αντί να φράξουμε τη διακρίνουσα αλλά τους πρώτους παράγοντες αυτής καθώς και τον βαθμό των σωμάτων, μπορούμε να έχουμε ένα γενικότερο αποτέλεσμα από αυτό του Hermite.

Θεώρημα IX.1.29. *Έστω* K *ένα αλγεβρικό σώμα αριθμών και* $S = \{p_1, p_2, \ldots, p_n\}$ *ένα πεπερασμένο σύνολο πρώτων ιδεωδών αυτού. Το σύνολο των επεκτάσεων* L/K *βαθμού* $[L/K] \leq n$ *στο οποίο διακλαδίζονται πρώτα ιδεώδη το πολύ από αυτά που ανήκουν στο* S *είναι πεπερασμένο.*

Η ιδέα της απόδειξης είναι να χρησιμοποιήσουμε το n *και το σύνολο* S *και να βρούμε ένα φράγμα της διακρίνουσας* $D_{K/\mathbb{Q}}$. *Στη συνέχεια εφαρμόζουμε το θεώρημα Hermite, [18, Th. 2.13. Ch. III], [17].*

IX.1.6 Το παράδειγμα του Artin

Το παράδειγμα αυτό δίνει μια αδιακλάδιστη επέκταση της οποίας η ομάδα Galois είναι η εικοσαεδρική ομάδα A_5. Όπως ο ίδιος ο Artin έχει σημειώσει για μια δεδομένη Galois επέκταση L/K με ομάδα G, υπάρχουν άπειρες το πλήθος επεκτάσεις E/K ώστε $L \cap E = K$ και LE να είναι αδιακλάδιστη υπεράνω της E. Για να πάρουμε μια τέτοια αρκεί να κατασκευάσουμε μια επέκταση η οποία απορροφά τοπικά όλη τη διακλάδωση της L και πρέπει να εξασφαλίσουμε ότι $E \cap L = K$. Για να γίνει αυτό χρειαζόμαστε θεωρήματα πυκνότητας από τη θεωρία κλάσεων σωμάτων.

Θεωρούμε το πολυώνυμο $f(x) = x^5 - x - 1$. Έστω α μια ρίζα του πολυωνύμου και $K = \mathbb{Q}(\alpha)$. Το πολυώνυμο είναι ανάγωγο υπεράνω του $\mathbb{Q}$, αφού εύκολα διαπιστώνουμε ότι είναι ανάγωγο στο $\mathbb{F}_3[x]$. Επομένως $[K : \mathbb{Q}] = 5$. Η διακρίνουσα του πολυωνύμου $x^5 + ax + b$ είναι $5^5b^4 + 2^8a^5$. Επομένως $D(f(x)) = 2869 = 19 \cdot 151$. Αφού η διακρίνουσα είναι ελεύθερη τετραγώνου, $D_{K/\mathbb{Q}} = 2869$ και έχουμε $R_K = \mathbb{Z}[\alpha]$. Η $D_{K/\mathbb{Q}} > 0$, επομένως πρέπει $(-1)^{r_2} = 1$. Αφού $2r_2 \leq 5$, $r_2 \neq 0$ ή $r_2 = 2$. Αυτό σημαίνει ότι $r_1 = 5$ ή $r_1 = 1$. Η παράγωγος $f'(x) = 5x^4 - 1$, έχει δύο πραγματικές ρίζες. Επομένως $r_1 = 1$ και $r_2 = 2$. Υπολογίζουμε τη σταθερά Minkowski $M_K = 3,334$. Από κάθε κλάση υπάρχει ένα τουλάχιστο ακέραιο ιδεώδες A με $N_{K/\mathbb{Q}}(A) = 2$ ή 3.

Επειδή 2 και 3 πρώτοι αριθμοί, έπεται ότι το $A = P$ πρώτο ιδεώδες με $P \mid 2$ ή $P \mid 3$ με $f(P/p\mathbb{Z}) = 1$.

Αλλά $f(0) = f(1) = f(-1) = 1$, συνεπώς το πολυώνυμο $f(x)$ δεν έχει ρίζα ούτε στον $\mathbb{F}_2[x]$ ούτε στον $\mathbb{F}_3[x]$. Συνεπώς από τον νόμο ανάλυσης δεν μπορεί ούτε το $f(P/p\mathbb{Z}) = 1$. Επομένως δεν υπάρχουν ιδεώδη A του K με $A \neq R_K$ και $N_{K/\mathbb{Q}}(A) = 2$ ή 3. Συνεπώς $h_K = 1$.

Θεωρούμε τώρα το σώμα ανάλυσης του $f(x)$ υπεράνω του $\mathbb{Q}$, έστω E. Στον $E[x]$, το $f(x)$ γράφεται

$$f(x) = \prod_{i=1}^{5}(x - \alpha_i).$$

Η ομάδα Galois $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(f(x))$ μπορεί να θεωρηθεί ως ομάδα μεταθέσεων των ριζών του $f(x)$, $\alpha_1, \alpha_2, \ldots, \alpha_5$.

Έστω Q ένα πρώτο ιδεώδες του E, $Q \mid 2$. Αν θεωρήσουμε το $f(x)$ modulo 2, έχουμε

$$f(x) \equiv (x^2 + x + 1)(x^3 + x^2 + 1) \mod 2$$

Επομένως η ομάδα Galois περιέχει τη μετάθεση $(ik)(lmn)$, ως προς κάποια αρίθμηση των δεικτών. Επειδή $f(x)$ modulo 3 είναι ανάγωγο, η ομάδα Galois περιέχει τον κύκλο (12345). Επίσης περιέχει και $\big((ik)(lmn)\big)^3 = (ik)$. Η ομάδα $\mathrm{Gal}(E/\mathbb{Q})$ είναι μια υποομάδα της S_5 που περιέχει έναν κύκλο μήκους 5 και μια αντιμετάθεση. Συνεπώς $\mathrm{Gal}(E/\mathbb{Q}) \cong S_5$.

Η S_5 περιέχει μοναδική υποομάδα δείκτη 2, την A_5. Επομένως υπάρχει μοναδικό υπόσωμα το $\mathbb{Q}(\sqrt{D_{K/\mathbb{Q}}})$ που περιέχεται στο E, και $\mathrm{Gal}(E/\mathbb{Q}(\sqrt{2869})) \cong A_5$, τη λεγόμενη και εικοσαεδρική, για γεωμετρικούς λόγους, ομάδα. Είναι η μοναδική απλή ομάδα τάξης 60.

Η παρατήρηση τώρα είναι η εξής: Ενώ το $\mathbb{Q}$ δεν επιτρέπει καμία επέκταση του $L/\mathbb{Q}$ στην οποία όλα τα πρώτα ιδεώδη $p\mathbb{Z}$ να μην διακλαδίζονται, όπως θα δείξουμε στο θεώρημα της διακρίνουσας, στην επέκταση $E/\mathbb{Q}(\sqrt{2869})$ δεν διακλαδίζεται κανένα πρώτο ιδεώδες του $\mathbb{Q}(\sqrt{2869})$.

Στο K διακλαδίζονται τα πρώτα ιδεώδη $P \mid p$ όπου $p \mid D_{K/\mathbb{Q}}$ δηλαδή τα $p = 19$ και $p = 151$. Συνεπώς και τα πρώτα ιδεώδη Q του E που διαιρούν το p για $p = 19$ και $p = 151$ επίσης διακλαδίζονται λόγω της πολλαπλασιαστικότητας του βαθμού διακλάδωσης.

Επίσης, αν ο πρώτος p δεν διακλαδίζεται στο K, δεν διακλαδίζεται και στο E. Οι μοναδικοί πρώτοι αριθμοί που διακλαδίζονται είναι $p = 19$ και $p = 151$. Έστω λοιπόν Q πρώτο ιδεώδες $Q \cap \mathbb{Z} = p\mathbb{Z}$ για $p = 19$ και $p = 151$. Αφού το Q διακλαδίζεται υπεράνω του p, το πολυώνυμο $\overline{f}(x) \equiv f(x) \mod Q$ έχει μια πολλαπλή ρίζα. Επειδή $f(\alpha) = 0 \Rightarrow f'(\alpha) = 5\alpha^4 - 1 = 0$. ($\alpha^5 - \alpha - 1 = 0, 5\alpha^4 - 1 = 0 \Rightarrow 4\alpha = 5$). Επομένως $\alpha = \overline{6}$ στο $\mathbb{F}_{19}$ και $\alpha = \overline{39}$ στο $\mathbb{F}_{151}$. Για $p = 19$, στο $\mathbb{F}_{19}[x]$,

$$(x - 6)^2 = x^2 + 7x - 2 \Rightarrow x^5 - x + 1 = (x^2 - 7x - 2)(x^3 - 7x^2 - 6x + 9).$$

Θέτουμε $g(x) = x^3 - 7x^2 - 6x + 9$, $g(\alpha) = g(\overline{6}) \neq \overline{0}$. Συνεπώς το $\overline{f}(x) \in \mathbb{F}_{19}[x]$ και επομένως και στο R_E/Q έχει την ανάλυση:

$$\overline{f}(x) = (x - \overline{\alpha}_1)^2(x - \overline{\alpha}_3)(x - \overline{\alpha}_4)(x - \overline{\alpha}_5)$$

με διαφορετικές ανά δύο ρίζες $\overline{\alpha}_1, \overline{\alpha}_3, \overline{\alpha}_4, \overline{\alpha}_5$.

Αν $\sigma \in G_T(Q/p\mathbb{Z})$, τότε $\sigma\alpha_3 = \alpha_3, \sigma\alpha_4 = \alpha_4$ και $\sigma\alpha_5 = \alpha_5$. Συνεπώς $\sigma = \mathrm{Id}_E$ ή $\sigma = (\alpha_1, \alpha_2)$. Συνεπώς

$$|G_T(Q/p\mathbb{Z})| \leq 2 \Rightarrow e(Q/19) \leq 2.$$

Άλλα $e(P/19) = 2$ συνεπώς $e(Q/P) = 1$. Για $p = 151$, στο $\mathbb{F}_{151}[x]$

$$(x - 39)^2 = x^2 - 78x + 11, x^5 - x + 1 = (x^2 - 7x - 2)(x^3 + 7x^2 - 6x + 9).$$

Εντελώς ανάλογα αν $g(x) = x^3 + 78x^2 + 33x + 55$, πάλι $g(\alpha) = g(\overline{39}) \neq 0$ και όπως παραπάνω $e(Q/P) = 1$.

Πρόκειται κατά τον Lang για ένα παράδειγμα “of which Artin was very fond”, [11, σελ. 121]

IX.2 Το θεώρημα των μονάδων του Dirichlet

IX.2.1 Εισαγωγή

Μία ακόμα σημαντική εφαρμογή του Θεωρήματος του Minkowski, είναι η χρήση του στην απόδειξη του θεωρήματος μονάδων του Dirichlet.

Βέβαια το θεώρημα αποδείχτηκε το 1846, 18 χρόνια πριν γεννηθεί ο Minkowski. Ο Dirichlet χρησιμοποιεί στην απόδειξη την αρχή του περιστερώνα. Στην αρχή είχε αποδείξει το θεώρημα σε μερικές ειδικές περιπτώσεις, όπως για κυβικά σώματα αριθμών. Το γενικό θεώρημα ισχυρίζεται ο ίδιος, ότι το εμπνεύστηκε καθώς παρακολουθούσε το Ορατόριο του Πάσχα στην Καπέλα Σιστίνα (Sistine Chapel) στη Ρώμη.

Θεώρημα IX.2.1 (Μονάδων του Dirichlet)**.** *Έστω* K *αλγεβρικό σώμα αριθμών,*

$$[K : \mathbb{Q}] = n = r_1 + 2r_2,$$

ταυτότητας $[r_1, r_2]$ *και διακρίνουσας* $D_{K/\mathbb{Q}}$*. Η ομάδα των μονάδων του σώματος* K *είναι πεπερασμένα παραγόμενη αβελιανή ομάδα βαθμού* $r = r_1 + r_2 - 1$*. Αναλυτικά,* R_K *περιέχει πολλαπλασιαστικά ανεξάρτητες μονάδες* $\varepsilon_1, \varepsilon_2, \ldots, e_r$ *άπειρης τάξης ώστε*

$$E(R_K) \cong E(R_K)_{\text{torsion}} \otimes \langle \varepsilon_1 \rangle \otimes \langle \varepsilon_2 \rangle \otimes \cdots \otimes \langle \varepsilon_r \rangle.$$

Το σύνολο $E(R_K)_{\text{torsion}}$ *είναι το σύνολο των ριζών της μονάδας που ανήκουν στο* K *και είναι κυκλική ομάδα τάξης διαιρέτη του* $2|D_{K/\mathbb{Q}}|$.

Σημείωση IX.2.2. Πολλαπλασιαστικά ανεξάρτητες σημαίνει ότι αν

$$\varepsilon_1^{m_1} \varepsilon_2^{m_2} \cdots e_r^{m_r} = 1$$

με $m_i \in \mathbb{Z}$, $i = 1, 2, \ldots, r$, τότε $m_1 = m_2 = \cdots = m_r = 0$. Ένα σύνολο $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r\}$ πολλαπλασιαστικά ανεξάρτητων μονάδων θα λέγεται ένα θεμελιώδες σύστημα μονάδων.

Προτού συνεχίσουμε με την απόδειξη του θεωρήματος, θα μελετήσουμε μερικά ειδικά παραδείγματα.

Παράδειγμα IX.2.3. Υποθέτουμε ότι το K έχει ταυτότητα $[r_1, r_2]$ και ότι $r = r_1 + r_2 - 1 = 0$. Αυτό σημαίνει αμέσως ότι η $E(R_K)$ είναι πεπερασμένης τάξης, περιέχει μόνο ρίζες της μονάδας. Αλλά για να ισχύει $r_1 + r_2 - 1 = 0$ πρέπει $[r_1, r_2] = [1, 0]$ ή $[r_1, r_2] = [0, 1]$, δηλαδή $n = r_1 + 2r_2 = 1$, συνεπώς $K = \mathbb{Q}$ με $E(\mathbb{Z}) = \{\pm 1\}$ ή $n = r_1 + 2r_2 = 2$, και το σώμα $K = \mathbb{Q}(\sqrt{|D_{K/\mathbb{Q}}|})$, $D_{K/\mathbb{Q}} < 0$ (είναι τετραγωνικό μιγαδικό). Έχουμε ήδη δει στην παράγραφο II.3 ότι $E(R_K) = \{\pm 1\}$ εκτός από το $K = \mathbb{Q}(i)$, για το οποίο ισχύει $E(R_K) = \{\pm 1, \pm i\}$ και μάλιστα η ομάδα είναι κυκλική τάξης $4 \mid 2|D_{K/\mathbb{Q}}| = 8$ και εκτός από το $K = \mathbb{Q}(\sqrt{-3})$ για το οποίο ισχύει $E(R_K) = \{\pm 1, \pm\omega, \pm\omega^2\}$ (όπου ω πρωταρχική 3-ρίζα της μονάδας) και η ομάδα είναι κυκλική τάξης $6 = 2|D_{K/\mathbb{Q}}|$.

Παράδειγμα IX.2.4. Έστω ότι το K έχει ταυτότητα $[r_1, r_2]$ με $r = r_1 + r_2 - 1 = 1$. Αυτό συμβαίνει τότε και μόνο τότε όταν $[r_1, r_2] = [2, 0]$ ή $[1, 1]$ ή $[0, 2]$. Αν $[r_1, r_2] = [2, 0]$, τότε το $n = 2$ και το σώμα K είναι τετραγωνικό πραγματικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{D_{K/\mathbb{Q}}})$, $D_{K/\mathbb{Q}} > 0$. Επειδή $K \subset \mathbb{R}$, $E(R_K)_{\text{torsion}} = \{\pm 1\}$, αλλά εδώ ο βαθμός είναι $r = 1$. Αυτό σημαίνει ότι υπάρχει μία θεμελιώδης μονάδα ε_1 τέτοια ώστε κάθε $\varepsilon \in E(R_K)$ να γράφεται μονοσήμαντα $\varepsilon = \pm\varepsilon_1^n$, $n \in \mathbb{Z}$. Είναι φανερό ότι αν ε_1, τότε $-\varepsilon_1, \frac{1}{\varepsilon_1}, -\frac{1}{\varepsilon_1}$ είναι επίσης θεμελιώδης. Γι' αυτό κανονικοποιούμε την επιλογή μας, επιλέγοντας για ε_1, αυτήν τη μονάδα για την οποία ισχύει $\varepsilon_1 > 1$. Για τον υπολογισμό των μονάδων στα πραγματικά τετραγωνικά σώματα αριθμών παραπέμπουμε στο [26].

Αν τώρα $[r_1, r_2] = [1, 1]$, τότε $n = r_1 + 2r_2 = 1 + 2 = 3$ το σώμα μας είναι κυβικό με μία πραγματική και δύο μιγαδικές ρίζες, για παράδειγμα $K = \mathbb{Q}(\sqrt[3]{2})$. Αργότερα θα δείξουμε ότι

$$E(R_K) = \{\pm\varepsilon^n | n \in \mathbb{Z}, \varepsilon = 1 + \sqrt[3]{2} + \sqrt[3]{4}\} = \langle \pm 1 \rangle \otimes \langle \varepsilon \rangle.$$

Αν τώρα $[r_1, r_2] = [0, 2]$, τότε το σώμα K είναι βαθμού $[K : \mathbb{Q}] = 4$, πλήρως μιγαδικό για παράδειγμα $K = \mathbb{Q}(\zeta_5)$. Αποδεικνύεται ότι

$$E(R_K) = \langle \zeta_{10} \rangle \otimes \langle \frac{1+\sqrt{5}}{2} \rangle.$$

Από την απόδειξη του θεωρήματος δεν προκύπτει μέθοδος υπολογισμού ενός συστήματος θεμελιωδών μονάδων. Για τον υπολογισμό της ομάδας των μονάδων σε συγκεκριμένα παραδείγματα χρειαζόμαστε πιο βελτιωμένες υπολογιστικές μεθόδους, τεχνικές αναγωγής δικτυωτών, δηλαδή μεθόδους εύρεσης μικρού μήκους διανυσμάτων σε δικτυωτά για παράδειγμα LLL.

IX.2.2 Απόδειξη του Θεωρήματος μονάδων

Έστω λοιπόν K αλγεβρικό σώμα αριθμών $[K : \mathbb{Q}] = n$, ταυτότητας $[r_1, r_2]$. Θα εμφυτεύσουμε την ομάδα K^* στον $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Υπενθυμίζουμε ότι, στην προηγούμενη παράγραφο είχαμε την κανονική εμφύτευση

$$\sigma : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

$$\sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \sigma_{r_1+2}(x), \ldots, \sigma_{r_1+r_2}(x)).$$

Επειδή η ομάδα των μονάδων είναι πολλαπλασιαστική ενώ τα δικτυωτά προσθετικά, θα ορίσουμε την ακόλουθη λογαριθμική εμφύτευση της ομάδας K^*:

$$L : E(R_K) \subset K^* \xrightarrow{\sigma} (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \xrightarrow{\ell} \mathbb{R}^{r_1+r_2}.$$

όπου αν

$$x = (x_1, x_2, \ldots, x_{r_1}, z_{r_1+1}, z_{r_1+2}, \ldots, z_{r_1+r_2})$$

η ℓ ορίζεται ως

$$\ell(x) = (\log|x_1|, \log|x_2|, \ldots, \log|x_{r_1}|, \log|z_{r_1+1}|^2, \log|z_{r_1+2}|^2, \ldots, \log|z_{r_1+r_2}|^2).)$$

Ας ονομάσουμε

$$\ell_k = \begin{cases} \log|x_k|, & \text{για } k = 1, 2, \ldots, r_1 \\ \log|z_k|^2, & \text{για } k = r_1+1, r_1+2, \ldots, r_1+r_2 \end{cases}$$

επομένως

$$\ell(x) = (\ell_1(x), \ldots, \ell_{r_1}(x), \ell_{r_1+1}(x), \ldots, \ell_{r_1+r_2}(x)).$$

Η προσθετική ιδιότητα των λογαρίθμων μας δίνει ότι η

$$\ell : (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \longrightarrow \mathbb{R}^{r_1+r_2}$$

είναι ομομορφισμός ομάδων. Προφανώς ισχύει

$$\log|N(x)| = \sum_{k=1}^{r_1+r_2} \ell_k(x).$$

Συνολικά η απεικόνιση

$$\begin{aligned} K^* &\xrightarrow{L} \mathbb{R}^{r_1+r_2} \\ \alpha &\longmapsto \ell(\sigma(\alpha)) \end{aligned}$$

είναι ομομορφισμός ομάδων της πολλαπλασιαστικής K^* στην προσθετική $\mathbb{R}^{r_1+r_2}$. Πράγματι

$$L(\alpha\beta) = \ell(\sigma(\alpha\beta)) = \ell(\sigma(\alpha)\sigma(\beta)) = \ell(\sigma(\alpha)) + \ell(\sigma(\beta)) = L(\alpha) + L(\beta).$$

Αν $\alpha \in K$,

$$\sum_{i=1}^{r_1+r_2} \ell(\sigma(\alpha)) = \log|N(\sigma(\alpha))| = \log(|\sigma_1(\alpha)|, \dots, |\sigma_{r_1}(\alpha)|, |\sigma_{r_1+1}(\alpha)|^2 \cdots |\sigma_{r_1+r_2}(\alpha)|^2)$$

και επειδή $|\sigma_k(\alpha)|^2 = \sigma_k(\alpha)\overline{\sigma}(\alpha)$, έχουμε

$$\sum_{i=1}^{r_1+r_2} \ell(\sigma(\alpha)) = \log|N_{K/\mathbb{Q}}(\alpha)|.$$

Επομένως, αν $\varepsilon \in E(R_K)$, τότε $N_{K/\mathbb{Q}}(\varepsilon) = \pm 1$, τότε $\sum_{i=1}^{r_1+r_2} \ell(\sigma(\varepsilon)) = 0$, δηλαδή το ε ανήκει στο υπερεπίπεδο του $\mathbb{R}^{r_1+r_2}$

$$H := \left\{ (x_1, x_2, \dots, x_{r_1}, z_1, z_2, \dots, z_{r_2} : \sum_{i=1}^{r_1} x_i + 2\sum_{j=1}^{r_2} z_j = 0 \right\}$$

διάστασης $\dim H = r_1 + r_2 - 1$.

Λήμμα IX.2.5. *Έστω* B *ένα συμπαγές υποσύνολο του* $\mathbb{R}^{r_1+r_2}$. *Το σύνολο*

$$B' = \{\varepsilon \in E(R_K) : L(\varepsilon) \in B\} = L(E(R_K)) \cap B$$

είναι πεπερασμένο.

Απόδειξη. Αφού το B είναι συμπαγές, είναι φραγμένο. Συνεπώς, για κάθε $\varepsilon \in B'$ υπάρχει $r \in \mathbb{R}$ ώστε $\|L(\varepsilon)\| < r$, όπου $\|\cdot\|$ είναι η συνηθισμένη μετρική στον $\mathbb{R}^{r_1+r_2}$. Επομένως

$$|\ell_k(\sigma(\varepsilon))| \le \|L(\varepsilon)\| < r \text{ για κάθε } k = 1, 2, \dots, r_1 + r_1,$$

δηλαδή $|\log|\sigma_k(\varepsilon)|| < r$, για $k = 1, 2, \dots, r_1 + r_2$.

Για $k = 1, 2, \dots, r_1$, έχουμε $-r < \log|\sigma_k(\varepsilon)| < r$, δηλαδή $e^{-r} < |\sigma_k(\varepsilon)| < e^r$.

Για $k = r_1 + 1, r_1 + 2, \dots, r_1 + r_2$, έχουμε $|\log|\sigma_k(\varepsilon)|| < r$, δηλαδή

$$|\log|\sigma_k(\varepsilon)^2| < r \Rightarrow e^{-r} < |\sigma_k(\varepsilon)|^2 < e^r.$$

Επομένως, υπάρχει $\alpha \in \mathbb{R}$ με $\alpha > 1$ τέτοιο ώστε για κάθε $\varepsilon \in B'$ να ισχύει

$$\alpha^{-1} < |\sigma_k(\varepsilon)| < \alpha, k = 1, 2, \dots, n.$$

Συνεπώς και όλες οι συμμετρικές συνάρτησεις των $\sigma_k(\varepsilon)$ είναι κατ' απόλυτη τιμή φραγμένες.

Το $\varepsilon \in R_K$, το χαρακτηριστικό πολυώνυμο είναι

$$f_\varepsilon(x) = \prod_{k=1}^{n} (x - \sigma_k(\varepsilon)).$$

Αυτό είναι δύναμη του ανάγωγου $f(x) := \mathrm{Irr}(\varepsilon, \mathbb{Q}) \in \mathbb{Z}[x]$. Επομένως $f_\varepsilon(x) \in \mathbb{Z}[x]$, δηλαδή οι συμμετρικές συναρτήσεις των $\sigma_k(\varepsilon)$ ανήκουν στο $\mathbb{Z}$. Επομένως το σύνολο τιμών των συμμετρικών συναρτήσεων είναι πεπερασμένο. Για τα στοιχεία $\varepsilon \in B'$ υπάρχουν πεπερασμένου πλήθους χαρακτηριστικά πολυώνυμα. Τελικά το σύνολο B' είναι πεπερασμένο. □

Λήμμα IX.2.6. *Η* $L : E(R_K) \xrightarrow{\sigma} (\mathbb{R}^*)^{r_1} \times (\mathbb{R}^*)^{r_2} \xrightarrow{\ell} \mathbb{R}^{r_1+r_2}$, *έχει πυρήνα το σύνολο των ριζών της μονάδας που ανήκουν στην* $E(R_K)$. *Η ομάδα αυτή είναι πεπερασμένη κυκλική άρτιας τάξης.*

Απόδειξη. Ο πυρήνας

$$\ker L = \{\varepsilon \in E(R_K) : L(\varepsilon) = (0, 0, \dots, 0)\}$$

Το σύνολο $B := \{(0, 0, \dots, 0)\}$ είναι συμπαγές και

$$\ker L = \{\varepsilon \in E(R_K) : \ell(\sigma_k(\alpha) \in B\} = L(E(R_K)) \cap B.$$

Επομένως, από το λήμμα IX.2.5, έπεται ότι ο πυρήνας είναι πεπερασμένος. Αλλά τότε η $\ker L$ είναι πεπερασμένη υποομάδα της K^*. Συνεπώς είναι κυκλική. Τώρα,

$$\varepsilon \in \ker L \Leftrightarrow L(\varepsilon) = \ell(\sigma(\varepsilon)) = (0, 0, \dots, 0) \Leftrightarrow |\sigma_k(\varepsilon)| = 1 \text{ για } k = 1, 2, \dots, n.$$

Επίσης αν $\varepsilon \in \ker L$, τότε και $\varepsilon^m \in \ker L$ για κάθε $m \in \mathbb{N}$, αφού $|\sigma_k(\varepsilon^m)| = |\sigma_k(\varepsilon)|^m = 1$. Όμως ο πυρήνας $\ker L$ είναι πεπερασμένος. Συνεπώς, υπάρχουν $m_1, m_2 \in \mathbb{N}$, $m_1 > m_2$ τέτοια ώστε $\varepsilon^{m_1} = e^{m_2} \Rightarrow \varepsilon^{m_1 - m_2} = 1$, δηλαδή το ε είναι ρίζα της μονάδας. Αποδείξαμε ότι όλα τα στοιχεία του $\ker L$ είναι ρίζες της μονάδας.

Ισχύει και το αντίστροφο. Αν $x \in E(R_K)$ είναι ρίζα της μονάδας, $x^m = 1$ για $m \in \mathbb{N}$ οπότε και

$$|\sigma_k(x)|^m = |\sigma_k(x^m)| = |\sigma_k(1)| = 1 \text{ για κάθε } k = 1, 2, \dots, n$$

δηλαδή $x \in \ker L$.

Πάντοτε η ομάδα $\ker L$, περιέχει την υποομάδα $\{\pm 1\}$. Συνεπώς η τάξη της $\ker L$ είναι άρτιος αριθμός. □

Παρατήρηση IX.2.7. Η ομάδα των ριζών της μονάδας ενός αλγεβρικού σώματος αριθμών K είναι κυκλική και η τάξη της διαιρεί το $2|D_{K/\mathbb{Q}}|$ [16, σελ. 99, prop. 3.4].

Ας περάσουμε τώρα στην εικόνα

$$L(E(R_K)) \subset \mathbb{R}^{r_1 + r_2}.$$

Σύμφωνα με το λήμμα IX.2.5, η εικόνα είναι μια διακριτή υποομάδα του $\mathbb{R}^{r_1+r_2}$, οπότε λόγω της πρότασης IX.1.2 είναι ένα ελεύθερο $\mathbb{Z}$-module βαθμού $r \le r_1 + r_2$.

Επειδή $\ker L$ πεπερασμένη και $L(E(R_K))$ πεπερασμένα παραγόμενη, έπεται ότι και η $E(R_K)$ είναι πεπερασμένα παραγόμενη αβελιανή ομάδα (πεπερασμένα παραγόμενο $\mathbb{Z}$-module). Σύμφωνα με το θεώρημα XIII.6.42 του παραρτήματος,

$$E(R_K) = \ker L \times \mathbb{Z}^r$$

και μάλιστα $\ker L$ είναι το $E(R_K)_{\text{torsion}}$ αυτής.

Θα αποδείξουμε ότι ο βαθμός της εικόνας $L(E(R_K))$ είναι ακριβώς $r = r_1 + r_2 - 1$. Έχουμε αποδείξει ήδη, ότι $L(E(R_K)) \subset H$,

$$H := \left\{ (x_1, x_2, \dots, x_{r_1}, z_1, z_2, \dots, z_{r_2}) \in \mathbb{R}^{r_1+r_2} : \sum_{i=1}^{r_1} + 2 \sum_{j=1}^{r_2} z_j = 0 \right\}$$

με διάσταση $\dim H = r_1 + r_2 - 1$. Επειδή το $L(E(R_K))$ είναι διακριτή (discrete) υποομάδα του H έπεται ότι έχει βαθμό

$$r \le r_1 + r_2 - 1.$$

Αυτό ήταν η εύκολη κατεύθυνση της απόδειξης. θα αποδείξουμε και το αντίθετο, δηλαδή ότι

$$r \ge r_1 + r_2 - 1,$$

ισοδύναμα ότι το $L(E(R_K))$ περιέχει $r = r_1 + r_2 - 1$, $\mathbb{R}$-γραμμικά ανεξάρτητα διανύσματα. Εδώ είναι που θα χρειαστούμε το θεώρημα του **Minkowski**.

Αρκεί να αποδείξουμε ότι για κάθε γραμμική μορφή

$$f : H \longrightarrow \mathbb{R}$$

υπάρχει $\varepsilon \in E(R_K)$ ώστε $f(L(\varepsilon)) \neq 0$. Υπενθυμίζουμε από τη γραμμική άλγεβρα ότι και ο χώρος των γραμμικών μορφών

$$H^* = \{f : H \longrightarrow \mathbb{R} : f \text{ γραμμική } \}$$

έχει και αυτός διάσταση $r_1 + r_2 - 1$ και ότι αν $\{w_1, w_2, \dots, w_r\}$ μια βάση του H, τότε υπάρχει μια βάση $\{f_1, f_2, \dots, f_r\}$ του H^* ώστε για κάθε $i = 1, 2, \dots, n$ $f_i(w_i) = 1$ και $f_i(w_j) = 0$ για κάθε $j \neq i$, $j \in \{1, 2, \dots, n\}$.

Ας υποθέσουμε ότι ο $L(E(R_K))$ δεν έχει διάσταση $r = r_1 + r_2 - 1$. Θα περιέχει ένα γνήσιο κομμάτι της βάσης. Χωρίς βλάβη της γενικότητας έστω

$$\{w_1, w_2, \dots, w_{r-1}\} \subset L(E(R_K))$$

και $w_r \notin L(E(R_K))$. Αυτό σημαίνει ότι για κάθε $\varepsilon \in E(R_K)$ ισχύει

$$L(\varepsilon) \in \langle w_1, w_2, \dots, w_{r-1} \rangle$$

δηλαδή ότι όλα τα στοιχεία $\varepsilon \in E(R_K)$, γράφονται ως γραμμικός συνδυασμός στοιχείων της βάσης $\{w_1, w_2, \dots, w_{r-1}\}$ και πάντοτε, δηλαδή για κάθε $\varepsilon \in E(R_K)$ ο συντελεστής του w_r είναι μηδέν. Αυτό όμως είναι αδύνατο αφού για $f := f_r$ υπάρχει $\varepsilon \in E(R_K)$ ώστε αν

$$L(\varepsilon) = \lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_r w_r,$$

τότε

$$f_r(L(\varepsilon)) = \lambda_r \neq 0.$$

Επειδή τώρα η συνάρτηση

$$\psi : H \ni y = (y_1, y_2, \dots, y_{r+1}) \longmapsto (y_1, y_2, \dots, y_r) \in \mathbb{R}^r$$

είναι ένας ισομορφισμός $\mathbb{R}$-διανυσματικών χώρων μπορούμε να γράψουμε τη γραμμική μορφή

$$f(y) = c_1 y_1 + c_2 y_2 + \cdots + c_r y_r : c_i \in \mathbb{R}.$$

Θα εφαρμόσουμε το θεώρημα του **Minkowski**. Χρειαζόμαστε ένα «καλό» σύνολο το οποίο να έχει μεταξύ άλλων και αρκετά μεγάλο όγκο. Κρατούμε σταθερό έναν πραγματικό αριθμό

$$\alpha \geq 2^n \left(\frac{1}{2\pi}\right)^{r_2} |D_{K/\mathbb{Q}}|^{1/2}.$$

Για κάθε r-άδα θετικών πραγματικών αριθμών $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ επιλέγουμε ένα $\lambda_{r+1} > 0$ ώστε

$$\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha.$$

Ορίζουμε το σύνολο:

$$B = \{(x_1, x_2, \dots, x_{r_1}, z_1, z_2, \dots, z_{r_2}) : x_i \in \mathbb{R}, z_j \in \mathbb{C}, \text{ και } |x_i| \leq \lambda_i, |z_j| \leq \lambda_{j+r_1}\}.$$

Το B είναι συμπαγές, κυρτό και συμμετρικό ως προς την αρχή των αξόνων (άσκηση). Έχει όγκο

$$\mathrm{Vol}(B) = \prod_{i=1}^{r_1} 2\lambda_i \prod_{j=r_1+1}^{r_1+r_2} \pi\lambda_j^2 = 2^{r_1}\pi^{r_2}\alpha \geq 2^{r_1}\pi^{r_2}2^n \left(\frac{1}{2\pi}\right)^{r_2} |D_{K/\mathbb{Q}}|^{1/2} \geq 2^{n-r_2}|D_{K/\mathbb{Q}}|^{1/2}.$$

Θεωρούμε το δικτυωτό $\sigma(R_K)$ του δακτυλίου των ακεραίων αλγεβρικών αριθμών του K. Από το πόρισμα IX.1.15 έχουμε

$$\mathrm{Vol}(\sigma(R_K)) = 2^{-r_2}|D_{K/\mathbb{Q}}|^{1/2}$$

και εφαρμόζουμε το θεώρημα του **Minkowski**, αφού $\mathrm{Vol}(B) \geq 2^n \mathrm{Vol}(\sigma(R_K))$. Υπάρχει $x_\lambda \in R_K \backslash \{0\}$ ώστε $\sigma(x_\lambda) \in B$. Αυτό σημαίνει ότι $|\sigma_i(x_\lambda)| \leq \lambda_i$ για κάθε $i = 1, 2, \ldots, n$. (Έχουμε θέσει $\lambda_{j+r_2} := \lambda_j$ για $j = r_1 + 1, \ldots, r_1 + r_2$ για τις συζυγείς εμφυτεύσεις $\overline{\sigma}_j$.) Τώρα $x_\lambda \in R_K$. Επομένως $N_{K/\mathbb{Q}}(x_\lambda) \in \mathbb{Z}$, οπότε

$$1 \leq |N_{K/\mathbb{Q}}(x_\lambda)| = |N(\sigma(x_\lambda))| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

Από την άλλη μεριά όμως για κάθε i

$$|\sigma_i(x_\lambda)| = |N(x_\lambda)| \cdot \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j \neq i} \lambda_j^{-1} = \lambda_i \alpha^{-1}.$$

Αποδείξαμε ότι για κάθε $i = 1, 2, \ldots, r$ ισχύει

$$\lambda_i \alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i \Rightarrow 0 \leq \log \lambda_i - \log |\sigma_i(x_\lambda)| \leq \log \alpha.$$

Επομένως

$$\begin{aligned} \left| f(L(x_\lambda)) - \sum_{i=1}^{r} c_i \log \lambda_i \right| &= \left| \sum_{i=1}^{r} c_i \log |\sigma_i(x_\lambda) - \sum_{i=1}^{r} c_i \log \lambda_i \right| \\ &\leq \sum_{i=1}^{r} |c_i| (\log |\sigma_i(x_\lambda)| - \log \lambda_i) \leq \sum_{i=1}^{r} |c_i| \log \alpha. \end{aligned}$$

Έστω τώρα β μια σταθερά

$$\beta > \sum_{i=1}^{r} |c_i| \log \alpha.$$

Για κάθε φυσικό αριθμό h διαλέγουμε r πραγματικούς αριθμούς $\lambda_{i,h}$ $i = 1, 2, \ldots, r$ ώστε

$$\sum_{i=1}^{r} c_i \log \lambda_{i,h} = 2\beta h.$$

Στη συνέχεια παίρνουμε

$$\lambda(h) = (\lambda_{1,h}, \lambda_{2,h}, \ldots, \lambda_{r,h})$$

και εφαρμόζουμε τα παραπάνω για κάθε φυσικό αριθμό $h \in \mathbb{N}$.

Από το θεώρημα **Minkowski** για κάθε $h \in \mathbb{N}$ υπάρχει $x_h := x_{\lambda(h)} \in R_K \backslash \{0\}$ ώστε

$$|f(L(x_h)) - 2\beta h| \leq \beta.$$

Συνεπώς, για κάθε φυσικό αριθμό $h \in N$

$$(2h - 1) < f(L(x_h)) < (2h + 1)\beta.$$

$$\begin{aligned} &\text{Για } h = 1, \quad \beta < f(L(x_1)) < 3\beta \\ &\text{Για } h = 2, \quad 3\beta < f(L(x_2)) < 5\beta \\ &\qquad\qquad \ldots\ldots \end{aligned}$$

Άρα για κάθε φυσικό αριθμό $h \in \mathbb{N}$ οι τιμές είναι διαφορετικές μεταξύ τους. Από την άλλη μεριά, επειδή $N_{K/\mathbb{Q}}(x_h) \leq \alpha$, υπάρχουν πεπερασμένα το πλήθος ιδεώδη με norm $\leq \alpha$, δηλαδή

υπάρχουν πεπερασμένου πλήθους κύρια ιδεώδη με norm $\leq \alpha$. Επειδή τα x_h είναι άπειρα το πλήθος υπάρχουν $(h,k) \in \mathbb{N} \times N$ ώστε

$$R_K x_h = R_K h_k,$$

δηλαδή υπάρχει μία μονάδα $\varepsilon \in E(R_K)$ ώστε

$$x_h = \varepsilon x_k.$$

Επομένως

$$L(\varepsilon) = L(x_k) - L(x_h) \Rightarrow f(L(\varepsilon)) = f(L(x_k)) - f(L(x_h)) \neq 0,$$

αφού τα $f(L(x_k))$ και $f(L(x_h))$ είναι διαφορετικά μεταξύ τους.

Παρατήρηση IX.2.8. Το θεώρημα Dirichlet έχει γενικευθεί και για την περίπτωση των λεγόμενων S-μονάδων. Στη γενική έκφραση φέρει τον τίτλο Θεώρημα Dirichlet-Chevalley-Hasse.

IX.2.3 Εφαρμογές του Θεωρήματος Dirichlet

Πρόταση IX.2.9. *Έστω $K \subset L$, $K \neq L$ αλγεβρικά σώματα αριθμών, $E(R_K), E(R_L)$ οι ομάδες των μονάδων και $\mu(R_K), \mu(R_L)$ οι ομάδες των ριζών της μονάδας των K και L αντίστοιχα. Οι ομάδες $E(R_K)/\mu(R_K)$ και $E(R_L)/\mu(R_L)$ είναι μεταξύ τους ισόμορφες τότε και μόνο τότε όταν το σώμα K είναι πλήρως πραγματικό, το σώμα L πλήρως μιγαδικό και $[L:K] = 2$.*

Απόδειξη. Έστω $N = [L:K]$. Υποθέτουμε, κατ' αρχήν την ισομορφία των ομάδων. Επομένως οι ομάδες θα έχουν τον ίδιο βαθμό δηλαδή

$$r_1(K) + r_2(K) = r_1(L) + r_2(L).$$

Επίσης

$$r_1(L) + 2r_2(L) = [L:\mathbb{Q}] = N[K:\mathbb{Q}] = Nr_1(K) + N2r_2(K),$$

από την οποία προκύπτει ότι

$$r_2(L) = (N-1)r_1(K) + (2N-1)r_2(K)$$

και

$$r_1(L) = r_1(K) + r_2(K) - r_2(L) = (2-N)r_1(K) + (2-2N)r_2(K).$$

Το $r_1(L) \geq 0$. Επομένως $N \leq 2$. Επειδή $K \neq L$ έπεται ότι $N = 2$. Συνεπώς $r_1(L) = -2r_2(K)$. Αυτό όμως ισχύει μόνο όταν

$$r_1(L) = r_2(K) = 0,$$

δηλαδή το L πλήρως μιγαδικό και το K πλήρως πραγματικό και $[L:K] = N = 2$.

Αντίστροφα, αν το K είναι πλήρως πραγματικό και L πλήρως μιγαδικό και $[L:K] = 2$, τότε $r_2(K) = 0$, $r_1(K) = [K:\mathbb{Q}]$, $r_1(L) = 0$, $r_2(L) = 2\frac{[K:\mathbb{Q}]}{2} = [K:\mathbb{Q}]$. Επομένως $r(K) = r(L)$ και συνεπώς οι ομάδες $E(R_K)/\mu(R_K)$ και $E(R_L)/\mu(R_L)$ είναι δύο ελεύθερες ομάδες ίδιου βαθμού, άρα είναι ισόμορφες. □

Ορισμός IX.2.10. Ένα σώμα θα λέγεται σώμα μιγαδικού πολλαπλασιασμού (CM-field) όταν είναι πλήρως μιγαδική τετραγωνική επέκταση ενός πλήρως πραγματικού σώματος αριθμών.

Παρατήρηση IX.2.11. Τα σώματα αυτά παίζουν ιδιαίτερο ρόλο στη θεωρία μιγαδικού πολλαπλασιασμού αβελιανών πολλαπλοτήτων.

Πόρισμα IX.2.12. *Έστω K, L αλγεβρικά σώματα αριθμών $K \subset L$, $K \neq L$. Η ομάδα πηλίκο $E(R_L)/E(R_K)$ είναι πεπερασμένη ακριβώς τότε όταν το σώμα L είναι CM-σώμα.*

Απόδειξη. Η ομάδα $E(R_L)/E(R_K)$ είναι πεπερασμένη σημαίνει ότι η $E(R_K)/\mu(R_K)$ έχει πεπερασμένο δείκτη στην $E(R_L)/\mu(R_L)$. Και οι δύο είναι αβελιανές ομάδες, οπότε θα πρέπει να συμπίπτουν οι βαθμοί, οπότε είναι ισόμορφες. Από την πρόταση IX.2.9 έπεται ότι το L είναι CM-σώμα.

Αντίστροφα, $E(R_K)/\mu(R_K) \subset E(R_L)/\mu(R_L)$. Το L είναι CM-σώμα ως προς το K, συνεπώς $r(K) = r(L)$ Επομένως $E(R_L)/E(R_K)$ είναι πεπερασμένη ομάδα. □

Σημείωση IX.2.13. Κλασική περίπτωση CM-σώματων είναι τα κυκλοτομικά σώματα $L = \mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$ και $K = L \cap \mathbb{R}$ το μέγιστο πραγματικό υπόσωμα του L. Συνήθως συμβολίζουμε το $\mathbb{Q}(\zeta_n) = K$ και $K^+ = K \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Παρατήρηση IX.2.14. Σε μία, κάπως διαφορετική απόδειξη του θεωρήματος του Dirichlet, αποδεικνύεται ότι αν σε κάποιο αλγεβρικό σώμα K ισχύει $r_1 > 0$, τότε υπάρχει μια μονάδα $\varepsilon \in E(R_K)$, $\varepsilon > 1$ για την οποία τα συζυγή $|\sigma_k(\varepsilon)| < 1$, για κάθε $k = 2, 3, \ldots, n$. Αυτό σημαίνει ότι το ε είναι πρωταρχικό στοιχείο της επέκτασης $K/\mathbb{Q}$, δηλαδή $K = \mathbb{Q}(\varepsilon)$.

IX.2.4 Παραδείγματα

Στην αρχή θα αναφερθούμε εν συντομία στις ρίζες της μονάδας.

Μερικές ασκήσεις στοιχειώδους θεωρίας αριθμών που αφορούν στη συνάρτηση του Euler.

1. Να αποδειχθεί ότι για κάθε θετικό ακέραιο n ισχύει $\varphi(n) \geq \sqrt{n/2}$.
2. Έστω n κάποιος φυσικός ακέραιος. Αν $\varphi(k) \leq n$ να αποδειχθεί ότι $k \leq 2n^2$.
3. Να αποδειχθεί ότι ισχύει $\varphi(k) = 1$ αν και μόνο αν $k = 1, 2$.
4. Να αποδειχθεί ότι $\varphi(k) = 2$ αν και μόνο αν $k = 3, 4, 6$.
5. Να αποδειχθεί ότι $\varphi(k) = 4$ αν και μόνο αν $k = 5, 8, 10, 12$.
6. Αν $n \geq 3$, τότε η τιμή $\varphi(n)$ είναι άρτιος.

Κάνοντας χρήση των παραπάνω αποτελεσμάτων μπορούμε να δώσουμε εκ νέου, μια απόδειξη στην

Πρόταση IX.2.15. *Αν K αλγεβρικό σώμα αριθμών, τότε ο δακτύλιος των ακεραίων αλγεβρικών αριθμών περιέχει πεπερασμένου πλήθους ρίζες της μονάδας.*

Απόδειξη. Έστω $[K : \mathbb{Q}] = n$ και ζ_k μια πρωταρχική k-ρίζα της μονάδας, $\zeta_k \in R_K$. Επομένως $\mathbb{Q}(\zeta_k) \subset K$, $[\mathbb{Q}(\zeta_k) : \mathbb{Q}] \leq [K : \mathbb{Q}] = n$ και $\varphi(k) \leq n$. Συνεπώς $k \in \{1, 2, \ldots, 2n^2\}$ δηλαδή το σύνολο των ριζών της μονάδας είναι πεπερασμένο. □

Πρόταση IX.2.16. *Έστω K αλγεβρικό σώμα αριθμών με $[K : \mathbb{Q}] = n \equiv 1 \mod 2$. Το σύνολο των ριζών της μονάδας στο K, $\mu(K) = \{\pm 1\}$.*

Απόδειξη. Έστω ζ_k μια πρωταρχική k-ρίζα της μονάδας του R_K. Επομένως θα έχουμε $\mathbb{Q}(\zeta_k) \subset K$, $[\mathbb{Q}(\zeta_k) : \mathbb{Q}] \mid [K : \mathbb{Q}]$ και επομένως $\varphi(k) \mid n$. Ο n είναι περιττός. Επομένως και ο $\varphi(k)$ είναι περιττός. Αλλά σύμφωνα με την άσκηση 6 για $k \geq 3$ ο $\varphi(k)$ είναι άρτιος, δηλαδή $k \leq 2$. Για $k = 1$, $\zeta_1 = 1$ και για $k = 2$, $\zeta_2 = -1$, δηλαδή $\mu(K) = \{\pm 1\}$. □

Πόρισμα IX.2.17. *Οι μοναδικές ρίζες της μονάδας που ανήκουν σε ένα κυβικό σώμα αριθμών είναι οι ± 1.*

Πρόταση IX.2.18. *Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = 4$. Οι μόνες δυνατές ρίζες της μονάδας $\neq \pm 1$ που θα μπορούσαν να ανήκουν στον R_K είναι οι $\zeta_3, \zeta_4, \zeta_5, \zeta_6, \zeta_8, \zeta_{10}, \zeta_{12}$.*

Απόδειξη. Όπως παραπάνω, αν ζ_k πρωταρχική ρίζα της μονάδας, $\zeta_k \in R_K$, τότε $\varphi(k) \mid 4$, δηλαδή $\varphi(k) = 1, 2$ ή 4. Από τις ασκήσεις προκύπτει ότι $k = 1, 2, 3, 4, 5, 6, 8, 10, 12$. □

Ας περάσουμε τώρα σε αλγεβρικά σώματα αριθμών με βαθμό της ομάδας των μονάδων > 0.

Η πιο απλή περίπτωση είναι αυτή των πραγματικών τετραγωνικών σωμάτων αριθμών. Επειδή $r_1 = 1$ και $2r_2 = 2$ η ομάδα των μονάδων $E(R_K)$ είναι αβελιανή ομάδα βαθμού 1, δηλαδή

$$E(R_K) = E(R_K)_{\text{torsion}} \otimes \langle \varepsilon_0 \rangle.$$

Για να προσδιορίσουμε τη μονάδα ε_0 χρειαζόμαστε τη θεωρία των συνεχών κλασμάτων και τη θεωρία των εξισώσεων του Pell. Για την περιγραφή ενός αλγορίθμου παραπέμπουμε στο [26].

Κυβικά σώματα αριθμών

Το αμέσως επόμενο βήμα είναι η μελέτη κυβικών σωμάτων αριθμών με μια θεμελιώδη μονάδα. Κάθε κυβικό σώμα αριθμών έχει μία ή τρεις πραγματικές εμφυτεύσεις. Η ομάδα των μονάδων έχει βαθμό 1 ακριβώς τότε όταν έχει μια πραγματική και δύο μιγαδικές εμφυτεύσεις. Αφού έχει δύο μιγαδικές εμφυτεύσεις, το θεώρημα του Stickelberger μας δίνει

$$\operatorname{sign}(D_{K/\mathbb{Q}}) = (-1)^1 = -1$$

δηλαδή $D_{K/\mathbb{Q}} < 0$. Η επέκταση $K/\mathbb{Q}$ είναι Galois αν και μόνο αν η διακρίνουσα $D_{K/\mathbb{Q}}$ είναι τέλειο τετράγωνο. Στην περίπτωσή μας η Galois θήκη του K, έστω N, είναι μια επέκταση $N/\mathbb{Q}$ με ομάδα Galois ισόμορφη με την S_3 η οποία περιέχει και την τετραγωνική επέκταση $\mathbb{Q}(\sqrt{|D_{K/\mathbb{Q}}|})$.

Η ομάδα των μονάδων είναι

$$E(R_K) = \langle \pm 1 \rangle \otimes \langle \varepsilon_0 \rangle,$$

όπου ε_0, όπως και στα πραγματικά τετραγωνικά σώματα αριθμών είναι η ελάχιστη πραγματική μονάδα με $\varepsilon_0 > 1$.

Στο [2, κεφάλαιο 13], ο E. Artin φράσσει τη θεμελιώδη μονάδα ε_0 μέσω της τιμής $|D_{K/\mathbb{Q}}|$ από κάτω. Συγκεκριμένα ισχύει

Θεώρημα IX.2.19 (Artin). *Ισχύει*

$$|D_{K/\mathbb{Q}}| < 4\varepsilon_0^3 + 24.$$

Παρατήρηση IX.2.20. Ο Keith Conrad [5] επεξεργάστηκε αναλυτικά την ιδέα του Artin. Το θεώρημα υπάρχει και στα [6]. Η απόδειξη ακολουθεί στην επόμενη σελίδα.

Άμεση και ιδιαίτερα χρήσιμη συνέπεια του θεωρήματος είναι το ακόλουθο:

Πόρισμα IX.2.21. *Έστω $\varepsilon \in E(R_K)$, $\varepsilon > 1$. Αν $4\varepsilon^{3/2} + 24 < |D_{K/\mathbb{Q}}|$, τότε το ε είναι η θεμελιώδης μονάδα $\varepsilon = \varepsilon_0$ του K.*

Απόδειξη. (του πορίσματος) Επιλέγουμε μια εμφύτευση του N στο $\mathbb{C}$ η οποία επεκτείνει την πραγματική εμφύτευση του K στο $\mathbb{R}$ και την κρατούμε σταθερή. Έτσι ταυτίζουμε το N με την εικόνα του στους μιγαδικούς αριθμούς. Από τη σχέση $E(R_K) = \langle \pm 1 \rangle \otimes \langle \varepsilon_0 \rangle$, έπεται ότι το $\varepsilon = \varepsilon_0^n$, για κάποιο θετικό ακέραιο n. Αν το $n \geq 2$, τότε θα είχαμε

$$|D_{K/\mathbb{Q}}| \leq 4\varepsilon_0^3 + 24 = 4\varepsilon^{3/n} + 24 \overset{n\geq 2}{\leq} 4\varepsilon^{3/2} + 24,$$

άτοπο, λόγω της υπόθεσης. Συνεπώς $n = 1$ και $\varepsilon = \varepsilon_0$. □

Παράδειγμα IX.2.22. Έστω $K = \mathbb{Q}(\sqrt[3]{2})$. Γνωρίζουμε από τα προηγούμενα ότι $R_K = \mathbb{Z}[\sqrt[3]{2}]$ και $D_{K/\mathbb{Q}} = -108$. Έχουμε

$$1 = (\sqrt[3]{2})^3 - 1 = \left(\sqrt[3]{2} - 1\right)\left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right).$$

Συνεπώς το $\varepsilon = 1 + \sqrt[3]{2} + \sqrt[3]{4} \in E(R_K)$. Υπολογίζουμε ότι $\varepsilon \approx 3,847$ και ότι $4e^{3/2} + 24 \approx 54,185 < 108$. Επομένως το $\varepsilon = \varepsilon_0$ είναι η θεμελιώδης μονάδα του $K = \mathbb{Q}(\sqrt[3]{2})$.

Παρατήρηση IX.2.23. Η πολυπλοκότητα των θεμελιωδών μονάδων καθαρών κυβικών σωμάτων αυξάνεται πάρα πολύ γρήγορα. Για παράδειγμα, η θεμελιώδης μονάδα του σώματος $\mathbb{Q}(\sqrt[3]{23})$ είναι:

$$2166673601 + 761875860\sqrt[3]{23} + 267901370\sqrt[3]{529}.$$

Συχνά προσπαθούμε να βρούμε στοιχεία με την ίδια norm στο σώμα και στη συνέχεια να ελέγξουμε αν αυτά είναι συνεταιρικά. Αν αυτό συμβαίνει, το πηλίκο τους είναι μονάδα του R_K.

Απόδειξη. (Θεωρήματος του Artin) Έστω ε μια πραγματική μονάδα του K, $\varepsilon > 1$, οπότε $\varepsilon \neq \pm 1$. Αυτό σημαίνει ότι $\varepsilon \notin \mathbb{Q}$, οπότε το $K = \mathbb{Q}(\varepsilon)$. Το σύνολο $\mathbb{Z}[\varepsilon]$ είναι μια τάξη του R_K. Από τη σχέση $\mathbb{Z}[\varepsilon] \subset R_K$, προκύπτει ότι

$$\mathrm{Disc}(\mathbb{Z}[\varepsilon]) = [R_K : \mathbb{Z}[\varepsilon]]^2 \cdot D_{K/\mathbb{Q}}.$$

Συνεπώς

$$|D_{K/\mathbb{Q}}| \leq |\mathrm{Disc}(\mathbb{Z}[\varepsilon])|.$$

Θα αποδείξουμε ότι

$$|\mathrm{Disc}(\mathbb{Z}[\varepsilon])| < 4\varepsilon^3 + 24.$$

Έστω $\sigma : K \hookrightarrow \mathbb{C}$ μια μη-πραγματική εμφύτευση του K. Η άλλη είναι η συζυγής της $\overline{\sigma}$. Η $N_{K/\mathbb{Q}}(\varepsilon) = \varepsilon \cdot \sigma(\varepsilon) \cdot \overline{\sigma}(\varepsilon) = \varepsilon|\sigma(\varepsilon)|^2 > 0$. Επομένως $N_{K/\mathbb{Q}}(\varepsilon) = 1$. Θέτουμε $u = \sqrt{\varepsilon}$ και έχουμε $1 = u^2|\sigma(\varepsilon)|^2$. Αυτό σημαίνει ότι $|\sigma(\varepsilon)| = \frac{1}{u}$ και σε πολικές συντεταγμένες $\sigma(\varepsilon) = u^{-1}e^{i\theta}$, για κάποιο $\theta \in \mathbb{R}$. Υπολογίζουμε τη διακρίνουσα της $\mathbb{Z}[\varepsilon]$

$$\begin{aligned}
\mathrm{Disc}\mathbb{Z}[\varepsilon] &= \big((\sigma(\varepsilon) - \varepsilon)(\overline{\sigma}(\varepsilon) - \varepsilon)(\sigma(\varepsilon) - \overline{\sigma}(\varepsilon)\big)^2 \\
&= \big((u^{-1}e^{i\theta} - u^2)(u^{-1}e^{-i\theta} - u^2)(u^{-1}e^{i\theta} - u^{-1}e^{-i\theta})\big)^2 \\
&= \big((u^{-2} + u^4 - 2u\cos\theta)(2iu^{-1}\sin\theta)\big)^2 \\
&= -4\sin^2\theta(u^3 + u^{-3} - 2\cos\theta)^2
\end{aligned}$$

Το $\varepsilon = u^2 > 1$. Συνεπώς και $u > 1$, οπότε $u^3 + u^{-3} > 2$ από όπου έχουμε ότι $a := \frac{u^3+u^{-3}}{2} > 1$. Η απόλυτη τιμή

$$|\mathrm{Disc}_{K/\mathbb{Q}}(\mathbb{Z}[\varepsilon])| = 4\sin^2\theta(2a - 2\cos\theta)^2 = 16(1 - \cos^2\theta)(a - \cos\theta)^2.$$

Θέτουμε $y = \cos\theta$. Το $y \in [-1, 1]$ και θα μελετήσουμε τη συνάρτηση

$$f(y) = 16(1 - y^2)(a - y)^2.$$

Επιθυμούμε να υπολογίσουμε τη μέγιστη τιμή της συνάρτησης αυτής. Έστω ότι αυτό συμβαίνει για την τιμή y_0. Η $f(y) \geq 0$ για κάθε τιμή του διαστήματος $[-1, 1]$, ενώ ισχύουν $f(1) = f(-1) = 0$ και $f(0) = 16a^2 > 0$. Επομένως $y_0 \in (-1, 1)$ και $f'(y_0) = 0$. Υπολογίζουμε την παράγωγο

$$f'(y) = 32(a - y)(2y^2 - ay - 1).$$

Η ρίζα της παραγώγου του πρωτοβάθμιου παράγοντα είναι $a > 1$. Επομένως

$$ay_0 = 2y_0^2 - 1. \tag{IX.2}$$

Έτσι έχουμε

$$|\mathrm{Disc}(\mathbb{Z}[\varepsilon])| = f(\cos\theta) < f(y_0) = 16(1 - y_0)(a - y_0)^2.$$

Χρησιμοποιούμε δύο φορές την (IX.2) και υπολογίζουμε ότι

$$16(1 - y_0^2)(a - y_0)^2 = 16(a^2 + 1 - y_0^4 - y_0^2).$$

Αντικαθιστούμε το a με $\frac{u^3+u^{-3}}{2}$ και βρίσκουμε

$$f(y_0) = 16\left(\frac{u^6}{4} + \frac{3}{2} + \left(\frac{u^{-6}}{4} - y_0^4 - y_0^2\right)\right).$$

Αν αποδείξουμε ότι $\frac{u^{-6}}{4} < y_0^2$, το δεξί μέλος της $f(y_0)$ γίνεται μικρότερο από το

$$16\left(\frac{u^6}{4} + \frac{3}{2}\right) = 4u^6 + 24 = 4\varepsilon^3 + 24,$$

δηλαδή

$$|\mathrm{Disc}(\mathbb{Z}[\varepsilon])| < 4\varepsilon^3 + 24$$

και τελειώσαμε.

Θεωρούμε λοιπόν τον τετραγωνικό παράγοντα της παραγώγου $f'(y)$,

$$\phi(y) = 2y^2 - ay - 1.$$

Επομένως $\phi(y_0) = 0$. Οι ρίζες του $\phi(y)$ έχουν γινόμενο $-1/2$, επομένως αντίθετα πρόσημα. Επίσης $\phi(1) = 1 - a < 0$ ενώ για αρκετά μεγάλο y, $\phi(y) > 0$. Αυτό σημαίνει ότι η $\phi(y)$ έχει μια ρίζα στο $(1, \infty)$. Αλλά το $y = \cos\phi \in (-1, 1)$. Επομένως $-1 < y_0 < 0$. Τώρα το $u > 1$, οπότε η ανισότητα $\frac{u^{-6}}{4} < y_0^2$ είναι ισοδύναμη προς $y_0 < \frac{-1}{2u^3}$. Από το γράφημα της $\phi(y)$, προκύπτει ότι το να αποδείξουμε ότι $y_0 < \frac{-1}{2u^3}$ είναι αρκετό, αφού το y_0 είναι η μικρότερη ρίζα του $\phi(y)$, να αποδείξουμε ότι $\phi(\frac{-1}{2u^3}) < 0$. Πράγματι,

$$\phi\left(\frac{-1}{2u^3}\right) = \frac{2}{4u^6} + \frac{a}{2u^3} - 1 = \frac{1}{2u^6} + \frac{1}{2u^3}\frac{u^3+u^{-3}}{2} - 1 = \frac{3}{4}\left(\frac{1}{u^6} - 1\right) < 0,$$

αφού $u > 1$ είναι μεταξύ τους συνεταιρικά. Επομένως το $\varepsilon = \frac{a-1}{a+1}$ είναι μονάδα του K. □

Παράδειγμα IX.2.24. Έστω α η πραγματική ρίζα του πολυωνύμου $f(x) = x^3 - x + 2$ και $K = \mathbb{Q}(\alpha)$. Το K είναι ένα κυβικό σώμα αριθμών με βαθμό 1. Έχουμε ήδη δει ότι $D_{K/\mathbb{Q}} = -104$ και ότι $R_K = \mathbb{Z}[\alpha]$. Το

$$f(x) = x^3 - x + 1 \equiv x(x+1)^2 \mod 2$$

Από τον νόμο ανάλυσης του Dedekind

$$2R_K = P^2Q, P \neq Q.$$

Αφού το α είναι ρίζα του $f(x)$, έχουμε

$$\alpha(\alpha - 1)(\alpha + 1) = -2$$

και $(\alpha, \alpha - 1) = (\alpha, \alpha + 1) = 1$. Η norm του α, $N_{K/\mathbb{Q}}(\alpha) = -2$. Επομένως $P = \langle 2, \alpha + 1\rangle = \langle 2, \alpha - 1\rangle$ και $Q = \langle 2, \alpha\rangle$. Επειδή $N_{K/\mathbb{Q}}(\alpha + 1) = -2 \in \langle \alpha + 1\rangle$. Ανάλογα $N_{K/\mathbb{Q}}(\alpha - 1) = -2 \in \langle \alpha - 1\rangle$.

Έχουμε $P = \langle \alpha+1\rangle = \langle \alpha-1\rangle$. Αυτό σημαίνει ότι τα $\alpha+1$ και $\alpha-1$ είναι μεταξύ τους συνεταιρικά. Επομένως, το $\varepsilon = \frac{\alpha-1}{\alpha+1}$ είναι μονάδα του K. Το $\alpha \approx -1,521$, οπότε $\varepsilon \approx 4,839$ και $4\varepsilon^{3/2}+24 \leq 4\cdot 5^{3/4}+24 \approx 4\cdot 11,118 + 24 < 104$. Άρα το $\varepsilon = \varepsilon_0$ είναι η κανονικοποιημένη (δηλαδή > 1) θεμελιώδης ρίζα του K.

Θεώρημα IX.2.25 (Ishida). *Έστω $\ell \in Z$, $\ell \geq 2$ έχει την ιδιότητα το $4\ell^3 + 27$ να είναι ελεύθερο τετραγώνου. Αν α είναι μια μοναδική πραγματική ρίζα του $x^3 + \ell x - 1$, τότε το $\alpha^{-1} = \varepsilon_0$ είναι η θεμελιώδης μονάδα του σώματος $K = \mathbb{Q}(\alpha)$.*

Απόδειξη. Θεωρούμε το πολυώνυμο

$$f(x) = x^3 + \ell x - 1.$$

Η παράγωγος $df/df = 3x^2 + \ell$ είναι θετικά ορισμένη συνεπώς το πολυώνυμο έχει μοναδική πραγματική ρίζα το α. Θεωρούμε το σώμα $K = \mathbb{Q}(\alpha)$. Το πολυώνυμο $f(x)$ έχει διακρίνουσα $D_{K/\mathbb{Q}}(\alpha) = -(4\ell^3 + 27) < 0$ και είναι ελεύθερη τετραγώνου. Επομένως, $R_K = \mathbb{Z}[\alpha]$ και $D_{K/\mathbb{Q}} = -(4\ell^3 + 27)$. Το α είναι ρίζα του $f(x)$. Άρα $\alpha^3 + \ell\alpha - 1 = 0 \Rightarrow \alpha(\ell + \alpha^2) = 1$ και $\alpha^{-1} = \ell + \alpha^2$. Είναι φανερό ότι $\alpha^{-1} > 1$ Επομένως το $\alpha^{-1} = \varepsilon_0^n$ για κάποιο φυσικό αριθμό $n \geq 1$. Θα αποδείξουμε ότι $n = 1$. Έστω ότι $n \geq 2$. Από το θεώρημα του Artin, έπεται ότι ισχύει

$$4\ell^3 + 27 = |D_{K/\mathbb{Q}}| < 4\varepsilon_0^3 + 24.$$

Συνεπώς $\ell < \varepsilon_0$ και

$$\ell^2 < \varepsilon_0^2 < \varepsilon_0^n = \alpha^{-1} - \ell + \alpha^2 < \ell + 1,$$

το οποίο για $\ell \geq 2$, είναι άτοπο. Επομένως, $\alpha^{-1} = \varepsilon_0$ η θεμελιώδης μονάδα του $\mathbb{Q}(\alpha)$.

□

Συχνά, προσπαθούμε να συσχετίσουμε την ομάδα μονάδων του K με την υποομάδα που παράγεται από ένα σύστημα υποομάδων ενός (ή περισσότερων) υποσωμάτων αυτού.

Έστω K ένα CM-σώμα, και K^+ το μέγιστο πραγματικό υπόσωμά του. Η επέκταση $[K : \mathbb{Q}] = 2n$ και $[K : K^+] = 2$. Το K έχει $2n$ μιγαδικές εμφυτεύσεις, ενώ το K^+ έχει n-πραγματικές εμφυτεύσεις. Επομένως

$$\operatorname{rank} E(R_K) = n - 1 = \operatorname{rank} E(R_{K^+}).$$

Αυτό σημαίνει ότι ο δείκτης $Q = [E(R_K) : E(R_{K^+})]$ είναι πεπερασμένος. Μάλιστα ισχύει

Πρόταση IX.2.26. *Ο δείκτης* $\delta_K := [E(R_K) : \mu(K)E(R_{K^+})]$ *είναι* 1 *ή* 2.

Απόδειξη. Πρώτα απ' όλα θα αποδείξουμε ότι η μιγαδική συζυγία στο $\mathbb{C}$ επάγει έναν αυτομορφισμό στο σώμα K ο οποίος είναι ανεξάρτητος της εμφύτευσης του K στο $\mathbb{C}$. Πράγματι, έστω

$$\sigma_i : K = \mathbb{Q}(\theta) \hookrightarrow \mathbb{Q}(\theta^{(i)}) \subset \mathbb{C}$$

και

$$\sigma_j : K = \mathbb{Q}(\theta) \hookrightarrow \mathbb{Q}(\theta^{(j)}) \subset \mathbb{C}$$

δύο εμφυτεύσεις του K. Θα αποδείξουμε ότι ισχύει:

$$\sigma_i^{-1}\big(\overline{\sigma_i(\alpha)}\big) = \sigma_j^{-1}\big(\overline{\sigma_j(\alpha)}\big), \text{ για κάθε } \alpha \in K.$$

Προφανώς η επέκταση $\sigma_i(K)/\sigma_i(K^+)$ είναι βαθμού 2, επομένως είναι Galois και η μιγαδική συζυγία αφήνει σταθερά τα στοιχεία του K^+. Επομένως $\overline{\sigma}_i(K) = \sigma_i(K)$. Συνεπώς ορίζεται και η $\sigma_i^{-1}(\overline{\sigma}_j)$. Ανάλογα ορίζεται και η $\sigma_j^{-1}(\overline{\sigma}_j)$. Και οι δύο είναι αυτομορφισμοί του K που αφήνουν τα στοιχεία του K^+ σταθερά, αφού το K^+ είναι πλήρως πραγματικά. Αφού το K είναι πλήρως μιγαδικό, έπεται ότι κανείς από τους παραπάνω αυτομορφισμούς δεν είναι ο ταυτοτικός αυτομορφισμός του K. Επειδή η ομάδα $\mathrm{Gal}(K/K^+)$ έχει τάξη 2, έπεται ότι αυτοί συμπίπτουν. Επομένως, όταν εργαζόμαστε σε CM σώμα η έννοια του μιγαδικού συζυγούς $\overline{\alpha}, \alpha \in K$ είναι καλά ορισμένη.

Προφανώς για κάθε ομορφισμό $\rho : K \to \mathbb{C}$ ισχύει $\rho(\overline{\alpha}) = \overline{\rho(\alpha)}$. Ιδιαίτερα, για $\alpha \in E(R_K)$, όλοι οι συζυγείς του $\epsilon/\overline{\epsilon}$ έχουν απόλυτη τιμή ίση με 1. Θα αποδείξουμε στο λήμμα XI.3.5 ότι είναι ρίζες της μονάδας συνεπώς $\epsilon/\overline{\epsilon} \in \mu(K)$.

Η συνάρτηση

$$\phi : E(R_K) \ni \epsilon \longmapsto \left[\frac{\epsilon}{\overline{\epsilon}}\right] \in \frac{\mu(K)}{\mu(K)^2}$$

είναι ομομορφισμός ομάδων.

Αν $\epsilon \in \ker\phi$, τότε υπάρχει $\zeta \in \mu(K)$ για το οποίο ισχύει $\epsilon/\overline{\epsilon} = \zeta^2$. Η σχέση αυτή γράφεται και ως $\epsilon\overline{\zeta}/\overline{\epsilon}\zeta = 1$ ($1/\zeta = \overline{\zeta}$), δηλαδή $\epsilon\overline{\zeta}/(\overline{\epsilon\overline{\zeta}}) = 1$, το οποίο σημαίνει ότι $\epsilon\overline{\zeta} \in K^+$, $\epsilon \in \mu(K) \cdot E(R_{K^+})$.

Αντίστροφα, αν $\epsilon = \zeta \cdot \epsilon^+ \in \mu(K)E(R_{K^+})$. Τότε

$$\frac{\epsilon}{\overline{\epsilon}} = \frac{\zeta\epsilon^+}{\overline{\zeta}\epsilon^+} = \zeta^2 \in \ker\phi.$$

Άρα $\ker\phi = \mu(K)E(R_{K^+})$. Τελικά έχουμε ότι

$$[E(R_K) : \ker\phi] \leq [\mu(K) : \mu(K)^2] \leq 2.$$

Το ερώτημα είναι, πότε ο δείκτης δ_K είναι 1 και πότε 2;

Αν το K είναι ένα μιγαδικό διτετραγωνικό σώμα αριθμών, περιέχει ακριβώς πραγματικό τετραγωνικό σώμα αριθμών, έστω K^+ και το K είναι ένα CM-σώμα. Έστω ϵ_0 μια θεμελιώδης μονάδα του K και ϵ^+ μια θεμελιώδης μονάδα του K^+. □

Πρόταση IX.2.27. *Ισχύουν:*

1. $\delta_K = 1$ *αν και μόνο αν η* ϵ^+ *είναι θεμελιώδης μονάδα του* K.
2. $\delta_K = 2$ *αν και μόνο αν* $\epsilon_0^2 = \zeta \cdot \epsilon^+$ *για* $\zeta \in \mu(K)$, *[6, Th. 42, σελ. 195].*

Αν τώρα K κυκλοτομικό σώμα, $K = \mathbb{Q}(\zeta_n)$, τότε αυτό είναι επίσης ένα CM-σώμα ως προς το μέγιστο πραγματικό υπόσωμα αυτού $K^+ = \mathbb{Q}(\zeta_n^+ + \zeta_n^{-1})$.

Πρόταση IX.2.28. *Έστω* $K = \mathbb{Q}(\zeta_n)$.

$$(\delta_K = 1) \Leftrightarrow (O\ n \text{ } \textit{είναι δύναμη πρώτου αριθμού.})$$

και φυσικά

$$(\delta_K = 2) \Leftrightarrow (O\ n \text{ } \textit{δεν είναι δύναμη πρώτου αριθμού.})$$

Απόδειξη. [25, Πορ. 4.13 σελ. 39]. □

Η γενική περίπτωση χαρακτηρισμού CM-σωμάτων με $d_K = 1$ ή $d_K = 2$ περιέχεται αναλυτικά στο [7, σελ. 46-78].

Έστω τώρα το $K/\mathbb{Q}$ πραγματική δικυκλική διτετραγωνική επέκταση. Το σώμα K περιέχει τρία πραγματικά τετραγωνικά υποσώματα, έστω K_1, K_2, K_3 και $\epsilon_1, \epsilon_2, \epsilon_3$ αντίστοιχα οι θεμελιώδεις μονάδες αυτών. Ο βαθμός (rank) του K είναι 3. Ένα σύστημα θεμελιωδών μονάδων του K, αποτελείται από μία από τις παρακάτω δυνατότητες:

1. $\epsilon_1, \epsilon_2, \epsilon_3$
2. $\sqrt{\epsilon_1}, \epsilon_2, \epsilon_3$ και αναγκαστικά $N_{K/\mathbb{Q}}(\epsilon_1) = +1$
3. $\sqrt{\epsilon_1}, \sqrt{\epsilon_2}, \epsilon_3$ και αναγκαστικά $N_{K/\mathbb{Q}}(\epsilon_1) = N_{K/\mathbb{Q}}(\epsilon_2) = 1$
4. $\sqrt{\epsilon_1\epsilon_2}, \epsilon_2, \epsilon_2$ και αναγκαστικά $N_{K/\mathbb{Q}}(\epsilon_1) = N_{K/\mathbb{Q}}(\epsilon_2) = N_{K/\mathbb{Q}}(\epsilon_3) = 1$
5. $\sqrt{\epsilon_1\epsilon_2}, \sqrt{\epsilon_3}, \epsilon_2$ και αναγκαστικά $N_{K/\mathbb{Q}}(\epsilon_1) = N_{K/\mathbb{Q}}(\epsilon_2) = N_{K/\mathbb{Q}}(\epsilon_3) = 1$
6. $\sqrt{\epsilon_1\epsilon_2}, \sqrt{\epsilon_2\epsilon_3}, \sqrt{\epsilon_3\epsilon_1}$ και αναγκαστικά $N_{K/\mathbb{Q}}(\epsilon_1) = N_{K/\mathbb{Q}}(\epsilon_2) = N_{K/\mathbb{Q}}(\epsilon_3) = 1$
7. $\sqrt{\epsilon_1\epsilon_2\epsilon_3}, \epsilon_2, \epsilon_3$ και αναγκαστικά $N_{K/\mathbb{Q}}(\epsilon_1) = N_{K/\mathbb{Q}}(\epsilon_2) = N_{K/\mathbb{Q}}(\epsilon_3) = 1$

[10]. Ο S. Kuroda δίνει και παραδείγματα για την κάθε δυνατότητα, για παράδειγμα για το σώμα $K = \mathbb{Q}(\sqrt{2}.\sqrt{3})$, οι θεμελιώδεις μονάδες των $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ και $\mathbb{Q}(\sqrt{6})$ είναι οι $\epsilon_1 = 1+\sqrt{2}$, $\epsilon_2 = 2+\sqrt{3}$ και $e_3 = 5+2\sqrt{6}$ και ένα πλήρες σύστημα θεμελιωδών μονάδων του K είναι $\epsilon_1, \sqrt{\epsilon_2}, \sqrt{\epsilon_3}$. Ότι υπάρχουν άπειρα σώματα για κάθε μία από τις επτά παραπάνω δυνατότητες αποδείχθηκε από τον T. Kubota, [9]. Εδώ ο δείκτης $[E(R_K) : \langle \epsilon_1, \epsilon_2, \epsilon_3 \rangle] \leq 8$.

Σχετικά με το θεώρημα του Dirichlet θα θέλαμε ακόμα να αναφέρουμε τα άρθρα: [3], [13], [23].

Για τον υπολογισμό ενός συστήματος θεμελιωδών μονάδων με χρήση προγραμμάτων και ηλεκτρονικού υπολογιστή παραπέμπουμε στα [19], [24].

Για παράδειγμα:

```
def NF(poly):
    K.<a>=NumberField(poly)
    OK=K.ring_of_integers()
    RK=OK.gens()
    D=K.discriminant()
    h=K.class_number()
    S=K.signature()
    G= K.unit_group (); G
    G.order()
    G.gens_values()
    print('Βάση ακεραιότητας του K=Q(a) οπου a πραγματικη ρίζα του',poly, 'είναι το', RK,',το K έχει διακρίνουσα D=',D,'
          και class number h=',h)
    print('Ταυτοτητα του K:',S,'.Ο γεννητορας ζ των ριζών της μονάδας και οι θεμελιώδεις μοναδες ε0,ε1 είναι [ζ,ε0,ε1]=',
          G.gens_values())
    return 0
```

```
NF(x^5-x-1)
```

```
Βάση ακεραιότητας του K=Q(a) οπου a πραγματικη ρίζα του x^5 - x - 1 είναι το (1, a, a^2, a^3, a^4) ,το K έχει διακρίνουσα D= 2
869 και class number h= 1
Ταυτοτητα του K: (1, 2) .Ο γεννητορας ζ των ριζών της μονάδας και οι θεμελιώδεις μοναδες ε0,ε1 είναι [ζ,ε0,ε1]= [-1, a^4 - 1, a^2
+ 1]

0
```

```
NF(x^3-2)
```

```
Βάση ακεραιότητας του K=Q(a) οπου a πραγματικη ρίζα του x^3 - 2 είναι το (1, a, a^2) ,το K έχει διακρίνουσα D= -108 και class n
umber h= 1
Ταυτοτητα του K: (1, 1) .Ο γεννητορας ζ των ριζών της μονάδας και οι θεμελιώδεις μοναδες ε0,ε1 είναι [ζ,ε0,ε1]= [-1, a - 1]

0
```

```
NF(x^2-3)
```

```
Βάση ακεραιότητας του K=Q(a) οπου a πραγματικη ρίζα του x^2 - 3 είναι το (1, a) ,το K έχει διακρίνουσα D= 12 και class number h
= 1
Ταυτοτητα του K: (2, 0) .Ο γεννητορας ζ των ριζών της μονάδας και οι θεμελιώδεις μοναδες ε0,ε1 είναι [ζ,ε0,ε1]= [-1, a - 2]
```

Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$ με ταυτότητα $[r_1, r_2]$ και έστω $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r\}$ ένα σύστημα θεμελιωδών μονάδων του K, $r = r_1 + r_2 - 1$.

Ορισμός IX.2.29. Ο ομαλοποιητής (regulator) του K είναι ο

$$\mathrm{Reg}_K := \left|\det(\log|\sigma_i(\varepsilon_j)|)_{i,j=1,2,\ldots,r}\right|.$$

Αποδεικνύεται ότι είναι ανεξάρτητος της επιλογής του συστήματος των θεμελιωδών μονάδων. Αν για παράδειγμα $K = \mathbb{Q}(\sqrt{D_{K/\mathbb{Q}}})$, τετραγωνικό πραγματικό και ε_0 η θεμελιώδης μονάδα του, τότε $\mathrm{Reg}_K = \log \varepsilon_0$. Ο κανονικοποιητής παίζει ρόλο για την ομάδα των μονάδων, αντίστοιχου αυτού που παίζει η διακρίνουσα για το R_K.

Το θεώρημα του Dirichlet είναι ιδιαίτερα χρήσιμο στην επίλυση διοφαντικών εξισώσεων με την p-αδική μέθοδο του Skolem καθώς και στον υπολογισμό του αριθμού κλάσεων h_K ενός αλγεβρικού σώματος αριθμών, αφού ο ομαλοποιητής συμμετέχει στον αναλυτικό τύπο του αριθμού κλάσεων.

IX.3 Ασκήσεις

1. Να αποδείξετε ότι δεν υπάρχει ανάγωγο μονικό πολυώνυμο $f(x) \in \mathbb{Z}[x]$, $\deg f(x) > 1$ το οποίο να έχει διακρίνουσα ίση με ± 1.
2. Έστω $m \in \mathbb{Z}$, $m \equiv 1 \mod 4$ και $d \in \mathbb{Z}$, $(m, d) = 1$. Υποθέτουμε ότι m, d είναι ελεύθεροι τετραγώνου. Έστω $\omega_m = \frac{1+\sqrt{m}}{2}$ και

$$\omega_d = \begin{cases} \sqrt{d}, & \text{αν } d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{αν } d \equiv 1 \mod 4 \end{cases}$$

   Να υπολογισθεί μια βάση ακεραιότητας του σώματος $M = \mathbb{Q}(\sqrt{m}, \sqrt{d})$ και η διακρίνουσα $D_{M/\mathbb{Q}}$.
3. Έστω $K = \mathbb{Q}(\sqrt{-5})$ και $L = K(\sqrt{5})$. Να αποδείξετε ότι δεν υπάρχει πρώτο ιδεώδες του K το οποίο να διακλαδίζεται στην επέκταση L/K. (Στην πραγματικότητα το L είναι το σώμα Hilbert του K).
4. Να αποδειχθεί ότι το $S(t)$ της εξίσωσης (IX.1) είναι κυρτό.
5. (α′) Αν K τετραγωνικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{m})$ και $\alpha \in R_K$ να αποδειχθεί ότι

$$N_{K/\mathbb{Q}}(\alpha) \equiv z^2 \mod m$$

   για κάποιο $z \in \mathbb{Z}$.

   (β′) Αν K πραγματικό τετραγωνικό σώμα διακρίνουσας $D_{K/\mathbb{Q}}$ και ε_0 η θεμελιώδης μονάδα αυτού να αποδειχθεί ότι $N_{K/\mathbb{Q}}(\varepsilon_0) = 1$.
6. (α′) Να αποδειχθεί ότι για κάθε φυσικό αριθμό n ισχύει $\varphi(n) \geq \sqrt{n/2}$.

   (β′) Αν $n \in \mathbb{N}$ και $\varphi(k) \leq n$, τότε $k \leq 2n^2$.

   (γ′) $\varphi(\kappa) = 1 \Leftrightarrow k = 1, 2$
7. (α′) Να αποδειχθεί ότι

$$\varphi(k) = 2 \Leftrightarrow k = 3, 4, 6.$$

   (β′) Να αποδειχθεί

$$\varphi(k) = 4 \Leftrightarrow k = 5, 8, 10, 12.$$

   (γ′) Αν $n \geq 3$, τότε $\varphi(n)$ είναι άρτιος.
8. Έστω K αλγεβρικό σώμα αριθμών με $[K : \mathbb{Q}] = n$ και n περιττός. Να αποδειχθεί ότι

$$E(R_K) = \{\pm 1\}.$$

9. Αν $[K : \mathbb{Q}] = 4$, ποιες είναι οι δυνατές ρίζες της μονάδας που ανήκουν στον K; Μπορείτε να χαρακτηρίσετε τα σώματα στα οποία ανήκουν;
10. Έστω $K = \mathbb{Q}(\alpha)$, $\alpha = \sqrt[3]{2}$. Να υπολογισθεί η διακρίνουσα του σώματος και μία βάση ακεραιότητας αυτού. Να αποδειχθεί ότι το στοιχείο

$$\varepsilon = 4 + 3\alpha + 2\alpha^2$$

    είναι μονάδα του K και μάλιστα η θεμελιώδης μονάδα αυτού.
11. Έστω $K = \mathbb{Q}(\alpha)$, α η πραγματική ρίζα του πολυωνύμου

$$x^3 + 10x + 1.$$

    Να υπολογισθεί η διακρίνουσα και μια βάση ακεραιότητας αυτού. Να υπολογισθεί η θεμελιώδης μονάδα ε_0 του K.
12. Να αποδειχθεί ότι η θεμελιώδης μονάδα του σώματος $K = \mathbb{Q}(\sqrt[3]{7})$ είναι η

$$\varepsilon_0 = 4 + 3\sqrt[3]{3} + 2(\sqrt[3]{[3]})^2$$

Βιβλιογραφία

[1] Alaca, Ş. & Williams, K. S. *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, 2004, pp. xviii+428. ISBN: 0-521; 0-521-54011-9.

[2] Artin, E. *Theory of Algebraic Numbers*. Vol. 1956/7. Notes by Gerhard Würges from lectures held at the Mathematisches Institut, Göttingen, Germany, in the Winter Semester. George Striker, Schildweg 12, Göttingen, 1959, p. 172.

[3] Berwick, W. E. H. *Algebraic Number-Fields with two Independent Units*. *Proc. London Math. Soc. (2)* 34.5 (1932), pp. 360–378. ISSN: 0024-6115. URL: https://doi.org/10.1112/plms/s2-34.1.360.

[4] Cassels, J. W. S. *An Introduction to the Geometry of Numbers*. Classics in Mathematics. Corrected reprint of the 1971 edition. Springer-Verlag, Berlin, 1997, pp. viii+344. ISBN: 3-540-61788-4.

[5] Conrad, K. *Dirichlet's Unit Theorem*. URL: https://home.mathematik.uni-freiburg.de/arithgeom/lehre/ss20/algzt/Keith%20Conrad%20-%20Unit%20theorem.pdf.

[6] Fröhlich, A. & Taylor, J. M. *Algebraic number theory*. Vol. 27. Cambridge Studies in advanced mathematics. Cambridge: Cambridge University Press, 1993, pp. xiv+355. ISBN: 0-521-43834-9.

[7] Hasse, H. *Über die Klassenzahl abelscher Zahlkörper*. Reprint of the 1952 edition, With an introduction to the reprint edition by Jacques Martinet. Akademie-Verlag, Berlin, 1985, pp. 12+xii+190. URL: https://doi.org/10.1007/978-3-642-69886-6.

[8] Janusz, G. J. *Algebraic number fields*. Second. Vol. 7. Graduate Studies in Mathematics. Providence, RI: American Mathematical Society, 1996, pp. x+276. ISBN: 0-8218-0429-4.

[9] Kubota, T. *Über den bizyklischen biquadratischen Zahlkörper*. *Nagoya Math. J.* 10 (1956), pp. 65–85. ISSN: 0027-7630. URL: http://projecteuclid.org/euclid.nmj/1118799770.

[10] Kuroda, S. *Über den Dirichletschen Körper*. *J. Fac. Sci. Imp. Univ. Tokyo Sect. I.* 4 (1943), pp. 383–406.

[11] Lang, S. *Algebraic Number Theory*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970, pp. xi+354.

[12] Leutbecher, A. *Zahlentheorie: Eine Einführung in die Algebra*. Springer-Lehrbuch. Springer, Berlin, 2013. ISBN: 9783642614057. URL: https://books.google.gr/books?id=PG2nBgAAQBAJ.

[13] Mäki, S. *The determination of units in real cyclic sextic fields*. Vol. 797. Lecture Notes in Mathematics. Springer, Berlin, 1980, pp. i+198. ISBN: 3-540-09984-0.

[14] Marcus, D. A. *Algebraic Number Fields*. Universitext. 2nd edition of [MR0457396], With a foreword by Barry Mazur. Springer, 2018, pp. xviii+203. ISBN: 978-3-319-90232-6; 978-3-319-90233-3.

[15] Milne, J. S. *Algebraic Number Theory (v3.08)*. Available at www.jmilne.org/math/. 2020.

[16] Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*. 3rd edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004, pp. xii+708. ISBN: 3-540-21902-1.

[17] Neukirch, J. *Algebraic Number Theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Berlin: Springer-Verlag, 1999, pp. xviii+571. ISBN: 3-540-65399-6.

[18] Neukirch, J. *Algebraische Zahlentheorie*. German. Springer-Verlag Berlin, 1992.

[19] Pohst, M. & Zassenhaus, H. *Algorithmic Algebraic Number Theory*. Vol. 30. Encyclopedia of Mathematics and its Applications. Revised reprint of the 1989 original. Cambridge University Press, Cambridge, 1997, pp. xiv+499. ISBN: 0-521-59669-6.

[20] Pollack, P. *A Conversational Introduction to Algebraic Number Theory, Arithmetic beyond* $\mathbb{Z}$. Vol. 84. Student Mathematical Library. American Mathematical Society, Providence, RI, 2017, pp. ix + 316. ISBN: 978-1-4704-3653-7.

[21] Ribenboim, P. *Classical Theory of Algebraic Numbers*. Universitext. Springer-Verlag, New York, 2001, pp. xxiv+681. ISBN: 0-387-95070-2.

[22] Samuel, P. *Algebraic Theory of Numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970, p. 109.

[23] Shen, Y. Y. *Unit groups and class numbers of real cyclic octic fields*. *Trans. Amer. Math. Soc.* 326.1 (1991), pp. 179–209. ISSN: 0002-9947. URL: https://doi.org/10.2307/2001860.

[24] Stein, W. *Algebraic Number Theory, a computational approach*. *Harvard. Massachusetts* (2012). URL: https://wstein.org/books/ant/ant.pdf.

[25] Washington, L. C. *Introduction to Cyclotomic Fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, pp. xiv+487. ISBN: 0-387-94762-0. URL: https://doi.org/10.1007/978-1-4612-1934-7.

[26] Αντωνιάδης, Ι. Α. & Κοντογεώργης, Α. *Θεωρία Αριθμών και Εφαρμογές*. Κάλλιπος, 2015, pp. ix+315. ISBN: 978-618-82124-5-9. URL: https://eclass.uoa.gr/modules/document/file.php/MATH443/NumberTheoryNov2016.pdf.

X

Διακρίνουσα, Διαφορίζουσα και το Θεώρημα των Kronecker-Weber

X.1 Εισαγωγή

Στο κεφάλαιο αυτό θα μελετήσουμε τρία ακόμα σημαντικά θεωρήματα, το θεώρημα της διακρίνουσας, το θεώρημα της διαφορίζουσας και το θεώρημα των Kronecker-Weber.

Έστω L/K μια επέκταση αλγεβρικών σωμάτων αριθμών. Η διακρίνουσα χαρακτηρίζει τα πρώτα ιδεώδη P του K τα οποία διακλαδίζονται στο L. Η διαφορίζουσα χαρακτηρίζει τα πρώτα ιδεώδη Q του L τα οποία διακλαδίζονται στην επέκταση L/K ως προς πρώτο ιδεώδες $P := Q \cap K$. Επίσης απαντά εν μέρει και στο ποιος είναι ο δείκτης διακλάδωσης $e(Q/P)$.

Το θεώρημα των Kronecker-Weber το έχουμε ήδη αναφέρει, VIII.5.1.

X.2 Διακρίνουσα

X.2.1 Βοηθητικές προτάσεις

Έστω L/K μία επέκταση αλγεβρικών σωμάτων αριθμών, R και S οι αντίστοιχοι δακτύλιοι των ακεραίων αλγεβρικών αριθμών. Η διακρίνουσα θα πρέπει να γενικεύει την έννοια της διακρίνουσας στην (απόλυτη) περίπτωση που το σώμα K ταυτίζεται με το σώμα των ρητών αριθμών $\mathbb{Q}$. Στην απόλυτη περίπτωση, ορίσαμε ως διακρίνουσα του αλγεβρικού σώματος αριθμών την τιμή της διακρίνουσας μιας βάσης ακεραιότητας αυτού. Αυτό ήταν δυνατό, επειδή ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του $\mathbb{Q}$ είναι το $\mathbb{Z}$, το οποίο είναι περιοχή κυρίων ιδεωδών. Το S όμως δεν είναι, εν γένει, ελεύθερο R-module. Στις σχετικές επεκτάσεις L/K έχουμε ήδη ορίσει τη σχετική διακρίνουσα μιας n-άδας στοιχείων του L όχι όμως και τη (σχετική) διακρίνουσα της επέκτασης L/K.

Έστω λοιπόν L/K επέκταση αλγεβρικών σωμάτων αριθμών, R και S οι αντίστοιχοι δακτύλιοι ακεραίων αλγεβρικών αριθμών και $\theta \in S$ για το οποίο ισχύει $L = K(\theta)$. Αν P πρώτο ιδεώδες του R, έχουμε ήδη αποδείξει ότι:

$$\text{Αν } p \nmid D_{L/K}(\theta) \text{ τότε το } P \text{ δεν διακλαδίζεται στο } L.$$

Ο τελικός σκοπός της παραγράφου είναι ο χαρακτηρισμός των πρώτων ιδεωδών του R που διακλαδίζονται στο L. Στην ειδική περίπτωση που $K = \mathbb{Q}$ και $[L : \mathbb{Q}] = 2$ έχουμε ήδη διαπιστώσει ότι

$$\big(\text{Το πρώτο ιδεώδες } p\mathbb{Z},\, p \in \mathbb{P} \text{ διακλαδίζεται στο σώμα } L\big) \Leftrightarrow \left(\frac{D_{L/\mathbb{Q}}}{p}\right) = 0 \Leftrightarrow p \mid D_{L/\mathbb{Q}}.$$

Ο κατάλληλος ορισμός τώρα είναι

Ορισμός Χ.2.1. Η σχετική διακρίνουσα της επέκτασης L/K ορίζεται ως το ιδεώδες του R, το οποίο παράγεται από όλες τις διακρίνουσες όλων των n-άδων στοιχείων του S. Θα το συμβολίζουμε

$$\mathcal{D}_{L/K} := \langle D_{L/K}(\omega_1, \omega_2, \dots, \omega_n) : \omega_1, \omega_2, \dots, \omega_n \in S \rangle_R.$$

Παραδείγματα Χ.2.2.

1. Υποθέτουμε ότι το S είναι ελεύθερο R-module και $\{\theta_1, \theta_2, \dots, \theta_n\}$ μια R-βάση αυτού:
$$S = R\theta_1 \oplus R\theta_2 \oplus \cdots \oplus R\theta_n,$$
δηλαδή υπάρχει μια βάση ακεραιότητας του S. Τότε για κάθε n-άδα στοιχείων του S, έστω $\omega_1, \omega_2, \dots, \omega_n$ ισχύει:
$$D_{L/K}(\omega_1, \omega_2, \dots, \omega_n) = (\det A)^2 D_{L/K}(\theta_1, \theta_2, \dots, \theta_n).$$
Το A είναι ο πίνακας μετασχηματισμού και $\det A \in R$. Επομένως,
$$\mathcal{D}_{L/K} = R \cdot D_{L/K}(\theta_1, \theta_2, \dots, \theta_n) = \langle D_{L/K}(\theta_1, \theta_2, \dots, \theta_n) \rangle,$$
είναι το ιδεώδες του R το οποίο παράγεται από τη (σχετική) διακρίνουσα $D_{L/K}(\theta_1, \theta_2, \dots, \theta_n)$.
2. Στην ειδική περίπτωση που $K = \mathbb{Q}$, υπάρχει πάντοτε βάση ακεραιότητας και συνεπώς έχουμε
$$\mathcal{D}_{L/\mathbb{Q}} = \mathbb{Z} D_{L/\mathbb{Q}} = \langle D_{L/\mathbb{Q}} \rangle.$$
3. Έστω ότι ο S είναι μονογενικός ως προς τον R, δηλαδή υπάρχει $\theta \in S : S = R[\theta]$ με βάση ακεραιότητας $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$, κάτι που βέβαια δεν είναι σωστό ούτε για τις απόλυτες επεκτάσεις όπως είδαμε με το αντιπαράδειγμα του Dedekind. Τότε
$$\mathcal{D}_{L/K} = R \cdot D_{L/K}(\theta).$$

Παρατήρηση Χ.2.3. Αν στο πρώτο παράδειγμα ήταν και το σύνολο $\{\omega_1, \omega_2, \dots, \omega_n\}$ βάση ακεραιότητας θα είχαμε ότι $\det A \in E(R)$ με $\det A^2 = 1$ η οποία όμως μονάδα θα μπορούσε να είναι $\neq 1$.

Θεώρημα Χ.2.4 (Θεώρημα της Διακρίνουσας)**.** *Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών με R, S οι αντίστοιχοι δακτύλιοι των ακέραιων αριθμών και P ένα πρώτο ιδεώδες του R. Ισχύει η ισοδυναμία*
$$\big(\textit{Το } P \textit{ διακλαδίζεται στο } L\big) \Leftrightarrow \big(P \mid \mathcal{D}_{L/K}\big)$$

Παραδείγματα Χ.2.5.

1. Έστω $[L : \mathbb{Q}] = 2$ και $P = p\mathbb{Z}$ ιδεώδες του K
$$\big(\text{Το } P \text{ διακλαδίζεται στο σώμα } L\big) \Leftrightarrow \left(\frac{D_{L/\mathbb{Q}}}{p}\right) = 0 \Leftrightarrow p\mathbb{Z} \mid \mathcal{D}_{L/\mathbb{Q}}.$$
2. Αν $S = R[\theta]$, τότε $\mathcal{D}_{L/K} = R \cdot D_{L/K}(\theta)$ και έχουμε ήδη αποδείξει ότι
$$\big(P \nmid D_{L/K}(\theta)\big) \Rightarrow P \text{ δεν διακλαδίζεται στο } L.$$
Σημειώνουμε ότι σε αυτή την ειδική περίπτωση που ο οδηγός της επέκτασης
$$\mathfrak{F} = \mathfrak{F}_{S/R[\theta]} = S$$
είναι τετριμμένος η απόδειξη του αντιστρόφου είναι πολύ εύκολη, αλλά δεν θα την κάνουμε εδώ μιας και θα αποδείξουμε το θεώρημα στην πλήρη γενικότητά του. Η απόδειξη της ειδικής αυτής περίπτωσης θα τεθεί ως άσκηση.

Θα ακολουθήσει μια σειρά λημμάτων.

Παρατήρηση X.2.6. Ο δακτύλιος πηλίκο S/PS γίνεται ένας R/P-διανυσματικός χώρος με πολλαπλασιασμό

$$\begin{aligned} R/P \times S/PS &\longrightarrow S/PS \\ (r+P, s+PS) &\longmapsto (r+P)(s+PS) = rs+PS \end{aligned}$$

Λήμμα X.2.7.

$$\dim_{R/P} S/PS = n = [L:K]$$

Απόδειξη. Έστω $PS = Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$ η μονοσήμαντη ανάλυση του PS σε γινόμενο πρώτων ιδεωδών του L. Αρκεί να δείξουμε ότι

$$\#S/PS = (\#R/P)^n.$$

Πράγματι,

$$\begin{aligned} \#S/PS &= N_{L/K}(Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}) \\ &= N_{L/K}(Q_1)^{e_1}N_{L/K}(Q_2)^{e_2}\cdots N_{L/K}(Q_r)^{e_r} \\ &= N_{K/\mathbb{Q}}(P)^{e_1f_1}\cdots N_{K/\mathbb{Q}}(P)^{e_rf_r} \\ &= (\#R/P)^{\sum_{i=1}^r e_if_i} = (\#R/P)^n. \end{aligned}$$

□

Λήμμα X.2.8. *Αν* $a, b \in S$ *και* $a \equiv b \mod PS$, *τότε*

$$\mathrm{Tr}_{L/K}(a) \equiv \mathrm{Tr}_{L/K}(b) \mod P$$

Το παραπάνω λήμμα είναι άμεση συνέπεια του επόμενου λήμματος:

Λήμμα X.2.9. *Έστω* $PS = Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$. *Αν* $\theta \in \cap_{i=1}^r Q_i$ *τότε* $\mathrm{Tr}_{L/K}(\theta) \in P$.

Παρατήρηση X.2.10. Από το λήμμα X.2.9 έπεται το X.2.8. Έστω $a \in PS$ δηλαδή $a \equiv 0 \mod PS$. Επειδή $PS \subset \cap_{i=1}^r Q_i$ έπεται ότι $\mathrm{Tr}_{L/K}(a) \in P$. Επομένως, αν $a \equiv b \mod PS$, τότε $a-b \in P$ και $\mathrm{Tr}_{L/K}(a-b) \in P$ οπότε $\mathrm{Tr}_{L/K}(a) - \mathrm{Tr}_{L/K}(b) \in P$ δηλαδή

$$\mathrm{Tr}_{L/K}(a) \equiv \mathrm{Tr}_{L/K}(b) \mod P.$$

Απόδειξη. (Του λήμματος X.2.9) Έστω $\widetilde{K}$ η κανονική θήκη της επέκτασης L/K. Υπενθυμίζουμε ότι αυτή είναι η ελάχιστη επέκταση Galois του K που περιέχει το L. Έστω $\sigma_1, \sigma_2, \ldots, \sigma_n$ οι K-μονομορφισμοί του L στο $\widetilde{K}$ και $\widehat{\sigma}_1, \widehat{\sigma}_2, \ldots, \widehat{\sigma}_n$ επεκτάσεις των $\sigma_1, \sigma_2, \ldots, \sigma_n$ στο $\widetilde{K}$. Αυτοί είναι K-αυτομορφισμοί του σώματος $\widetilde{K}$. Επομένως

$$\mathrm{Tr}_{L/K}(\theta) = \sigma_1(\theta) + \sigma_2(\theta) + \cdots + \sigma_n(\theta) = \widehat{\sigma}_1(\theta) + \widehat{\sigma}_2(\theta) + \cdots + \widehat{\sigma}_n(\theta).$$

Έστω τώρα U πρώτο ιδεώδες του $\widetilde{K}$, $U \mid P$. Ισχυριζόμαστε ότι

$$\widehat{\sigma}_i(\theta) \in U \text{ για κάθε } i = 1, 2, \ldots, n. \tag{X.1}$$

Αν δεχτούμε την (X.1), έχουμε τελειώσει αφού

$$\mathrm{Tr}_{L/K}(\theta) \in U \cap K = P.$$

Θα αποδείξουμε τώρα την (Χ.1). Τα $\widehat{\sigma}_i^{-1}(U)$ είναι πρώτα ιδεώδη του $\widetilde{K}$. Επομένως τα

$$\widehat{\sigma}_i^{-1}(U) \cap L$$

είναι πρώτα ιδεώδη του S που περιέχουν το P. Συνεπώς υπάρχει για κάθε i ένα $j \in \{1, 2, \dots, n\}$ ώστε

$$\widehat{\sigma}_i^{-1}(U) \cap L = Q_j.$$

Το $\theta \in \cap_{j=1}^{r} Q_j$ συνεπώς $\theta \in Q_j$ άρα $\theta \in \widehat{\sigma}_i^{-1}(U) \cap L$, αφού $\theta \in L$. Καταλήγουμε ότι $\theta \in \widehat{\sigma}_i^{-1}(U)$ και τελικά $\widehat{\sigma}_i(\theta) \in U$, για κάθε $i = 1, 2, \dots, n$. □

Λήμμα Χ.2.11. *Υποθέτουμε ότι τα* $\omega_1, \omega_2, \dots, \omega_n$ *και* $\omega_1', \omega_2', \dots, \omega_n' \in S$ *και επιπλέον ισχύει*

$$\omega_i \equiv \omega_i' \mod PS.$$

Τότε ισχύει ότι

$$D_{L/K}(\omega_1, \omega_2, \dots, \omega_n) \equiv D_{L/K}(\omega_1', \omega_2', \dots, \omega_n') \mod P.$$

Απόδειξη. Λόγω της υπόθεσης έχουμε

$$\omega_i\omega_j \equiv \omega_i'\omega_j' \mod PS \text{ για κάθε } i, j \in \{1, 2, \dots, n\}.$$

Από το λήμμα Χ.2.8 συνεπάγεται ότι

$$\mathrm{Tr}_{L/K}(\omega_i\omega_j) \equiv \mathrm{Tr}_{L/K}(\omega_i'\omega_j') \mod P$$

συνεπώς

$$\det(\mathrm{Tr}_{L/K}(\omega_i\omega_j)) = D_{L/K}(\omega_1, \omega_2, \dots, \omega_n) \equiv \det(\mathrm{Tr}_{L/K}(\omega_i'\omega_j')) = D_{L/K}(\omega_1', \omega_2', \dots, \omega_n') \mod P$$

□

Λήμμα Χ.2.12. *Έστω* $\omega_1, \omega_2, \dots, \omega_n \in S$ *για τα οποία τα* $\overline{\omega}_i = \omega_i + PS$, $i = 1, 2, \dots, n$ *είναι βάση του* R/P*-διανυσματικού χώρου* S/PS. *Αν*

$$D_{L/K}(\omega_1, \omega_2, \dots, \omega_n) \equiv 0 \mod P \text{ τότε } P \mid \mathcal{D}_{L/K}.$$

Απόδειξη. Αρκεί να δείξουμε ότι η υπόθεση συνεπάγεται ότι για κάθε n-άδα $\theta_1, \theta_2, \dots, \theta_n \in S$ ισχύει $D_{L/K}(\theta_1, \theta_2, \dots, \theta_n) \equiv 0 \mod P$. Τα $\{\overline{\omega}_i : i = 1, 2, \dots, n\}$ είναι βάση του R/P-διανυσματικού χώρου S/PS. Επομένως

$$(\overline{\theta}_1, \overline{\theta}_2, \dots, \overline{\theta}_n))^T = \overline{A}(\overline{\omega}_1, \overline{\omega}_2, \dots, \overline{\omega}_n)^T \text{ με } \overline{A} = (\overline{\alpha}_{ij}) \in M_n(R/P).$$

Συνεπώς υπάρχει $A = (\alpha_{ij}) \in M_n(R)$ ώστε

$$(\theta_1, \theta_2, \dots, \theta_n)^T \equiv A(\omega_1, \omega_2, \dots, \omega_n)^T \mod PS.$$

Από το λήμμα Χ.2.11 προκύπτει ότι

$$D_{L/K}(\theta_1, \theta_2, \dots, \theta_n) \equiv D_{L/K}\big((\omega_1, \omega_2, \dots, \omega_n)A^T\big) \mod P.$$

Τέλος,

$$D_{L/K}\big((\omega_1, \omega_2, \dots, \omega_n)A^T\big) = (\det A)^2 \cdot D_{L/K}(\omega_1, \omega_2, \dots, \omega_m).$$

Η $\det A \in R$ και $D_{L/K}(\omega_1, \omega_2, \dots, \omega_n) \equiv 0 \mod P$, δηλαδή για κάθε $\theta_1, \theta_2, \dots, \theta_n \in S$ ισχύει

$$D_{L/K}(\theta_1, \theta_2, \dots, \theta_n) \equiv 0 \mod P.$$

Επομένως $P \mid \mathcal{D}_{L/K}$. □

Λήμμα Χ.2.13. *Έστω* $PS = Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$, $\omega_1, \omega_2, \ldots, \omega_n \in S$ *και* $\omega_1 \in \cap_{i=1}^{r} Q_i$. *Ισχύει*

$$D_{L/K}(\omega_1, \omega_2, \ldots, \omega_n) \equiv 0 \mod P.$$

Απόδειξη. Το $\omega_1 \in \cap_{i=1}^{r} Q_i$ συνεπώς για κάθε $j \in \{1, 2, \ldots, r\}$ έχουμε $\omega_1\omega_j \in \cap_{i=1}^{r} Q_i$. Από το λήμμα Χ.2.9 έχουμε ότι $\mathrm{Tr}_{L/K}(\omega_1\omega_j) \in P$. Επομένως

$$D_{L/K}(\omega_1, \omega_2, \ldots, \omega_n) = \det(\mathrm{Tr}_{L/K}(\omega_i\omega_j)) \in P,$$

εξ ορισμού της ορίζουσας και επειδή η πρώτη γραμμή ή στήλη αποτελείται από στοιχεία που ανήκουν στο P. □

Χ.2.2 Τα πρώτα ιδεώδη του K που διακλαδίζονται στο L διαιρούν τη διακρίνουσα

Λόγω των λημμάτων Χ.2.12 και Χ.2.13 αρκεί να δείξουμε ότι υπάρχει μία βάση του R/P-διανυσματικού χώρου S/PS $\overline{\omega}_1, \overline{\omega}_2, \ldots, \overline{\omega}_n$, για την οποία ισχύει

$$\omega_1 \in \cap_{i=1}^{r} Q_i.$$

Τα $PS = Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$. Υποθέτουμε ότι το P διακλαδίζεται στο L. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $e_1 \geq 2$. Επομένως

$$\frac{S}{PS} \supset \frac{Q_1^{e_1-1}Q_2^{e_2}\cdots Q_r^{e_r}}{PS} \supsetneq \langle\overline{0}\rangle$$

Ισχύριζόμαστε ότι το $\frac{Q_1^{e_1-1}Q_2^{e_2}\cdots Q_r^{e_r}}{PS}$ είναι R/P-διανυσματικός υπόχωρος του S/PS.

Αν το δεχθούμε προς το παρόν έχουμε τελειώσει. Πράγματι, θεωρούμε μια βάση $\overline{\omega}_1, \overline{\omega}_2, \ldots, \overline{\omega}_t$ του διανυσματικού υποχώρου και την επεκτείνουμε σε μία βάση

$$\overline{\omega}_1, \overline{\omega}_2, \ldots, \overline{\omega}_t, \overline{\omega}_{t+1}, \ldots, \overline{\omega}_n \text{ του } S/PS$$

Το $e_1 - 1 > 0$, άρα $\omega_1 \in Q_1^{e_1-1}Q_2^{e_2}\cdots Q_r^{e_r} \subset \cap_{i=1}^{r} Q_i$. Από το λήμμα Χ.2.12 προκύπτει ότι

$$D_{L/K}(\omega_1, \omega_2, \ldots, \omega_n) \equiv 0 \mod P$$

και από το λήμμα Χ.2.13 έπεται ότι $P \mid \mathcal{D}_{L/K}$.

Θα αποδείξουμε τώρα τον ισχυρισμό ότι

$$\frac{Q_1^{e_1-1}Q_2 \cdot Q_r^{e_r}}{PS}$$

είναι R/P-διανυσματικός χώρος. Πράγματι, είναι αβελιανή προσθετική ομάδα αφού αν $\alpha + PS, \beta + PS$ ανήκουν στο ιδεώδες πηλίκο τότε και η διαφορά τους

$$(\alpha + PS) - (\beta + PS)$$

επίσης ανήκει στο ιδεώδες $Q_1^{e_1-1}Q_2^{e_2}\cdots Q_r^{e_r}$. Αρκεί ακόμη να δείξουμε ότι

$$R/P \cdot \frac{Q_1^{e_1-1}Q_2 \cdot Q_r^{e_r}}{PS} \subset \frac{Q_1^{e_1-1}Q_2 \cdot Q_r^{e_r}}{PS}.$$

Αυτό όμως είναι προφανές διότι ο «αριθμητής» είναι ιδεώδες του S και $R \subset S$.

Χ.2.3 Βοηθητικές προτάσεις για την απόδειξη του αντιστρόφου

θα αποδείξουμε μια σειρά από προτάσεις για την απόδειξη του ότι

$$\left(\text{Αν } P \text{ πρώτο ιδεώδες του } K \text{ και το } P \text{ δεν διακλαδίζεται στο } L \text{ τότε } \left(P \nmid \mathcal{D}_{L/K}\right)\right.$$

Εδώ θα χρειαστούμε μια διαδικασία που λέγεται τοπικοποίηση (localization) ενός δακτυλίου.

Ορισμός Χ.2.14. Έστω R αντιμεταθετικός δακτύλιος με μοναδιαίο $1 \in R$. Ο R θα λέγεται *τοπικός* δακτύλιος (local ring) ακριβώς τότε όταν έχει ακριβώς ένα μέγιστο ιδεώδες.

Παρατήρηση Χ.2.15. Αν ο R είναι τοπικός δακτύλιος, τότε το μοναδικό μέγιστο ιδεώδες αυτού είναι το

$$P = R \backslash E(R).$$

Αν πάλι R αντιμεταθετικός δακτύλιος με μοναδιαίο και $R\backslash E(R)$ είναι ιδεώδες του R, τότε ο R είναι τοπικός δακτύλιος (άσκηση).

Έστω τώρα R ακέραια περιοχή και $P \neq R$ ένα πρώτο ιδεώδες αυτής, το υποσύνολο

$$R_P = \left\{ \frac{a}{b} : a \in R, b \in R \backslash P \right\}$$

του σώματος πηλίκων $K = \mathrm{Quot}(R)$ είναι τοπικός δακτύλιος. Το μοναδικό μέγιστο ιδεώδες αυτού είναι το $R_P \cdot P$.
Προσοχή: Από εδώ και κάτω K αλγεβρικό σώμα αριθμών και R ο δακτύλιος των ακεραίων και P ένα πρώτο ιδεώδες του R.

Λήμμα Χ.2.16. *Έστω $\pi \in P \backslash P^2$, δηλαδή το π είναι πρώτο στοιχείο για το ιδεώδες P. Ισχύουν τα ακόλουθα:*

1. $\langle \pi \rangle = R\pi = P \cdot \Delta$, *$\Delta$ ακέραιο ιδεώδες του R* , $P \nmid \Delta$.
2. *Αν $a \in K^*$, τότε υπάρχει ακριβώς ένα $\nu \in \mathbb{Z}$ και $\alpha, \beta \in R \backslash P$ ώστε* $a = \pi^\nu \frac{\alpha}{\beta}$.
3. $R_P = \left\{ a = \pi^\nu \frac{\alpha}{\beta} : \alpha, \beta \in R \backslash P, \nu \geq 0 \right\} \cup \{0\}$.
4. $R_P P = \{ a = \pi^\nu \frac{\alpha}{\beta} : \alpha, \beta \in R \backslash P, \nu \geq 1 \} \cup \{0\} = R_P \pi$.

Απόδειξη. 1. Το $\pi \in P$ συνεπώς $P \mid \langle \pi \rangle$. Επομένως $\langle p \rangle = P^m \Delta$, με $P \nmid \Delta$. $\pi \notin P^2$ συνεπώς $P^2 \nmid \langle \pi \rangle$. Άρα $m = 1$.

2. Θα αποδείξουμε πρώτα την ύπαρξη. Το κύριο ιδεώδες του a γράφεται

$$\langle a \rangle = P^\nu \frac{A}{B},$$

όπου $\nu \in \mathbb{Z}$ και $P \nmid A, B$. Επομένως

$$\langle a/\pi^\nu \rangle = \frac{A}{\Delta^\nu B} = \frac{A^{h_K}}{\Delta^\nu B A^{h_K - 1}},$$

όπου h_K είναι ο αριθμός κλάσεων ιδεωδών του K. Αλλά A^{h_K} είναι κύριο ιδεώδες, έστω $A^{h_K} = \langle \alpha \rangle$ οπότε και το $\Delta^\nu B A^{h_K - 1}$ είναι κύριο ιδεώδες που παράγεται από το β, έστω ίσο με $\langle \beta \rangle$. Το

$$\left\langle \frac{a}{\pi^\nu} \right\rangle = \frac{\langle \alpha \rangle}{\langle \beta \rangle} \Rightarrow a = \pi^\nu \frac{\epsilon \alpha}{\beta},$$

$\epsilon \in E(R)$. Το $\epsilon\alpha \in R\backslash P$, αφού $\langle \epsilon\alpha \rangle = A^{h_K}$ και $P \nmid A$. Επίσης, $\beta \in R\backslash P$, αφού $\langle \beta \rangle = \Delta^{\nu} B A^{h_K - 1}$ και $P \nmid \Delta^{\nu} B A^{h_K - 1}$.

Θα δείξουμε τώρα τη μοναδικότητα. Αρκεί να δείξουμε ότι αν $\pi^{\nu} \frac{\alpha}{\beta} = 1$, $\alpha, \beta \in R\backslash P$, τότε $\nu = 0$. Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι $\nu \geq 0$. Αν λοιπόν $\pi^{\nu} \frac{\alpha}{\beta} = 1$ τότε $\pi^{\nu}\alpha = \beta \in R\backslash P$ και $\pi^{\nu} \notin P$ δηλαδή έχουμε $\pi \in P$ και $\pi^{\nu} \notin P$ συνεπώς $\nu = 0$.

3. Το $R_P = \left\{ \frac{\gamma}{\delta} : \gamma \in R, \delta \in R\backslash P \right\}$ επομένως η σχέση του περιέχεσθαι «$\supset$» είναι προφανής.
Έστω τώρα $a \in R_P$ συνεπώς $a = \frac{\alpha}{\beta}$, $\alpha \in R$ και $\beta \in R\backslash P$. Άρα το a γράφεται

$$a = \pi^{\nu} \frac{\alpha'}{\beta'}, \alpha', \beta' \in R\backslash P.$$

Αρκεί να δείξουμε ότι $\nu \geq 0$. Το $\frac{\alpha}{\beta} = \pi^{\nu} \frac{\alpha'}{\beta'}$ συνεπώς $\pi^{\nu}\alpha'\beta = \alpha\beta'$. Αν ήταν $\nu < 0$, τότε $\pi^{-\nu}\alpha\beta' = \alpha'\beta \in R\backslash P$ ενώ $\pi^{-\nu}\alpha\beta' \in P$, αφού $-\nu \geq 0$, άτοπο.

4. $R_P P = \left\{ \frac{\alpha}{\beta} : \alpha \in P, \beta \in R\backslash P \right\}$ (άσκηση). Επομένως

$$R_P P = \left\{ \pi^{\nu} \frac{\alpha}{\beta} : \alpha, \beta \in R\backslash P, \nu \geq 1 \right\} \cup \{0\} = R_P \pi.$$

□

Επανερχόμαστε στις αρχικές μας υποθέσεις. L/K είναι επέκταση αλγεβρικών σωμάτων αριθμών, R και S οι αντίστοιχοι δακτύλιοι των ακέραιων αλγεβρικών αριθμών και P ένα πρώτο ιδεώδες του R.

Λήμμα X.2.17. *Έστω $\omega_1, \omega_2, \ldots, \omega_n \in S$, $\nu := (\omega_1, \omega_2, \ldots, \omega_n)^T$ ώστε το $\overline{\omega}_i = \omega_i + PS$, $i = 1, 2, \ldots, n$ να αποτελούν μια βάση του R/P-διανυσματικού χώρου S/PS και $A \in M_n(K)$. Αν*

$$A\nu \in \times_{i=1}^{n} = PS \times PS \times \cdots \times PS, \text{ τότε } A \in M_n(R_P \cdot P)$$

Απόδειξη. Από το (2) του λήμματος X.2.16 και τη μορφή των στοιχείων του R_P στο (3) προκύπτει ότι υπάρχει φυσικός αριθμός $m \geq 0$ ώστε $\pi^m A \in M_n(R_P)$.

Ισχυριζόμαστε ότι $m \geq 0$, $\pi^m A \in M_n(R_P)$ και $A\nu \in \times_{i=1}^{n} PS$ συνεπώς $\pi^{m-1} A \in M_n(R_P)$. Άμεση συνέπεια του ισχυρισμού είναι ότι, επαγωγικά, προκύπτει $\pi^{-1} A \in M_n(R_P)$ και συνεπώς $A \in M_n(R_P\pi) = M_n(R_P P)$.

Τώρα θα αποδείξουμε τον ισχυρισμό. Από $\pi^m A \in M_n(R_P)$, έπεται ότι υπάρχει $a \in R\backslash P$ ώστε $\pi^m aA \in M_n(R)$. Έστω $A = (\alpha_{ij})_{n \times n}$. Λόγω της υπόθεσης $A\nu \in \times_{i=1}^{n} PS$, έπεται ότι, για κάθε $i = 1, 2, \ldots, n$

$$\sum_{j=1}^{n} (\pi^m a \alpha_{ij}) \omega_j \in \pi^m a PS \subset PS,$$

αφού $m \geq 0$. Τα $\pi^m a \alpha_{ij} \in R$. Επομένως, για κάθε $i = 1, 2, \ldots, n$

$$\sum_{j=1}^{n} \overline{(\pi^m a \alpha_{ij})} \overline{\omega}_j = \overline{0}.$$

Το σύνολο $\{\overline{\omega}_1, \overline{\omega}_2, \ldots, \overline{\omega}_n\}$ είναι R/P-βάση του S/PS. Συνεπώς, για κάθε $i, j \in \{1, 2, \ldots, n\}$ ισχύει

$$\overline{\pi^m a \alpha_{ij}} = \overline{0},$$

δηλαδή $\pi^m a \alpha_{ij} \in PS$. Όμως $\pi^m a \alpha_{ij} \in R$, άρα $\pi^m a \alpha_{ij} \in PS \cap R = P$. Τελικά, έχουμε $\pi^m aA \in M_n(P)$ συνεπώς $\pi^m A \in M_n(R_P\pi)$, το A $R\backslash P$ οπότε και $\pi^{m-1} A \in M_n(R_P)$. □

Λήμμα X.2.18. *Αν το σύνολο $\{\overline{\omega}_1, \overline{\omega}_2, \ldots, \overline{\omega}_n\}$ είναι βάση του R/P-διανυσματικού χώρου S/PS, τότε το σύνολο $\{\omega_1, \omega_2, \ldots, \omega_n\}$ είναι βάση της επέκτασης L/K.*

Απόδειξη. Αφού $[L : K] = n$ αρκεί να αποδείξουμε ότι τα $\omega_1, \omega_2, \ldots, \omega_n$ είναι K-γραμμικά ανεξάρτητα. Έστω

$$\sum_{i=1}^{n} r_i \omega_i = 0 : r_i \in K, \text{ όχι όλα τα } r_i = 0.$$

Από το 2) του λήμματος Χ.2.16 έχουμε $r_i = \pi^{\nu_i} \frac{\alpha_i}{\beta_i}$, $\nu_i \in \mathbb{Z}$, $\alpha_i, \beta_i \in R \backslash P$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι τα $\beta_i = 1$. Πολλαπλασιάζοντας, αν χρειαστεί, με κατάλληλη δύναμη του π, μπορούμε να θεωρήσουμε ότι για κάποιο από τα r_i, $r_i \neq 0$ το $\nu_i = 0$. Έστω $r_1 = \alpha_1$ και $\nu_1 = 0$.

Από τη σχέση $\sum_{i=1}^{n} r_i \omega_i = 0$ έπεται ότι $\sum_{i=1}^{n} \overline{r}_i \overline{\omega}_i = \overline{0}$. Το σύνολο $\{\overline{\omega}_1, \overline{\omega}_2, \ldots, \overline{\omega}_n\}$ είναι βάση του S/PS. Επομένως, για κάθε $i = 1, 2, \ldots, n$ ισχύει $\overline{r}_i = \overline{0}$ οπότε, όπως παραπάνω, για κάθε $i = 1, 2, \ldots, n$ ισχύει $r_i \in P$, συνεπώς και $r_1 = \alpha_1 \in P$, άτοπο αφού $\alpha_1 \in R \backslash P$. □

Χ.2.4 Η απόδειξη του αντιστρόφου του δεύτερου μέρους του θεωρήματος της διακρίνουσας

Θα αποδείξουμε ότι αν P δεν διακλαδίζεται στην L/K τότε $P \nmid \mathcal{D}_{L/K}$. Αρκεί να αποδείξουμε ότι υπάρχει R/P-βάση $\overline{\omega}_1, \overline{\omega}_2, \ldots, \overline{\omega}_n \in S/SP$ με

$$D_{L/K}(\omega_1, \omega_2, \ldots, \omega_n) \not\equiv 0 \mod P.$$

Το P δεν διακλαδίζεται στο L, σημαίνει ότι

$$PS = Q_1 Q_2 \cdots Q_r, \; Q_i \neq Q_j \text{ για κάθε } i \neq j.$$

Επομένως η απεικόνιση

$$\begin{aligned} \phi : \frac{S}{PS} &\longrightarrow \frac{S}{Q_1} \times \frac{S}{Q_2} \times \cdots \times \frac{S}{Q_r} \\ s + PS &\longmapsto \phi(s + PS) = (s + Q_1, s + Q_2, \ldots, s + Q_r) \end{aligned}$$

είναι, σύμφωνα με το θεώρημα του Κινέζου, ένας R/P-ισομορφισμός διανυσματικών χώρων. Το σύνολο των προτύπων μιας βάσης είναι επίσης βάση του S/PS. Επομένως υπάρχει μια βάση του S/PS της μορφής $\overline{\omega}_{i,\mu} = \omega_{i,\mu} + PS$, για $i = 1, 2, \ldots, r$ και $\mu = 1, 2, \ldots, f_i = f(Q_i/P)$ είναι βάση του S/Q_i και επιπροσθέτως $\omega_{i,\mu} \equiv 0 \mod Q_j$ για $i \neq j$.

Ισχυριζόμαστε ότι

$$D_{L/K}(\{\omega_{i,\mu}\}) \not\equiv 0 \mod P. \tag{Χ.2}$$

Ως γνωστό $D_{L/K}(\{\omega_{i,\mu}\} = \det(\mathrm{Tr}_{L/K}(\omega_{i,m}\omega_{i,\nu}))$. Από τη σχέση $\omega_{i,\mu} \equiv 0 \mod Q_j$, για κάθε $j \neq i$ προκύπτει ότι

$$\omega_{i,\mu}\omega_{j,\nu} \equiv 0 \mod \bigcap_{\ell=1}^{r} Q_\ell \text{ για } i \neq j. \tag{Χ.3}$$

Επομένως από το λήμμα Χ.2.8 έχουμε

$$\mathrm{Tr}_{L/K}(\{\omega_{i,\mu}\omega_{j,\nu}\}) \equiv 0 \mod P, \text{ για κάθε } i, j \in \{1, 2, \ldots, n\}, i \neq j$$

οπότε και

$$D_{L/K}(\{\omega_{i,\mu}\}) = \prod_{i=1}^{r} \det\left(\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu})_{\mu,\nu=1,2,\ldots,f_i} \mod P.\right)$$

Για να αποδείξουμε λοιπόν τον ισχυρισμό, αρκεί να αποδείξουμε ότι:

Για κάθε $i = 1, 2, \ldots, r$ $\det \mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu})_{\mu,\nu=1,2,\ldots,f_i} \not\equiv 0 \mod P$.

Λόγω της γνωστής σχέσης $Q_i \cap K = P$ αρκεί να αποδείξουμε ότι

$$\text{Για κάθε } i = 1, 2, \ldots, r \det(\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu}))_{\mu,\nu=1,2,\ldots,f_i} \not\equiv 0 \mod Q_i \tag{Χ.4}$$

Από το λήμμα X.2.18 το σύνολο $\{\omega_{i,\mu} : i = 1, 2, \dots, r, \mu = 1, 2, \dots f_i(Q_j/P)\}$ είναι βάση της επέκτασης L/K. Έστω λοιπόν V η βάση

$$V = (v_1, v_2, \dots v_r)^T, \text{ όπου } v_i = (\omega_{i1}, \omega_{i2}, \dots, \omega_{if_i})^T)$$

της επέκτασης L/K.

$$\omega_{i,\mu}\omega_{i,\nu}V = D_{\omega_{i,\mu}\omega_{i,\nu}}V, \text{ με } D_{\omega_{i,\mu}\omega_{i,\nu}} \in M_n(K)$$

συνεπώς

$$\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu}) = \mathrm{tr}(D\omega_{i,\mu}\omega_{i,\nu}).$$

Τα $\overline{\omega}_{i,\mu} = \omega_{i,\mu} + PS$ αποτελούν βάση του S/PS και

$$\omega_{i,\mu}(\omega_{i,\nu}\omega_{j,k}) \equiv 0 \mod \bigcap_{\ell=1}^{r} Q_\ell, \text{ για κάθε } j \neq i.$$

Η τομή

$$\cap_{\ell=1}^{r} Q_\ell = Q_1 Q_2 \cdots Q_r = PS.$$

Αυτό σημαίνει ότι υπάρχει $A^{(i)}_{\mu\nu} \in M_{f_i}(R)$ ώστε

$$\omega_{i,\mu}\omega_{i,\nu}V = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & A^{(i)}_{\mu,\nu} & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \cdot V \mod PS \tag{X.5}$$

δηλαδή

$$\left(D_{\omega_{i,\mu}\omega_{i,\nu}} - \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & A^{(i)}_{\mu,\nu} & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \right) V \in PS.$$

Από το λήμμα X.2.17 προκύπτει ότι

$$D_{\omega_{i,\mu}\omega_{i,\nu}} - \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & A^{(i)}_{\mu,\nu} & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in M_n(R_P \cdot P)$$

συνεπώς

$$\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu}) = \mathrm{tr}(D\omega_{i,\mu}\omega_{i,\nu}) \equiv \mathrm{tr}(A^{(i)}_{\mu,\nu}) \mod R_P \cdot P$$

Επειδή $\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu}) \in R$ και $\mathrm{tr}(A^{(i)}_{\mu,\nu}) \in R$ έχουμε

$$\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu}) - \mathrm{tr}(A^{(i)}_{\mu,\nu}) \in R_P \cdot P \cap R.$$

Αλλά $R_P \cdot P \cap R = P$ (άσκηση). Επομένως

$$\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu}) \equiv \mathrm{tr}(A^{(i)}_{\mu,\nu}) \mod P$$

Τέλος κάνουμε μια νέα θεώρηση του ίχνους του πίνακα $A^{(i)}_{\mu,\nu}$, $\mu, \nu = 1, 2, \dots, f_i$. Κρατούμε σταθερό το i. Το

$$\overline{v}_i = (\omega_{i1} + Q_i, \omega_{i2} + Q_i, \dots, \omega_{if_i} + Q_i)^T$$

είναι μια βάση του R/P-διανυσματικού χώρου S/Q_i συνεπώς το $\overline{v}_i$ είναι μια βάση της επέκτασης $\overline{L}/\overline{K}$, όπου $\overline{L} = S/Q_i$ και $\overline{K} = (R + Q_i)/Q_i$, η εμφύτευση του R/P στο $\overline{L}$.

Η $\overline{L}/\overline{K}$ είναι επέκταση πεπερασμένων σωμάτων άρα είναι αλγεβρική και διαχωρίσιμη. Η σχέση (X.5) γράφεται

$$\overline{\omega}_{i,\mu}\overline{\omega}_{i,\nu}\overline{V} = \overline{A^{(i)}_{\mu,\nu}} \cdot \overline{V},$$

όπου η παύλα $\bar{\cdot}$, σημαίνει modulo Q_i. Τελικά

$$\mathrm{Tr}_{\overline{L}/\overline{K}}(\overline{\omega}_{i,\mu}\overline{\omega}_{i,\nu}) = \mathrm{tr}(\overline{A}^{(i)}_{\mu,\nu}).$$

Η προηγούμενη αποδειχθείσα σχέση

$$\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu}) \equiv \mathrm{tr}(A^{(i)}_{\mu,\nu}) \mod P$$

συνεπάγεται

$$\begin{aligned}\det(\mathrm{Tr}_{L/K}(\omega_{i,\mu}\omega_{i,\nu})_{\mu,\nu}) + Q_i &= \det(A^{(i)}_{\mu,\nu}) + Q_i = \det(\overline{A^{(i)}_{\mu,\nu}}) \\ &= \det(\mathrm{Tr}_{\overline{L}/\overline{K}}(\overline{\omega}_{i,\mu}\overline{\omega}_{i,\nu})) \\ &= D_{\overline{L}/\overline{K}}(\overline{\omega}_{i1}, \overline{\omega}_{i2}, \ldots, \overline{\omega}_{i,f_i}) \neq \overline{0} \text{ για κάθε } i = 1, 2, \ldots, r\end{aligned}$$

επειδή τα $\overline{\omega}_{i1}, \overline{\omega}_{i2}, \ldots, \overline{\omega}_{i,f_i}$ αποτελούν βάση της $\overline{L}/\overline{K}$ αποδείξαμε την εξίσωση (Χ.4) και συνεπώς το θεώρημα της διακρίνουσας.

Χ.3 Διαφορίζουσα

Χ.3.1 Εισαγωγικά στοιχεία

Στον πραγματικό διανυσματικό χώρο $\mathbb{R}^n$ έχουμε το συνηθισμένο εσωτερικό γινόμενο μέσω του οποίου ορίζεται η έννοια του ορθογωνίου συμπληρώματος. Έτσι αν $V \subset \mathbb{R}^n$ ένας διανυσματικός υπόχωρος του $\mathbb{R}^n$ τότε το ορθογώνιο συμπλήρωμα του V είναι

$$V^\perp = \{w \in \mathbb{R}^n : w \perp V\} = \{w \in \mathbb{R}^n : w \cdot V = 0\}.$$

Ας υπενθυμίσουμε, τις γνωστές άλλωστε, ιδιότητες

$$\begin{aligned}\mathbb{R}^n &= V \oplus V^\perp \\ (V^\perp)^\perp &= V \\ V_1 \subset V_2 &\Leftrightarrow V_2^\perp \subset V_1^\perp.\end{aligned}$$

Ένα δικτυωτό L του $\mathbb{R}^n$, όπως το έχουμε ήδη ορίσει, είναι η ελεύθερη αβελιανή ομάδα που παράγεται από μια βάση $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ του $\mathbb{R}^n$,

$$L = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n.$$

Ανάλογα προς το ορθογώνιο συμπλήρωμα ορίζουμε

Ορισμός Χ.3.1. Έστω L ένα δικτυωτό του $\mathbb{R}^n$. Το $\mathbb{Z}$-δυϊκό του L, είναι το

$$L^* = \{w \in \mathbb{R}^n : w \cdot L \subset \mathbb{Z}\}.$$

Παρατήρηση Χ.3.2. 1. Το L^* δεν είναι ορθογώνιο συμπλήρωμα του L.

2. Αν $L = \oplus_{i=1}^n \mathbb{Z}\alpha_i$, ένα δικτυωτό του $\mathbb{R}^n$ τότε το $L^* = \oplus_{i=1}^n \mathbb{Z}\alpha_i^*$, όπου $\{\alpha_1^*, \alpha_2^*, \ldots, \alpha_n^*\}$ η δυϊκή βάση της $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ ως προς το εσωτερικό γινόμενο του $\mathbb{R}^n$. Δηλαδή το L^* είναι επίσης δικτυωτό του $\mathbb{R}^n$. Πράγματι, έστω $w \in \mathbb{R}^n$. Το γράφουμε ως γραμμικό συνδυασμό στοιχείων της δυϊκής βάσης. Αν λοιπόν

$$w = \sum_{i=1}^n \beta_i \alpha_i^* \text{ τότε } w\alpha_i = \beta_i.$$

Επομένως $w \in L^* \Leftrightarrow \beta_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$.

3. Ισχύουν ιδιότητες ανάλογες προς το ορθογώνιο συμπλήρωμα:
   (α′) Αν L δικτυωτό του $\mathbb{R}^n$, τότε $(L^*)^* = L$
   (β′) Αν L_1, L_2 δικτυωτά του $\mathbb{R}^n$, τότε $L_2^* \subset L_1^*$
   (γ′) $(L_1 + L_2)^* = L_1^* \cap L_2^*$
   (δ′) $(L_1 \cap L_2)^* = L_1^* + L_2^*$.

Έστω τώρα K ένα, οποιοδήποτε, σώμα και V ένας K-διανυσματικός χώρος, διάστασης $\dim_K V = n$. Μία διγραμμική μορφή επί του V είναι μία συνάρτηση

$$B : V \times V \to K$$

η οποία είναι K-γραμμική ως προς κάθε μία από τις δύο μεταβλητές.

Κάθε K-διγραμμική μορφή του V απεικονίζει ένα γραμμικά εξαρτημένο σύνολο διανυσμάτων $u_1, u_2, \ldots, u_n \in V$ μέσω των τιμών $B(u_i, u_j)$ σε κάποιον ιδιάζοντα (degenerate) πίνακα, δηλαδή πίνακα ορίζουσας ίσης με μηδέν. Αυτό επειδή υπάρχει κάποιο διάνυσμα u_k το οποίο είναι K-γραμμικός συνδυασμός των υπολοίπων.

Η διγραμμική μορφή

$$B : V \times V \to K$$

θα λέγεται μη-ιδιάζουσα (non-degenerate) όταν υπάρχει μια K-βάση $v_1, v_2, \ldots, v_n$ του V της οποίας ο πίνακας $\Delta(v_1, v_2, \ldots, v_n) = B(v_i, v_j) : 1 \le i, j \le n$ είναι αντιστρέψιμος. Είναι φανερό ότι αν αυτό ισχύει για κάποια βάση τότε ισχύει για οποιαδήποτε βάση.

Ορισμός X.3.3. Αν $u_1, u_2, \ldots, u_n$ στοιχεία του V, τότε η ορίζουσα του πίνακα $(B(u_i, u_j)), 1 \le i, j \le n$ θα λέγεται διακρίνουσα του $\{u_1, u_2, \ldots, u_n\}$.

Είναι φανερό ότι αν $\{v_1, v_2, \ldots, v_n\}$ βάση του V και $w_1, w_2, \ldots, w_n$ οποιαδήποτε στοιχεία του V και

$$w_i = \sum_{j=1}^{n} a_{ij} v_j : a_{ij}, A = (a_{ij})_{1 \le i,j \le n},$$

τότε

$$\Delta(w_1, w_2, \ldots, w_n) = (\det A)^2 \Delta(v_1, v_2, \ldots, v_n).$$

Επομένως, αν τα $w_1, w_2, \ldots, w_n$ είναι γραμμικά εξαρτημένα τότε $\Delta(w_1, w_2, \ldots, w_n) = 0$. Επίσης ισχύει, ότι αν $\{v_1, v_2, \ldots, v_n\}$ είναι μια βάση του V τότε, η διγραμμική μορφή $B : V \times V \to K$ είναι ιδιάζουσα αν και μόνο αν $\Delta(v_1, v_2, \ldots, v_n) = 0$.

Ορισμός X.3.4. Δύο βάσεις του V, $\{v_1, v_2, \ldots, v_n\}$ και $\{w_1, w_2, \ldots, w_n\}$ θα λέγονται δυϊκές ή συμπληρωματικές (complementary) όταν

$$B(v_i, w_j) = \delta_{ij}, \delta_{ij} \text{ το σύμβολο του Kronecker.}$$

Πρόταση X.3.5. *Η διγραμμική μορφή $B : V \times V \to K$ είναι μη-ιδιάζουσα τότε και μόνο τότε όταν κάθε βάση του V έχει μια (δυϊκή) συμπληρωματική βάση. Στην περίπτωση αυτή η συμπληρωματική βάση είναι μοναδική.*

Απόδειξη. "⇐" Αν η βάση $\{v_1, v_2, \ldots, v_n\}$ έχει μια συμπληρωματική βάση $\{w_1, w_2, \ldots, w_n\}$ οπότε η

$$B(w_i, w_k) = \sum_{j=1}^{n} a_{ij} B(v_j, w_k) = a_{ik}$$

συνεπώς $\Delta(w_1, w_2, \ldots, w_n) = \det(A) \neq 0$, συνεπώς η B μη-ιδιάζουσα.

"⇒" Έστω τώρα ότι η B είναι μη-ιδιάζουσα. Για κάθε $v \in V$, έστω $B_v \in V^*$, όπου ο V^* είναι ο δυϊκός χώρος του V η

$$B_v : V \to K, B_v(w) = B(v, w).$$

Είναι γνωστό ότι η συνάρτηση

$$\begin{aligned} V &\longrightarrow V^* \\ \nu &\longmapsto B_\nu \end{aligned}$$

είναι ένας ισομορφισμός K-διανυσματικών χώρων. Η δυϊκή (συμπληρωματική) βάση του V είναι ουσιαστικά η δυϊκή βάση του V^*. □

Χ.3.2 Η διγραμμική μορφή ίχνος

Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών και $[L : K] = n$. Η απεικόνιση

$$\begin{aligned} B : L \times L &\longrightarrow L \\ (\alpha, \beta) &\longmapsto B(\alpha, \beta) = \mathrm{Tr}_{L/K}(\alpha\beta) \end{aligned}$$

είναι μια συμμετρική μορφή του L. Μάλιστα είναι μη-ιδιάζουσα, αφού αν $L = K(\theta)$ το σύνολο $\{1, \theta, \ldots, \theta^{n-1}\}$ είναι μια βάση της επέκτασης και

$$\Delta(1, \theta, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq k} (\sigma_k(\theta) - \sigma_i(\theta))^2 \neq 0.$$

Παρατήρηση Χ.3.6. Στη θεωρία αριθμών η πεπερασμένη επέκταση L/K είναι πάντα διαχωρίσιμη. Αν επιθυμούσαμε να δούμε τα πράγματα γενικότερα, από την αλγεβρική σκοπιά, τότε αποδεικνύεται ότι η συνάρτηση ίχνος είναι μη-ιδιάζουσα (και συνεπώς και επί) ακριβώς τότε όταν η L/K είναι διαχωρίσιμη, [3, Satz 7, σελ. 189].

Σε κάθε αλγεβρικό σώμα αριθμών K, $[K : \mathbb{Q}] = n$ ένα δικτυωτό του K είναι μια ελεύθερη αβελιανή ομάδα που παράγεται (ως $\mathbb{Z}$-module) από μια $\mathbb{Q}$-βάση του K. Τέτοια δικτυωτά είναι ο δακτύλιος των ακεραίων αλγεβρικών R_K, τα (κλασματικά) ιδεώδη του K καθώς και οι τάξεις αυτού.

Αντί λοιπόν να ενδιαφερόμαστε για διανύσματα με εσωτερικό γινόμενο στο $\mathbb{Z}$, εξετάζουμε αλγεβρικούς αριθμούς με σύζευξη ίχνους ακέραιους αριθμούς.

Ορισμός Χ.3.7. Αν L είναι ένα δικτυωτό του K, τότε το δυϊκό δικτυωτό του L είναι το

$$L^* = \{\alpha \in K : \mathrm{Tr}_{L/K}(\alpha L) \subset \mathbb{Z}\}.$$

Παρατήρηση Χ.3.8. Είναι φανερό ότι για να ελέγξουμε αν $\alpha \in K$ ανήκει στο L^* αρκεί να διαπιστώσουμε ότι $\mathrm{Tr}_{L/K}(\alpha\nu_i) \in \mathbb{Z}$, όπου $\{\nu_1, \nu_2, \ldots, \nu_n\}$ μία K-βάση του L.

Παράδειγμα Χ.3.9. Έστω $K = \mathbb{Q}(i)$ και $L = \mathbb{Z}[i]$. Έστω τώρα $a + bi \in \mathbb{Q}(i)$. Το $a + bi \in L^*$ αν και μόνο αν $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi) \in \mathbb{Z}$ και $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}} = \big((a + bi)i\big) \in \mathbb{Z}$ το οποίο συμβαίνει όταν $2a \in \mathbb{Z}$ και $-2b \in \mathbb{Z}$ δηλαδή

$$L^* = \mathbb{Z}[i]^* = \frac{1}{2}\mathbb{Z} + \frac{1}{2}\mathbb{Z}i = \frac{1}{2}\mathbb{Z}[i].$$

Αν

$$L = (1 + 2i)\mathbb{Z}[i] = \mathbb{Z}(1 + 2i) + \mathbb{Z}(-2 + i),$$

αποδεικνύεται ότι

$$L^* = \frac{1}{2(1 + 2i)}\mathbb{Z}[i] \text{ (άσκηση)}.$$

Παρατήρηση Χ.3.10. 1. Υπάρχει κάποια σχέση ανάμεσα στο δυϊκό δικτυωτό και στο αντίστροφο ιδεώδες. Αν θεωρήσουμε το L στο δεύτερο παράδειγμα ως το ιδεώδες $\langle 1 + 2i \rangle$ τότε το $A^* = \frac{1}{2}A^{-1}$.

2. Ορίσαμε το L^* ως το δυϊκό δικτυωτό του L. Θα πρέπει να αποδείξουμε ότι είναι δικτυωτό.

Πρόταση X.3.11. *Έστω K αλγεβρικό σώμα αριθμών $[K:\mathbb{Q}]=n$, L ένα δικτυωτό του K και $\{v_1,v_2,\dots,v_n\}$ μια $\mathbb{Z}$-βάση του L. Το*

$$L^*=\oplus_{i=1}^n \mathbb{Z}v_i^*,$$

όπου $\{v_1^*,v_2^*,\dots,v_n^*\}$ είναι η δυϊκή βάση της $\{v_1,v_2,\dots,v_n\}$ ως προς τη σύζευξη ίχνους.

Απόδειξη. Γράφουμε $\alpha\in K$ ως προς τη δυϊκή βάση

$$\alpha=\sum_{i=1}^n \beta_i v_i^*,\ \beta_i\in\mathbb{Q}, i=1,2,\dots,n.$$

$$\begin{aligned}\alpha\in L^* &\Leftrightarrow \mathrm{Tr}_{L/K}(\alpha L)\in\mathbb{Z}\Leftrightarrow \big(\mathrm{Tr}_{L/K}(\alpha v_i)\in\mathbb{Z}\text{ για κάθε } i=1,2,\dots,n\big)\\ &\Leftrightarrow \big(\beta_i\in\mathbb{Z}\text{ για κάθε } i=1,2,\dots,n\big)\end{aligned}$$

□

Άσκηση Αν L δικτυωτό του K και $\alpha\in K^*$ να αποδειχθεί ότι

$$(\alpha L)^*=\frac{1}{\alpha}L^*.$$

Το πιο σημαντικο δικτυωτό του K είναι ο δακτύλιος των ακεραίων αλγεβρικών αυτού R_K. Επομένως

$$R_K^*=\{\alpha\in K:\mathrm{Tr}_{L/K}(\alpha R_K)\subset\mathbb{Z}\}$$

Παρατήρηση X.3.12. Το R_K^* δεν είναι το σύνολο $\alpha\in K$ για τα οποία το ίχνος $\mathrm{Tr}_{L/K}(\alpha)\in\mathbb{Z}$, αλλά είναι ένα σύνολο μικρότερο από αυτό. Όμως επειδή όλα τα στοιχεία $\alpha\in R_K$ έχουν $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)\in\mathbb{Z}$, έπεται ότι $R_K\subset R_K^*$.

Πρόταση X.3.13. *Αν A κλασματικό ιδεώδες του K, τότε και το A^* είναι κλασματικό ιδεώδες του K και μάλιστα ισχύει $AA^*=R_K^*$.*

Απόδειξη. Εξ ορισμού το

$$A^*=\{\alpha\in K:\mathrm{Tr}_{K/\mathbb{Q}}(\alpha A)\subset\mathbb{Z}\}.$$

Το A^* είναι ένα κλασματικό ιδεώδες του R_K. Έχουμε ήδη δει ότι είναι ένα πεπερασμένο παραγόμενο $\mathbb{Z}$-module, αφού είναι δικτυωτό. Αυτό που απομένει να αποδειχθεί είναι ότι αν $\alpha\in A^*$ και $r\in R_K$ τότε και $r\alpha\in A^*$. Πράγματι, για κάθε $\beta\in A$ ισχύει

$$\mathrm{Tr}_{K/\mathbb{Q}}((r\alpha)\beta)=\mathrm{Tr}_{K/\mathbb{Q}}(\alpha(r\beta))\in\mathbb{Z},$$

αφού $r\beta\in A$ και $\alpha\in A^*$. Στη συνέχεια θα αποδείξουμε ότι $AA^*=R_K^*$. Έστω $\alpha\in A^*$. Για κάθε $\beta\in A$ έχουμε

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta R_K)\subset\mathbb{Z}\text{ αφού }\beta R_K\subset A\Rightarrow\alpha\beta\in R_K^*.$$

Αφού ισχύει για κάθε $\beta\in A$ έχουμε $\alpha A\subset R_K^*$ και αυτό για κάθε $\alpha\in A^*$. Συνεπώς $A^*A\subset R_K^*$ ($A^*\subset A^{-1}R_K^*$).

Αντίστροφα, τώρα, έστω $\alpha\in R_K^*$. Θεωρούμε το ίχνος

$$\mathrm{Tr}_{K/\mathbb{Q}}\big((\alpha A^{-1})A\big)=\mathrm{Tr}_{K/\mathbb{Q}}(\alpha R_K)\subset\mathbb{Z}.$$

Αυτό σημαίνει ότι $\alpha A^{-1}\subset A^*$, για κάθε $\alpha\in R_K^*$ δηλαδή $R_K^*A^{-1}\subset A^*$ και τελικά έχουμε την ισότητα.

□

Παρατήρηση Χ.3.14. Από την απόδειξη της πρότασης έχουμε ότι για κάθε ιδεώδες A του K το αντίστροφο του A^*, $(A^*)^{-1}$ είναι ένα ακέραιο ιδεώδες του K.

Ορισμός Χ.3.15. Ως *διαφορίζουσα (different)* του σώματος K ορίζεται το ακέραιο ιδεώδες του K,

$$\mathrm{Diff}_{K/\mathbb{Q}} = (R_K^*)^{-1} = \{\alpha \in K, \alpha R_K^* \subset R_K\}. \tag{Χ.6}$$

Παράδειγμα Χ.3.16. Για $K = \mathbb{Q}(i)$ το $\mathrm{Diff}_{K/\mathbb{Q}} = 2\mathbb{Z}[i]$.

Πρόταση Χ.3.17. *Το δυϊκό δικτυωτό R_K^* είναι το μέγιστο κλασματικό ιδεώδες του K για το οποίο όλα τα στοιχεία του έχουν ακέραιο ίχνος.*

Απόδειξη. Έστω A ένα κλασματικό ιδεώδες του K. Το $A = AR_K$ επομένως $\mathrm{Tr}_{K/\mathbb{Q}}(A) \in \mathbb{Z}$ αν και μόνο αν $\mathrm{Tr}_{K/\mathbb{Q}}(AR_K) \subset \mathbb{Z}$ αν και μόνο αν $A^* \subset R_K^*$. □

Η παρακάτω πρόταση σχετίζει τις έννοιες διακρίνουσα και διαφορίζουσα ενός αλγεβρικού σώματος αριθμών K.

Πρόταση Χ.3.18 (Το πρώτο θεώρημα του Dedekind)**.** *Έστω K αλγεβρικό σώμα αριθμών, με $[K : \mathbb{Q}] = n$. Ισχύει*

$$|N_{K/\mathbb{Q}}(\mathrm{Diff}_{K/\mathbb{Q}})| = |\mathcal{D}_{K/\mathbb{Q}}|.$$

Πρώτα θα αποδείξουμε το ακόλουθο:

Λήμμα Χ.3.19. *Αν A, B ιδεώδη του K και $B \subset R_K$, τότε $N_{K/\mathbb{Q}}(B) = [A : AB]$.*

Απόδειξη. (του λήμματος) Από την υπόθεση $B \subset R_K$ έπεται ότι $AB \subset A$. Έστω m ένας φυσικός για τον οποίο ισχύει $mA \subset R_K$. Η απεικόνιση

$$\begin{aligned} A &\longrightarrow mA \\ \alpha &\longmapsto m\alpha \end{aligned}$$

είναι ένας ισομορφισμός αβελιανών ομάδων ο οποίος απεικονίζει το ιδεώδες AB στο mAB. Επομένως,

$$[A : AB] = [mA : mAB] = \frac{[R_K : mAB]}{[R_K : mA]} = \frac{N_{K/\mathbb{Q}}(mAB)}{N_{K/\mathbb{Q}}(mA)} = N_{K/\mathbb{Q}}(B).$$

□

Απόδειξη. (της πρότασης)

$$[R_K^* : R_K] = [R_K^* : (R_K^* \mathrm{Diff}_{K/\mathbb{Q}})],$$

αφού $R_K^* \mathrm{Diff}_{K/\mathbb{Q}} = R_K$ και σύμφωνα με το λήμμα

$$[R_K^* : (R_K^* \mathrm{Diff}_{K/\mathbb{Q}})] = N_{L/\mathbb{Q}}(\mathrm{Diff}_{K/\mathbb{Q}}).$$

Θα υπολογίσουμε τον δείκτη $[R_K^* : R_K]$ και με άλλο τρόπο. Θυμόμαστε ότι αν έχουμε δύο πεπερασμένα παραγόμενα ελεύθερα $\mathbb{Z}$-modules $M_2 \subset M_1$ με τον ίδιο βαθμό, τότε

$$[M_1 : M_2] = |\det(A)|,$$

όπου A ο πίνακας που εκφράζει την $\mathbb{Z}$-βάση του M_2 μέσω της $\mathbb{Z}$-βάσης του M_1. Έστω λοιπόν $\{\omega_1, \omega_2, \ldots, \omega_n\}$ μια $\mathbb{Z}$-βάση του R_K, και $\mathrm{Diff}_{K/\mathbb{Q}}^{-1} = R_K^*$. Το R_K^* έχει ως $\mathbb{Z}$-βάση τη δυϊκη ως προς το $\mathrm{Tr}_{K/\mathbb{Q}}$ $\{\omega_1^*, \omega_2^*, \ldots, \omega_n^*\}$. Το $M_1 = R_K^*$ και το $M_2 = R_K$. Γράφουμε τα ω_i ως γραμμικούς συνδυασμούς των ω_i^*. Αν $\omega_j = \sum_{i=1}^n a_{ij}\omega_i^*$. Ισχύει

$$\mathrm{Tr}_{K/\mathbb{Q}}(\omega_j\omega_i) = \mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j) = a_{ij}.$$

Συνεπώς

$$\left(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j)\right)_{1\le i,j\le n} = \left(a_{ij}\right)_{1\le i,j\le n}.$$

Επομένως,

$$[R_K^* : R_K] = |\det(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j)_{1\le i,j\le n})| = |D_{K/\mathbb{Q}}|.$$

□

Παρατήρηση X.3.20. 1. Έχουμε τρία δικτυωτά

$$\mathrm{Diff}_{K/\mathbb{Q}} \subset R_K \subset R_K^*$$

με τον ίδιο δείκτη $[R_K^* : R_K] = [R_K : \mathrm{Diff}_{K/\mathbb{Q}}] = |D_{K/\mathbb{Q}}|$. Το $R_K \subsetneq R_K^* \Leftrightarrow |D_{K/\mathbb{Q}}| > 1$. Η τελευταία σχέση ισχύει για όλα τα αλγεβρικά σώματα αριθμών K, $K \neq 0$. Επομένως, για κάθε $K \neq \mathbb{Q}$ ισχύει $R_K \subsetneq R_K^*$. Η διαφορίζουσα του σώματος K, ακριβέστερα η norm αυτής, μπορεί να θεωρηθεί ως ένα μέτρο για το κατά πόσο απέχει το δικτυωτό R_K από το να είναι αυτοδυϊκό.

2. Αν $K = \mathbb{Q}(\sqrt{d})$, d ελεύθερο τετραγώνου, τότε

$$N_{K/\mathbb{Q}}(\mathrm{Diff}_{K/\mathbb{Q}}) = |D_{K/\mathbb{Q}}| = \begin{cases} 4|d|, & \text{αν } d \equiv 2,3 \mod 4 \\ |d|, & \text{αν } d \equiv 1 \mod 4 \end{cases}$$

3. Σύμφωνα με το θεώρημα της διακρίνουσας και την παραπάνω πρόταση θα πρέπει να υπάρχει κάποια σχέση ανάμεσα στη διαφορίζουσα και στους διακλαδιζόμενους πρώτους. Αυτό θα το μελετήσουμε αναλυτικά στη συνέχεια. Πάντως, άμεση συνέπεια της πρότασης είναι ότι ένα ιδεώδες A του R_K διαιρεί τη διαφορίζουσα, $A \mid \mathrm{Diff}_{K/\mathbb{Q}}$ τότε και μόνο τότε όταν $\mathrm{Tr}_{K/\mathbb{Q}}(A^{-1}) \in \mathbb{Z}$. Πράγματι, $A \mid \mathrm{Diff}_{K/\mathbb{Q}}$ αν και μόνο αν $\mathrm{Diff}_{K/\mathbb{Q}} \subset A$ αν και μόνο αν $A^{-1} \subset R_K^* = \mathrm{Diff}_{K/\mathbb{Q}}^{-1}$. Αλλά $A^{-1} \subset R_K^* \Leftrightarrow \mathrm{Tr}_{K/\mathbb{Q}}(A^{-1}) \in \mathbb{Z}$.

Στη συνέχεια θα προχωρήσουμε σε σχετικές επεκτάσεις L/K αλγεβρικών σωμάτων αριθμών.

Πρόταση X.3.21. *Έστω R_K, R_L οι δακτύλιοι των ακεραίων αλγεβρικών αριθμών και $\mathrm{Tr}_{L/K}$ το σχετικό ίχνος. Το σύνολο*

$$R_{L/K}^* = \{\alpha \in L : \mathrm{Tr}_{L/K}(\alpha R_L) \subset R_K\}$$

είναι ένα δικτυωτό του L και μάλιστα κλασματικό ιδεώδες, του οποίου το αντίστροφο είναι ένα ακέραιο ιδεώδες του R_L, έστω $\mathrm{Diff}_{L/K}$. Επίσης το $R_{L/K}^*$ είναι το μεγαλύτερο κλασματικό ιδεώδες του L του οποίου το ίχνος $\mathrm{Tr}_{L/K}(R_{L/K}^*) \subset R_K$. Τέλος αν A ιδεώδες του K και Q ιδεώδες του L, τότε ισχύει $\mathrm{Tr}_{L/K}(Q) \subset A \Leftrightarrow Q \subset A\mathrm{Diff}_{L/K}^{-1}$.

Απόδειξη. Όπως και στην απόλυτη περίπτωση $R_L \subset R_{L/K}^*$. Τώρα αν $\alpha \in R_{L/K}^*$, τότε $\mathrm{Tr}_{L/K}(\alpha R_L) \subset R_K$. Επομένως

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{Tr}_{L/K}(\alpha)) \subset \mathrm{Tr}_{K/\mathbb{Q}}(R_K) \subset \mathbb{Z}.$$

Αυτό σημαίνει ότι

$$R_L \subset R_{L/K}^* \subset R_L^* = \mathrm{Diff}_{L/\mathbb{Q}}^{-1}.$$

Το $R_{L/K}^*$ είναι κλασματικό ιδεώδες του L. Πράγματι, και πάλι το μόνο που χρειάζεται να αποδείξουμε είναι ότι $\alpha \in R_{L/K}^*$, τότε και το $\alpha R_L \subset R_{L/K}^*$, το οποίο προφανώς ισχύει.

Αφού τώρα $R_{L/K}^*$ ιδεώδες που περιέχει το R_L το αντίστροφό του είναι ένα κύριο ιδεώδες το οποίο θα συμβολίζουμε ως $\mathrm{Diff}_{L/K}$, δηλαδή $\mathrm{Diff}_{L/K} = (R_{L/K}^*)^{-1}$. Η συνάρτηση ίχνος είναι K-γραμμική. Επομένως ισχύει

$$\mathrm{Tr}_{L/K}(Q) \subset A \Leftrightarrow A^{-1}\mathrm{Tr}_{L/K}(Q) \subset R_K \Leftrightarrow \mathrm{Tr}_{L/K}(A^{-1}Q) \subset R_K.$$

Τέλος, όπως και στην απόλυτη περίπτωση το $R_{L/K}^*$ είναι το μέγιστο κλασματικό ιδεώδες του R_L του οποίου τα στοιχεία έχουν σχετική norm στον δακτύλιο R_K. Επομένως, αφού $R_{L/K}^* = \mathrm{Diff}_{L/K}^{-1}$, ισχύει $\mathrm{Tr}_{L/K}(A^{-1}Q) \subset R_K \Leftrightarrow A^{-1}Q \subset \mathrm{Diff}_{L/K}^{-1}$. □

Ορισμός Χ.3.22. Το ακέραιο ιδεώδες του L, $\mathrm{Diff}_{L/K}$ λέγεται σχετική διαφορίζουσα της επέκτασης L/K. (Η $N_{L/K}(\mathrm{Diff}_{L/K}) = \mathcal{D}_{L/K}$ είναι η σχετική διακρίνουσα της επέκτασης).

Πρόταση Χ.3.23 (Μεταβατικότητα της διαφορίζουσας και τις διακρίνουσας)**.** *Αν* L/K *και* M/L *επεκτάσεις αλγεβρικών σωμάτων αριθμών, τότε*

$$\mathrm{Diff}_{M/K} = \mathrm{Diff}_{L/K}\mathrm{Diff}_{M/L} \text{ και } \mathcal{D}_{M/K} = (\mathcal{D}_{L/K})^{[M:L]}N_{L/K}(\mathcal{D}_{M/L}).$$

Απόδειξη. Θα αποδείξουμε ότι

$$\mathrm{Diff}^{-1}_{M/L} = \mathrm{Diff}_{L/K}\mathrm{Diff}^{-1}_{M/K},$$

με εφαρμογή της προηγούμενης πρότασης στις επεκτάσεις M/L, L/K και M/K, ότι και τα δύο μέλη της ισότητας περιέχουν ακριβώς τα ίδια κλασματικά ιδεώδη του L.

Το

$$Q \subset \mathrm{Diff}^{-1}_{M/L} \Leftrightarrow \mathrm{Tr}_{M/L}(Q) \subset R_L \Leftrightarrow \mathrm{Tr}_{M/L}(\mathrm{Diff}^{-1}_{L/K}Q) \subset \mathrm{Diff}^{-1}_{L/K}.$$

Η τελευταία σχέση του περιέχεσθαι είναι ισοδύναμη με την $\mathrm{Tr}_{M/K}(\mathrm{Diff}^{-1}_{L/K}Q) \subset R_K$ και αυτή ισοδύναμη με την $\mathrm{Diff}^{-1}_{L/K}Q \subset \mathrm{Diff}^{-1}_{M/K}$, δηλαδή $Q \subset \mathrm{Diff}_{L/K}\mathrm{Diff}^{-1}_{M/K}$. Αποδείξαμε τη μεταβατικότητα της διαφορίζουσας.

Τώρα

$$\begin{aligned}\mathcal{D}_{M/K} &= N_{M/K}(\mathrm{Diff}_{M/K}) = N_{M/K}(\mathrm{Diff}_{L/K}\mathrm{Diff}_{M/K}) = N_{M/K}(\mathrm{Diff}_{L/K})N_{M/K}(\mathrm{Diff}_{M/L})\\ &= N_{L/K}(N_{M/K}(\mathrm{Diff}_{L/K}))N_{L/K}(N_{M/L}(\mathrm{Diff}_{M/L})) = N_{L/K}(\mathrm{Diff}^{[M:L]}_{L/K})N_{L/K}(\mathcal{D}_{M/L})\\ &= \mathcal{D}^{[M:L]}_{L/K}N_{L/K}(\mathcal{D}_{M/L}).\end{aligned}$$

□

Παρατήρηση Χ.3.24. Σύμφωνα με τις προτάσεις Χ.3.18 και Χ.3.23, κάθε υπόσωμα K ενός αλγεβρικού σώματος αριθμών L δηλώνει την παρουσία του μέσω ενός παράγοντα στην απόλυτη διακρίνουσα $D_{L/\mathbb{Q}}$ του L, συγκεκριμένα τον παράγοντα $D^{[L:K]}_{K/\mathbb{Q}}$.

Παράδειγμα Χ.3.25. Το πολυώνυμο

$$f(x) = x^4 - 2x^3 + x^2 + 1 \in \mathbb{Q}[x]$$

είναι ανάγωγο υπεράνω του $\mathbb{Q}$ και έχει διακρίνουσα $D(f(x)) = 272 = 2^4 \cdot 17$. Επομένως και η τάξη $\mathbb{Z}[\alpha]$ όπου α ρίζα του $f(x)$ έχει διακρίνουσα ίση με $2^4 \cdot 17$. Το $f(x) = (x^2 - x - i)(x^2 - x + i)$. Επομένως το σώμα $L = \mathbb{Q}(\alpha)$, περιέχει και το $\alpha^2 - \alpha = i$, δηλαδή το L περιέχει το τετραγωνικό σώμα $K = \mathbb{Q}(i)$ το οποίο έχει διακρίνουσα $D_K = -4$. Επομένως από τον τελευταίο τύπο το $4^2 \mid D_{L/\mathbb{Q}}$. Αυτό σημαίνει ότι η τάξη $\mathbb{Z}[\alpha]$ έχει δείκτη 1 στον R_L. Επομένως $R_L = \mathbb{Z}[\alpha]$, και $D_{L/\mathbb{Q}} = 272$.

Πρόταση Χ.3.26 (Μικρό θεώρημα της διαφορίζουσας)**.** *Έστω* L/K *επέκταση αλγεβρικών σωμάτων αριθμών και* R_K, R_L *οι αντίστοιχοι δακτύλιοι των ακέραιων αλγεβρικών αριθμών. Έστω* Q *ένα πρώτο ιδεώδες του* L *και* $P = Q \cap K$. *Τότε ισχύει το*

$$Q^{e-1} \mid \mathrm{Diff}_{L/K}, \text{ όπου } e := e(Q/P).$$

Απόδειξη. Σύμφωνα με την πρόταση Χ.3.21, αρκεί να δείξουμε ότι $\mathrm{Tr}_{L/K}(QA) \subset P$. Πράγματι, η σχέση αυτή είναι ισοδύναμη προς την $QA \subset P\mathrm{Diff}^{-1}_{L/K}$ και από αυτή προκύπτει ότι

$$\mathrm{Diff}_{L/K} \subset PR_LQ^{-1}A^{-1} = Q^{e-1},$$

δηλαδή $Q^{e-1} \mid \mathrm{Diff}_{L/K}$.

Έστω $\widetilde{K}$ η κανονική θήκη της επέκτασης L/K, $R_{\widetilde{K}}$ ο δακτύλιος των ακεραίων αλγεβρικών του $\widetilde{K}$ και $\sigma_1, \sigma_2, \dots, \sigma_n$ ένα πλήρες σύστημα αντιπροσώπων των συμπλόκων $\sigma\mathrm{Gal}(\widetilde{K}/L)$ της ομάδας $\mathrm{Gal}(\widetilde{K}/K)$. Το σχετικό ίχνος ενός στοιχείου $\alpha \in L$ είναι

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha).$$

Έστω $p \in \mathbb{P}$, $p\mathbb{Z} = P \cap \mathbb{Q}$. Για όλα τα $\beta \in R_L$ ισχύει η ισοτιμία

$$\mathrm{Tr}_{L/K}(\beta)^p \equiv \mathrm{Tr}_{L/K}(\beta^p) \mod p.$$

Αυτό ισχύει επειδή η διαφορά τους ανήκει στο $pR_{\widetilde{K}} \cap K \subset P$. Επαγωγικά ισχύει

$$\mathrm{Tr}_{L/K}(\alpha)^{p^N} \equiv \mathrm{Tr}_{L/K}(\alpha^{p^N}) \mod P,$$

ειδικά και για όλα τα $\alpha \in QA$ και $N \in \mathbb{N}$. Τώρα, αν $N \geq e$ ισχύει

$$\alpha^{p^N} \in Q^{p^N} A^{p^N} \subset Q^e A = PR_L \subset PR_{\widetilde{K}}.$$

Επειδή η επέκταση $\widetilde{K}/K$ είναι Galois έχουμε $\sigma_j(\alpha^{p^N}) \in PR_{\widetilde{K}}$, για κάθε $j = 1, 2, \dots, n$. Επομένως και το ίχνος

$$\mathrm{Tr}_{L/K}(\alpha^{p^N}) = \mathrm{Tr}_{L/K}(\alpha)^{p^n} \in PR_{\widetilde{K}} \cap K = P.$$

Αλλά το P είναι πρώτο ιδεώδες. Συνεπώς $\mathrm{Tr}_{L/K}(\alpha) \in P$ και αυτό για όλα τα $\alpha \in QA$, δηλαδή $\mathrm{Tr}_{L/K}(QA) \subset P$. □

X.3.3 Η διαφορίζουσα μιας μονογενούς τάξης

Στη συνέχεια θα υπολογίζουμε τη δυϊκή βάση μιας μονογενούς τάξης $R_K[\alpha]$ του L, όπου α πρωταρχικό στοιχείο της επέκτασης L/K.

Πρόταση X.3.27. *Έστω α ένα πρωταρχικό στοιχείο της διαχωρίσιμης επέκτασης L/K, $[L : K] = n$ και $f(x) = \mathrm{Irr}(\alpha, K)$. Η δυϊκή ως προς το ίχνος $\mathrm{Tr}_{L/K}$ βάση της βάσης $\{\alpha^k : 0 \leq k \leq n-1\}$ είναι η $\{\frac{\beta_i}{f'(\alpha)} : 0 \leq i \leq n-1\}$. Οι αριθμητές β_i είναι οι συντελεστές του πολυωνύμου*

$$\frac{f(x)}{x - \alpha} = \sum_{i=0}^{n-1} \beta_i x^i.$$

Απόδειξη. Έστω M ένα σώμα ανάλυσης του πολυωνύμου $f(x) \in K[x]$, το οποίο περιέχει το σώμα L. Εξ ορισμού, όλες οι ρίζες του πολυωνύμου $f(x)$, έστω $\alpha_1, \alpha_2, \dots, \alpha_n$, ανήκουν στο M. Μια όμορφη ταυτότητα του Euler είναι η

$$\sum_{j=1}^{n} \frac{1}{f'(\alpha_j)} \frac{f(x)}{x - \alpha_j} = 1.$$

Και τα δύο μέλη της ισότητας είναι πολυώνυμα βαθμού $< n$ και έχουν ίσες n τιμές, για $\alpha_1, \alpha_2, \dots, \alpha_n$. Ανάλογα, σύμφωνα με το ίδιο επιχείρημα ισχύουν

$$\sum_{j=1}^{n} \frac{\alpha_k^k}{f'(\alpha_j)} \cdot \frac{f(x)}{x - \alpha_j} = x^k, \text{ για κάθε } k, 0 \leq k \leq n-1.$$

Οι K-μονομορφισμοί του L στο M, σ_j, $j = 1, 2, \dots, n$ δίνουν $\sigma(\alpha) = \alpha_j$. Επομένως,

$$\sum_{j=1}^{n} \sum_{i=0}^{n-1} \sigma_j(\alpha^k) \sigma_j\left(\frac{\beta_i}{f'(\alpha)}\right) x^i = x^k, 0 \leq k \leq n-1.$$

Αν τώρα συγκρίνουμε τους συντελεστές του x^i και στις δύο πλευρές, έχουμε

$$\sum_{j=1}^{n} \sigma_j \left(\frac{\alpha^k \beta_i}{f'(\alpha)} \right) = \mathrm{Tr}_{M/K} \left(\frac{\alpha^k \beta_i}{f'(\alpha)} \right) = \delta_{ik}, 0 \leq i, k \leq n-1.$$

□

Θεώρημα Χ.3.28. *Έστω* L/K *επέκταση αλγεβρικών σωμάτων αριθμών* $[L : K] = n$ *και* R_K, R_L *οι αντίστοιχοι δακτύλιοι των ακεραίων αλγεβρικών αριθμών. Για κάθε πρωταρχικό ακέραιο στοιχείο* α *της επέκτασης* L/K *έχουμε την τάξη* $R_K[\alpha]$ *του* L. *Το*

$$R_K[\alpha]^* := f'(\alpha)^{-1} R_K[\alpha],$$

όπου $f(x) := \mathrm{Irr}(\alpha, K)$. *Επίσης το κύριο ιδεώδες*

$$\langle f'(\alpha) \rangle = f'(\alpha) R_L = \mathrm{Diff}_{L/K} \cdot \mathfrak{F},$$

όπου $\mathrm{Diff}_{L/K}$ *η σχετική διαφορίζουσα της* L/K *και* $\mathfrak{F}$ *ο οδηγός (conductor, Führer) της τάξης* $R_K[\alpha]$ *στο* R_L.

Σημείωση Χ.3.29. Ο ορισμός του $\mathfrak{F}$ είναι

$$\mathfrak{F} = \mathfrak{F}_{R_K[\alpha]} = \{\alpha \in R_L : \alpha R_L \subset R_K[\alpha]\}$$

και είναι το μεγαλύτερο ιδεώδες του R_L που περιέχεται στο $R_K[\alpha]$.

Απόδειξη. (του θεωρήματος) Το σύνολο $\{\alpha^i : 0 \leq i \leq n-1\}$ είναι μια K-βάση του σώματος L. Επομένως το $R_K[\alpha]$ είναι ένα δικτυωτό του L. Σύμφωνα με την προηγούμενη πρόταση

$$R_K[\alpha]^* = f'(\alpha)^{-1} \sum_{i=0}^{n-1} \beta_i R_K.$$

Αρκεί επομένως να αποδείξουμε ότι

$$\sum_{i=0}^{n-1} \beta_i R_K = R_K[\alpha].$$

Αφού $\alpha \in R_L$, έπεται ότι $f(x) \in R_K[x]$, οπότε από την ταυτότητα

$$f(x) = (x - \alpha) \sum_{i=0}^{n-1} \beta_i x^i = \beta_{n-1} x^n + \sum_{m=1}^{n-1} (\beta_{m-1} - \alpha \beta_m) x^m + \alpha \beta_0$$

προκύπτει ότι, εκτός από το $\beta_{n-1} = 1$ και τα $\beta_{m-1} - \alpha\beta_m \in R_K$ για $m = 1, \ldots, n-1$. Συνεπώς και το $B_{m-1} \in R_K$ για $m = n, n-1, \ldots, 1$, οπότε το

$$B := \sum_{i=0}^{n-1} \beta_i R_K \subset R_K[\alpha].$$

Επιπλέον το $1 \in \beta_{n-1} R_K$ και επαγωγικά

$$\alpha^j \in \sum_{i=n-j-1}^{n-1} \beta_i R_K, \text{ για } j = 1, 2, \ldots, n-1$$

δηλαδή $R_K[\alpha] \subset B$, συνεπώς και η ισότητα.

Για το δεύτερο μέρος: Από τη σχέση $R_K[\alpha] \subset R_L$ έπεται ότι

$$\mathrm{Diff}_{L/K}^{-1} = R_{L/K}^* \subset R_K[\alpha]^* = f'(\alpha)^{-1}R_K[\alpha]$$

και

$$\mathrm{Diff}_{L/K}^{-1} \subset f'(\alpha)^{-1}R_L$$

δηλαδή

$$f'(\alpha)R_L \subset \mathrm{Diff}_{L/K} \Rightarrow \mathrm{Diff}_{L/K} \mid \langle f'(\alpha)\rangle.$$

Επομένως,

$$\langle f'(\alpha)\rangle = f'(\alpha)R_L = \mathrm{Diff}_{L/K}\cdot\mathfrak{F},$$

όπου $\mathfrak{F}$ είναι το ιδεώδες

$$\mathfrak{F} = \mathrm{Diff}_{L/K}^{-1}f'(\alpha)R_L = R_{L/K}^*f'(\alpha), (R_L \subset R_{L/K}^*)$$

και

$$\mathfrak{F} = R_{L/K}^*f'(\alpha) \subset f'(\alpha)R_K[\alpha]^* = R_K[a].$$

Αποδείξαμε ότι το $\mathfrak{F}$ είναι ένα ιδεώδες του L που περιέχεται στην τάξη $R_K[\alpha]$. Για να αποδείξουμε ότι είναι ο οδηγός αρκεί να αποδείξουμε ότι είναι το μεγαλύτερο. Έστω λοιπόν A ένα ιδεώδες του R_L το οποίο περιέχεται στην τάξη $R_K[\alpha]$.

$$A \subset R_K[\alpha] \Leftrightarrow f'(\alpha)^{-1}R_K[\alpha] = R_K[a]^* \subset A^*.$$

Το A είναι ιδεώδες του R_L και περιέχεται στο $R_K[A]$. Αν λοιπόν πολλαπλασιάσουμε και τα δύο μέλη της τελευταίας ισότητας με A, προκύπτει

$$f'(\alpha)R_K[\alpha]A = f'(\alpha)^{-1}A \subset A^*A = \mathrm{Diff}_{L/K}^{-1}.$$

Σύμφωνα με την πρόταση X.3.27 $A^*A = \mathrm{Diff}_{L/K}^{-1}$. Επομένως $A \subset f'(\alpha)\mathrm{Diff}_{L/K}^{-1} = \mathfrak{F}$.

□

X.3.4 Το δεύτερο θεώρημα του Dedekind

Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών και $\alpha \in L$. Η διαφορίζουσα του στοιχείου α ως προς το σώμα K ορίζεται μέσω του χαρακτηριστικού πολυωνύμου του α, $\chi_{\alpha,L/K}(x)$:

$$\delta(\alpha) = \delta_{L/K}(\alpha) = \chi'_{\alpha,L/K}(\alpha).$$

Από τον ορισμό είναι φανερό ότι

$$\delta_{L/K}(\alpha) \neq 0 \Leftrightarrow \text{ το } \alpha \text{ είναι πρωταρχικό στοιχείο της επέκτασης } L/K, L = K[\alpha].$$

Θεώρημα X.3.30 (2ο Θεμελιώδες θεώρημα του Dedekind)**.** *Έστω* L/K *επέκταση αλγεβρικών σωμάτων αριθμών,* R *και* S *οι δακτύλιοι των ακεραίων αλγεβρικών αριθμών των* K *και* L *αντίστοιχα. Η διαφορίζουσα* $\mathrm{Diff}_{L/K}$ *της επέκτασης* L/K *είναι ο μέγιστος κοινός διαιρέτης όλων των ιδεωδών που παράγεται από τις διαφορίζουσες όλων των στοιχείων* $\alpha \in S$

$$\mathrm{Diff}_{L/K} = \sum_{\alpha\in S}\delta_{L/K}(\alpha)S$$

Απόδειξη. Αν $\alpha \in S$ και α πρωταρχικό στοιχείο της L/K, τότε αν $f(x) = \mathrm{Irr}(\alpha, K)$ ισχύει

$$\langle f'(\alpha)\rangle = \mathrm{Diff}_{L/K} \cdot \mathfrak{F}_{R[\alpha]}.$$

Επειδή το α είναι πρωταρχικό της επέκτασης L/K, το πολυώνυμο $f(x)$ ταυτίζεται με το χαρακτηριστικό $\chi_{\alpha,L/K}(x)$. Επομένως, ισχύει

$$\langle \delta_{L/K}(\alpha)\rangle = \mathrm{Diff}_{L/K} \cdot \mathfrak{F}_{R[\alpha]}.$$

Συνεπώς $\mathrm{Diff}_{L/K} \mid \langle \delta_{L/K}(\alpha)\rangle$, για κάθε πρωταρχικό α, $\alpha \in S$. Επομένως για να αποδείξουμε το θεώρημα αρκεί να αποδείξουμε ότι:

Λήμμα Χ.3.31. *Για κάθε πρώτο ιδεώδες Q του S υπάρχει ένα πρωταρχικό $\alpha \in S$, για το οποίο ισχύει $Q \nmid \mathfrak{F}_{R[\alpha]}$.*

Κατ' αρχή θα αποδείξουμε το εξής: Αν A ένα ιδεώδες του S, τότε σε κάθε κλάση $a + A$, $a \in S$ περιέχεται ένα τουλάχιστο πρωταρχικό στοιχείο της επέκτασης L/K. Προφανώς, το $A \cap R$ είναι διάφορο του κενού. Επομένως, το $A \cap R$ είναι ένα ιδεώδες του R και έχει άπειρο πλήθος στοιχείων. Η επέκταση όμως L/K περιέχει πεπερασμένο πλήθος ενδιάμεσων σωμάτων. Για κάθε α της κλάσης που θεωρήσαμε για την οποία ο βαθμός $[K[\alpha] : K]$ είναι μέγιστος, έχουμε $L = K(\alpha)$. Η απόδειξη είναι ανάλογη αυτής της θεωρίας σωμάτων.

Θεωρούμε ένα $\beta \in S$ και το σώμα $K(\alpha+\beta a)$ με $a \in A \cap R$. Υπάρχουν τουλάχιστο δύο $a_1, a_2 \in A \cap R$, $a_1 \neq a_2$ για τα οποία ισχύουν

$$L_1 = K(\alpha + \beta a_1) = K(\alpha + \beta a_2).$$

Το στοιχείο $(\alpha + \beta a_1) - (\alpha + \beta a_2) = \beta(a_1 - a_2) \in L_1$ και αφού $a_1 \neq a_2$ έχουμε $\beta \in L_1$ οπότε και το $\alpha \in L_1$. Σύμφωνα με την επιλογή του α ισχύει $L_1 = K(\alpha)$. Επομένως το $\beta \in K(\alpha)$, για κάθε $\beta \in S$, δηλαδή τελικά $L = K(\alpha)$. Στη συνέχεια θα αποδείξουμε το λήμμα Χ.3.31. Έστω Q κάποιο πρώτο ιδεώδες του S και $p \in \mathbb{P}$, $p \in Q$. Επομένως $pS = Q^e A$, όπου A ιδεώδες $Q \nmid A$ και $e \geq 1$. Αν μας δοθεί μια κλάση $\theta_1 + Q^2$, όπου το θ_1 είναι μια πρωταρχική ρίζα modulo Q, τότε υπάρχει ένα θ στην κλάση για το οποίο ισχύει

$$\theta^{N_{L/\mathbb{Q}}(Q)} - \theta \in Q \backslash Q^2.$$

Πράγματι, αν το θ_1 είχε την ζητούμενη ιδιότητα, τελειώσαμε. Αν όχι, τότε $\theta_1^{N_{L/\mathbb{Q}}(Q)} - \theta_1 \in Q^2$. Για κάθε $\alpha \in Q \backslash Q^2$ ισχύει

$$(\theta_1 + \alpha)^{N_{L/\mathbb{Q}}(Q)} \equiv \theta_1^{N_{L/\mathbb{Q}}(Q)} \equiv \theta_1 \mod Q^2 \neq \theta_1 + \alpha \mod Q^2.$$

Αν εφαρμόσουμε το κινέζικο θεώρημα υπολοίπων έχουμε στην κλάση $\theta + Q^2$, ένα στοιχείο θ_0 με $\theta_0 \equiv 0 \mod A$. Σύμφωνα με τα παραπάνω, υπάρχει ένα στοιχείο $\alpha \in \theta_0 + Q^2 A$, το οποίο είναι πρωταρχικό της επέκτασης L/K, δηλαδή $L = K(\alpha)$. Ο ισχυρισμός μας ότι $\mathfrak{F}_{R[\alpha]} + Q = S$, θα έχει αποδειχθεί, αν αποδείξουμε ότι υπάρχει ένα $y \in S$, ώστε το ιδεώδες yS να είναι πρώτο προς το Q και να ισχύει $yS \in R[\alpha]$. Το σύνολο

$$\Sigma_Q = \{0, \alpha, \alpha^2, \ldots, \alpha^{N_{L/\mathbb{Q}}(Q)-1}\}$$

είναι πλήρες σύστημα αντιπροσώπων των κλάσεων υπολοίπων modulo Q και το στοιχείο

$$\pi := \alpha^{N_{L/\mathbb{Q}}(Q)} - \alpha \in Q \backslash Q^2$$

και $\pi \in R[\alpha]$. Τότε σύμφωνα με την πρόταση VII.3.4 για κάθε φυσικό αριθμό m το σύνολο των αθροισμάτων

$$\sum_{i=0}^{m-1} \gamma_i \pi^i : \gamma_i \in \Sigma_Q$$

αποτελεί ένα πλήρες σύστημα αντιπροσώπων των κλάσεων υπολοίπων modulo Q^m. Επομένως η τάξη $R[\alpha]$ περιέχει ένα πλήρες σύστημα υπολοίπων των κλάσεων του S modulo Q^m για κάθε φυσικό αριθμό m.

Παραγοντοποιούμε την norm $N := N_{L/\mathbb{Q}}(\delta(\alpha))$ στη μορφή

$$N = p^k b, k \in \mathbb{N}, b \in \mathbb{Z}\backslash p\mathbb{Z}$$

και θέτουμε $y = \alpha^k b$. Το $\alpha \in \theta_0 + Q^2 A$ και $\theta_0 \in A$, δηλαδή $\alpha \in A$ και επομένως είναι πρώτο προς το Q. Απομένει ακόμη να δείξουμε ότι

$$yS \subset R[\alpha].$$

Το χαρακτηριστικό πολυώνυμο του $\delta(\alpha)$ υπεράνω του $\mathbb{Q}$ $\chi_{\delta(\alpha),L/\mathbb{Q}}(x) \in \mathbb{Z}[x]$, έχει ρίζα του το $\delta(\alpha)$. Επομένως ο σταθερός όρος ο οποίος είναι $\pm N$ ανήκει στο ιδεώδες $\langle\delta(\alpha)\rangle = \delta(\alpha)S$. Από το προηγούμενο θεώρημα όμως ισχύει

$$\langle\delta(\alpha)\rangle = \delta(\alpha)S = \mathrm{Diff}_{L/K}\mathfrak{F}_{R[x]} \subset R[\alpha], (\alpha \in S).$$

Επιλέγουμε ένα m, $m \geq ek$. Για κάθε $x \in S$ υπάρχει ένας αντιπρόσωπος $\beta \in R[\alpha]$ ώστε $x - \beta \in Q^m$. Επομένως $(x-\beta)y = (x-\beta)\alpha^k b$. Το $x - \beta \in Q^m \subset Q^{ek}$ και το $\alpha^k \in A^k$. Άρα το

$$(x-\beta)y = (x-\beta)\alpha^k b \in Q^{ek}A^k b = (Q^e A)^k b = (p^k b)S = NS.$$

Τέλος $NS \subset R[\alpha]$, αφού $N \in \langle\delta(\alpha)\rangle = \delta(\alpha)S$ και $\alpha \in S$. Το $\beta \in R[\alpha]$, το $y \in R[\alpha]$ και $xy - \beta y \in R[\alpha]$. Συνεπώς $xy \in R[\alpha]$ για όλα τα $x \in S$, δηλαδή $yS \subset R[\alpha]$. □

Πόρισμα X.3.32. *Υποθέτουμε ότι K_1, K_2 είναι πεπερασμένες επεκτάσεις ένος αλγεβρικού σώματος αριθμών K και είναι υποσώματα ενός σώματος $\overline{K}$. Αν $L = K_1K_2$ και P ένα πρώτο ιδεώδες του K, τότε*

$$P \mid \mathcal{D}_{L/K} \Leftrightarrow P \mid \mathcal{D}_{K_1/K} \text{ είτε } P \mid \mathcal{D}_{K_2/K}.$$

Απόδειξη. Από την πρόταση X.3.23 έπεται ότι $\mathcal{D}_{K_1/K} \mid \mathcal{D}_{L/K}$ και $\mathcal{D}_{K_2/K} \mid \mathcal{D}_{L/K}$. Επομένως, αν P διαιρεί τη διακρίνουσα $\mathcal{D}_{K_1/K}$ είτε τη διακρίνουσα $\mathcal{D}_{K_2/K}$, τότε θα διαιρεί και την $\mathcal{D}_{L/K}$.

Αντίστροφα, έστω $P \mid \mathcal{D}_{L/K}$ και $P \nmid \mathcal{D}_{K_1/K}$. Θα αποδείξουμε ότι τότε, κατ' ανάγκη $P \mid \mathcal{D}_{K_2/K}$. Από την υπόθεση $P \mid \mathcal{D}_{L/K}$ έπεται ότι υπάρχει ένα πρώτο ιδεώδες Q του L, $Q \cap K = P$ το οποίο διαιρεί τη διαφορίζουσα $\mathrm{Diff}_{L/K}$. Το Q δεν διαιρεί το ιδεώδες $\mathrm{Diff}_{K_1/K}R_L$, αφού το P δεν διαιρεί το $N_{K_1/K}(\mathrm{Diff}_{K_1/K})$. Από την ισότητα

$$\mathrm{Diff}_{L/K} = \mathrm{Diff}_{K_1/K}\mathrm{Diff}_{K_2/K}$$

προκύπτει ότι $Q \mid \mathrm{Diff}_{L/K_1}$.

Έστω τώρα α ένα πρωταρχικό στοιχείο της επέκτασης K_2/K. Το $L = K_1K_2 = K_1K(\alpha) = K_1(\alpha)$, δηλαδή το α είναι και πρωταρχικό στοιχείο της επέκτασης L/K_1.

Έστω $f(x) = \mathrm{Irr}(\alpha, K)$ και $g(x) = \mathrm{Irr}(\alpha, K_1)$ εξ ορισμού το $\alpha \in R_L$ οπότε και οι συντελεστές των πολυωνύμων $f(x), g(x)$ ανήκουν στους δακτυλίους R_K και R_{K_1} αντίστοιχα. Το $g(x) \mid_{R_{K_1}} f(x)$, επομένως

$$f(x) = g(x)h(x), \text{ με } h(x) \in R_{K_1}[x].$$

Συνεπώς $f'(\alpha) = g'(\alpha)h(\alpha) \in \langle g'(\alpha)\rangle = g'(\alpha)L$. Σύμφωνα με το θεώρημα X.3.30

$$g'(\alpha)L \subset \mathrm{Diff}_{L/K_1} \text{ και } \mathrm{Diff}_{L/K_1} \subset Q,$$

αφού $Q \mid \mathrm{Diff}_{L/K_1}$. Επομένως

$$\delta_{K_2/K}(\alpha) = f'(\alpha) \in Q \cap K_2,$$

για όλα τα πρωταρχικά στοιχεία α της K_2/K. Από το θεώρημα Χ.3.30, έπεται ότι η διαφορίζουσα $\mathrm{Diff}_{K_2/K}$ της επέκτασης K_2/K διαιρείται από το πρώτο ιδεώδες $Q \cap K_2$, κάτι το οποίο συνεπάγεται ότι η σχετική norm

$$N_{K_2/K}(\mathrm{Diff}_{K_2/K}) = \mathcal{D}_{K_2/K}$$

διαιρείται από το P.

□

Παρατήρηση Χ.3.33. Επειδή θα τα χρειαστούμε στην επόμενη παράγραφο, από την απόδειξη έχουμε:

Για κάθε πρώτο ιδεώδες Q του L υπάρχει ένα πρωταρχικό στοιχείο α, $\alpha \in S$ της επέκτασης L/K με τις ιδιότητες:

1. Ο οδηγός $\mathfrak{F}_{R[\alpha]}$ είναι πρώτος προς το Q,
2. Το $\alpha \in A$, όπου $pS = Q^e A$ με $Q \cap \mathbb{Q} = p\mathbb{Z}$ και $Q \nmid A$.
3. Για κάθε φυσικό αριθμό m η τάξη $R[\alpha]$ περιέχει ένα πλήρες σύστημα αντιπροσώπων των κλάσεων υπολοίπων του S modulo Q^m.

Χ.3.5 Το τρίτο θεμελιώδες θεώρημα του Dedekind

Στην παράγραφο αυτή θα μελετήσουμε τον εκθέτη των πρώτων ιδεωδών του L που εμφανίζονται στην ανάλυση της (σχετικής) διακρίνουσας $\mathcal{D}_{L/K}$ σε γινόμενο πρώτων ιδεωδών. Αυτό θα γίνει σε πρώτο βήμα για επεκτάσεις Galois και στη συνέχεια στη γενική περίπτωση. Εδώ υπεισέρχεται και η θεωρία διακλαδώσεων του Hilbert.

Ορισμός Χ.3.34. Για ένα ιδεώδες A του δακτυλίου R_K του αλγεβρικού σώματος αριθμών K, και Q ένα πρώτο ιδεώδες του R_K ορίζουμε ως $\nu_Q(A) \in \mathbb{N}$ τον εκθέτη του Q στη μονοσήμαντη ανάλυση του A ως γινόμενο πρώτων ιδεώδων.

Θεώρημα Χ.3.35. *Υποθέτουμε ότι η L/K είναι μια Galois επέκταση αλγεβρικών σωμάτων αριθμών, R και S οι δακτύλιοι των ακέραιων αλγεβρικών αριθμών αντίστοιχα, Q ένα πρώτο ιδεώδες του S και $P = Q \cap R$. Με G_{-1} θα συμβολίζουμε την ομάδα ανάλυσης $G_Z(Q/P)$ και G_n, $n \neq 0$ οι αντίστοιχες ομάδες διακλαδώσεων (G_0 είναι η ομάδα αδράνειας), τότε:*

$$\nu_Q(\mathrm{Diff}_{L/K}) = \sum_{n=0}^{\infty} (n+1)|G_n \backslash G_{n+1}| = \sum_{n=0}^{\infty} (|G_n| - 1)$$

Απόδειξη. Έστω α όπως στην προηγούμενη παρατήρηση, $L = K(\alpha)$, $PS = Q^e A$, $\alpha \in A$ και $Q \nmid \mathfrak{F}_{R[\alpha]}$. Έστω

$$\chi_{\alpha,L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (x - \sigma(\alpha))$$

το χαρακτηριστικό πολυώνυμο του α. Το διαφορικό του α είναι

$$\delta_{L/K}(\alpha) = \chi'_{\alpha,L/K}(\alpha) = \prod_{\substack{\sigma \in \mathrm{Gal}(L/K) \\ \sigma \neq \mathrm{Id}_L}} (\alpha - \sigma(\alpha)).$$

Από τη σχέση $\langle \delta_{L/K}(\alpha) \rangle = \mathrm{Diff}_{L/K} \cdot \mathfrak{F}_{R[\alpha]}$ και το γεγονός ότι $Q \nmid \mathfrak{F}_{R[\alpha]}$, έπεται

$$\nu_Q(\mathrm{Diff}_{L/K}) = \nu_Q(\delta_{L/K}(\alpha)).$$

Συνεπώς θα πρέπει να μελετήσουμε τη συνεισφορά κάθε όρου $\alpha - \sigma(\alpha)$ στις δυνάμεις του Q ανάλογα με τα διάφορα στοιχεία της ομάδας Galois. Να σημειώσουμε όμως κατ'αρχήν ότι τα αθροίσματα είναι πεπερασμένα, αφού υπάρχει n φυσικός τέτοιος ώστε $G_n = \{\mathrm{Id}_L\}$.

Για κάθε $\sigma \in G \backslash G_{-1}$ ισχύει $\sigma^{-1}(Q) \neq Q$. Το $\sigma^{-1}(Q)$ είναι ένα πρώτο ιδεώδες του S. Αφού το $\alpha \in A$, έπεται ότι $\sigma(\alpha) \in Q$, ενώ το $\alpha \notin Q$.

Επομένως, για όλα τα στοιχεία $\sigma \in \mathrm{Gal}(L/K) \backslash G_{-1}$ έχουμε $\alpha - \sigma(\alpha) \in S \backslash Q$. Δηλαδή οι παράγοντες αυτοί δεν συνεισφέρουν κάτι στις δυνάμεις του Q.

Έστω τώρα $\sigma \in G_{-1} \backslash G_0$. Υπενθυμίζουμε ότι υπάρχει ένας ισομορφισμός

$$G_{-1}/G_0 \cong \mathrm{Gal}\left(\frac{S/Q}{R/P}\right),$$

δηλαδή κάθε αυτομορφισμός $\sigma \in G_{-1} \backslash G_0$ δρα, μη-τετριμμένα, στις κλάσεις της S/Q και έχοντας υπ' όψιν ότι για το συγκεκριμένο α που επιλέξαμε ότι η τάξη $R[\alpha]$ περιέχει ένα πλήρες σύστημα αντιπροσώπων των κλάσεων $\gamma + Q$ του Q στο S, έχουμε ότι αν $\sigma \in G_{-1}$, μόνο όταν ισχύει $\sigma(\alpha) \equiv \alpha \mod Q$ αν και μόνο αν $\sigma \in G_0$. Και πάλι έχουμε:

Για όλα τα $\sigma \in G_{-1} \backslash G_0$ ισχύει $\alpha - \sigma(\alpha) \in S \backslash Q$.

Έστω τώρα $n \geq 1$. Αν $\sigma \in G_n \backslash G_{n+1}$, έχουμε

$$\sigma(\alpha) \equiv \alpha \mod Q^{n+1} \text{ για κάθε } \alpha \in S.$$

Συνεπώς

$$\inf\{v_Q(x - \sigma(x)) : x \in S\} = n + 1.$$

Γράφουμε το $x = \beta + \gamma$ με $\beta = \sum_{i=0}^{N-1} b_i \alpha^i \in R[\alpha]$ για $\gamma \in Q^{n+2}$. Επομένως ισχύει

$$x - \sigma(x) \equiv (\beta - \sigma(\beta)) \mod Q^{n+2}$$

Η διαφορά όμως $\beta - \sigma(\beta)$, αν αντικαταστήσουμε το β με το ίσον του, παραγοντοποιείται στην τάξη $R[\alpha]$ με έναν παράγοντα το $\alpha - \sigma(\alpha)$. Επομένως

$$v_Q(\beta - \sigma(\beta)) \geq v_Q(\alpha - \sigma(\alpha))$$

από την οποία προκύπτει ότι για όλα τα $\sigma \in G_n \backslash G_{n+1}$, ισχύει

$$v_Q(\alpha - \sigma(\alpha)) = n + 1.$$

□

Παρατήρηση X.3.36.

1. Ο H. Hasse [10, σελ. 49] χρησιμοποιεί τον ορισμό του Kronecker για τη σχετική διαφορίζουσα $\mathrm{Diff}_{L/K}$, των επεκτάσεων Galois L/K για να αποφύγει τη διαδικασία του Dedekind.
2. Στη θεωρία διακλαδώσεων του Hilbert γνωρίζουμε και τις τάξεις των ομάδων G_n $n = -1, 0, 1, 2, \ldots$ Θα μπορούσαμε να τις αντικαταστήσουμε στον τύπο που διατυπώσαμε στο Θεώρημα.

Στο κεφάλαιο της Θεωρίας Διακλαδώσεων είχαμε χαρακτηρίσει το σώμα ανάλυσης και το σώμα αδράνειας ως maximal ως προς κάποια ιδιότητα. Το ίδιο θα κάνουμε τώρα για τις ομάδες διακλαδώσεως.

Πρόταση X.3.37. *Έστω L/K μια επέκταση Galois αλγεβρικών σωμάτων αριθμών με ομάδα Galois $G = \mathrm{Gal}(L/K)$. Έστω ακόμη Q ένα πρώτο ιδεώδες του K, G_m, $m \geq -1$ η ακολουθία των υποομάδων διακλάδωσης του Hilbert και K_m το σώμα σταθερών στοιχείων της G_m. Για κάθε φυσικό αριθμό $n \geq 0$ και οποιοδήποτε ενδιάμεσο σώμα K' της L/K βαθμού $[K' : K] = [K_n : K]$. Ισχύει*

$$v_Q(\mathrm{Diff}_{L/K'}) \leq v_Q(\mathrm{Diff}_{L/K_n}).$$

Μάλιστα η ισότητα ισχύει αν και μόνο αν $K' = K_n$.

Απόδειξη. Έστω $G' = \mathrm{Gal}(L/K')$. Λόγω της υπόθεσης $[K' : K] = [K_n : K]$ έπεται ότι $|G_n| = |G'|$. Η m-στή ομάδα διακλάδωσης του Q στην επέκταση L/K_n είναι

$$G_m(L/K_n) = \begin{cases} G_n, & \text{αν } m \le n \\ G_m & \text{αν } m > n \end{cases}$$

Επιπλέον ισχύει

$$|G_m \cap G'| \le \begin{cases} |G'| = |G_n|, & \text{αν } m \le n \\ |G_m|, \text{ αν } m > n. \end{cases}$$

□

Εαν λοιπόν εφαρμόσουμε το προηγούμενο θεώρημα για τις επεκτάσεις Galois L/K' και L/K_n ,έχουμε

$$\nu_Q(\mathrm{Diff}_{L/K'}) \le \nu_Q(\mathrm{Diff}_{L/K_n}).$$

Η ισότητα ισχύει όταν στις παραπάνω εκτιμήσεις ισχύουν οι ισότητες. Όταν $m = n$

$$|G_n \cap G'| = |G_n|$$

και επειδή $|G'| = |G_n|$ έχουμε $G_n = G'$, οπότε $K_n = K'$.

Θεώρημα Χ.3.38 (Τρίτο θεμελιώδες θεώρημα του Dedekind)**.** *Έστω K'/K μια επέκταση αλγεβρικών σωμάτων αριθμών με (σχετική διαφορίζουσα) $\mathrm{Diff}_{K'/K}$ και δακτυλίους των ακεραίων αλγεβρικών αριθμών R_K και $R_{K'}$. Για κάθε πρώτο ιδεώδες P' του $R_{K'}$ με $P = K \cap P'$ και δείκτη διακλαδώσεως $e = e(P'/P)$ ισχύει:*

$$\nu_{P'}(\mathrm{Diff}_{K'/K}) = e - 1, \text{ όταν } e \not\equiv 0 \mod p$$
$$\nu_{P'}(\mathrm{Diff}_{K'/K}) \ge 2, \text{ όταν } e \equiv 0 \mod p$$

Το $p\mathbb{Z} = P \cap \mathbb{Z}$. Ιδιαίτερα

$$(P' \mid \mathrm{Diff}_{L/K}) \Leftrightarrow (e(P'/P) > 1)$$

Αν πάρουμε την norm έχουμε το θεώρημα της διακρίνουσας.

Απόδειξη. Επιλέγουμε μία επέκταση Galois L/K η οποία περιέχει το K' ως ενδιάμεσο σώμα. Η επέκταση L/K' είναι επίσης Galois. Έστω $G := \mathrm{Gal}(L/K)$ και $G' := \mathrm{Gal}(L/K')$. Στον δακτύλιο των ακεραίων αλγεβρικών αριθμών S του L θεωρούμε ένα πρώτο ιδεώδες Q για το οποίο $Q \cap R_{K'} = P'$. Όπως έχουμε δει, αν G_n η n-στή ομάδα διακλαδώσεως του Q ως προς το σώμα K' είναι η $G'_n = G' \cap G_n$, $n \in \mathbb{N}$ από το θεώρημα Χ.3.35 αν $\nu_n = |G_n|$ και $\nu'_n = |G'_n|$ έχουμε

$$\nu_Q(\mathrm{Diff}_{L/K}) = \sum_{n=0}^{\infty} (\nu_n - 1)$$
$$\nu_Q(\mathrm{Diff}_{L/K'}) = \sum_{n=0}^{\infty} (\nu'_n - 1).$$

Αλλά $\mathrm{Diff}_{L/K} = \mathrm{Diff}_{L/K'}\mathrm{Diff}_{K'/K}$. Συνεπώς

$$\nu_Q(\mathrm{Diff}_{K'/K}S) = \nu_Q(\mathrm{Diff}_{L/K}) - \nu_Q(\mathrm{Diff}_{L/K'}) = \sum_{n=0}^{\infty} (\nu_n - \nu'_n).$$

Από την πολλαπλασιαστικότητα των δεικτών διακλαδώσεων, αν $e' = e(Q/P')$, τότε $ee' = e(Q/P) = \nu_0$ οπότε

$$\nu_{P'}(\mathrm{Diff}_{K'/K}) = \frac{1}{e'}\nu_Q(\mathrm{Diff}_{K'/K}S) = \frac{1}{e'}\sum_{n=0}^{\infty}(\nu_n - \nu'_n) \ge$$
$$\ge \frac{1}{e'}(\nu_0 - \nu'_0) = \frac{1}{e'}(ee' - e') = e - 1. \qquad \text{(X.7)}$$

Στη συνέχεια, έχουμε

$$ee' = |G_0| = [G_0 : G_1]|G_1|.$$

Το $p \nmid [G_0 : G_1]$. Επομένως, η πιο μεγάλη δύναμη του p που διαιρεί το ee' δίνεται μέσω του παράγοντα $|G_1|$. Ανάλογα

$$e' = |G_0'| = [G_0' : G_1']|G_1'|, p \nmid [G_0' : G_1'].$$

Συνεπώς η πιο μεγάλη δύναμη του p που διαιρεί το e' δίνεται μέσω του παράγοντα $|G_1'|$. Επομένως $p \nmid e$ αν και μόνο αν $G_1 = G_1'$. Αλλά $G_n' = G_n \cap G'$ και η ακολουθία $\{G_n\}$ είναι φθίνουσα, οπότε $G_n = G_n'$ για κάθε $n \geq 1$, δηλαδή $v_n = v_n'$ για όλα τα $n \geq 1$, οπότε ισχύει στη θέση της ανισότητας της σχέσης (X.7) η ισότητα

$$v_P(\mathrm{Diff}_{K'/K}) = e - 1.$$

□

Παρατήρηση X.3.39. Όταν το $p \mid e$, τότε είναι δυνατόν $v_{P'}(\mathrm{Diff}_{K'/K})$ να είναι μεγαλύτερη του e.

Έστω $K = \mathbb{Q}(\sqrt{10})$. Εδώ διακλαδίζονται οι πρώτοι 2 και 5. Το $\langle 2\rangle P_2^2$ και το $\langle 5\rangle = P_5^2$. Η διαφορίζουσα

$$\mathrm{Diff}_{K/\mathbb{Q}} = \langle 2\sqrt{d}\rangle = \langle 2\sqrt{10}\rangle = P_2^3 P_5.$$

Η πολλαπλότητα του P_5 στην $\mathrm{Diff}_{K/\mathbb{Q}}$ είναι $e(P_5/5) - 1 = 1$ και το $2 \mid e(P_2/2) = 2$. Όμως η πολλαπλότητα του P_2 στη διαφορίζουσα είναι $3 > e(P_2/2) = 2$.

Αφορμή για τη διαφοροποίηση αυτή αποτέλεσε ο ακόλουθος:

Ορισμός X.3.40. Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών και R, S οι δακτύλιοι των ακεραίων αλγεβρικών αντίστοιχα. Έστω Q ένα πρώτο ιδεώδες του L και

$$Q \cap K = P \text{ και } P \cap \mathbb{Z} = p\mathbb{Z}, p \in \mathbb{Z}$$

$$PS = Q^e A, Q \nmid A$$

Έστω $e = e(Q/P)$ ο δείκτης διακλαδώσεως.

- Αν $p \nmid e$, τότε η διακλάδωση λέγεται ομαλή (tame).
- Αν $p \mid e$, τότε η διακλάδωση λέγεται άγρια (wild).

Ορισμός X.3.41. Μία επέκταση αλγεβρικών σωμάτων αριθμών L/K θα λέγεται ομαλά διακλαδιζόμενη όταν κάθε πρώτο ιδεώδες Q του S είναι το πολύ ομαλά διακλαδιζόμενο, δηλαδή μη-διακλαδιζόμενη ή ομαλά διακλαδιζόμενη ως προς το πρώτο ιδεώδες $P = Q \cap K$ του R.

Στη συνέχεια θα εξετάσουμε την περίπτωση των πολυωνύμων Eisenstein.

Θεώρημα X.3.42. *Υποθέτουμε ότι το πολυώνυμο*

$$f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k \in \mathbb{Z}[x]$$

είναι πολυώνυμο Eisenstein ως προς κάποιο αριθμό p*, δηλαδή* $a_k \in p\mathbb{Z}$ $(0 \leq k \leq n-1)$ *και* $a_0 \not\equiv 0 \bmod p^2$.

Αν α *μια ρίζα του* $f(x)$*, τότε ο δακτύλιος* R_K *των ακεραίων αλγεβρικών του σώματος* $K = \mathbb{Q}(\alpha)$ *έχει ένα μοναδικό πρώτο ιδεώδες* P*, για τον οποίο* $p \in P$*. Ο βαθμός αδρανείας* $f(P/p\mathbb{Z}) = 1$.

Επομένως ισχύει $pR_K = P^n$*. Επιπλέον, ο οδηγός της τάξης* $\mathbb{Z}[\alpha]$*,* $\mathfrak{F}_{\mathbb{Z}[\alpha]}$ *δεν διαιρείται από το* P *και ιδιαίτερα το* $p \nmid [R_K : \mathbb{Z}[\alpha]]$.

Απόδειξη. Το πολυώνυμο $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$. Επομένως $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ και η norm $N_{K/\mathbb{Q}}(\alpha) = (-1)^n a_0$.

Έστω P ένα πρώτο ιδεώδες του K, $P \cap \mathbb{Z} = p\mathbb{Z}$. Το $p \mid a_k$, $0 \le k \le n-1$ και $a_k \in \mathbb{Z}$. Άρα όλα τα $a_k \in P$ $(0 \le k \le n-1)$ οπότε και το $\alpha^n \in P$ και, αφού το P πρώτο ιδεώδες, $\alpha \in P$, δηλαδή $P \mid \langle\alpha\rangle = \alpha R_K$. Αυτό σημαίνει ότι

$$\langle\alpha\rangle = P\cdots A, A \text{ ακέραιο ιδεώδες του } K.$$

Παίρνουμε την norm:

$$|a_0| = |N_{K/\mathbb{Q}}(A) = N_{K/\mathbb{Q}}(\langle\alpha\rangle) = N_{K/\mathbb{Q}}(P) \cdot N_{K/Q}(A).$$

Αλλά $p \parallel a_0$, $(\nu_P(a_0) = 1)$. Επομένως, $N_{K/\mathbb{Q}}(P) = p$ και $N_{K/\mathbb{Q}}(A) = |a_0|/p \in \mathbb{Z}\backslash p\mathbb{Z}$.

Το συμπέρασμα είναι ότι $f(P/p\mathbb{Z}) = 1$ και ότι δεν υπάρχει άλλο πρώτο ιδεώδες του K το οποίο να περιέχει τον πρώτο αριθμό p, δηλαδή $r = 1$, όποτε $pR_K = p^n$.

Η τάξη $\mathbb{Z}[\alpha]$ περιέχει το α και αν Σ_p ένα πλήρες σύστημα αντιπροσώπων modulo p, $\Sigma_p = \{0, 1, 2, \ldots, p-1\}$, τότε σύμφωνα με VII.3.4 για κάθε φυσικό $m \in \mathbb{N}$ το σύνολο

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \Sigma_p$$

αποτελεί ένα πλήρες σύστημα αντιπροσώπων του R_K modulo P^m. Η norm $N_{K/\mathbb{Q}}(f'(\alpha)) = p^k \cdot b$ με κατάλληλο $k \in \mathbb{N}$ και $b \in \mathbb{Z}\backslash p\mathbb{Z}$. Θα αποδείξουμε ότι

$$bR_K \subset \mathbb{Z}[\alpha].$$

Αυτό, όπως είδαμε και σε προηγούμενο θεώρημα, σημαίνει ότι

$$\mathfrak{F}_{\mathbb{Z}[\alpha]} + P = R_K.$$

Κάθε στοιχείο $x \in R_K$ έχει έναν αντιπρόσωπο $\beta \in \mathbb{Z}[\alpha]$ τέτοιον ώστε $x - \beta \in P^{nk} = \langle p^k\rangle = p^k R_K$. Επομένως,

$$b(x-\beta) \in p^k bR_K = N_{K/\mathbb{Q}}(f'(\alpha))R_K \subset f'(\alpha)R_K \subset \mathfrak{F}_{\mathbb{Z}[\alpha]} \subset \mathbb{Z}[\alpha].$$

Όμως το $b\beta \in \mathbb{Z}[\alpha]$, άρα και το $bx \in \mathbb{Z}[\alpha]$ για όλα τα $x \in R_K$, δηλαδή ισχύει $bR_K \subset \mathfrak{F}_{\mathbb{Z}[\alpha]}$ και συνεπώς έχουμε

$$\mathfrak{F}_{\mathbb{Z}[\alpha]} + P = R_K \Rightarrow P \nmid \mathfrak{F}_{\mathbb{Z}[\alpha]}.$$

Από

$$[R_K : \mathfrak{F}_{\mathbb{Z}[\alpha]}] = N_{K/\mathbb{Q}}(\mathfrak{F}_{\mathbb{Z}[\alpha]}) = [R_K : \mathbb{Z}[\alpha]][\mathbb{Z}[\alpha] : \mathfrak{F}_{\mathbb{Z}[\alpha]}],$$

συμπεραίνουμε και ότι $p \nmid [R_K : \mathbb{Z}[\alpha]]$. □

Του προηγούμενου θεωρήματος ισχύει και το αντίστροφο

Θεώρημα Χ.3.43. *Έστω K ένα αλγεβρικό σώμα αριθμών $[K : \mathbb{Q}] = n$ και R_K ο δακτύλιος των ακεραίων αλγεβρικών αριθμών αυτού. Υποθέτουμε ότι ένας πρώτος αριθμός p διακλαδίζεται πλήρως στο K*

$$pR_K = P^n,$$

τότε κάθε στοιχείο $\alpha \in P\backslash P^2$, είναι πρωταρχικό στοιχείο της επέκτασης $K/\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$ και το $f(x) = \mathrm{Irr}(\alpha, K)$ είναι ένα πολυώνυμο Eisenstein ως προς το πρώτο p.

Απόδειξη. Αν πάρουμε norms

$$N_{K/\mathbb{Q}}(pR_K) = N_{K/\mathbb{Q}}(P)^n \Rightarrow p^n = (N_{K/\mathbb{Q}}P)^n \Rightarrow N_{K/\mathbb{Q}}(P) = p.$$

Έστω $\alpha \in P\backslash P^2$. Επομένως $\langle\alpha\rangle = \alpha R_K = PA$ με $P \nmid A$. Γνωρίζουμε ότι το χαρακτηριστικό πολυώνυμο του α $\chi_\alpha(x)$ υπέρ του $\mathbb{Q}$ είναι μονικό, έχει βαθμό $n = [K : \mathbb{Q}]$ και συντελεστές ακέραιους αριθμούς.

θα αποδείξουμε ότι το πολυώνυμο $\chi_\alpha(x)$ είναι Eisenstein ως προς το p. Αυτό συνεπάγεται ότι είναι ανάγωγο στο $\mathbb{Q}[x]$, οπότε $K = \mathbb{Q}(\alpha)$. Έστω λοιπόν ότι

$$\chi_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, a_i \in \mathbb{Z}.$$

Η norm $N_{K/\mathbb{Q}}(\alpha) = \pm a_0$. Θα αποδείξουμε ότι $p \parallel a_0$. Η norm

$$|a_0| = |N_{K/\mathbb{Q}}(\alpha)| = N_{K/\mathbb{Q}}(\langle\alpha\rangle) = N_{K/\mathbb{Q}}(P)N_{K/\mathbb{Q}}(A) = pN_{K/\mathbb{Q}}(A).$$

Επομένως, $p \mid a_0$. Αρκεί να δείξουμε ότι $p \nmid N_{K/\mathbb{Q}}(A)$. Οι πρώτοι αριθμοί που διαιρούν την $N_{K/\mathbb{Q}}(A)$ είναι οι πρώτοι αριθμοί που προκύπτουν από τα πρώτα ιδεώδη της ανάλυσης του A, όταν πάρουμε την τομή του με το $\mathbb{Z}$. Αφού $P \nmid A$, έπεται ότι το P είναι το μοναδικό πρώτο ιδεώδες του K που διαιρεί το p, δηλαδή $p \nmid N_{K/\mathbb{Q}}(A)$.

Στη συνέχεια θα δείξουμε ότι το p διαιρεί όλα τα a_i. Υποθέτουμε ότι $n \geq 2$ και ότι για κάποιο i $(1 \leq i \leq n-1)$ έχουμε

$$a_0, a_1, \ldots, a_{i-1} \equiv 0 \mod p$$

θα αποδείξουμε ότι και $a_i \equiv 0 \mod p$. Θεωρούμε την ισότητα

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

και έχουμε

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_i\alpha^i \equiv 0 \mod pR_K \tag{X.8}$$

Από τη σχέση

$$\langle\alpha\rangle = PA \Rightarrow \langle\alpha^n\rangle = P^nA^n = \langle p\rangle A^n \subset \langle p\rangle = pR_K$$

επομένως $\alpha^n \in pR_K$. Πολλαπλασιάζουμε την (X.8) με α^{n-1-i} και λαμβάνοντας υπόψη την $\alpha^n \in pR_K$ καταλήγουμε στην

$$a_i\alpha^{n-1} \equiv 0 \mod pR_K \Rightarrow a_i\alpha^{n-1} = p\beta(\beta \in R_K) \Rightarrow N_{K/Q}(a_i\alpha^{n-1}) = N_{K/\mathbb{Q}}(p)N_{K/\mathbb{Q}}(\beta)$$

συνεπώς

$$a_i^n N_{K/\mathbb{Q}}(\alpha)^{n-1} = p^n N_{K/\mathbb{Q}}(\beta).$$

Το δεξί μέλος είναι ακέραιο πολλαπλάσιο του p^n. Το αριστερό είναι $a_i^n N_{K/\mathbb{Q}}(\alpha)^{n-1} = \pm a_i^n a_0^{n-1}$. Το $p \parallel a_0$ επομένως $p \mid a_i$. □

Παρατήρηση X.3.44. Στο θεώρημα X.3.42 είδαμε ότι το $P \nmid \mathfrak{F}_{\mathbb{Z}[\alpha]}$. Επομένως $\nu_P(\mathrm{Diff}_{K/\mathbb{Q}}) = \nu_P(\delta_{K/\mathbb{Q}}(\alpha))$ και

$$\delta_{K/\mathbb{Q}}(\alpha) = \sum_{m=1}^{n} m a_m \alpha^{m-1}.$$

Οι ν_P-τιμές των προσθετέων που είναι διάφορες του μηδενός ανήκουν σε διαφορετικές κλάσεις υπολοίπων modulo n, αφού $\nu_P(\alpha) \in n\mathbb{Z}$ για κάθε $a \in \mathbb{Z}$. Επομένως

$$\nu_P(\mathrm{Diff}_{K/\mathbb{Q}}) = \min_{1\leq m\leq n}(m - 1 + n\nu_p(ma_m))$$

Παράδειγμα X.3.45. Έστω $K = \mathbb{Q}(\sqrt[3]{2})$. Η τάξη $\mathbb{Z}[\sqrt[3]{2}] \subset R_K$. Θα αποδείξουμε με άλλο τρόπο από ότι έχουμε ήδη κάνει ότι $R_K = \mathbb{Z}[\sqrt[3]{2}]$. Η διακρίνουσα

$$D_{K/\mathbb{Q}}(\{1, \sqrt[3]{2}, \sqrt[3]{4}\}) = [R_K : \mathbb{Z}[\sqrt[3]{2}]]^2 D_{K/\mathbb{Q}} = -108 = -4 \cdot 27.$$

Οι μοναδικοί πρώτοι παράγοντες της διακρίνουσας είναι το 2 και το 3. Συνεπώς αυτοί είναι και οι πρώτοι αριθμοί υποψήφιοι για πιθανή διακλάδωση. Το $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ είναι πολυώνυμο

Eisenstein για $p = 2$ και $K = \mathbb{Q}(\sqrt[3]{2})$. Επομένως ο $p = 2$ διακλαδίζεται πλήρως στο K, $\langle 2\rangle = 2R_K = P_2^3$. Επίσης το στοιχείο $\alpha = \sqrt[3]{2} + 1$ είναι ρίζα του πολυωνύμου

$$(x-1)^3 - 2 = x^3 - 3x^2 + 3x - 3,$$

το οποίο είναι Eisenstein για $p = 3$ και $K = \mathbb{Q}(\alpha)$. Επομένως και το 3 διακλαδίζεται πλήρως στο K, $\langle 3\rangle = 3R_K = P_3^3$. Σύμφωνα με το θεώρημα Χ.3.38 $P_2^{3-1} = P_2^2$ και P_3^3 διαιρούν τη διαφορίζουσα $\mathrm{Diff}_{K/\mathbb{Q}}$, οπότε και

$$P_2^2P_3^3 \mid \mathrm{Diff}_{K/\mathbb{Q}} \Rightarrow N_{K/\mathbb{Q}}(P_2^2P_3^2) \mid N_{K/\mathbb{Q}}(\mathrm{Diff}_{K/\mathbb{Q}}) = D_{K/\mathbb{Q}} \Rightarrow 108 \mid D_{K/\mathbb{Q}}.$$

Επομένως $D_{K/\mathbb{Q}} = -108$, $R_K = \mathbb{Z}[\sqrt[3]{2}]$ και $\mathrm{Diff}_{K/\mathbb{Q}} = P_2^2P_3^3$.

Θα μπορούσαμε τη διαφορίζουσα να την υπολογίσουμε και από τον τελευταίο τύπο της παρατήρησης. Για το $f(x) = x^3 - 2$, $f'(\sqrt[3]{2}) = 3(\sqrt[3]{2})^2$ και $\nu_{P_2}(\mathrm{Diff}_{L/K}) = (3 - 1 + 3\nu_2(3)) = 2$, ενώ

$$\nu_{P_3}(\mathrm{Diff}_{L/K}) = \min_{1\le m\le 3}\{(1-1+3\nu_3(1-3)), (2-1+3\nu_3(2(-6))), (3-1+3\nu_3(3\cdot 3))\} = \min\{3,4,8\} = 3.$$

Παρατήρηση Χ.3.46. 1. Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών και R, S οι δακτύλιοι των ακέραιων αλγεβρικών αριθμών αντίστοιχα. Έστω I ένα ιδεώδες του S. Μια απεικόνιση

$$D : R_L \longrightarrow R_L/I$$

θα λέγεται I-derivation (I-παράγωγος) υπέρ το K, όταν

$$D(x+y) = D(x) + D(y)$$
$$D(xy) = xD(y) + D(x)y \text{ για όλα τα } x, y \in S$$

και $D(x) = 0$ για κάθε $x \in R$. Μια I-derivation υπεράνω του K θα λέγεται ουσιώδης (essential) όταν η εικόνα της περιέχει τουλάχιστον ένα στοιχείο το οποίο δεν είναι διαιρέτης του μηδενός. Ο A. Weil [26], διατύπωσε, χωρίς απόδειξη, ότι ένα ιδεώδες I διαιρεί τη διαφορίζουσα της L/K, $\mathrm{Diff}_{L/K}$ αν και μόνο αν υπάρχει μια ουσιώδης I-derivation υπεράνω του K. Το θέμα επεξεργάστηκαν στα τέλη της δεκαετίας του 60 οι J. Neukirch [22] και W. Narkiewicz [18]. Ο αναγνώστης μπορεί αν δει και το [19, σελ. 160-166].

2. Μετά την ανάπτυξη της θεωρίας των τοπικών σωμάτων, η πιο φυσιολογική προσέγγιση, τόσο της παραγράφου της διαφορίζουσας όσο και του θεωρήματος των Kronecker-Weber που θα αναπτύξουμε στην επόμενη παράγραφο, είναι πρώτα για τοπικά σώματα και μετά για αλγεβρικά σώματα αριθμών.

   Προτιμήσαμε εδώ την κλασική προσέγγιση. Ίσως επανέλθουμε στο θέμα σε κάποια άλλη ευκαιρία.

3. Με χρήση του τρίτου θεμελιώδους θεωρήματος του Dedekind Χ.3.38 ο E. Artin [1] επανέρχεται στο παράδειγμα του Dedekind $K = \mathbb{Q}(\theta)$, θ ρίζα του πολυωνύμου $x^3 + x^2 - 2x + 8$ και αποδεικνύει, χωρίς τη χρήση υπολογιστή,

$$f(x) \equiv (x - 149)^2(x + 299) \mod 503$$

από το οποίο προκύπτει ότι $503 = P^2Q$.

Χ.4 Το θεώρημα των Kronecker-Weber

Στην παράγραφο αυτή θα αποδείξουμε το σημαντικό θεώρημα:

Θεώρημα Χ.4.1. *Κάθε αβελιανή επέκταση του $\mathbb{Q}$ περιέχεται σε κάποιο κυκλοτομικό σώμα αριθμών.*

X.4.1 Προκαταρκτικά

Για λόγους ευκολίας στην έκφραση θα ονομάζουμε κυκλοσώματα όχι μόνο τα κυκλοτομικά σώματα $\mathbb{Q}(\zeta_m)$ αλλά και τα υποσώματά τους. Αυτό ισχύει μόνο για την παρούσα παράγραφο. Στη διαδικασία της απόδειξης επιλέγουμε έναν πρώτο αριθμό ℓ και θεωρούμε την κλάση όλων των αβελιανών αλγεβρικών σωμάτων αριθμών K στα οποία διακλαδίζεται ο πρώτος αριθμός ℓ και μόνο αυτός.

Παρατήρηση X.4.2. Αν K_1 και K_2 είναι δύο σώματα της κλάσης, τότε και η σύνθεσή τους $L = K_1K_2$ ανήκει στην κλάση αφού, όπως γνωρίζουμε, και η επέκταση $L/\mathbb{Q}$ είναι αβελιανή και μάλιστα διακλαδίζεται μόνο στο ℓ. Αυτό είναι άμεση συνέπεια του θεωρήματος της μεταφοράς της Θεωρίας Galois καθώς και του πορίσματος X.3.32. Επίσης είναι φανερό ότι αν ένα σώμα L ανήκει στην κλάση, τότε ανήκουν και τα υποσώματά του.

Έστω λοιπόν L ένα σώμα της κλάσης, $G = \mathrm{Gal}(L/\mathbb{Q})$ και $\mathcal{L}$ ένα πρώτο ιδεώδες του L, $\mathcal{L} \mid \ell$, S ο δακτύλιος των ακεραίων αλγεβρικών αριθμών αυτού. Επειδή η ομάδα G είναι αβελιανή, η ακολουθία των υποομάδων του Hilbert εξαρτάται αποκλειστικά από το ℓ και όχι από την επιλογή του ιδεώδους $\mathcal{L}$. Για λόγους ομοιομορφίας θα συμβολίζουμε επίσης με G_{-1} και G_0 τις ομάδες αναλύσης και αδράνειας. Η επέκταση $K_0/\mathbb{Q}$ όπου K_0 το σώμα αδράνειας, δηλαδή το σώμα σταθερών στοιχείων της $G_0(\mathcal{L}/\ell)$, είναι μη διακλαδιζόμενη. Σύμφωνα με το θεώρημα του Minkowski το $K = \mathbb{Q}$. Αυτό σημαίνει ότι $G = G_0$ και ότι το ℓ αναλύεται πλήρως στην επέκταση $L/\mathbb{Q}$. Στη συνέχεια θα αποδείξουμε ότι όλα τα τετραγωνικά σώματα αριθμών είναι κυκλοσώματα. Πράγματι αν $\ell \neq 2$, τότε υπάρχει μοναδικό τετραγωνικό σώμα αριθμών στο οποίο ο μοναδικός διακλαδιζόμενος πρώτος είναι ο ℓ. Αυτό είναι το $\mathbb{Q}(\sqrt{\ell^*})$, $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$. Επίσης υπάρχουν ακριβώς τρία τετραγωνικά σώματα αριθμών στα οποία διακλαδίζεται ο πρώτος $\ell = 2$ και αυτά είναι τα $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, με διακρίνουσες, αντίστοιχα $-8, -4, 8$. Και τα τρία είναι υποσώματα του $\mathbb{Q}(\zeta_8)$, αφού $\sqrt{-1} = \zeta_8^2$, $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, και $\zeta_8 = \frac{1}{2}(\sqrt{2}+\sqrt{-2})$, δηλαδή και τα τρία είναι κυκλοσώματα. Σε προηγούμενο κεφάλαιο έχουμε ήδη αποδείξει ότι το

$$\mathbb{Q}(\sqrt{\ell^*}) \subset \mathbb{Q}(\zeta_\ell).$$

Επίσης είναι γνωστό ότι η σύνθεση δύο σωμάτων

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_k),$$

όπου k είναι το ελάχιστο κοινό πολλαπλάσιο των m, n. Επομένως όλα τα τετραγωνικό σώματα αριθμών είναι κυκλοσώματα.

Πρόταση X.4.3. *Για κάθε πρώτο ℓ, $\ell \neq 2$, υπάρχει ακριβώς ένα αβελιανό σώμα αριθμών K βαθμού $[K : Q] = \ell$, στο οποίο ο μοναδικός διακλαδιζόμενος πρώτος αριθμός είναι ο ℓ. Μάλιστα το σώμα αυτό είναι το μοναδικό υπόσωμα βαθμού ℓ, $K(\ell, \ell)$ το οποίο περιέχεται στο κυκλοτομικό σώμα $Q(\zeta_{\ell^2})$.*

Απόδειξη. **Βήμα 1** Σε πρώτο βήμα αποδεικνύουμε γενικά ότι αν K αβελιανό αλγεβρικό σώμα αριθμών βαθμού επέκτασης πρώτου αριθμού ℓ, $\ell \neq 2$ στο οποίο σώμα ο πρώτος ℓ διακλαδίζεται, τότε έχει διακρίνουσα $D_{K/\mathbb{Q}}$ με εκθέτη του ℓ

$$\nu_\ell(D_{K/\mathbb{Q}}) = 2(\ell - 1).$$

Έστω λοιπόν $\mathcal{L}$ ένα πρώτο ιδεώδες του K, $\mathcal{L} \mid \ell$. Αφού $K/\mathbb{Q}$ Galois, βαθμού επέκτασης πρώτου αριθμού έπεται ότι η ομάδα Galois, έστω $H = \mathrm{Gal}(K/\mathbb{Q})$, είναι κυκλική τάξης πρώτου αριθμού ℓ. Αυτή έχει ακριβώς δύο υποομάδες, τον εαυτό της και την $\{\mathrm{Id}_K\}$. Επειδή ο ℓ διακλαδίζεται στο K, έπεται ότι η ομάδα αδράνειας $H_0 = H_0(\mathcal{L}/\ell) \neq \{\mathrm{Id}_L\}$. Κατ' ανάγκη λοιπόν $H = H_0$. Επίσης από το θεώρημα VII.3.5 έπεται ότι $e_0 = 1$, δηλαδή $H = H_0 = H_1$. Αυτό σημαίνει ότι βαθμός διακλάδωσης είναι ℓ και συνεπώς το $\mathcal{L}$ διακλαδίζεται πλήρως στο K,

$$\ell S = \mathcal{L}^\ell,$$

οπότε $f(\mathcal{L}/\ell\mathbb{Z}) = 1$, δηλαδή $N_{K/\mathbb{Q}}(\mathcal{L}) = \ell$.

Έστω τώρα r ο ελάχιστος φυσικός αριθμός για τον οποίο $H_r = \{\mathrm{Id}_K\}$. Επομένως $r > 1$ και $H_{r-1} = H$. Από το τρίτο θεμελιώδες θεώρημα του Dedekind X.3.38, προκύπτει ότι

$$v_{\mathcal{L}}(\mathrm{Diff}_{K/\mathbb{Q}}) = r(\ell - 1).$$

Όμως από την παρατήρηση X.3.44 αν

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0,$$

τότε

$$v_{\mathcal{L}}(\mathrm{Diff}_{K/\mathbb{Q}}) = \min_{1\le m<n}(m - 1 - nv_p(ma_m)).$$

Επομένως, αν $\pi \in \mathcal{L}\backslash\mathcal{L}^2$

$$v_{\mathcal{L}}(\mathrm{Diff}_{K/\mathbb{Q}}) \le v_\ell(\ell\pi^\ell) = \ell - 1 + \ell v_\ell(\ell) = 2\ell - 1.$$

Επειδή $\ell > 2$, έπεται ότι $r = 2$, δηλαδή

$$v_\ell(D_{K/\mathbb{Q}}) = 2(\ell - 1).$$

Βήμα 2 Το σώμα $K = K(\ell, \ell)$ που θεωρήσαμε στη διατύπωση της πρότασης, είναι υπόσωμα του $\mathbb{Q}(\zeta_m)$, $m = \ell^2$ στο οποίο ως γνωστό, ο πρώτος ℓ διακλαδίζεται πλήρως. Η επέκταση $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ είναι κυκλική βαθμού $\varphi(\ell^2) = \ell(\ell - 1)$. Συνεπώς ως υπόσωμα του $\mathbb{Q}(\zeta_m)$, είναι το μοναδικό υπόσωμα με βαθμό επέκτασης ℓ στο οποίο ο μοναδικός πρώτος που διακλαδίζεται και μάλιστα πλήρως είναι ο ℓ.

Έστω τώρα ότι υπάρχει και κάποιο άλλο σώμα K' με αυτές τις ιδιότητες. Η σύνθεση $L = K \cdot K'$ είναι επίσης αβελιανή επέκταση του $\mathbb{Q}$ στην οποία ο μοναδικός πρώτος που διακλαδίζεται είναι ο ℓ. Έστω $\mathcal{L}$ ένα πρώτο ιδεώδες του L, $\mathcal{L} \mid \ell$ και $G = \mathrm{Gal}(L/\mathbb{Q})$.

Σύμφωνα με το θεώρημα της μεταφοράς της θεωρίας Galois, ο βαθμός $[L : \mathbb{Q}] \mid \ell^2$. Από τη θεωρία διακλάδωσης του Hilbert έπεται ότι ισχύει $G = G_0 = G_1$. Έστω s ο δείκτης για τον οποίο ισχύει

$$G = G_0 = G_1 = \cdots = G_{s-1} \neq G_s.$$

Τότε το $s > 1$ και η ομάδα $G/G_s = G_{s-1}/G_s$ είναι ισόμορφη προς μια υποομάδα της προσθετικής ομάδας $S/\mathcal{L} \cong \mathbb{Z}/\ell\mathbb{Z}$. Επομένως $[G : G_s] = \ell$.

Βήμα 3 Όλα τα υποσώματα K'' του L, βαθμού $[K'' : \mathbb{Q}] = \ell$ αντιστοιχούν σε υποομάδες της G, έστω G'' με δείκτη $[G : G''] = \ell$, και σε όλα ο μοναδικός διακλαδιζόμενος πρώτος είναι ο ℓ. Σύμφωνα με το βήμα (1) της απόδειξης όλα έχουν τη διακρίνουσα

$$\mathcal{D}_{K''/\mathbb{Q}} = \ell^{2(\ell-1)}\mathbb{Z}.$$

Συνεπώς η διακρίνουσα $\mathcal{D}_{L/K''}$ είναι ανεξάρτητη του K''. Ξεχωριστό από όλα αυτά τα σώματα είναι το σώμα K_s που αντιστοιχεί στην ομάδα G_s του βήματος (2). Ο λόγος είναι ότι η διαφορίζουσα Diff_{L/K_s} περιέχει μέγιστη $\mathcal{L}$-δύναμη, από όλα τα άλλα

$$v_{\mathcal{L}}(\mathrm{Diff}_{L/K''}) \le v_L(\mathrm{Diff}_{L/K_s}).$$

Επειδή έχουν τον ίδιο βαθμό $[K'' : \mathbb{Q}] = [K_s : \mathbb{Q}] = \ell$ από την πρόταση X.3.37, προκύπτει ότι $K'' = K_s$, το μοναδικό ενδιάμεσο σώμα βαθμού ℓ και $G'' = G_s$ η μοναδική υποομάδα της G δείκτου ℓ. Αυτό σημαίνει ότι η ομάδα G είναι κυκλική, αφού μη-κυκλικές αβελιανές ομάδες τάξης δύναμης ενός πρώτου αριθμού περιέχουν τουλάχιστο δύο υποομάδες δείκτου ℓ. Συνεπώς $K = K'$. □

Στη συνέχεια θα μελετήσουμε τα κυκλικά κυκλοσώματα. Έστω $q > 1$ μια δύναμη του πρώτου αριθμού ℓ. Συμβολίζουμε με $K(\ell, q)$το μοναδικό ενδιάμεσο σώμα της κυκλικής επέκτασης $\mathbb{Q}(\zeta_{\ell \cdot q})$, βαθμού $[K(\ell, q) : \mathbb{Q}] = q$, όταν $\ell \neq 2$. Συμβολίζουμε με $K(2, q)$ το μέγιστο πραγματικό υπόσωμα του κυκλοτομικού σώματος $\mathbb{Q}(\zeta_{4 \cdot q})$ βαθμού $[K(2, q) : \mathbb{Q}] = q$, όταν $\ell = 2$. Για κάποιο πρώτο p, $p \equiv 1 \mod q$, έστω $K(p, q)$ το μοναδικό υπόσωμα του κυκλοτομικού σώματος $\mathbb{Q}(\zeta_p)$ βαθμού $[K(p, q) : \mathbb{Q}] = q$.

Στη συνέχεια ισχυριζόμαστε ότι για όλους τους πρώτους $\widetilde{p}$, $\widetilde{p} \equiv 1 \mod q$ καθώς και $\widetilde{p} = \ell$, το σώμα $K(\widetilde{p}, q)$ βαθμού $[K(\widetilde{p}, q) : \mathbb{Q}] = q$ διακλαδίζεται μόνο στο $\widetilde{p}$ και η επέκταση $K(\widetilde{p}, q)/\mathbb{Q}$ έχει Galois ομάδα κυκλική.

Αν το $\widetilde{p} \neq 2$, αυτό είναι προφανές, αφού είναι γνωστό ότι η ομάδα $(\mathbb{Z}/\widetilde{p}^n\mathbb{Z})^*$ των πρώτων κλάσεων υπολοίπων modulo $\widetilde{p}^n$ είναι, για κάθε n, κυκλική. Αν τώρα το $\widetilde{p} = 2$ και το $\ell = 2$, τότε η ομάδα Galois

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_{4q})/\mathbb{Q})$$

είναι ισόμορφη προς την ομάδα $(\mathbb{Z}/4q\mathbb{Z})^*$ η οποία δεν είναι κυκλική αλλά ευθύ γινόμενο δύο κυκλικών υποομάδων παραγόμενων από τα στοιχεία $(-1+4q\mathbb{Z})$ και $(5+4q\mathbb{Z})$. Ο αυτομορφισμός του σώματος $\mathbb{Q}(\zeta_{4q})$, ο οποίος αντιστοιχεί στη μιγαδική συζυγία $\sigma : \zeta_{4q} \mapsto \zeta_{4q}^{-1}$ αντιστοιχεί στο στοιχείο $-1 + 4q\mathbb{Z}$ της ομάδας $(\mathbb{Z}/4q\mathbb{Z})^*$. Επομένως η ομάδα πηλίκο $G/\langle\sigma\rangle$ είναι κυκλική και αντιστοιχεί στο μέγιστο πραγματικό υπόσωμα του $\mathbb{Q}(\zeta_{4q})$, δηλαδή είναι η $K(2, q)$.

Πρόταση X.4.4. *Έστω ℓ ένας πρώτος αριθμός και $q > 1$ μια δύναμη του ℓ. Έστω $K/\mathbb{Q}$ μια κυκλική επέκταση, βαθμού $[K : \mathbb{Q}] = q$ η οποία περιέχει το σώμα $K(\ell, \ell)$. Θεωρούμε τη σύνθεση*

$$L := K \cdot K(\ell, q).$$

Το σώμα L μπορεί να παρασταθεί και ως σύνθεση

$$L := K' \cdot K(\ell, q),$$

αλλά με ένα σώμα K' που έχει βαθμό q', με q' δύναμη του ℓ και $q' < q$.

Απόδειξη. Η επέκταση $L/\mathbb{Q} = K \cdot K(\ell, q)/\mathbb{Q}$ είναι αβελιανή ως σύνθεση δύο αβελιανών επεκτάσεων. Η ομάδα Galois $\widetilde{G} := \mathrm{Gal}(L/\mathbb{Q})$ εμφυτεύεται ως μια υποομάδα του ευθέως γινομένου δύο κυκλικών ομάδων των

$$G = \mathrm{Gal}(K/\mathbb{Q}) \text{ και } G' = \mathrm{Gal}(K(\ell, q)/\mathbb{Q}).$$

Αφού οι τάξεις των ομάδων G και G' είναι q, έπεται ότι η τάξη κάθε στοιχείου της ομάδας $\widetilde{G}$ διαιρεί το q. Το $K(\ell, \ell) \subset K$, εξ υποθέσεως και το $K(\ell, \ell) \subset K(\ell, q)$. Άρα

$$K(\ell, \ell) \subset K \cap K(\ell, q).$$

Επομένως

$$|\widetilde{G}| = qq' < |G| \cdot |G'| = q^2 \Rightarrow q' < q.$$

Για κάθε αυτομορφισμό σ της $\widetilde{G}$ θεωρούμε τον περιορισμό του σ, $\mathrm{res}\sigma$, στο υπόσωμα $K(\ell, q)$ του L. Η απεικόνιση

$$\begin{aligned} \rho : \widetilde{G} &\longrightarrow G' \\ \sigma &\longmapsto \mathrm{res}\sigma \end{aligned}$$

είναι επιμορφισμός ομάδων. Επομένως, υπάρχει $\sigma \in \widetilde{G}$ ώστε

$$\langle\rho(\sigma)\rangle = \mathrm{Gal}(K(\ell, q)/\mathbb{Q}).$$

Το $\langle\sigma\rangle$ είναι μια κυκλική υποομάδα της ομάδας $\widetilde{G}$ τάξης q και ο πυρήνας $\ker\rho$ του επιμορφισμού έχει τάξη q'. Επιπλέον ισχύει $\ker\rho \cap \langle\sigma\rangle = \{1_{\widetilde{G}}\}$.

Επομένως, $\widetilde{G} = \ker\rho \times \langle\sigma\rangle$. Η αβελιανή ομάδα $\widetilde{G}$ έχει ελάχιστο αριθμό γεννητόρων ≤ 2, έπεται ότι κατ' ανάγκη και ο πυρήνας $\ker\rho$ είναι κυκλική ομάδα. Επομένως το σώμα K' των σταθερών στοιχείων του σ στο L έχει μια ομάδα Galois ισόμορφη προς την κυκλική ομάδα $\ker\rho$, δηλαδή $L = K' \cdot K(\ell, q)$. □

Χ.5 Απόδειξη του θεωρήματος Kronecker-Weber

(1) Κάθε πεπερασμένη αβελιανή ομάδα $\neq \{\mathrm{Id}\}$ περιέχει μια κυκλική ομάδα τάξης δύναμης πρώτου αριθμού $q > 1$, ως ευθύ προσθετέο. Επομένως αβελιανές επεκτάσεις του $\mathbb{Q}$ είναι συνθέσεις πεπερασμένου πλήθους σωμάτων, κυκλικών επεκτάσεων του $\mathbb{Q}$ και κάθε ένα από τα σώματα αυτά έχει βαθμό επέκτασης υπεράνω του $\mathbb{Q}$ δύναμη πρώτου αριθμού.

Επίσης η σύνθεση από πεπερασμένα το πλήθος κυκλοσώματα είναι επίσης ένα κυκλόσωμα, οπότε αρκεί να αποδείξουμε το θεώρημα για κυκλικές επεκτάσεις του $\mathbb{Q}$, $K/\mathbb{Q}$ βαθμού $[K : \mathbb{Q}]$ δύναμη πρώτου αριθμού $q = \ell^m$, $\ell \in \mathbb{P}$. Αυτό επιτυγχάνεται επαγωγικά ως προς τον εκθέτη m. Την περίπτωση $\ell = 2$ και $m = 1$, δηλαδή για τετραγωνικά σώματα αριθμών την έχουμε ήδη μελετήσει.

2 Έστω τώρα $\ell > 2$ ή $m > 1$. Υποθέτουμε ότι ισχύει ο ισχυρισμός για ℓ-δυνάμεις $q' < q$. Θεωρούμε την ακολουθία των υποομάδων της κυκλικής ομάδας G

$$G = G^{\ell^0} \geq G^{\ell} \geq G^{\ell^2} \geq \cdots \geq G^{q} = \{\mathrm{Id}_K\},$$

όπου $G^{\ell^\nu} = \{\sigma^{\ell^\nu} : \sigma \in G\}$ για $\nu = 0, \ldots, q$. Στη συνέχεια θεωρούμε τα αντίστοιχα σώματα σταθερών στοιχείων $K_i = \mathrm{Fix}G^{\ell^\nu}$:

$$K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_m = K.$$

Εστιάζουμε στο σώμα K_1. Η απόδειξη του επαγωγικού βήματος για το m επιτυγχάνεται μέσω της επαγωγής ως προς το πλήθος r των διαφορετικών μεταξύ τους πρώτων αριθμών p, $p \neq \ell$ οι οποίοι διακλαδίζονται στο σώμα K.

2a Έστω $r = 0$. Αυτό σημαίνει ότι στο σώμα K_1 διακλαδίζεται το πολύ στο ℓ. Αν $\ell > 2$, τότε σύμφωνα με την πρόταση Χ.4.3

$$K_1 = K(\ell, \ell).$$

Αν $\ell = 2$, επειδή υποθέτουμε ότι $m > 1$, έχουμε

$$K_1 = \mathbb{Q}(\sqrt{2}).$$

Πράγματι, το σώμα K, περιέχει το σώμα σταθερών στοιχείων του $\mathbb{Q}$-αυτομορφισμού του K ο οποίος δίνεται μέσω της μιγαδικής συζυγίας. (Η επέκταση $K/\mathbb{Q}$ είναι αβελιανή). Επομένως, αν το K είναι πραγματικό, τότε το σώμα αυτό είναι το $K = K_m$, ενώ αν το K δεν είναι πραγματικό, τότε το σώμα αυτό είναι το K_{m-1}. Σε κάθε περίπτωση το σώμα K_1 περιέχεται στο K_{m-1} $(m > 1)$, δηλαδή το K_1 είναι πραγματικό τετραγωνικό σώμα αριθμών. Άρα, είναι το $K_1 = \mathbb{Q}(\sqrt{2}) = K(2, 2)$ το οποίο περιέχεται στο K. Αυτό μας επιτρέπει να εφαρμόσουμε την πρόταση Χ.4.4.

Η σύνθεση σωμάτων $L := K \cdot K(\ell, q)$ έχει και μια παράσταση $L = K' \cdot K(\ell, q)$ με κάποιο κυκλικό σώμα K' βαθμού $[K' : \mathbb{Q}] = q'$, q' είναι δύναμη του ℓ και $q' < q$. Σύμφωνα με την υπόθεση της μαθηματικής επαγωγής, το K' είναι κυκλόσωμα και συνεπώς και το K αφού είναι υπόσωμα της σύνθεσης $L = K' \cdot K(\ell, q)$.

2b Έστω τώρα $r > 0$. Υποθέτουμε ότι κάθε κυκλικό σώμα K βαθμού επέκτασης

$$[K : \mathbb{Q}] = q := \ell^m, \ell \in \mathbb{P}$$

με λιγότερους από r και διαφορετικούς του ℓ διακλαδιζόμενους πρώτους είναι κυκλόσωμα.

Σύμφωνα με την απόδειξη του βήματος (2a) μπορούμε να υποθέσουμε ότι υπάρχει ένας πρώτος p, $p \neq \ell$ ο οποίος διακλαδίζεται στο K_1. Έστω P ένα πρώτο ιδεώδες του K, $P \cap \mathbb{Q} = p\mathbb{Z}$. Το K_1 είναι ένα ενδιάμεσο σώμα. Έστω $P' = P \cap K$. Επειδή $e(P/P') \neq e(P/p\mathbb{Z})$, αφού p διακλαδίζεται

στο K_1, έχουμε ότι το σώμα K_1 δεν περιέχεται στο σώμα αδρανείας του P. Επομένως $G_{-1}(P/p\mathbb{Z}) = G_0(P/p\mathbb{Z}) = G$.

Επίσης επειδή $q = \ell^m$, $\ell \in \mathbb{P}$ και $p \neq \ell$, έχουμε $(p, q) = 1$. Συνεπώς $G_1(P/p\mathbb{Z}) = \{\mathrm{Id}_K\}$. Από τα παραπάνω συνάγουμε ότι η ομάδα

$$G = \frac{G_0(P/p\mathbb{Z})}{G_1(P/p\mathbb{Z})}.$$

Αλλά η ομάδα πηλίκο G_0/G_1 είναι ισόμορφη προς μια υποομάδα της $\mathbb{F}_p^*$, οπότε

$$p = N_{K/\mathbb{Q}}(P) \equiv 1 \mod q.$$

Επομένως, μπορούμε να χρησιμοποιήσουμε το $K(p, q)$.

2c Στη συνέχεια θεωρούμε το σώμα $K(p, q)$, βαθμού $[K(p, q) : \mathbb{Q}] = q$ καθώς και την κυκλική ομάδα Galois της επέκτασης $K(p, q)/\mathbb{Q}$. Θα μελετήσουμε και πάλι τη σύνθεση

$$L = K \cdot K(p, q).$$

Είναι όπως και πριν, η επέκταση $L/\mathbb{Q}$ μια αβελιανή επέκταση με ομάδα Galois

$$\widetilde{G} = \mathrm{Gal}(L/\mathbb{Q}),$$

ισόμορφη προς κάποια υποομάδα του ευθέως γινομένου δύο κυκλικών ομάδων τάξεως q. Συνεπώς

$$|\widetilde{G}| = q'q \text{ με } q' \mid q.$$

Όπως και στην πρόταση X.4.4, η $\widetilde{G}$ είναι το ευθύ γινόμενο δύο κυκλικών ομάδων, μιας τάξης q και της άλλης τάξης q'. Έστω P ένα πρώτο ιδεώδες του L, $P \cap \mathbb{Q} = p\mathbb{Z}$. Η πρώτη ομάδα διακλάδωσης $\widetilde{G}_1(P/p)$ έχει τάξη δύναμη του p. Στην περίπτωσή μας, η τάξη αυτή θα πρέπει να διαιρεί το qq'. Συνεπώς, $\widetilde{G}_1(P/p\mathbb{Z}) = \{\mathrm{Id}_L\}$, αφού $p \neq \ell$. Ως γνωστό η ομάδα πηλίκο $\widetilde{G}_0(P/p\mathbb{Z})/\widetilde{G}_1(P/p\mathbb{Z})$ είναι κυκλική. Άρα η $\widetilde{G}_0(P/p\mathbb{Z})$ είναι κυκλική και η τάξη της είναι δύναμη του $\ell \leq q$. Η τάξη της όμως συγχρόνως διαιρείται και από το $e(P/p\mathbb{Z}) = q$. Επομένως, η $\widetilde{G}_0(P/p\mathbb{Z})$ έχει τάξη q.

Η $\widetilde{G}$ έχει τάξη qq', η $\widetilde{G}_0$ έχει τάξη q. Άρα το σώμα αδρανείας του P, έστω K' έχει βαθμό $[K' : \mathbb{Q}] = q'$. Στο σώμα K' διακλαδίζονται το πολύ οι πρώτοι $p_1, p_2, \ldots, p_r$. Στο σώμα $K(p, q)$ διακλαδίζεται (πλήρως) μόνο το ℓ και είναι $\ell \neq p_i$ $i = 1, 2, \ldots, r$. Επομένως, στην τομή $K' \cap K(p, q)$ δεν διακλαδίζεται κανένας πρώτος. Σύμφωνα με το θεώρημα του **Minkwoski**

$$K' \cap K(p, q) = \mathbb{Q}.$$

Επομένως ο βαθμός επέκτασης

$$[K' \cdot K(p, q) : \mathbb{Q}] = [K(p, q) : \mathbb{Q}][K' : \mathbb{Q}] = qq' = [L : \mathbb{Q}].$$

Αυτό σημαίνει ότι το $L = K' \cdot K(p, q)$. Λόγω της γνωστής δομής της $\widetilde{G}$, όπως και στην πρόταση X.4.4, το σώμα K' έχει κυκλική ομάδα Galois τάξης q'.

Το K' είναι το σώμα αδρανείας του p. Επομένως, αφού ο p, σίγουρα δεν διακλαδίζεται στο K', έπεται ότι το πλήθος των πρώτων αριθμών που διακλαδίζονται στο K και είναι διάφοροι του ℓ είναι μικρότερο αυτών που διακλαδίζονται στο K.

Σύμφωνα με την υπόθεση της μαθηματικής επαγωγής, το K' είναι κυκλόσωμα. Επομένως και η σύνθεση δύο κυκλοσωμάτων $L = K' \cdot K(p, q)$ είναι κυκλόσωμα και το K ως υπόσωμα του κυκλοσώματος L είναι επίσης κυκλόσωμα. □

Παρατήρηση X.5.1. Από την απόδειξη του Θεωρήματος των Kronecker-Weber προκύπτουν τα εξής:

1. Αν K είναι μία αβελιανή επέκταση του $\mathbb{Q}$ βάθμου $[K : \mathbb{Q}] = 2^m$, για κάποιο θετικό ακέραιο m και ισχύει ότι στο K ο μοναδικός διακλαδιζόμενος πρώτος είναι το 2, τότε

$$K \subset \mathbb{Q}(\zeta_{2^{m+2}}).$$

2. Αν K είναι μια αβελιανή επέκταση του $\mathbb{Q}$ βαθμού $[K:\mathbb{Q}] = \ell^m$, όπου $\ell \in \mathbb{P}$, m κάποιος θετικός ακέραιος και ο μοναδικός πρώτος που διακλαδίζεται στο K είναι ο ℓ, τότε

$$K \subset \mathbb{Q}(\zeta_{\ell^{m+1}}).$$

Στην πραγματικότητα είναι το μοναδικό υπόσωμα του $\mathbb{Q}(\zeta_{\ell^{m+1}})$, αφού κάθε ℓ-ομάδα τάξης ℓ^m, $\ell \in \mathbb{P}$, $m \geq 1$ έχει μοναδική υποομάδα τάξης $m-1$.

3. Έστω K μια αβελιανή επέκταση του $\mathbb{Q}$ βαθμού $[K:\mathbb{Q}] = \ell^m$, $\ell \in \mathbb{P}$, $m \geq 1$ και $p \in \mathbb{P}$, $p \neq \ell$ ο οποίος διακλαδίζεται στο K, δηλαδή $r \geq 1$. Υπάρχει ένα σώμα K' με τις ακόλουθες ιδιότητες:
   (i) Ο p δεν διακλαδίζεται στο K' και κάθε πρώτος αριθμός ο οποίος δεν διακλαδίζεται στο K δεν διακλαδίζεται ούτε στο K'.
   (ii) Ο βαθμός του K', $[K':\mathbb{Q}] = \ell^k = q' < q = \ell^m$.
   (iii) Αν $K \subset \mathbb{Q}(\zeta_d)$ και $p \nmid d$, τότε το $K \subset \mathbb{Q}(\zeta_{dp})$

Με βάση τα παραπάνω θα αποδείξουμε την

Πρόταση Χ.5.2. *Έστω K μια αβελιανή επέκταση του $\mathbb{Q}$ βαθμού $[K:\mathbb{Q}] = \ell^m$, $\ell \in \mathbb{P}$, $m \geq 1$. Αν $p_1, p_2, \ldots, p_r$ πρώτοι, διαφορετικοί του ℓ, είναι οι διακλαδιζόμενοι πρώτοι στο σώμα K, και αν ο ℓ δεν διακλαδίζεται στο K, τότε*

$$K \subset \mathbb{Q}(\zeta_{p_1 p_2 \cdots p_r}).$$

Αν $\ell = 2$ και διακλαδίζεται στο K, τότε

$$K \subset \mathbb{Q}(\zeta_{2^{m+2} p_1 p_2 \cdots p_r}).$$

Αν $\ell \neq 2$ και διακλαδίζεται στο K, τότε

$$K \subset \mathbb{Q}(\zeta_{\ell^{m+1} p_1 p_2 \cdots p_r})$$

Απόδειξη. Επαγωγικά, ως προς r, το πλήθος των διακλαδιζόμενων πρώτων διαφορετικών του ℓ.

Αν λοιπόν $r = 0$, τότε, λόγω του θεωρήματος του Minkowski, ο ℓ διακλαδίζεται στο K και αφού $r = 0$ είναι ο μοναδικός διακλαδιζόμενος πρώτος. Αν $\ell = 2$, τότε ισχύει η πρώτη από τις παρατηρήσεις, ενώ αν $\ell \neq 2$, τότε ισχύει η δεύτερη, δηλαδή για $r = 0$ η πρόταση είναι αληθής.

Υποθέτουμε ότι η πρόταση είναι αληθής για $0 \leq k < r$. Επειδή $r \geq 1$ ιδιότητα 3(i) από τις παρατηρήσεις μας δίνει την ύπαρξη του K' με πλήθος πρώτων αριθμών διάφορων του ℓ οι οποίοι διακλαδίζονται στο K', $r' < r$.

Υποθέτουμε, κατ' αρχήν ότι ο ℓ δεν διακλαδίζεται στο K. Τότε δεν διακλαδίζεται ούτε στο K', 3(i). Πιθανόν κάποιο γνήσιο υποσύνολο του συνόλου $\{p_1, p_2, \ldots, p_{r-1}\}$ να διακλαδίζεται στο K'. Λόγω της υπόθεσης της μαθηματικής επαγωγής το

$$K' \subset \mathbb{Q}(\zeta_{p_1 p_2 \cdots p_{r-1}}).$$

Αν $d = p_1 p_2 \cdots p_{r-1}$, $K' \subset \mathbb{Q}(\zeta_d)$, οπότε η 3(iii) μας δίνει το επιθυμητό αποτέλεσμα. Στη συνέχεια υποθέτουμε ότι ο ℓ διακλαδίζεται στο K. Ανεξάρτητα από το αν ο ℓ διακλαδίζεται στο K' ή όχι έχουμε

$$K' \subset \mathbb{Q}(\zeta_{2^{k+2} p_1 p_2 \cdots p_{r-1}}), \text{ όταν } \ell = 2$$

και από την 3(ii)

$$K' \subset \mathbb{Q}(\zeta_{\ell^{k+1} p_1 p_2 \cdots p_{r-1}}), \text{ όταν } \ell \neq 2.$$

Από την 2(ii) έχουμε ότι

$$K' \subset \mathbb{Q}(\zeta_{2^{m+2} p_1 p_2 \cdots p_{r-1}}), \text{ αν } \ell = 2$$

και

$$K' \subset \mathbb{Q}(\zeta_{\ell^{m+1} p_1 p_2 \cdots p_{r-1}}), \text{ αν } \ell \neq 2.$$

Θέτουμε

$$d := \begin{cases} 2^{m+2}p_1p_2\cdots p_{r-1}, & \text{αν } \ell = 2 \\ \ell^{m+1}p_1p_2\cdots p_{r-1}, & \text{αν } \ell \neq 2 \end{cases}$$

και έχουμε για το K το ζητούμενο

$$K \subset \mathbb{Q}(\zeta_{dp_r}).$$

□

Παρατήρηση X.5.3. Εάν λάβουμε υπόψη ότι:

1. Κάθε αβελιανή επέκταση $K/\mathbb{Q}$ είναι σύνθεση αβελιανών επεκτάσεων βαθμού δυνάμεων πρώτων αριθμών
2. Κάθε πρώτος αριθμός ο οποίος διακλαδίζεται στο K κατ' ανάγκη διακλαδίζεται σε ένα τουλάχιστον από τα σώματα των οποίων η σύνθεση μας δίνει το K και
3. Εφαρμόζουμε την προηγούμενη πρόταση και έχουμε:

Θεώρημα X.5.4. *Έστω* K *μια αβελιανή επέκταση του* $\mathbb{Q}$*, βαθμού* $[K : \mathbb{Q}] = n$ *και* $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}q_1^{\beta_1}q_2^{\beta_2}\cdots q_t^{\beta_t}$ *η ανάλυση του* n *σε γινόμενο πρώτων παραγόντων. Υποθέτουμε ότι οι πρώτοι* $p_1, p_2, \ldots, p_s$ *διακλαδίζονται στο* K *ενώ οι* $q_1, q_2, \ldots, q_t$ *όχι. Έστω* $n' := p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ *και* r *το γινόμενο όλων των πρώτων αριθμών που διακλαδίζονται στο* K *με επιπλέον του παράγοντα* 2 *όταν το* 2 *διακλαδίζεται στο* K *και* $2 \mid n$*. Τότε*

$$K \subset \mathbb{Q}(\zeta_{n\cdot r}).$$

Παράδειγμα X.5.5. Έστω $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$ και $g(x) = x^3 - 7x + 7$ και K, L τα σώματα ανάλυσης των $f(x)$ και $g(x)$ αντίστοιχα. Η διακρίνουσα του $f(x)$ είναι $\mathrm{Disc}(f(x)) = 3^4$ και είναι τέλειο τετράγωνο. Η διακρίνουσα του $g(x)$ είναι $\mathrm{Disc}g(x)) = 7^2$ και είναι επίσης τέλειο τετράγωνο. Επομένως έχουμε δύο κυκλικές επεκτάσεις του $\mathbb{Q}$ βαθμού 3, $K = \mathbb{Q}(\alpha)$ και $L = \mathbb{Q}(\beta)$, όπου α, β ρίζες των αναγώγων υπεράνω του $\mathbb{Q}$ πολυωνύμων $f(x)$ και $g(x)$.

Έστω $M = KL = \mathbb{Q}(\alpha, \beta)$, η σύνθεση αυτών των δύο σωμάτων. Επειδή $K \cap L = \mathbb{Q}$, έπεται ότι η επέκταση $M/\mathbb{Q}$ είναι μια αβελιανή επέκταση με $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Ο μόνος πρώτος που θα μπορούσε να διακλαδίζεται στο K είναι ο 3. Πράγματι, σύμφωνα με το θεώρημα του Minkowski ο 3 διακλαδίζεται στο K. Επίσης, ο 7 διακλαδίζεται στο L. Επομένως οι 3 και 7 διακλαδίζονται στο $M = KL$. Δεν υπάρχουν άλλοι διακλαδιζόμενοι στο M, αφού αν ένας πρώτος p δεν διακλαδίζεται στα K και L, τότε δεν διακλαδίζεται ούτε στο M. Για το K έχουμε $n' = 3$ και $r = 3$. Επομένως $K \subset \mathbb{Q}(\zeta_9)$. Στο L έχουμε $n' = 1$ και $r = 7$, επομένως $L \subset \mathbb{Q}(\zeta_7)$. Τελικά $M \subset \mathbb{Q}(\zeta_{63})$.

Επειδή το $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ το $K \notin \mathbb{Q}(\zeta_3)$. Συνεπώς το $m = 63$ είναι ο οδηγός της επέκτασης $M/\mathbb{Q}$.

Ιστορικά στοιχεία Επειδή πρόκειται για ένα εξαιρετικά σημαντικό θεώρημα καλό είναι νομίζουμε να κλείσουμε με μερικά ιστορικά στοιχεία.

Η πρώτη αναφορά στο θεώρημα γίνεται από τον Kronecker το 1853: *Über die algebraischen auflösbaren Gleichungern*, Monatsberichte Preuss. Akad. Wiss. 1853 365-374.

Η διατύπωση ήταν: «Αν ένα πολυώνυμο με ρητούς συντελεστές έχει αβελιανή Galois ομάδα, τότε οι ρίζες του μπορούν να εκφραστούν ως γραμμικός συνδυασμός των ριζών της μονάδας με ρητούς συντελεστές».

Επανέρχεται το 1877 με πιο μοντέρνα μαθηματική έκφραση:

«Κάθε επέκταση Galois των ρητών αριθμών με αβελιανή ομάδα Galois είναι υπόσωμα ενός κυκλοτομικού σώματος » *Über Abelsche Gleichungen*, Monatsberichte Preuss. Akad. Wiss. (1877) 845-851.

Η πρώτη απόδειξη δόθηκε από τον H. Weber (*Theorie der Abelschen Zahlkörper* Acta Mathematica 9 193-263 (1886)) και 9 105-130 (1887). Ο H. Weber έχει περιλάβει την απόδειξή του στο σημαντικό, όχι μόνο για την εποχή του αλλά και μέχρι σήμερα, τρίτομο έργο *Lehrbuch der Algebra*

2. Auflage Vieweg, Braunschwieg 1898,1899,1908. Το θεώρημα αποτελεί το περιεχόμενο των παραγράφων 23 και 24 του 2ου τόμου. Αργότερα διαπιστώθηκε ότι η απόδειξή του δεν ήταν πλήρως σωστή.

Το 1896 ο D. Hilbert έδωσε τελικά την πρώτη, γεινκά αποδεκτή, σωστή απόδειξη Ein neuer Beweis der Kroneckerscchen Fundamentalsatzes über Abelsche Zahlkörper, Nachr. Ges. Wiss Göttingen 1896 29-39). Η εργασία περιέχεται και στο Zahlbericht του Hilbert το οποίο δημοσιεύθηκε το 1897. Η παρούσα παρουσίαση στηρίζεται στις ιδέες του Hilbert.

Αργότερα όταν εμφανίστηκε η θεωρία των p-αδικών αριθμών και των τοπικών σωμάτων, θεωρήθηκε πιο φυσιολογική η απόδειξη του θεωρήματος πρώτα στα p-αδικά σώματα και στη συνέχεια στο $\mathbb{Q}$. Η πρώτη γνωστή σε μας απόδειξη προς αυτή την κατεύθυνση είναι το I. R. Shafarevich: *A new proof of the Kronecker-Weber theorem*, [24]. Ανάλογη διαδικασία ισχύει και για τη διακρίνουσα και για τη διαφορίζουσα.

Έτσι συνήθως σήμερα στα περισσότερα βιβλία ακολουθείται αυτή η διαδικασία στα πλαίσια του τοπικού-γενικού αξιώματος. Παραδείγματος χάρη στα βιβλία των W. Narciewicz [19], J. Neukirch [21], [20], L. Washington [25], J.W.S Cassels [5], Fröhlich-Taylor [8] και άλλων.

Εμείς δεν επιθυμούσαμε να επιβαρύνουμε περισσότερο την ύλη του παρόντος βιβλίου. Έτσι ακολουθήσαμε την κλασική μέθοδο. Η ίδια βασική ιδέα, αλλά διαφορετική επιμέρους διαδικασία, αποτελεί και το περιεχόμενο της πτυχιακής εργασίας της κυρίας Κωνστάντιας Μανούσου-Σωτηροπούλου [27]. Ότι το θέμα συνεχίζει να ενδιαφέρει αποδεικνύεται ότι και σε άλλα μέρη του κόσμου πτυχιακές εργασίες ασχολούνται με το ίδιο θέμα [4], [2]. Προφανώς και παραλείπουμε τα ονόματα άλλων Μαθηματικών που έχουν αποδείξει το θεώρημα. Η πιο πρόσφατη γνωστή σε μας απόδειξη είναι του F. Lemmermeyer, [14]. Φυσικά στη θεωρία κλάσεων σωμάτων το θεώρημα των Kronecker-Weber είναι πόρισμα.

X.6 Ασκήσεις

1. Αν K αλγεβρικό σώμα αριθμών και $R_K = \mathbb{Z}[\theta]$, να αποδείξετε το θεώρημα της διακρίνουσας.
2. Αν $L = (1+2i)\mathbb{Z}[i]$, να αποδείξετε ότι $L^* = \frac{1}{2(1+2i)}\mathbb{Z}[i]$.
3. Αν L δικτυωτό του K και $\alpha \in K^*$, να αποδείξετε ότι $(\alpha L)^* = \frac{1}{\alpha}L^*$.
4. Αν $K = \mathbb{Q}(\sqrt{d})$, τετραγωνικό σώμα αριθμών, $\alpha \in \mathbb{Z}$, ελεύθερο τετραγώνου, τότε να αποδείξετε ότι
$$\mathrm{Diff}_{K/\mathbb{Q}} = \begin{cases} \langle 2\sqrt{d}\rangle, & \text{όταν } d \not\equiv 1 \mod 4 \\ \langle \sqrt{d}\rangle, & \text{όταν } d \equiv 1 \mod 4 \end{cases}$$
5. Έστω α μια ρίζα του πολυωνύμου
$$f(x) = x^3 + x - 1 \in \mathbb{Q}[x],$$
$K = \mathbb{Q}(\alpha)$ και L σώμα ανάλυσης του $f(x)$ υπεράνω του $\mathbb{Q}$ περιέχει το K.
   (α′) Να αποδείξετε ότι $R_K = \mathbb{Z}[\alpha]$
   (β′) Να υπολογίσετε τον αριθμό κλάσεων του K
   (γ′) Υπάρχει τετραγωνικό σώμα αριθμών που περιέχεται στο L; Αν ναι, ποιο είναι αυτό;
   (δ′) Να αποδείξετε ότι μόνο ο πρώτος 31 μπορεί να διακλαδίζεται στο L.
   (ε′) Να αποδείξετε ότι το 31 στο K αναλύεται στη μορφή $31 = \pi_1\pi_2^2$, όπου π_1, π_2 ανάγωγα στοιχεία του R_K.
   (στ′) Να αποδείξετε ότι μόνο ο $p = 31$ διακλαδίζεται στην επέκταση $L/\mathbb{Q}$.
   (ζ′) Να αποδείξετε ότι κανένα πρώτο ιδεώδες του K δεν διακλαδίζεται στην επέκταση L/K.

Βιβλιογραφία

[1] Artin, E. *Theory of Algebraic Numbers*. Vol. 1956/7. Notes by Gerhard Würges from lectures held at the Mathematisches Institut, Göttingen, Germany, in the Winter Semester. George Striker, Schildweg 12, Göttingen, 1959, p. 172.

[2] Baggett, J. *An Exposition on the Kronecker-Weber Theorem*. University of Alaska Fairbanks, 2011. URL: https://books.google.gr/books?id=nbF7twAACAAJ.

[3] Bosch, S. *Algebra*. Springer-Lehrbuch. Springer Berlin, 2013. ISBN: 9783662056493. URL: https://books.google.gr/books?id=4BiyBgAAQBAJ.

[4] Branchereau, R. *The Kronecker-Weber Theorem*. MA thesis. ETH, Zürich, 2016. URL: https://people.math.ethz.ch/~pink/Theses/2016-Bachelor-Romain-Branchereau.pdf.

[5] Cassels, J. W. S. *An Introduction to the Geometry of Numbers*. Classics in Mathematics. Corrected reprint of the 1971 edition. Springer-Verlag, Berlin, 1997, pp. viii+344. ISBN: 3-540-61788-4.

[6] Conrad, K. *The different ideal*. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf.

[7] Deuring, M. *Klassenkörpertheorie: Vorlesung gehalten im Sommersemester 1965 und Wintersemester 1965-66 in Göttingen*. τ. 1. 1966. URL: https://books.google.gr/books?id=CKPNxgEACAAJ.

[8] Fröhlich, A. & Taylor, J. M. *Algebraic number theory*. Vol. 27. Cambridge Studies in advanced mathematics. Cambridge: Cambridge University Press, 1993, pp. xiv+355. ISBN: 0-521-43834-9.

[9] Hasse, H. *Number Theory*. German. Classics in Mathematics. Reprint of the 1980 English edition [Springer, Berlin; MR0562104 (81c:12001b)], Edited and with a preface by Horst Günter Zimmer. Springer-Verlag, Berlin, 2002, pp. xviii+638. ISBN: 3-540-42749-X.

[10] Hasse, H. *Vorlesungen über Klassenkörpertheorie*. Thesaurus Mathematicae, Band 6. Physica-Verlag, Würzburg, 1967, pp. iii+275.

[11] Hasse, H. *Zahlentheorie*. Dritte berichtigte Auflage. Akademie-Verlag, Berlin, 1969, pp. xvi+611.

[12] Hilbert, D. *The Theory of Algebraic Number Fields*. Translated from the German and with a preface by Iain T. Adamson, With an introduction by Franz Lemmermeyer and Norbert Schappacher. Springer-Verlag, Berlin, 1998, pp. xxxvi+350. ISBN: 3-540-62779-0. URL: https://doi.org/10.1007/978-3-662-03545-0.

[13] Holzer, L. *Zahlentheorie. II*. Mathematisch-Naturwissenschaftliche Bibliothek, Bd. 14. B. G. Teubner Verlagsgesellschaft, Leipzig, 1959, pp. v+127.

[14] Lemmermeyer, F. *Kronecker-Weber via Stickelberger*. *J. Théor. Nombres Bordeaux* 17.2 (2005), pp. 555–558. ISSN: 1246-7405. URL: http://jtnb.cedram.org/item?id=JTNB_2005__17_2_555_0.

[15] Leutbecher, A. *Zahlentheorie: Eine Einführung in die Algebra*. Springer-Lehrbuch. Springer, Berlin, 2013. ISBN: 9783642614057. URL: https://books.google.gr/books?id=PG2nBgAAQBAJ.

[16] Mann, H. B. *Introduction to Algebraic Number Theory*. With a chapter by Marshall Hall, Jr. The Ohio State University Press, Columbus, Ohio, 1955, pp. vii+168.

[17] Marcus, D. A. *Algebraic Number Fields*. Universitext. 2nd edition of [MR0457396], With a foreword by Barry Mazur. Springer, 2018, pp. xviii+203. ISBN: 978-3-319-90232-6; 978-3-319-90233-3.

[18] Narkiewicz, W. *On a theorem of A. Weil on derivations in number fields*. *Colloq. Math.* 20 (1969), pp. 57–58. ISSN: 0010-1354. URL: https://doi.org/10.4064/cm-20-1-57-58.

[19] Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*. 3rd edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004, pp. xii+708. ISBN: 3-540-21902-1.

[20] Neukirch, J. *Algebraic Number Theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Berlin: Springer-Verlag, 1999, pp. xviii+571. ISBN: 3-540-65399-6.

[21] Neukirch, J. *Algebraische Zahlentheorie*. German. Springer-Verlag Berlin, 1992.

[22] Neukirch, J. *Zur Differententheorie*. *Arch. Math. (Basel)* 18 (1967), pp. 241–249. ISSN: 0003-889X. URL: https://doi.org/10.1007/BF01900629.

[23] Ribenboim, P. *Classical Theory of Algebraic Numbers*. Universitext. Springer-Verlag, New York, 2001, pp. xxiv+681. ISBN: 0-387-95070-2.

[24] Šafarevič, I. R. *A new proof of the Kronecker-Weber theorem*. *Trudy Mat. Inst. Steklov., v. 38*. Trudy Mat. Inst. Steklov., v. 38. Izdat. Akad. Nauk SSSR, Moscow, 1951, pp. 382–387.

[25] Washington, L. C. *Introduction to Cyclotomic Fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, pp. xiv+487. ISBN: 0-387-94762-0. URL: https://doi.org/10.1007/978-1-4612-1934-7.

[26] Weil, A. *Differentiation in algebraic number fields*. *Bulletin of the AMS* 49 (1943), p. 41.

[27] Μανούσου-Σωτηροποούλου, Κ. *Το Θεώρημα Kronecker-Weber*. MA thesis. Πανεπιστήμιο Κρήτης, 2014. URL: http://users.math.uoc.gr/~antoniad/kronecker_weber.pdf.

XI

Εικασία Fermat, η κλασική προσέγγιση

XI.1 Ιστορική εισαγωγή

Fermat (1601-1665)

1637 Η διοφαντική εξίσωση $X^n + Y^n = Z^n$, $n \in \mathbb{N}, n \geq 3$ δεν έχει μη τετριμμένη $XYZ \neq 0$ ακέραια λύση. Ο Fermat απέδειξε την εργασία του για $n = 4$.

1670 Ο γιός του, Samuel de Fermat δημοσίευσε τις σημειώσεις του πατέρα του στο βιβλίο του Bachet, ο οποίος είχε εκδώσει το έργο του Διόφαντου στα λατινικά. Ο τίτλος ήταν «Παρατηρήσεις στον Διόφαντο».

1770 Ο Euler απέδειξε την εικασία για $n = 3$.

1816 Ο Gauss δεν έδειξε ενδιαφέρον για την εικασία. Στις 21-3-1816 έγραψε στον Olbers ότι «είναι ένα μεμονωμένο αποτέλεσμα και με ενδιαφέρει πολύ λίγο».

1825 Ο Dirichlet απέδειξε την περίπτωση για $n = 5$. Η απόδειξή του δεν ήταν πλήρης. Αυτό το παρατήρησε ο Legendre, ο οποίος έδωσε στη συνέχεια ανεξάρτητη και πλήρη λύση της περίπτωσης αυτής.

1828 Ο Dirichlet συμπλήρωσε τη δική του απόδειξη.

1832 Ο Dirichlet προσπάθησε την περίπτωση $n = 7$. Κατά τη διαδικασία διεπίστωσε ότι η μέθοδός του βολεύει καλύτερα την περίπτωση $n = 14$ την οποία και έλυσε.

1839 Ο Lamé απέδειξε την περίπτωση $n = 7$. Στο μεταξύ ο Legendre παρουσίασε το θεώρημα της Sophie Germain.

1823 Αν p πρώτος, $p \neq 2$ και $2p + 1$ επίσης πρώτος τότε ισχύει η πρώτη περίπτωση της εικασίας Fermat για τον πρώτο αυτόν p.

1847 Την 1η Μαρτίου του 1847 ο Lamé υπέβαλε μια εργασία του στην Ακαδημία Επιστημών των Παρισίων με την «απόδειξη» της εικασίας. Το ότι η απόδειξη δεν ήταν εντελώς σωστή το διεπίστωσε ο Liouville.

Ο Lamé θεώρησε το n περιττό, εισήγαγε τις μιγαδικές ρίζες της μονάδας $\zeta_n = e^{\frac{2\pi i}{n}}$ και παραγοντοποίησε την εξίσωση $x^n + y^n = z^n$ σε γινόμενο γραμμικών παραγόντων ως εξής:

$$x^n + y^n = (x + y)(x + \zeta_n y)\cdots(x + \zeta_n^{n-1} y). \tag{XI.1}$$

Θεώρησε το $x^n - y^n$ σαν πολυώνυμο του x με συντελεστή στο $\mathbb{C}[y]$. Αυτό είναι ίσο με μηδέν, όταν $x^n = y^n$, δηλαδή όταν $x = \zeta_n^k y$ για $0 \leq k \leq n-1$. Συνεπώς το πολυώνυμο $x^n - y^n$ διαιρείται από τα $x - \zeta_n^k y$ για $0 \leq k \leq n-1$. Επομένως το γινόμενο

$$(x - y)(x - \zeta_n y)\cdots(x - \zeta_n^{n-1} y)$$

διαιρεί το $x^n - y^n$. Όμως το γινόμενο είναι και αυτό πολυώνυμο βαθμού n και επειδή είναι και τα δύο μονικά προκύπτει η ισότητα

$$x^n - y^n = (x - y)(x - \zeta_n y)\cdots(x - \zeta_n^{n-1} y).$$

Αντικαθιστούμε το y με το $-y$ θυμούμαστε ότι n περιττός. Συνεπώς έχουμε τη σχέση (XI.1).

Το «επιχείρημα» στη συνέχεια ήταν ότι οι γραμμικοί παράγοντες του γινομένου ήταν ανά δύο πρώτοι μεταξύ τους, συνεπώς από τη σχέση $z^n = x^n + y^n$ ο καθένας τους ήταν n-στή δύναμη μιγαδικού αριθμού και έτσι κατέληξε στο συμπέρασμα-απόδειξη της εικασίας.

Για πλήρη απόδειξη, στην περίπτωση μονοσήμαντης ανάλυσης δες Borevich-Shafarevich [2, p.173-182].

Ο Liouville ήταν ο πρώτος που παρατήρησε ότι το τελευταίο επιχείρημα εξαρτάται από τη μοναδικότητα της παραγοντοποίησης. Υποψιάστηκε ότι δεν ισχύει. Εστράφη λοιπόν το ενδιαφέρον στην ύπαρξη ή μη της μονοσήμαντης ανάλυσης.

1847 Ο Wanzel απέδειξε το μονοσήμαντο της ανάλυσης για $n = 2, 3, 4$ και διαπίστωσε ότι η μέθοδός του δεν καλύπτει την περίπτωση $n = 23$. Την ύπαρξη του προβλήματος της μη-μονοσήμαντης ανάλυσης την είχε διαπιστώσει ήδη τρία χρόνια νωρίτερα ο Kummer.

1844 Ο Kummer έστειλε γράμμα στον Liouville, καθ' υπόδειξη του Dirichlet και τον ενημέρωσε σχετικά. Τον ενημέρωσε επίσης ότι έχει αναπτύξει μια μέθοδο, εισάγοντας μια καινούργια έννοια, αυτή των «ιδεωδών αριθμών».

1850 Έτσι στα 1850, δημοσίευσε μια εργασία στην οποία αποδείκνυε την εικασία του Fermat για μια μεγάλη κατηγορία εκθετών πρώτων αριθμών. Χαρακτηριστικά αναφέρουμε ότι η απόδειξη ισχύει για κάθε $p < 100$ εκτός από τρεις εξαιρέσεις $p = 37, 59, 67$. Τελικά αργότερα κατάφερε να αποδείξει την εικασία και για τους $p = 37, 59$ και 67, [12].

Σημαντική ήταν και η συνεισφορά του H.S. Vandiver στη δεκαετία του 1920. Αλλά η διαδικασία ήταν βήμα-βήμα για συγκεκριμένους μικρούς πρώτους αριθμούς και με τη βοήθεια του υπολογιστή. Έτσι στα 1976 ο S. Wagstaff [14] απέδειξε ότι η εικασία του Fermat είναι αληθής για όλους τους πρώτους p, $p < 125000$ και οι J. Buhler, R. Crandall, R. Ernvall και T. Metsänylä [4] μελέτησαν τους irregular πρώτους μέχρι τα 12 εκατομμύρια, ενώ το 2017 W. Hart, D. Harvey και W. Ong έφτασαν στα 2 δισεκατομμύρια. [7].

Ο στόχος μας είναι να παρουσιάσουμε τα αποτελέσματα του Kummer φυσικά με τη σημερινή ορολογία. Χρησιμοποιούμε το βιβλίο του P. Ribenboim "13 Lectures on Fermat's Last Theorem" [10] και το βιβλίο των I. Stewart και F. Tall "Algebraic Number Theory and Fermat's Last Theorem" [13], όπως και τον Borevich-Shafarevich [2] και L. Washington [15].

XI.2 Εισαγωγή

$$X^n + Y^n = Z^n \tag{XI.2}$$

Παρατήρηση XI.2.1. Αν (x, y, z) μη-τετριμμένη λύση της (XI.2) και $d = \text{ΜΚΔ}(x, y, z)$, τότε προφανώς και $(x/d, y/d, z/d)$ επίσης λύση. Επομένως αρκεί να ελέγξουμε την ύπαρξη μόνο των λεγόμενων πρωταρχικών λύσεων, δηλαδή λύσεων με $d = 1$.

Παρατήρηση XI.2.2. Στη συγκεκριμένη περίπτωση, η έννοια της πρωταρχικής λύσης ταυτίζεται με αυτή της έννοιας των πρώτων μεταξύ τους ανά δύο αφού αν $d = \text{ΜΚΔ}(x, y) > 1$, τότε υπάρχει πρώτος q με $q \mid x$ και $q \mid y$ οπότε και $q \mid z^n = x^n + y^n$ συνεπώς και $q \mid \text{ΜΚΔ}(x, y, z) = 1$. Επομένως θα ψάξουμε για την ύπαρξη λύσεων (x, y, z), όπου τα x, y, z, είναι ανά δύο πρώτα μεταξύ τους.

Παρατήρηση XI.2.3. Αν η (XI.2) δεν έχει μη-τετριμμένη λύση για κάποιο n, τότε δεν έχει μη-τετριμμένη λύση και κάθε πολλαπλάσιο του n. Πράγματι αν η

$$X^{nm} + Y^{nm} = Z^{nm}$$

είχε λύση (x, y, z), τότε και η (XI.2) θα είχε λύση την (x^m, y^m, z^m).

Παρατήρηση XI.2.4. Κάθε ακέραιος ≥ 3 διαιρείται είτε από το 4 είτε από κάποιον περιττό πρώτο p. Συνεπώς αρκεί να αποδείξουμε την εικασία για $n = 4$ και n περιττό πρωτο p. Η περίπτωση $n = 4$ θα εξεταστεί στις ασκήσεις.

Από εδώ και κάτω θα θεωρήσουμε την περίπτωση $n = p$ περιττός πρώτος και θα επεκταθούμε στην αριθμητική του σώματος $K = \mathbb{Q}(\zeta_p)$, $\zeta = e^{\frac{2\pi i}{p}}$. Θα γράφουμε για συντομία ζ αντί για ζ_p.

XI.3 Κυκλοτομικά σώματα $K = \mathbb{Q}(\zeta_p)$, $p \in \mathbb{P}$

Υπενθυμίζουμε ότι ο δακτύλιος των ακεραίων αλγεβρικών είναι ο $R = \mathbb{Z}[\zeta]$, η διακρίνουσα του $K = \mathbb{Q}(\zeta)$ είναι η $D_K = (-1)^{\frac{p-1}{2}} p^{p-2}$. Ο νόμος ανάλυσης στο $K = \mathbb{Q}(\zeta)$ δίνεται ως εξής: Αν $Q = \langle 1 - \zeta \rangle$, τότε $pR = Q^{p-1}$, και $N_K(Q) = p$. Για κάθε άλλο πρώτο q, $q \neq p$ ισχύει ότι $e = 1$ και f είναι ο ελάχιστος φυσικός ώστε

$$q^f \equiv 1 \mod p$$

και $r = \frac{p-1}{f}$. Το μέγιστο πραγματικό υπόσωμα του $K = \mathbb{Q}(\zeta)$ είναι το σώμα $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$.

XI.3.1 Οι μονάδες του $K = \mathbb{Q}(\zeta_p)$

Ο στόχος αυτής της παραγράφου είναι να αποδείξουμε το ακόλουθο:

Θεώρημα XI.3.1 (1ο Λήμμα του Kummer)**.** *Κάθε μονάδα $\epsilon \in E(R_K)$ του κυκλοτομικού σώματος $K = \mathbb{Q}(\zeta)$ έχει τη μορφή*

$$\epsilon = \eta \zeta^s,$$

όπου η η πραγματική μονάδα του K, δηλαδή $\eta \in E(R_0)$, $R_0 = \mathbb{Z}[\zeta + \zeta^{-1}]$ και $s \in \mathbb{Z}$.

Η απόδειξη θα πραγματωθεί σε μια σειρά λημμάτων.

Λήμμα XI.3.2 (Βήμα 1)**.** *Οι μόνες ρίζες της μονάδας που ανήκουν στο κυκλοτομικό σώμα αριθμών $K = \mathbb{Q}(\zeta)$ είναι οι $\pm\zeta^s$, $s \in \mathbb{Z}$*

Απόδειξη. Πρώτα από όλα θα αποδείξουμε ότι $i \notin \mathbb{Q}(\zeta)$. Πράγματι, αν $i \in \mathbb{Q}(\zeta)$ επειδή $2 = i(1-i)^2$ έπεται ότι $\langle 2 \rangle = \langle (1-i) \rangle^2 = P^2$. Αυτό σημαίνει ότι το ιδεώδες $\langle 2 \rangle$ διακλαδίζεται στο σώμα K. Αυτό όμως είναι άτοπο, διότι ο μόνος πρώτος που διακλαδίζεται στο K είναι ο περιττός πρώτος p.

Έστω τώρα q πρώτος $q \neq 2$ και $q \neq p$. Ισχυριζόμαστε ότι $\zeta_q \notin \mathbb{Q}(\zeta)$. Αν ίσχυε $\zeta_q \in \mathbb{Q}(\zeta)$, θα είχαμε $\mathbb{Q}(\zeta_q) \subset \mathbb{Q}(\zeta)$. Στο σώμα $\mathbb{Q}(\zeta_q)$ ισχύει η ανάλυση του ιδεώδους $\langle q \rangle = \langle (1 - \zeta_q) \rangle^{q-1}$. Αυτό σημαίνει ότι το q διακλαδίζεται στο $\mathbb{Q}(\zeta_q)$ και συνεπώς και στο $\mathbb{Q}(\zeta)$, άτοπο. Άρα $\zeta_q \notin \mathbb{Q}(\zeta)$ για κάθε περιττό q, $q \neq p$.

Στη συνέχεια θα αποδείξουμε ότι $e^{\frac{2\pi i}{p^2}} \notin \mathbb{Q}(\zeta_p)$. Το $e^{\frac{2\pi i}{p^2}}$ είναι ρίζα του πολυωνύμου $x^{p^2} - 1$ αλλά όχι του $x^p - 1$, είναι πρωταρχική p^2-ρίζα του 1. Επομένως είναι ρίζα του πολυωνύμου

$$f(x) = \frac{x^{p^2} - 1}{x^p - 1} = \sum_{t=0}^{p-1} x^{tp}.$$

Το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$, αφού το $f(x+1)$ είναι ανάγωγο στο $\mathbb{Q}[x]$, σύμφωνα με το κριτήριο του Eisenstein εφαρμοσμένο για τον πρώτο p. Δηλαδή $f(x) = \mathrm{Irr}(e^{\frac{2\pi i}{p^2}}, \mathbb{Q})$. Συνεπώς

$$[\mathbb{Q}(e^{\frac{2\pi i}{p^2}}) : \mathbb{Q}] = \deg f(x) = p(p-1) > p-1.$$

Επομένως δεν ισχύει ότι $e^{\frac{2\pi i}{p^2}} \in \mathbb{Q}(\zeta)$, διότι τότε

$$[\mathbb{Q}(e^{\frac{2\pi i}{p^2}}) : \mathbb{Q}] \leq p-1,$$

άτοπο. Άρα $e^{\frac{2\pi i}{p^2}} \notin \mathbb{Q}(\zeta)$.

Αν τώρα υποθέσουμε ότι μια ρίζα της μονάδας (για κάποιο φυσικό m) $\zeta_m = e^{\frac{2\pi i}{m}} \in \mathbb{Q}(\zeta)$, σύμφωνα με τα παραπάνω ισχύουν $4 \nmid m$, $q \nmid m$, για κάθε $q \neq p, 2$ και $p^2 \nmid m$, συνεπώς κατ' ανάγκη $m \mid 2p$. Το τελευταίο μας λέει ότι το σώμα K περιέχει το πολύ τις $2p$-ρίζες της μονάδας. □

Λήμμα XI.3.3 (Βήμα 2). *Για κάθε ακέραιο αλγεβρικό $\alpha \in \mathbb{Q}(\zeta)$ ισχύει ότι υπάρχει ακέραιος $b \in \mathbb{Z}$ ώστε*

$$\alpha \equiv b \mod Q, Q = \langle 1-\zeta \rangle.$$

Απόδειξη. Είναι γνωστό ότι $N_K(Q) = p$. Άρα ο δακτύλιος R_K/Q έχει p-στοιχεία. Οι ακέραιοι αριθμοί $0, 1, 2, \ldots, p-1$ ανήκουν σε διαφορετικά στοιχεία του R_K/Q ανά δύο, δηλαδή σε διαφορετικές κλάσεις modulo Q. Πράγματι, αν $r, s \in \{0, 1, 2, \ldots, p-1\}$, και $r \equiv s \mod Q$, τότε $r - s \in Q$. Όμως $r - s \in \mathbb{Z}$ συνεπώς $r - s \in Q \cap \mathbb{Z} = p\mathbb{Z}$, συνεπώς $r \equiv s \mod p \Rightarrow p \mid |r-s|$. Επειδή $|r-s| < p \Rightarrow |r-s| = 0$ και $r = s$. Άρα για κάθε $\alpha \in R_K$ υπάρχει $b \in \mathbb{Z}$ $b \in \{0, 1, 2, \ldots, p-1\}$ ώστε να ισχύει $a \equiv b \mod Q$. □

Πόρισμα XI.3.4. *Για κάθε $\alpha \in R_K$ υπάρχει $a \in \mathbb{Z}$ ώστε να ισχύει*

$$\alpha^p \equiv a \mod Q^p$$

Απόδειξη. Από το XI.3.3 έχουμε ότι για κάθε $\alpha \in R_K$ υπάρχει $b \in \mathbb{Z}$ ώστε $\alpha \equiv b \mod Q$ συνεπώς

$$\alpha^p - b^p = \prod_{j=0}^{p-1} (\alpha - \zeta^j b).$$

Το $Q = \langle 1-\zeta \rangle$ συνεπώς $\zeta \equiv 1 \mod Q$. Επομένως, κάθε παράγοντας του γινομένου ειναι ισότιμος προς $\alpha - b \mod Q$. Συνεπώς $\alpha^p - b^p \equiv 0 \mod Q^p$, δηλαδή το πόρισμα ισχύει για $a = b^p$. □

Λήμμα XI.3.5 (Βήμα 3ο). *Αν α ακέραιος αλγεβρικός αριθμός $\alpha \in \widetilde{\mathbb{Z}}$ του οποίου όλοι οι συζυγείς αριθμοί (όλες οι ρίζες του αναγώγου πολυωνύμου $f(x) = \mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$) έχουν απόλυτη τιμή 1, τότε ο α είναι ρίζα της μονάδας.*

Απόδειξη. Έστω α_i, $i = 1, 2, \ldots, n$ οι συζυγείς του α,

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

Για κάθε ακέραιο $\ell > 0$ θεωρούμε το πολυώνυμο

$$f_\ell(x) = (x-\alpha_1^\ell)(x-\alpha_2^\ell)\cdots(x-\alpha_n^\ell).$$

Από το βασικό θεώρημα των συμμετρικών πολυωνύμων, έπεται ότι $f_\ell(x) \in \mathbb{Z}[x]$ για κάθε $\ell \in \mathbb{Z}, \ell > 0$. Αν $f_\ell(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, τότε για κάθε $0, 1, 2, \ldots, n-1$ ισχύει $|a_j| \leq \binom{n}{j}$.

Αυτό προκύπτει άμεσα από τις σχέσεις ριζών-συντελεστών και του γενονότος ότι όλες οι ρίζες των πολυωνύμων $f_\ell(x)$ έχουν απόλυτη τιμή 1. Αυτό σημαίνει ότι υπάρχουν πεπερασμένου πλήθους πολυώνυμα, με συντελεστές ακεραίους, των οποίων οι συντελεστές πληρούν την παραπάνω ανισότητα. Συνεπώς υπάρχουν τουλάχιστον δύο ακέραιοι ℓ, m, $\ell \neq m$ ώστε

$$f_\ell(x) = f_m(x).$$

Αυτό σημαίνει ότι υπάρχει μια μετάθεση π του συνόλου $\{1, 2, \dots, n\}$ για την οποία ισχύει $\alpha_j^\ell = \alpha_{\pi(j)}^m$, για $j = 1, 2, \dots, m$. Επαγωγικά, έπεται ότι

$$\alpha_j^{\ell^r} = \alpha_{\pi^r(j)}^{m^r}.$$

Επειδή, $\pi^{n!}(j) = j$, έχουμε

$$\alpha_j^{\ell^{n!}} = \alpha_j^{m^{n!}} \Rightarrow \alpha_j^{(\ell^{n!} - m^{n!})} = 1,$$

Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $\ell^{n!} - m^{n!} > 0$. Ο εκθέτης είναι $\neq 0$, αφού $\ell^{n!} \neq m^{n!}$ συνεπώς α_j είναι ρίζα της μονάδας για κάθε $j = 1, 2, \dots, n-1$. □

Απόδειξη. (Θεωρήματος XI.3.1-1ου λήμματος του Kummer) Έστω ϵ μια μονάδα του $K = \mathbb{Q}(\zeta)$. Μία βάση ακεραιότητας του R_K είναι η $\mathfrak{B} = \{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$. Αφού $\epsilon \in R_K$ υπάρχει $f(x) \in \mathbb{Z}[x]$, $\deg f(x) < p - 1$ ώστε $\epsilon = f(\zeta)$. Οι συζυγείς του ϵ είναι οι $\epsilon^{(i)} = f(\zeta^i)$, $i = 1, 2, \dots, p-1$ και

$$N_K(\epsilon) = \epsilon^{(1)}\epsilon^{(2)} \cdots \epsilon^{(p-1)} = \pm 1,$$

αφού $\epsilon \in E(R_K)$.

Συνεπώς και όλα τα συζυγή της ϵ είναι επίσης μονάδες του K. Προφανώς,

$$\epsilon^{(p-i)} = f(\zeta^{p-i}) = f(\zeta^{-i}) = f(\overline{\zeta}^i) = \overline{f(\zeta^i)} = \overline{\epsilon}^i,$$

όπου $\overline{\alpha}$ συμβολίζει τον μιγαδικό συζυγή του α. Επομένως

$$\epsilon^{(p-i)}\epsilon^{(i)} = \overline{\epsilon}^{(i)}\epsilon^{(i)} = |\epsilon^{(i)}|^2 > 0.$$

Άρα

$$N_K(\epsilon) = (\epsilon^{(1)}\epsilon^{(p-1)})(\epsilon^{(2)}\epsilon^{(p-2)}) \cdots > 0$$

Το συμπέρασμα λοιπόν είναι $N_K(\epsilon) = 1$. Τώρα, τα πηλίκα $\epsilon^{(i)}/\epsilon^{(p-i)}$ είναι μονάδες του K και για κάθε $i = 1, 2, \dots$

$$|\epsilon^{(i)}/\epsilon^{(p-i)}| = |\epsilon^{(i)}/\overline{\epsilon}^{(i)}| = |\epsilon^{(i)}|/|\overline{\epsilon}^{(i)}| = 1.$$

Από το λήμμα XI.3.5 έχουμε ότι τα πηλίκα αυτά είναι ρίζες της μονάδας. Σύμφωνα με το λήμμα XI.3.2 θα είναι της μορφής $\epsilon/\epsilon^{(p-1)} = \pm\zeta^t$, $t \in \mathbb{Z}$. Επειδή $\zeta^t = \zeta^{p+t}$ και ένας από τους t και $p + t$ είναι άρτιος μπορούμε να γράψουμε

$$\epsilon/\epsilon^{(p-1)} = \pm\zeta^{2s}, s > 0.$$

Θα πρέπει να βρούμε το σωστό πρόσημο. θα αποδείξουμε ότι αυτό είναι το «συν». Θεωρούμε τον ακέραιο αλγεβρικό του K, $\zeta^{-s}\epsilon \in R_K$. Σύμφωνα με το λήμμα XI.3.3 υπάρχει $a \in \mathbb{Z}$ ώστε

$$\zeta^{-s}\epsilon = a \mod Q$$

Παίρνουμε τα μιγαδικά συζυγή

$$\overline{\zeta}^{-s}\overline{\epsilon} \equiv a \mod \overline{Q},$$

δηλαδή

$$\zeta^s\epsilon^{(p-1)} \equiv a \mod \overline{Q}.$$

Το $Q = \langle 1-\zeta\rangle$ συνεπώς $\overline{Q} = \langle 1-\overline{\zeta}\rangle = \langle 1-\zeta^{p-1}\rangle$. Από τον νόμο ανάλυσης $\langle 1-\zeta^{p-1}\rangle = Q$. Από τα παραπάνω προκύπτει η ισοτιμία

$$\zeta^{-s}\epsilon \equiv \zeta^{s}\epsilon^{(p-1)} \mod Q$$

συνεπώς

$$\epsilon/\epsilon^{(p-1)} \equiv \zeta^{2s} \mod Q.$$

Αν στη σχέση $\epsilon/\epsilon^{(p-1)} = \pm\zeta^{2s}$ είχαμε το πλήν θα είχαμε

$$\zeta^{2s} \equiv -\zeta^{2s} \mod Q$$

συνεπώς $Q \mid 2\zeta^{2s}$ άρα $N_K(Q) \mid N_K(2)N_K(\zeta)^{2s}$. Καταλήγουμε στο ότι $p \mid 2^{p-1}$, άτοπο αφού p περιττός. Επομένως ισχύει

$$\epsilon/\epsilon^{(p-1)} = \zeta^{2s},$$

δηλαδή

$$\zeta^{-s}\epsilon = \zeta^{s}\epsilon^{(p-1)},$$

οπότε

$$\overline{\zeta^{-s}\epsilon} = \overline{\zeta}^{-s}\overline{\epsilon} = \zeta^{s}\epsilon^{(p-1)} = \zeta^{-s}\epsilon$$

συνεπώς ο $\zeta^{-s}\epsilon \in \mathbb{R}$. Αν $\zeta^{-s}\epsilon := \eta \in \mathbb{R}$, τότε $\epsilon = \zeta^{s}\eta$. □

Παρατήρηση XI.3.6. Δείτε και το λήμμα 3.37 σελ. 74 των σημείωσεων [16].

Αυτό μας εξασφαλίζει ότι ϵ είναι ρίζα της μονάδας επί μονάδα πραγματική αλλά φυσικά όχι ότι η ρίζα της μονάδας είναι της μορφής ζ^{s}.

XI.4 Τα θεωρήματα του Kummer

Ο πιο μικρός p για τον οποίο το σώμα $K = \mathbb{Q}(\zeta_p)$ δεν έχει μονοσήμαντη ανάλυση είναι ο $p = 23$.

Πρόταση XI.4.1. $h_{\mathbb{Q}(\zeta_{23})} > 1$.

Απόδειξη. Είναι γνωστό ότι $\mathbb{Q}(\sqrt{-23}) \subset \mathbb{Q}(\zeta_{23})$. Από τον νόμο ανάλυσης στα τετραγωνικά σώματα αριθμών, έχουμε $\left(\frac{-23}{2}\right) = 1$, αφού $-23 \equiv 1 \mod 8$. Επομένως $2R_{\mathbb{Q}(\sqrt{-23})} = P\overline{P}$, όπου $P = \langle 2, \frac{1+\sqrt{-23}}{2}\rangle$. Έστω Q πρώτο ιδεώδες του K ώστε να ισχύει $Q \cap R_{\mathbb{Q}(\sqrt{-23})} = P$. Η $N_{K/\mathbb{Q}(\sqrt{-23})}(Q) = P^{f}$. Επίσης $[K:\mathbb{Q}] = \phi(23) = 23-1 = 22$, $[\mathbb{Q}(\sqrt{-23}):\mathbb{Q}] = 2$ άρα $[\mathbb{Q}(\zeta_{23}):\mathbb{Q}(\sqrt{-23})] = 11$. Επειδή f διαιρεί τον βαθμό της επέκτασης, ισχύει $f = 1$ ή $f = 11$. Το $\mathbb{Q}(\sqrt{-23})$ έχει αριθμό κλάσεων ιδεωδών $h_{\mathbb{Q}(\sqrt{-23})} = 3$. Επομένως έχουμε ότι το P δεν είναι κύριο ιδεώδες του K ενώ το P^3 είναι. Συνεπώς ούτε το P^{11} είναι κύριο, αλλιώς P^3 κύριο και P^2 κύριο συνεπώς και το P είναι κύριο, άτοπο.

Τελικά καταλήγουμε ότι το P^{f} ($f = 1$ είτε $f = 11$) δεν είναι κύριο. Αλλά ούτε το Q είναι κύριο, αφού αν το Q ήταν κύριο θα ήταν και η norm $N_{K/\mathbb{Q}(\sqrt{-23})}(Q) = P^{f}$ κύριο, άτοπο. □

Σημείωση XI.4.2. Μια στοιχειώδη απόδειξη μπορεί να βρει κανείς στο βιβλίο του Marcus, [9]. Εκεί αποδεικνύεται ότι μια συγκεκριμένη ανάλυση δεν είναι μονοσήμαντη.

Σημείωση XI.4.3. Το ότι το P δεν είναι κύριο φαίνεται και από τη θεωρία των τετραγωνικών μορφών, δεν αντιστοιχεί στην κύρια κλάση. Πράγματι, η κλάση που αντιστοιχεί στο $P = \langle 2, \frac{1+\sqrt{-23}}{2}\rangle = \langle a, \frac{-b+\sqrt{\Delta}}{2}\rangle$ είναι η $ax^2+bxy+cy^2$, $c = \frac{b^2-\Delta}{4a}$, δηλαδή $2x^2-xy+3y^2$.

Παρατήρηση XI.4.4. Οι Montgomery και απέδειξαν, ανεξάρτητα ο ένας του άλλου, ότι ο αριθμός κλάσεων του κυκλοτομικού σώματος αριθμών $K = \mathbb{Q}(\zeta_p)$ είναι $h_K = 1$ αν και μόνο αν $p \le 19$, [15].

Είναι σαφές ότι ο Kummer χρειάστηκε να αποδείξει ότι αν $A \lhd R_{\mathbb{Q}(\zeta_p)}$ ώστε A^k κύριο ιδεώδες και Μ.Κ.Δ$(k, h_K) = 1$, τότε κατ' ανάγκη το A κύριο, στην περίπτωση που το k ήταν το p της εξίσωσης του Fermat.

Αναγκαστικά λοιπόν, θεώρησε πρώτους p, ώστε $p \nmid h_{\mathbb{Q}(\zeta_p)}$. Αυτούς τους πρώτους τους ονόμασε ομαλούς (regular). Τώρα, αν η εξίσωση του Fermat

$$x^p + y^p = z^p$$

έχει λύση (x, y, z) με Μ.Κ.Δ.$(x, y, z) = 1$, τότε το p έχει δύο δυνατότητες

I Το $p \nmid x$, $p \nmid y$, $p \nmid z$.

II Το p διαιρεί ακριβώς έναν από τους x, y, z.

Αυτές θα λέγονται πρώτη και δεύτερη περίπτωση της εικασίας Fermat. Θα μελετηθούν ξεχωριστά. Όλα βέβαια, για regular πρώτους.

XI.4.1 Πρώτη περίπτωση της εικασίας

Θεώρημα XI.4.5 (Πρώτη περίπτωση της εικασίας Fermat για ομαλούς πρώτους)**.** *Αν p περιττός πρώτος, ο οποίος είναι ομαλός η εξίσωση του Fermat*

$$x^p + y^p = z^p$$

δεν έχει λύση $(x, y, z) \in \mathbb{Z}^3$ για την οποία $p \nmid xyz$.

Απόδειξη. Η απόδειξη θα γίνει με απαγωγή στο άτοπο. Υποθέτουμε ότι η εξίσωση έχει μια ακέραια λύση x, y, z με $p \nmid xyz$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι οι x, y, z είναι ανά δύο πρώτοι μεταξύ τους.

Παραγοντοποιούμε το αριστερό μέρος της εξίσωσης στο $R_K = \mathbb{Z}[\zeta]$ και έχουμε

$$\prod_{i=0}^{p-1} (x + \zeta^i y) = z^p.$$

Από τη σχέση αυτή έπεται ότι

$$\prod_{i=0}^{p-1} \langle x + \zeta^i y \rangle = \langle z \rangle^p.$$

Λήμμα XI.4.6 (Βήμα 1ο)**.** *Θα αποδείξουμε ότι τα ιδεώδη $\langle x + \zeta^i y \rangle$ είναι ανά-δύο πρώτα μεταξύ τους.*

Πράγματι, αν P πρώτο ιδεώδες του K και

$$P \mid \langle x + \zeta^k y \rangle \text{ και } P \mid \langle x + \zeta^\ell y \rangle$$

για $0 \le k < \ell < p - 1$, τότε $x + \zeta^k y \in P$ και $x + \zeta^\ell y \in P$, επομένως

$$(x + \zeta^k y) - (x + \zeta^\ell y) = \zeta^k y - \zeta^\ell y = y\zeta^k(1 - \zeta^{\ell - k}) \in P.$$

Γνωστό, ότι

$$\langle 1 - \zeta^{\ell - k} \rangle = \langle 1 - \zeta \rangle = Q$$

και ζ^k μονάδα του R_K. Επομένως

$$y(1 - \zeta) \in P \Rightarrow y \in P \text{ είτε } (1 - \zeta) \in P.$$

Αν $y \in P$, τότε από την αρχική σχέση, $P \mid \langle z \rangle^p \Rightarrow P \mid \langle z \rangle \Rightarrow z \in P$. Επειδή Μ.Κ.Δ$((y, z) = 1$ υπάρχουν $a, b \in \mathbb{Z}$ ώστε $ay + bz = 1$ και επομένως $1 \in P$, άτοπο.

Αν $(1-\zeta) \in P$, τότε $P \mid \langle 1-\zeta\rangle = Q$. Όμως Q πρώτο ιδεώδες του R_K συνεπώς $P = Q$. Εδώ η σχέση $z \in Q = P$ δίνει $Q \mid \langle z\rangle$ συνεπώς $N_K(Q) \mid N_K(z)$ συνεπώς $p \mid z^{p-1}$ και τελικά $p \mid z$, άτοπο αφού έχουμε υποθέσει ότι $p \nmid xyz$.

Ο R_K είναι περιοχή Dedekind, άρα έχουμε μονοσήμαντη ανάλυση σε γινόμενο πρώτων ιδεωδών. Από αυτό προκύπτει ότι λόγω του λήμματος XI.4.6

$$\langle x+\zeta y\rangle = A^p, \text{ όπου } A \lhd R_K.$$

Εδώ χρησιμοποιούμε το γεγονός ότι ο πρώτος p είναι ομαλός. Συνεπώς υπάρχει $\alpha \in R_K$ ώστε $A = \langle\alpha\rangle$. Από τη σχέση $\langle x+\zeta y\rangle = \langle\alpha^p\rangle$ οπότε υπάρχει $\epsilon \in E(R_K)$ ώστε $x+\zeta y = \epsilon\alpha^p$. Από το 1ο λήμμα του Kummer, έχουμε ότι $\epsilon = \zeta^s\eta$, $\eta \in \mathbb{R}$. Άρα, $x+\zeta y = \eta\zeta^s\alpha^p$. Από το πόρισμα του λήμματος XI.3.3 έπεται ότι υπάρχει $a \in \mathbb{Z}$ ώστε

$$\alpha^p \equiv a \mod Q^p$$

Επομένως

$$x+\zeta y \equiv \eta a\zeta^s \mod Q^p$$

Επειδή

$$\langle p\rangle = Q^{p-1} \Rightarrow \langle p\rangle \mid Q^p$$

συνεπώς $x+\zeta y \equiv \eta a\zeta^s \mod \langle p\rangle$. Το ζ^{-s} είναι μονάδα του R_K. Πολλαπλασιάζουμε με αυτή την μονάδα

$$\zeta^{-s}(x+\zeta y) \equiv \eta a \mod \langle p\rangle$$

Παίρνουμε τα μιγαδικά συζυγή

$$\zeta^s(x+\zeta^{-1}y) \equiv \eta a \mod \langle p\rangle$$

Επομένως,

$$x\zeta^{-s} + y\zeta^{1-s} - x\zeta^s - y\zeta^{s-1} \equiv 0 \mod \langle p\rangle \tag{XI.3}$$

Το $1+\zeta$ είναι μονάδα του R_K. (Στην

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1}),$$

θέτουμε $x = -1$. Το γινόμενο $(-1-\zeta)(-1-\zeta^i)\cdots = 1$.) Στην τελευταία ισοτιμία, μελετούμε τις δυνατές τιμές τους. Έστω ότι $s \equiv 0 \mod p$. Τότε $\zeta^s = 1$ και η ισοτιμία (XI.3) γίνεται

$$y(\zeta-\zeta^{-1}) \equiv 0 \mod \langle p\rangle$$

συνεπώς

$$y(1+\zeta)(1-\zeta) \equiv 0 \mod \langle p\rangle$$

Το $(1+\zeta)$ είναι μονάδα επομένως

$$y(1-\zeta) \equiv 0 \mod \langle p\rangle$$

Το $\langle p\rangle = Q^{p-1} = \langle 1-\zeta\rangle^{p-1}$ και $p-1 \geq 2$. Αυτό σημαίνει ότι $y \equiv 0 \mod \langle 1-\zeta\rangle$ άρα $y \in \langle 1-\zeta\rangle$ δηλαδή $(1-\zeta) \mid y \Rightarrow N_K(\langle 1-\zeta\rangle) = p \mid N_K(y) = y^{p-1} \Rightarrow p \mid y$, το οποίο είναι αντίθετο στην υπόθεση $p \nmid xyz$. Άρα $s \not\equiv 0 \mod p$.

Ομοίως και το $s \not\equiv 1 \mod p$ (άσκηση).

Η τελευταία ισοδυναμία (XI.3) γράφεται

$$\text{υπάρχει } \alpha \in R_K = \mathbb{Z}[\zeta] \text{ ώστε } \alpha p = x\zeta^{-s} + y\zeta^{1-s} - x\zeta^s - y\zeta^{s-1}.$$

Σύμφωνα με αυτά που αποδείξαμε κανένας από τους εκθέτες $-s, 1-s, s, s-1$ δεν διαιρείται με p.

$$\alpha = \frac{x}{p}\zeta^{-s} + \frac{y}{p}\zeta^{1-s} - \frac{x}{p}\zeta^s - \frac{y}{p}\zeta^{s-1}. \tag{XI.4}$$

Το α είναι ακέραιος αλγεβρικός. Μια βάση του $R_K = \mathbb{Z}[\zeta]$ είναι το σύνολο $B = \{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$. Αν και οι τέσσερις εκθέτες είναι μεταξύ τους μη-ισοδύναμοι modulo p, τότε για να είναι ο $\alpha \in R_K$ πρέπει $\frac{x}{p} \in \mathbb{Z}$, συνεπώς $p \mid x$, άτοπο. Αυτό σημαίνει ότι υπάρχει κάποιο ζευγάρι εκθετών που είναι ισοδύναμοι modulo p. Όμως επειδή $s \not\equiv 0, 1 \mod p$ η μοναδική δυνατότητα που απομένει είναι

$$1 - s \equiv s \mod p \text{ δηλαδή } 2s \equiv 1 \mod p$$

αλλά τότε η (XI.4) γράφεται

$$\alpha p\zeta^s = x + y\zeta - x\zeta^{2s} - y\zeta^{2s-1} = x + y\zeta - x\zeta - y = (x - y)(1 - \zeta).$$

Παίρνουμε norm και των δύο μελών

$$N_K(\alpha)N_K(p)N_K(\zeta^s) = N_K(x - y)N_K(1 - \zeta) \Rightarrow N_K(\alpha)p^{p-1}(\pm 1) = N_K(x - y)N_K(1 - \zeta)$$

$$\Rightarrow p \mid (x - y)^{p-1} \Rightarrow p \mid (x - y) \Rightarrow x \equiv y \mod p$$

Για λόγους συμμετρίας της $x^p + y^p = z^p$ (εδώ φαίνεται γιατί τη γράφουμε συχνά και ως $x^p + y^p + z^p = 0$) έχουμε και $y \equiv z \mod p$. Συνεπώς

$$0 = x^p + y^p + z^p \equiv 3x^p \mod p$$

Επειδή $p \nmid x$ έχουμε $p = 3$. Αυτή την περίπτωση θα την εξετάσουμε τώρα ξεχωριστά. Παρατηρούμε ότι αν $a \in \mathbb{Z}, 3 \nmid a$, $a^3 \equiv \pm 1 \mod 9$. Επομένως η $x^3 + y^3 + z^3 = 0$ για x, y, z με $3 \nmid xyz$ δίνει

$$\pm 1 \pm 1 \pm 1 \equiv 0 \mod 9$$

η οποία είναι αδύνατη. Συνεπώς και για $p = 3$ η εξίσωση δεν έχει λύση και η απόδειξη τελείωσε. □

Παρατήρηση XI.4.7. Το 1985 οι Adleman, Heath-Brown και Fourry, [1], [6] απέδειξαν ότι υπάρχει ένα άπειρο σύνολο S πρώτων αριθμών για το οποίο η πρώτη περίπτωση της εικασίας του Fermat ισχύει για κάθε πρώτο αριθμό $p \in S$.

Το θεώρημα αντιπροσώπευε ένα σημαντικό βήμα στην εποχή του. Για πρώτη φορά αποδεικνυόταν ότι η πρώτη περίπτωση της εικασίας του Fermat ίσχυε για άπειρο πλήθος πρώτων αριθμών. Επειδή όμως το σύνολο S δεν είναι effectively ορισμένο, δεν ήταν δυνατόν με τη μέθοδο της απόδειξης να αποδειχτεί ότι η πρώτη περίπτωση της εικασίας ισχύει για κάθε πρώτο αριθμό.

XI.5 Η δευτερη περίπτωση της εικασίας του Fermat (για ομαλούς πρώτους)

Θεώρημα XI.5.1. *Για κάθε ομαλό πρώτο p η εξίσωση του Fermat*

$$x^p + y^p = z^p \tag{XI.5}$$

δεν έχει ακέραια λύση x, y, z με $xyz \neq 0$, $p \nmid xy$, $p \mid z$.

Απόδειξη. Η μέθοδος που θα εφαρμόσουμε εδώ είναι η γνωστή μέθοδος της καθόδου του Fermat. Πρώτα απ'όλα, χωρίς βλάβη της γενικότητας, υποθέτουμε ότι υπάρχει λύση σύμφωνα με τη διατύπωση του θεωρήματος και τον επιπλέον περιορισμό ότι Μ.Κ.Δ.$(x, y, z) = 1$ ή ισοδύναμα οι x, y, z είναι ανά δύο πρώτοι μεταξύ τους.

Επίσης παρατηρούμε ότι η υπόθεση ότι $p \nmid xy$ και $p \mid z$, σημαίνει ότι ακριβώς ένας από τους ακεραίους x, y, z διαιρείται με p. Αν για παράδειγμα $p \mid y$, τότε γράφουμε την εξίσωση στη μορφή

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

Από τον γνωστό νόμο ανάλυσης

$$\langle p\rangle = \langle 1-\zeta\rangle^{p-1}$$

συνεπώς υπάρχει $\epsilon \in E(R_K)$ ώστε $p = (1-\zeta)^{p-1}\epsilon$. Ο z γράφεται στη μορφή

$$z = p^k z_0, p \nmid z_0, \text{ και } k \geq 1.$$

Επομένως η εξίσωση παίρνει τη μορφή

$$x^p + y^p = \epsilon(1-\zeta)^{pm} z_0^p \tag{XI.6}$$

όπου $m = k(p-1)$. Εδώ το ϵ είναι διαφορετική μονάδα από την προηγούμενη. Αρκεί να αποδείξουμε ότι η εξίσωση (XI.6), δεν έχει λύση.

Θα αποδείξουμε μάλιστα κάτι πιο ισχυρό. Όχι μόνο ότι δεν έχει λύση $(x,y,z_0) \in \mathbb{Z}^3$ με $p \nmid xyz_0$, αλλά ότι δεν είναι επιλύσιμη ούτε σε $x,y,z_0 \in R = \mathbb{Z}[\zeta]$ τα οποία να είναι πρώτοι προς τον $1-\zeta$.

Υποθέτουμε λοιπόν ότι η (XI.6) έχει λύσεις σύμφωνα με τις παραπάνω προϋποθέσεις και επιλέγουμε εκείνη η οποία αντιστοιχεί στην ελάχιστη τιμή του $m \geq 1$. Θα καταλήξουμε σε άτοπο κατασκευάζοντας μια λύση της (XI.6) η οποία θα έχει στη θέση του m, φυσικό αριθμό $< m$. Έστω λοιπόν (x,y,z_0) αυτή η λύση με τον ελάχιστο φυσικό m, ώστε τα x,y,z_0 να είναι πρώτα προς το $1-\zeta$. Το $\epsilon \in E(R_K)$. Εδώ εννοούμε ότι τα κύρια ιδεώδη έχουν μέγιστο κοινό διαιρέτη R_K.

Όπως κάναμε και στην πρώτη περίπτωση της εικασίας του Fermat, παραγοντοποιούμε και περνούμε στην ισότητα των αντίστοιχων ιδεωδών

$$\prod_{k=0}^{p-1} \langle x+\zeta^k y\rangle = Q^{pm} A^p, \tag{XI.7}$$

όπου $Q = \langle 1-\zeta\rangle \nmid A$ και $A = \langle z_0\rangle$. Επειδή $pm \geq p > 0$ στο δεξιό μέλος υπάρχει το Q, άρα το Q διαιρεί κάποιον παράγοντα του αριστερού μέλους, δηλαδή υπάρχει i, $0 \leq i \leq p-1$ ώστε $Q \mid \langle x+\zeta^i y\rangle$. Γράφουμε το $x+\zeta^i y$ ως εξής:

$$x+\zeta^i y = (x+\zeta^k y) - \zeta^k(1-\zeta^{i-k})y \text{ για κάθε } k = 0,1,2,\ldots,p-1.$$

Το $Q \mid \langle 1-\zeta^{i-k}\rangle = \langle 1-\zeta\rangle = Q$ και $Q \mid \langle x+\zeta^i y\rangle$ συνεπώς

$$Q \mid \langle x+\zeta^k y\rangle, \text{ για κάθε } k = 0,1,2,\ldots,p-1 \tag{XI.8}$$

Θα αποδείξουμε όμως ότι τα ιδεώδη $\langle x+\zeta^k y\rangle$ είναι ανά δύο διαφορετικά modulo Q^2. Πράγματι, αν για κάποια k,i $0 \leq \kappa < i \leq p-1$ ίσχυε

$$x+\zeta^k y \equiv x+\zeta^i y \mod Q^2$$

θα είχαμε $\zeta^k y(1-\zeta^{i-k}) \equiv 0 \mod Q^2$ το οποίο όμως είναι αδύνατο αφού $Q = \langle 1-\zeta^{i-k}\rangle$ και το $\langle \zeta^k y\rangle = \langle y\rangle$ είναι πρώτο ως προς το Q εξ υποθέσεως του y.

Συνεπώς, τα πηλίκα

$$\frac{x+\zeta^k y}{1-\zeta} : k = 0,1,2,\ldots,p-1 \tag{XI.9}$$

είναι ανά δύο, μη ισοδύναμα modulo Q, αλλιώς θα είχαμε δύο της μορφής $x+\zeta^k y$ και $x+\zeta^\ell y$, $k \neq \ell$ ισοδύναμα modulo Q^2. Είναι γνωστό ότι $N_K(Q) = p$, δηλαδή $\#R/Q = p$. Επομένως τα πηλίκα αυτά απαρτίζουν ένα πλήρες σύστημα υπολοίπων modulo Q. Συνεπώς, ένα ακριβώς από αυτά αντιπροσωπεύει τη μηδενική κλάση $0 \mod Q$, δηλαδή το κύριο ιδεώδες κάποιου (ακριβώς ενός) πηλίκου της εξίσωσης (XI.9) θα διαιρείται από το Q. Συνεπώς, ακριβώς ένα από τα ιδεώδη της εξίσωσης (XI.8), δηλαδή $\langle x+\zeta^k y\rangle$ θα διαιρείται από το Q^2. (Αν

$$\frac{x+\zeta^k y}{1-\zeta} \equiv 0 \mod Q^2 \Rightarrow \langle x+\zeta^k y\rangle \equiv 0 \mod Q^2,$$

αφού $Q = \langle 1-\zeta \rangle$). Επειδή στη σχέση (XI.6), το y μπορεί να αντικατασταθεί από έναν, οποιονδήποτε από τους αριθμούς $\zeta^k y$ (σημείωση: $y^p = (\zeta^k y)^p$ για κάθε $k = 0, 1, 2, \ldots, p-1$ και το $\zeta^k y$ συνεχίζει να είναι πρώτο προς το Q). Χωρίς βλάβη της γενικότητας λοιπόν μπορούμε να υποθέσουμε ότι

$$Q^2 \mid (x + y). \tag{XI.10}$$

Επομένως, όλοι οι υπόλοιποι παράγοντες της (XI.7)

$$x + \zeta^k y : k = 1, 2, \ldots, p-1$$

διαιρούνται με Q, αλλά όχι με το Q^2. Το αριστερό μέλος της (XI.7) διαιρείται τουλάχιστο με $Q^2 Q^{p-1} = Q^{p+1}$ συνεπώς στη σχέση (XI.7) το $m > 1$. Έστω $\mathfrak{m} = \text{Μ.Κ.Δ.}(\langle x \rangle, \langle y \rangle)$. Εξ υποθέσεως των x, y τα $\langle x \rangle, \langle y \rangle$ δεν διαιρούνται από το Q, δηλαδή

$$Q \nmid \mathfrak{m}. \tag{XI.11}$$

Τώρα $\mathfrak{m} \mid \langle x \rangle$ και $\mathfrak{m} \mid \langle y \rangle$ συνεπώς $x + \zeta y \in \mathfrak{m}$ και

$$\mathfrak{m} \mid \langle x + \zeta y \rangle. \tag{XI.12}$$

Το $Q \mid \langle x + \zeta y \rangle$, οπότε λόγω της (XI.11) έχουμε

$$Q\mathfrak{m} \mid \langle x + \zeta y \rangle. \tag{XI.13}$$

Ανάλογα το

$$\mathfrak{m} \mid \langle x + y \rangle \tag{XI.14}$$

και επειδή $Q \parallel \langle x + \zeta^k y$ για κάθε $k = 1, 2, \ldots, p-1$, έπεται ότι $Q^{p-1} \parallel \prod_{k=1}^{p-1} \langle x + \zeta^k y \rangle$ ενώ από τη σχέση (XI.7)

$$Q^p \mathfrak{m} \parallel \prod_{k=0}^{p-1} x + \zeta^k y \rangle.$$

Αυτό σημαίνει ότι

$$Q^{p\mathfrak{m}-(p-1)} = Q^{p(\mathfrak{m}-1)+1} \parallel \langle x + y \rangle. \tag{XI.15}$$

Από τις (XI.11), (XI.14), (XI.15) έχουμε

$$Q^{p(\mathfrak{m}-1)+1}\mathfrak{m} \mid \langle x + y \rangle \Rightarrow \langle x + y \rangle = Q^{p(\mathfrak{m}-1)+1}\mathfrak{m}B_0 \tag{XI.16}$$

και από την (XI.13)

$$\langle x + \zeta^k y \rangle = Q\mathfrak{m}B_K \text{ για } k = 1, 2, \ldots, p-1. \tag{XI.17}$$

Στο επόμενο βήμα θα αποδείξουμε ότι τα B_k, $k = 0, 1, 2, \ldots, p-1$ είναι ανά δύο πρώτα μεταξύ τους. Πράγματι, έστω ότι για δύο B_i, B_k $0 \le i < k \le p-1$ υπάρχει πρώτο ιδεώδες P_1 το οποίο $P_1 \mid B_i$ και $P_1 \mid B_k$. Επομένως θα έχουμε

$$Q\mathfrak{m}P_1 \mid \langle x + \zeta^i y \rangle \text{ και } Q\mathfrak{m}P_1 \mid \langle x + \zeta^k y \rangle \tag{XI.18}$$

Ξαναθυμίζουμε τη σχέση

$$x + \zeta^k y = x + \zeta^i y - \zeta^i y(1 - \zeta^{k-i})$$

άρα

$$Q\mathfrak{m}P_1 \mid \zeta^i y(1 - \zeta^{k-i}). \tag{XI.19}$$

Επίσης γράφουμε

$$x + \zeta^k y = x(1 - \zeta^{k-i}) + \zeta^{k-i}(x + \zeta^i y)$$

άρα και

$$Q\mathfrak{m}P_1 \mid x(1 - \zeta^{k-i}). \tag{XI.20}$$

Από τις (XI.19) και (XI.20) έχουμε ότι $\mathfrak{m}P_1 \mid \langle y\rangle$ και $\mathfrak{m}P_1 \mid \langle x\rangle$. Αυτό όμως είναι άτοπο, αφού $\mathfrak{m} = \text{Μ.Δ.Κ.}(\langle x\rangle, \langle y\rangle)$.

Η σχέση (XI.7) τώρα γράφεται

$$\mathfrak{m}^p Q^{p\,m} B_0 B_1 \cdots B_{p-1} = Q^{p\,m} A^p \Rightarrow \mathfrak{m}^p B_0 B_1 \cdots B_{p-1} = A^p.$$

Επειδή τα B_i είναι ανά δύο πρώτα μεταξύ τους, έπεται ότι υπάρχουν $C_i \lhd R_K$ για τα οποία ισχύει $B_i = C_i^p$, $i = 0, 1, 2, \ldots, p-1$. Επομένως

$$\langle x + y\rangle = Q^{p(m-1)+1}\mathfrak{m}C_0^p \tag{XI.21}$$

$$\langle x + \zeta^k y\rangle = Q^{p(m-1)+1}\mathfrak{m}C_k^p, k = 1, 2, \ldots, p-1 \tag{XI.22}$$

Πολλαπλασιάζουμε τις (XI.21) και (XI.22 «χιαστί» και έχουμε

$$\langle x + \zeta^k y\rangle Q^{p(m-1)} = \langle x + y\rangle (C_k C_0^{-1})^p. \tag{XI.23}$$

Το $Q = \langle 1 - \zeta\rangle$ είναι κύριο ιδεώδες συνεπώς και το $(C_k C_0^{-1})^p$ κύριο ιδεώδες.

Εδώ χρησιμοποιούμε την υπόθεση ότι το p είναι ομαλός, δηλαδή $p \nmid h_{\mathbb{Q}(\zeta)}$ και καταλήγουμε στο ότι και $C_k C_0^{-1}$ είναι επίσης κύριο ιδεώδες για κάθε $k = 1, 2, \ldots, p-1$. Έστω

$$C_k C_0^{-1} = \langle \alpha_k/\beta_k\rangle, 1 \le k \le p-1 \quad \alpha_k, \beta_k \in R = \mathbb{Z}[\zeta]. \tag{XI.24}$$

Τα ιδεώδη C_k $1 \le k \le p-1$ και C_0 είναι πρώτα ως προς Q, αφού τα B_i είναι πρώτα προς το Q. Επομένως $\alpha_k \notin Q$, $\beta_k \notin Q \Rightarrow Q \nmid \langle \alpha_k\rangle$ και $Q \nmid \langle \beta_k\rangle$. Τώρα, ισότητα δύο κυρίων ιδεωδών σημαίνει ότι οι γεννήτορες είναι συνεταιρικοί. Επομένως

$$(x + \zeta^k y)(1-\zeta)^{p(m-1)} = (x + y)\left(\frac{\alpha_k}{\beta_k}\right)^p \epsilon_k, \text{ για } 1 \le k \le p-1 \tag{XI.25}$$

Τα $\epsilon_k \in E(R)$. Η ακόλουθη ισότητα είναι προφανής:

$$(x + \zeta y)(1 + \zeta) - (x + \zeta^2 y) = \zeta(x + y). \tag{XI.26}$$

Πολλαπλασιάζουμε και τα δύο μέλη της (XI.26) με $(1-\zeta)^{p(m-1)}$ και έχουμε

$$(x + \zeta y)(1 + \zeta)(1-\zeta)^{p(m-1)} - (x + \zeta^2 y)(1-\zeta)^{p(m-1)} = \zeta(1-\zeta)^{p(m-1)}(x + y). \tag{XI.27}$$

Γράφουμε την (XI.25), για $k = 1$ και $k = 2$

$$(x + zy)(1-\zeta)^{p(m-1)} = (x + y)\left(\frac{\alpha_1}{\beta_1}\right)^p \epsilon_1 \tag{XI.28}$$

$$(x + \zeta^2 y)(1-\zeta)^{p(m-1)} = (x + y)\left(\frac{\alpha_2}{\beta_2}\right)^p \epsilon_2 \tag{XI.29}$$

Επομένως,

$$(x + \zeta y)(1-\zeta)^{p(m-1)}(1+\zeta) \overset{(XI.28)}{=} (x + y)\left(\frac{\alpha_1}{\beta_1}\right)^p (1+\zeta)\epsilon_1.$$

Αφαιρούμε την (XI.29)

$$(x + \zeta y)(1-\zeta)^{p(m-1)}(1+\zeta) - (x + \zeta^2 y)(1-\zeta)^{p(m-1)} = \tag{XI.30}$$

$$= (x + y)\left(\frac{\alpha_1}{\beta_2}\right)^p (1+\zeta)\epsilon_1 - (x + y)\left(\frac{\alpha_2}{\beta_2}\right)^p \epsilon_2.$$

Το πρώτο μέλος της (XI.30) ταυτίζεται με το πρώτο μέλος της (XI.27). Επομένως,

$$(x + y)\left(\frac{\alpha_1}{\beta_1}\right)^p (1+\zeta)\epsilon_1 - (x + y)\left(\frac{\alpha_2}{\beta_2}\right)^p \epsilon_2 = \zeta(1-\zeta)^{p(m-1)}(x + y). \tag{XI.31}$$

Απλοποιούμε με $(x+y)$ και διαιρούμε με $\epsilon_1(1+\zeta)$, συγχρόνως πολλαπλασιάζουμε με $(\beta_1\beta_2)^p$:

$$(\alpha_1\beta_2)^p - \frac{\epsilon_2}{\epsilon_1(1+\zeta)}(\alpha_2\beta_1)^p = \frac{\zeta}{\epsilon_1(1+\zeta)}(1-\zeta)^{p(m-1)}(\beta_1\beta_2)^p. \tag{XI.32}$$

Επομένως, καταλήξαμε σε μία εξίσωση της μορφής:

$$\alpha^p + \epsilon_0\beta^p = \epsilon'(1-\zeta)^{p(m-1)}\gamma^p \tag{XI.33}$$

όπου τα $\alpha, \beta, \gamma \in R_K = \mathbb{Z}[\zeta]$ είναι πρώτα προς το Q και $\epsilon_0, \epsilon' \in E(R_K)$.

Θέλουμε να τη μετασχηματίσουμε στη μορφή (XI.6). Μόνο στη θέση του m θα έχουμε τώρα το $m-1$ και έτσι θα έχουμε τώρα το $m-1$ και έτσι θα έχουμε καταλήξει σε άτοπο. Έχουμε ήδη δείξει ότι $m > 1$ συνεπώς $m-1 \geq 1$ συνεπώς $p(m-1) \geq p$. Η (XI.33) επομένως γράφεται

$$\alpha^p + \epsilon_0\beta^p \equiv 0 \mod Q^p \tag{XI.34}$$

Το β πρώτο προς το Q συνεπώς υπάρχει $\beta' \in R_K$ ώστε

$$\beta\beta' \equiv 1 \mod Q^p$$

Πολλαπλασιάζουμε την (XI.34) με το $(\beta')^p$ και έχουμε

$$\epsilon_0 \equiv \delta^p \mod Q^p,$$

όπου $\delta = (-\alpha\beta')^p$, $\delta \in R = \mathbb{Z}[\zeta]$. Από το Βήμα 2 (λήμμα XI.3.3) και το πόρισμα XI.3.4 έχουμε

$$\delta \equiv a \mod Q, \text{ για κάποιο } a \in \mathbb{Z}$$

και $\delta^p \equiv a^p \mod Q^p$. Επομένως έχουμε $\epsilon_0 \equiv a^p \mod Q^p$, $a \in \mathbb{Z}$.

Εδώ χρειαζόμαστε το ακόλουθο:

Θεώρημα XI.5.2 (2ο Λήμμα του Kummer)**.** *Έστω p κάποιος ομαλός πρώτος και $\epsilon \in E(R)$ όπου $R = \mathbb{Z}[\zeta]$. Υποθέτουμε ότι $\epsilon \equiv a \mod p$. Το συμπέρασμα είναι ότι υπάρχει μονάδα $\eta \in E(R)$ για την οποία ισχύει $\epsilon = \eta^p$.*

Σημείωση XI.5.3. $Q^p = Q^{p-1}Q = \langle p \rangle Q$.

Άρα η ισοτιμία

$$\delta^p \equiv a^p \mod Q^p$$

γράφεται

$$\delta^p \equiv b \mod p$$

$b = a^p \in \mathbb{Z}$ και συνεπώς το λήμμα εφαρμόζεται. Η εξίσωσή μας τελικά παίρνει τη μορφή

$$\alpha^p + (\eta\beta)^p = \epsilon'(1-\zeta)^{p(m-1)}\gamma^p,$$

δηλαδή όπως η (XI.6) αλλά με εκθέτη $m-1$ στη θέση του m, άτοπο, αφού ο m ήταν ο ελάχιστος μ' αυτή την ιδιότητα. Συνεπώς, η (XI.6) δεν έχει λύση (x, y, z) με $p \mid z$ και $p \nmid xy$ και το Θεώρημα έχει αποδειχθεί. □

Το θεώρημα XI.5.2 για την απόδειξή του χρειάζεται τη χρήση των p-αδικών αριθμών και παραλείπεται. Για μια απόδειξη δείτε το [2, σελ. 402] και [15, σελ. 79]. Στο τελευταίο δίνεται μια απόδειξη με p-αδικές L-συναρτήσεις και θεωρία κλάσεων σωμάτων.

Παρατήρηση XI.5.4. Με βάση τους πίνακες που έχουν υπολογιστεί, αν μετρήσουμε τους ομαλούς πρώτους, ας πούμε μέσα σε κάποιο διάστημα $(0, x)$, τότε οι ομαλοί πρώτοι είναι περισσότεροι από τους ανώμαλους. Για παράδειγμα μέχρι το 100 οι ανώμαλοι πρώτοι είναι μόνο 3, οι $37, 59, 67$, ενώ όλοι οι πρώτοι είναι 23. Τη δεκαετία του $'60$ ο Siegel εκτίμησε προσεγγιστικά $1 - e^{-1/2} \approx 39\%$ των πρώτων είναι ανώμαλοι και το $e^{-1/2} \approx 61\%$ είναι ομαλοί. Όλοι οι ανώμαλοι πρώτοι μέχρι το 125000 έχουν υπολογιστεί από τον Wagstaff [14].

XI.6 Η αναλυτική θεωρία

Θα μείνουμε όμως, για λίγο στην κλασική θεωρία. Κατ' αναλογία προς την ζήτα συνάρτηση Riemann, ο Dedekind όρισε την ζήτα συνάρτηση αλγεβρικού σώματος αριθμών.

Ορισμός XI.6.1. Έστω K αλγεβρικό σώμα αριθμών

$$\zeta_K(s) := \sum_{A \lhd R} \frac{1}{N_K(A)^s}, s \in \mathbb{C}, \mathrm{Re}(s) > 1.$$

Αποδεικνύεται ότι η $\zeta_K(x)$ συγκλίνει απόλυτα, για $\mathrm{Re}(s) > 1$ και παριστά στο ημιεπίπεδο αυτό μια ολόμορφη συνάρτηση.

Ερώτημα: Αναλυτική επέκταση;
Απάντηση: Έστω $n = [K : \mathbb{Q}]$. Η $\zeta_K(s)$ επεκτείνεται μερόμορφα στο ημιεπίπεδο $\mathrm{Re}(s) > 1 - \frac{1}{n}$ με μοναδικό απλό πόλο για $s = 1$.
Ερώτηση: Ποιο είναι το υπόλοιπο (residuum) για $s = 1$; Έχει αριθμητική σημασία;
Απάντηση: Ναι!

$$\mathrm{Re}_{s=1}(\zeta_K(s)) = \lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}_K}{w\sqrt{|D_K|}} h_k.$$

Εδώ τα $r_1, r_2, w, \sqrt{|D_K|}$ μας είναι ήδη γνωστά. Ο Reg_K είναι μια πολύπλοκη ποσότητα (πιο δύσκολα υπολογίσιμη από τον h_K) και συνεπώς ο τύπος δεν έχει πρακτική σημασία για τον υπολογισμό του h_K.

Αν $f(A) = \frac{1}{N_K(A)^s}$ για κάθε $A \lhd R$, τότε

$$f(A \cdot B) = \frac{1}{N_K(AB)^s} = \frac{1}{N_K(A)^s N_K(B)^s} = f(A)f(B)$$

πλήρως πολλαπλασιαστική. Συνεπώς,

$$\zeta_K(s) = \prod_{P \in \mathbb{P}(K)} \frac{1}{1 - N_K(P)^{-s}}.$$

Παράδειγμα XI.6.2. Η ζ-συνάρτηση του τετραγωνικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{D})$, όπου D η διακρίνουσα του K. Υπενθυμίζουμε τον νόμο ανάλυσης στο K.

$$\langle p \rangle = pR = \begin{cases} PP', N_K(P) = N_K(P') = p, & \text{αν } \left(\frac{D}{p}\right) = 1 \\ P, N_K(P) = p^2, & \text{αν } \left(\frac{D}{p}\right) = -1 \\ P^2, N_K(P) = p, & \text{αν } \left(\frac{D}{p}\right) = 0 \end{cases}$$

Επομένως η ζήτα συνάρτηση γράφεται

$$\begin{aligned} \zeta_K(s) &= \prod_{P \in \mathbb{P}} \frac{1}{1 - N_K(P)^{-s}} \\ &= \prod_{\substack{P \in \mathbb{P} \\ (\frac{D}{p})=1}} \frac{1}{(1-p^{-s})^2} \prod_{\substack{P \in \mathbb{P} \\ (\frac{D}{p})=-1}} \frac{1}{1-p^{-2s}} \prod_{\substack{P \in \mathbb{P} \\ (\frac{D}{p})=0}} \frac{1}{1-p^{-s}} \\ &= \prod_{P \in \mathbb{P}} \frac{1}{1-p^{-s}} \prod_{\substack{P \in \mathbb{P} \\ (\frac{D}{p})=1}} \frac{1}{1-p^{-s}} \prod_{\substack{P \in \mathbb{P} \\ (\frac{D}{p})=-1}} \frac{1}{1+p^{-s}} \prod_{\substack{P \in \mathbb{P} \\ (\frac{D}{p})=0}} \frac{1}{1-0\cdot p^{-s}} \\ &= \zeta_{\mathbb{Q}}(s) \prod_{P \in \mathbb{P}} \frac{1}{1 - \left(\frac{D}{p}\right) p^{-s}} \\ &= \zeta_{\mathbb{Q}}(s) L(s, \chi), \text{ με } \chi(p) = \left(\frac{D}{p}\right). \end{aligned}$$

Έστω τώρα $K = \mathbb{Q}(\zeta_p)$, $p \neq 2$. Πότε είναι ο p ομαλός; Αποδεικνύεται ότι

$$h_K = h_1 h_2, h_1, h_2 \in \mathbb{N},$$

όπου h_1, h_2 ο πρώτος και δεύτερος παράγοντας του αριθμού κλάσεων, h_1 είναι ο αριθμός κλάσεων του μέγιστου πραγματικού υποσώματος $K_0 = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ και $h_2 = [E : E_0]$, όπου E είναι η υποομάδα όλων των πραγματικών μονάδων της $E(R_K)$ και E_0 η υποομάδα αυτής που παράγεται από τις κυκλοτομικές μονάδες, δηλαδή των μονάδων της μορφής

$$\Theta_k = \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}}, \text{ για } k = 2, 3, \ldots, \frac{p-1}{2}.$$

XI.6.1 Συνθήκες υπό τις οποίες ισχύει $p \mid h_1$

Θα ορίσουμε τους αριθμούς Bernoulli

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} z^k, |z| < 1$$

Ισχύει: $B_k = 0$ για k περιττό $k \neq 1$ ενώ

$$B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}, \ldots$$

Θεώρημα XI.6.3. *Για $p \in \mathbb{P}$, $p \neq 2$ το $p \mid h_1$ αν και μόνο αν υπάρχει άρτιος k από τους $2, 4, \ldots, p-3$ ώστε ο p να διαιρεί τον αριθμητή του B_k.*

Θεώρημα XI.6.4. *Αν $p \nmid h_1$, τότε $p \nmid h_2$, συνεπώς και $p \nmid h$.*

Από τα παραπάνω προκύπτει ότι

Θεώρημα XI.6.5. *Ο $p \geq 3$ είναι ομαλός αν και μόνο αν ο p δεν διαιρεί τους αριθμητές των αριθμών Bernoulli $B_2, B_4, \ldots, B_{p-3}$.*

Εικασία Vandiver και Kummer Ισχύει πάντοτε $p \nmid h_2$.

Το 2011 η εικασία αποδείχθηκε [3] για όλους τους πρώτους $< 163 \cdot 10^6$ αποτέλεσμα που επεκτάθηκε για όλους τους πρώτους μικρότερους από 2 δισεκατομύρια το 2017, [7]. Η εικασία του Vandiver είναι μέχρι σήμερα ανοιχτή.

Τέλος, η ειρωνεία της τύχης!

Εικασία Υπάρχουν άπειροι, ομαλοί πρώτοι.

Η εικασία είναι μέχρι σήμερα ανοιχτή ενώ

Θεώρημα XI.6.6. *Υπάρχουν άπειροι ανώμαλοι πρώτοι.*

Για την απόδειξη χρειαζόμαστε ιδιότητες των αριθμών Bernoulli, για την απόδειξη των ιδιοτήτων αυτών παραπέμπουμε στο [2, κεφ. V, σελ. 408-414]

1. Για τους αριθμούς Bernoulli B_{2k} ισχύει:

$$\frac{|B_{2k}|}{2k} \to \infty,$$

όταν $k \to \infty$.

2. Θεώρημα του Staudt: Έστω p ένας πρώτος αριθμός και m κάποιος άρτιος ακέραιος. Αν $(p-1) \nmid m$, τότε ο αριθμός Bernoulli B_m είναι p-ακέραιος, δηλαδή ο p δεν διαιρεί τον παρονομαστή του B_m.
   Αν $(p-1) \mid m$, τότε ο pB_m είναι p-ακέραιος και επιπλέον ισχύει
$$pB_m \equiv -1 \mod p$$

3. Ισοτιμίες του Kummer. Αν p ένας πρώτος αριθμός για τον οποίο ισχύει $(p-1) \nmid m$, όπου m άρτιος, θετικός ακέραιος αριθμός, τότε ο B_m/m είναι p-ακέραιος και ισχύει η ισοτιμία
$$\frac{B_{m+p-1}}{m+p-1} \equiv \frac{B_m}{m} \mod p^2$$

Απόδειξη. (Του θεωρήματος) Όπως και στην απόδειξη ύπαρξης άπειρων πρώτων του Ευκλείδη, υποθέτουμε ότι οι ανώμαλοι πρώτοι είναι πεπερασμένου πλήθους έστω $p_1, p_2, \ldots, p_s$. Αρκεί να βρούμε έναν ακόμη ανώμαλο πρώτο διαφορετικό των p_i, $i = 1, 2, \ldots, s$.

Θεωρούμε τον φυσικό αριθμό
$$n = r(p_1 - 1)(p_2 - 1)\cdots(p_s - 1).$$

Από την 1. συνεπάγεται ότι για αρκετά μεγάλο r ο ρητός αριθμός B_n/n είναι μεγαλύτερος του 1. Έστω p ένας πρώτος ο οποίος διαιρεί τον αριθμητή του B_n (Εννοείται, αφού γράψουμε τον αριθμό πρώτα σε ανάγωγα κλάσματα).

Αν $(p-1) \mid n$, τότε από την 2., έπεται ότι ο p θα διαιρούσε τον παρονομαστή του B_n. Αυτό όμως είναι αδύνατο λόγω της συγκεκριμένης επιλογής του p. Επομένως $(p-1) \nmid n$. Αλλά $(p_i - 1) \mid n$ για κάθε $i = 1, 2, \ldots, n$. Αυτό σημαίνει ότι ο p είναι διαφορετικός των $p_1, p_2, \ldots, p_s$ αλλά και του 2, αφού $2 - 1 = 1 \mid n$.

Στη συνέχεια διαιρούμε τον n με τον $p-1$ και έστω m το υπόλοιπο της διαίρεσης του n με το $p-1$, $n = m + a(p-1)$. Ισχύει $2 \mid m$ και $2 \le m \le p-3$. Αφού $(p-1) \nmid n$, έπεται ότι και $(p-1) \nmid m$. Σύμφωνα με την 3., στον δακτύλιο των p-ακεραίων ισχύει
$$\frac{B_m}{m} \equiv \frac{B_n}{n} \mod p$$

Αλλά $\frac{B_n}{n} \equiv 0 \mod p$. Συνεπώς και $\frac{B_m}{m} \equiv 0 \mod p$, οπότε και $B_m \equiv 0 \mod p$. Ο m είναι ένας άρτιος $m \in \{2, 4, 6, \ldots, p-3\}$ και για αυτόν ισχύει $B_m \equiv 0 \mod p$. Από το θεώρημα XI.6.5 έπεται ότι ο p είναι ανώμαλος. □

XI.7 Ασκήσεις

1. Να αποδειχθεί ότι στο θεώρημα (πρώτη περίπτωση της εικασίας Fermat) ισχύει $s \not\equiv 1 \mod p$
2. Να αποδειχτεί η εικασία του Fermat για $n = 4$.
3. Να αποδειχθεί ότι ο δακτύλιος των ακέραιων αλγεβρικών του σώματος $K_0 = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ είναι $R_0 = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.
4. Εντελώς ανάλογα να αποδειχτεί ότι για το $K_0 = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ ισχύει $R_0 = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.
5. Ο αριθμός $\alpha = \frac{4}{5} + \frac{3}{5}i$ έχει μέτρο 1, και ο συζυγής του το ίδιο. Είναι ο α ρίζα της μονάδας;
6. Να αποδειχθεί ότι όλα τα κυκλοτομικά σώματα $K = \mathbb{Q}(\zeta_m)$, για $m = 3, 4, 5, 6, 7, 8$ έχουν αριθμό κλάσεων ιδεωδών 1.

Βιβλιογραφία

[1] Adleman, L. M. & Heath-Brown, D. R. *The first case of Fermat's last theorem*. *Invent. Math.* 79.2 (1985), pp. 409–416. ISSN: 0020-9910. URL: https://doi.org/10.1007/BF01388981.

[2] Borevich, Z. & Shafarevich, R. I. *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York-London, 1966, pp. x+435.

[3] Buhler, J. & Harvey, D. *Irregular primes to 163 million*. *Math. Comp.* 80.276 (2011), pp. 2435–2444. ISSN: 0025-5718. URL: https://doi.org/10.1090/S0025-5718-2011-02461-0.

[4] Buhler, J. et al. *Irregular primes and cyclotomic invariants to 12 million*. Vol. 31. 1-2. Computational algebra and number theory (Milwaukee, WI, 1996). 2001, pp. 89–96. URL: https://doi.org/10.1006/jsco.1999.1011.

[5] Edwards, H. M. *Fermat's Last Theorem*. Vol. 50. Graduate Texts in Mathematics. A genetic introduction to algebraic number theory, Corrected reprint of the 1977 original. Springer-Verlag, New York, 1996, pp. xvi+410. ISBN: 0-387-90230-9; 0-387-95002-8.

[6] Fouvry, É. *Sur le premier cas du théorème de Fermat*. *Séminaire de théorie des nombres, Paris 1983–84*. Vol. 59. Progr. Math. Birkhäuser Boston, Boston, MA, 1985, pp. 91–104.

[7] Hart, W., Harvey, D. & Ong, W. *Irregular primes to two billion*. *Math. Comp.* 86.308 (2017), pp. 3031–3049. ISSN: 0025-5718. URL: https://doi.org/10.1090/mcom/3211.

[8] Lang, S. *Cyclotomic Fields I and II*. second. Vol. 121. Graduate Texts in Mathematics. With an appendix by Karl Rubin. Springer-Verlag, New York, 1990, pp. xviii+433. ISBN: 0-387-96671-4. URL: https://doi.org/10.1007/978-1-4612-0987-4.

[9] Marcus, D. A. *Algebraic Number Fields*. Universitext. 2nd edition of [MR0457396], With a foreword by Barry Mazur. Springer, 2018, pp. xviii+203. ISBN: 978-3-319-90232-6; 978-3-319-90233-3.

[10] Ribenboim, P. *13 lectures on Fermat's last theorem*. Springer-Verlag, New York-Heidelberg, 1979, xvi+302 pp. (1 plate). ISBN: 0-387-90432-8.

[11] Ribenboim, P. *Fermat's Last Theorem, for amateurs*. Springer-Verlag, New York, 1999, pp. xiv+407. ISBN: 0-387-98508-5.

[12] Rosen, M. *Remarks on the history of Fermat's last theorem 1844 to 1984*. *Modular Forms and Fermat's Last Theorem (Boston, MA, 1995)*. Springer, New York, 1997, pp. 505–525.

[13] Stewart, I. & Tall, D. *Algebraic Number Theory and Fermat's Last Theorem*. 4th edition. CRC Press, Boca Raton, FL, 2016, pp. xix+322. ISBN: 978-1-4987-3839-2.

[14] Wagstaff Jr., S. S. *The irregular primes to* 125000. *Math. Comp.* 32.142 (1978), pp. 583–591. ISSN: 0025-5718. URL: https://doi.org/10.2307/2006167.

[15] Washington, L. C. *Introduction to Cyclotomic Fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, pp. xiv+487. ISBN: 0-387-94762-0. URL: https://doi.org/10.1007/978-1-4612-1934-7.

[16] Αντωνιάδης, Ι. Α. *L-σειρές*. Ηράκλειο: Πανεπιστήμιο Κρήτης, 1999.

XII

Εικασία Fermat, Η μοντέρνα προσέγγιση

XII.1 Εισαγωγή

Ενώ οι προσπάθειες για την απόδειξη της εικασίας του Fermat συνεχίζονταν και η θεωρία των κυκλοτομικών σωμάτων επεκτεινόταν προς διάφορες κατευθύνσεις, δύο άλλοι κλάδοι της Θεωρίας Αριθμών γνώριζαν τεράστια ανάπτυξη.

Ο ένας είναι η αριθμητική των ελλειπτικών καμπυλών. Η μέθοδος της προσέγγισης αυτής της προβληματικής είναι κυρίως γεωμετρική και αλγεβρική. Ο άλλος κλάδος είναι η θεωρία των modular μορφών. Εδώ η μέθοδος είναι κυρίως αναλυτική. Από τη φύση της προβληματικής τους λοιπόν οι δύο κλάδοι θεωρήθηκαν για αρκετό χρονικό διάστημα ότι δεν έχουν κάποια σχέση μεταξύ τους.

Αυτό βέβαια αποδείχθηκε τελικά ότι ήταν λάθος. Στο παρόν κεφάλαιο θα ασχοληθούμε με βασικές έννοιες των δύο αυτών κλάδων.

Γενικά για τη θεωρία των αλγεβρικών καμπυλών παραπέμπουμε στο [11] για τη θεωρία των ελλειπτικών καμπυλών στο [24], για τη θεωρία των modular συναρτήσεων στο [16].

XII.2 Βασικές έννοιες ελλειπτικών καμπυλών

Οι ελλειπτικές καμπύλες είναι μια συγκεκριμένη κλάση αλγεβρικών καμπυλών. Φυσικό είναι να εξετάσουμε εν συντομία τις αλγεβρικές καμπύλες.

XII.2.1 Αφινικές αλγεβρικές καμπύλες

Έστω K ένα σώμα και $\overline{K}$ μια (ως γνωστό μοναδική κατά προσέγγιση ισομορφίας) αλγεβρική θήκη του K. Το αφινικό επίπεδο υπεράνω του K, $\mathbb{A}^2_K$ ορίζεται ως το σύνολο

$$\mathbb{A}^2_K(\overline{K}) = \{P = (x, y) : x, y \in \overline{K}\}$$

και έχει τις ακόλουθες ιδιότητες

1. Για κάθε επέκταση $L \supset K$ το σύνολο των L-ρητών σημείων του $\mathbb{A}^2_K$ είναι το

$$\mathbb{A}^2_K(L) = \{(x, y) : x, y \in L\} = L \times L.$$

2. Μια ομαλή συνάρτηση επί του $\mathbb{A}^2_K$ δίνεται μέσω ενός πολυωνύμου $f(x, y) \in K[x, y]$. Για κάθε επέκταση $L \subset K$ το πολυώνυμο f ορίζει μια συνάρτηση

$$\begin{aligned} f_L : \mathbb{A}^2_K(L) &\longrightarrow L \\ (x, y) &\longmapsto f_L(x, y) := f(x, y) \end{aligned}$$

3. Μία ρητή συνάρτηση επί του $\mathbb{A}^2_K$ δινεται μέσω ενός στοιχείου

$$f = \frac{g}{h} \in K(x,y), \text{ όπου } K(x,y) \text{ είναι το σώμα πηλίκων του } K[x,y].$$

Η ρητή συνάρτηση f θα λέγεται ομαλή στο $P = (x,y) \in \mathbb{A}^2_K(L)$, όταν $h(x,y) \neq 0$. Η f ορίζει τότε για κάθε $L \supset K$ μία συνάρτηση

$$f_L : \{P \in \mathbb{A}^2_K(L) : f \text{ ομαλή στο } P\} \longrightarrow L.$$

Από τα παραπάνω προκύπτει ότι οι ομαλές συναρτήσεις είναι οι ρητές συναρτήσεις οι οποίες είναι ομαλές παντού, δηλαδή για όλα τα σημεία του $\mathbb{A}^2_K(L)$ και για όλα τα σώματα $L \supset K$.

Τέλος, το σώμα των ρητών συναρτήσεων του αφινικού επιπέδου $\mathbb{A}^2_K$, $K(x,y)$ λέγεται το σώμα συναρτήσεων του $\mathbb{A}^2_K$.

Μια αφινική (επίπεδη) καμπύλη C υπεράνω του K ορίζεται μέσω ενός πολυωνύμου $f \in K[x,y]$ με $\deg(f) \geq 1$. Θα γράφουμε

$$C : f(x,y) = 0$$

1. Για κάθε επέκταση $L \supset K$ το σύνολο των L-ρητών σημείων της καμπύλης

$$C(L) := \{P \in \mathbb{A}^2_K(L) : f_L(P) = 0\} = \{(x,y) \in L \times L : f(x,y) = 0\}.$$

2. Οι ομαλές (regular) συναρτήσεις επί της C είναι κλάσεις ισοδυναμίας πολυωνύμων του $K[x,y]$. (Δύο πολυώνυμα g και h του $K[x,y]$ είναι ισοδύναμα όταν $f \mid (g-h)$). Κάθε αντιπρόσωπος, έστω g, μιας κλάσης ισοδυναμίας ορίζει μια συνάρτηση

$$g_L : C(L) \ni (x,y) \longmapsto g(x,y) \in L$$

η οποία εξαρτάται αποκλειστικά από την κλάση ισοδυναμίας. Το σύνολο των ομαλών συναρτήσεων επί της C ορίζει έναν δακτύλιο, τον αφινικό δακτύλιο συντεταγμένων της C,

$$K[C] \cong \frac{K[X,Y]}{\langle f(x,y)\rangle}$$

3. Μια ρητή συνάρτηση επί της C είναι μια κλάση ισοδυναμίας ρητών συναρτήσεων

$$g/h \in K(x,y),$$

όπου f και h δεν έχουν κοινό διαιρέτη, διάφορο σταθεράς. Το g_1/h_1 είναι ισοδύναμο προς το g_2/h_2, όταν

$$f \mid (g_1h_2 - g_2h_1).$$

Μια ρητή συνάρτηση ϕ θα λέγεται ομαλή στο σημείο $P \in C(L)$, όταν υπάρχει κάποιος αντιπρόσωπος της g/h με $h_L(P) \neq 0$. Έτσι για κάθε $L \supset K$ ορίζει η ϕ μια συνάρτηση

$$\phi_L : \{P \in C(L) : g/h \text{ ομαλή στο } P\} \longrightarrow L.$$

4. Η C λέγεται ανάγωγη όταν το πολυώνυμο $f(x,y) \in K[x,y]$ είναι ανάγωγο. Η C λέγεται γεωμετρικά ανάγωγη όταν το πολυώνυμο $f(x,y)$ είναι απολύτως ανάγωγο, δηλαδή είναι ανάγωγο στον δακτύλιο $\overline{K}[x,y]$.

Αν η C είναι ανάγωγη, τότε το πολυώνυμο $f(x,y)$ είναι ανάγωγο, συνεπώς το ιδεώδες $\langle f(x,y)\rangle = K[x,y]f(x,y)$ είναι πρώτο, δηλαδή ο δακτύλιος συντεταγμένων $K[C]$ είναι ακέραια περιοχή.

Οι ρητές συναρτήσεις επί της C τότε αποτελούν το σώμα πηλίκων του $K[C]$, το σώμα συναρτήσεων $K(C)$ της C.

Παραδείγματα XII.2.1. 1. Έστω η αφινική καμπύλη «ο άξονας των x» $C : Y = 0$. Επομένως $f(x,y) = y$. Τα L-ρητά σημεία αυτής είναι $C(L) = L \times \{0\}$. Ο δακτύλιος συντεταγμένων είναι

$$K[C] = \frac{K[x,y]}{\langle f(x,y)\rangle} = \frac{K[x,y]}{y} \cong K[x]$$

και το σώμα συναρτήσεων

$$K(C) \cong K(x).$$

2. Έστω $C : x^2 + y^2 = 1$, επομένως $f(x,y) = x^2 + y^2 - 1$. Για κάθε σώμα L, $L \supset \mathbb{Q}$ έχουμε τα ρητά σημεία $(0, \pm 1)$ και $(\pm 1, 0)$. Μπορεί να αποδείξει κανείς (άσκηση) ότι

$$C(L) = \left\{ \left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2} \right) : t \in L, t^2 \neq -1 \right\} \cup \{(0,-1\}.$$

Έστω $g(x,y) = \frac{y-1}{x}$ μια ρητή συνάρτηση της C. Θα εξετάσουμε πού είναι ομαλή. Είναι σίγουρα ομαλή στα σημεία που η x-συνιστώσα δεν μηδενίζεται. Επομένως απομένουν προς έλεγχο τα σημεία $(0, \pm 1)$. Στο $(0,-1)$ η ρητή συνάρτηση $g(x,y)$ μηδενίζεται στον παρανομαστή, αλλά ο αριθμητής έχει την τιμή -2. Αυτό σημαίνει ότι η $g(x,y)$ δεν είναι ομαλή στο $(0,-1)$.

Στο $(0,1)$ μηδενίζονται τόσο ο αριθμητής όσο και ο παρονομαστής. Μπορούμε όμως να γράψουμε

$$\frac{y-1}{x} = \frac{(y-1)(y+1)}{x} = \frac{y^2-1}{x(y+1)} =\sim \frac{-x^2}{x(y+1)} = -\frac{x}{y+1}.$$

Αυτό σημαίνει ότι στο $(0,1)$ η συνάρτηση ορίζεται και έχει τιμή ίση με το μηδέν.

3. Κάθε καμπύλη της μορφής

$$C : y^2 = x^3 + ax + b$$

είναι γεωμετρικά ανάγωγη αφού κάθε παραγοντοποίησή της θα πρέπει να είναι της μορφής

$$f(x,y) = y^2 - x^3 - ax - b = (y - g(x))(y - h(x)) = y^2 - (g(x) + h(x))y + g(x)h(x),$$

δηλαδή θα είχαμε $h(x) = -g(x)$ και

$$x^3 + ax + b = g(x)^2,$$

το οποίο είναι αδύνατο, αφού το αριστερό πολυώνυμο είναι βαθμού 3 και το δεξιό είναι άρτιου βαθμού.

Στη συνέχεια υποθέτουμε ότι η καμπύλη $C : f(x,y) = 0$ είναι γεωμετρικά ανάγωγη. Αν το σημείο $P = (0,0)$ είναι σημείο της καμπύλης, τότε το ανάπτυγμα Taylor της καμπύλης στο P έχει τη μορφή:

$$0 = f(x,y) = f_1(x,y) + f_2(x,y) + \cdots$$

όπου $f_m(x,y)$ ομογενές πολυώνυμο βαθμού m. Αν d είναι ο ελάχιστος ακέραιος για τον οποίο το (εδώ όχι κατ' ανάγκη ανάγωγο) πολυώνυμο $f_d(x,y) \neq 0$, τότε η καμπύλη $f_d(x,y) = 0$ είναι μια προσέγγιση της C σε μία αρκετά μικρή περιοχή του σημείου $(0,0)$.

Ορισμός XII.2.2. Η καμπύλη θα λέγεται ομαλή ή μη-ιδιάζουσα στο P όταν ισχύει $f_1(x,y) \neq 0$, δηλαδή όταν η καμπύλη προσεγγίζεται στο σημείο P από μία ευθεία γραμμή.

Η $f_1(x,y)$ έχει τη μορφή

$$f_1(x,y) = Ax + By \text{ με } A = \left.\frac{\partial f}{\partial x}\right|_{P=(0,0)} \text{ και } B = \left.\frac{\partial f}{\partial y}\right|_{P=(0,0)}.$$

Συνεπώς η καμπύλη θα είναι ομαλή στο $P(0,0)$ όταν μία τουλάχιστον από τις δύο παραγώγους στο P είναι διάφορη του μηδενός.

Αν το P είναι ιδιάζον και d είναι ο ελάχιστος ακέραιος για τον οποίο το πολυώνυμο $f_d(x,y)$ είναι διάφορο του μηδενός, τότε αυτό αναλύεται σε γραμμικούς παράγοντες (σε μία αλγεβρική θήκη του σώματος ορισμού K)

$$f_d(x,y) = \prod_{i=1}^{d}(\alpha_i x + \beta_i y)$$

και οι d ευθείες $\alpha_i x + \beta_i y$ λέγονται *εφαπτόμενες της καμπύλης* στο P (προσέχοντας, φυσικά την πολλαπλότητα αν κάποιοι παράγοντες επαναλαμβάνονται).

Αν το $P \neq (0,0)$ τότε κάνουμε επιτρεπτή αλλαγή συντεταγμένων η οποία να στέλνει το P στο $(0,0)$ (ή ισοδύναμα υπολογίζουμε το ανάπτυγμα Taylor στο P).

Αλλά ποιες είναι οι επιτρεπτές αλλαγές συνεταγμένων; Στο αφινικό επίπεδο είναι μη-ιδιάζοντες γραμμικοί μετασχηματισμοί ακολουθούμενοι από μία μεταφορά,

$$v \mapsto Mv + w, M \in \mathrm{GL}_2(K), w \in \mathbb{A}^2(K).$$

Αν L είναι μια ευθεία του επιπέδου και C μία αφινική καμπύλη οι οποίες τέμνονται στο σημείο $P = (x_0, y_0)$, για να υπολογίσουμε την πολλαπλότητα τομής αντικαθιστούμε τη μία μεταβλητή (αφού λύσουμε τη γραμμική εξίσωση της ευθείας ως προς την άλλη) στην καμπύλη και λύνουμε μια εξίσωση μίας μεταβλητής.

Παραδείγματα XII.2.3.

1. Αν $L : x + y + 1 = 0$ και $C : y = x^2 + x$, βρίσκουμε $x^2 + 2x + 1 = 0$ το οποίο σημαίνει ότι η ευθεία τέμνει την καμπύλη με πολλαπλότητα 2 στο σημείο $P = (-1, 0)$.
2. Αν $L : y - x = 0$ και $C : x^2 + y^2 = 1$, τότε η ευθεία τέμνει την καμπύλη σε δύο σημεία $P_1 = (\sqrt{2}/2, \sqrt{2}/2)$ και $P_2 = (-\sqrt{2}/2, -\sqrt{2}/2)$ με πολλαπλότητα ένα στο καθένα. Τα σημεία αυτά είναι $\mathbb{Q}(\sqrt{2})$-ρητά αλλά όχι $\mathbb{Q}$-ρητά.

Παρατήρηση XII.2.4. Αν η καμπύλη C δεν είναι ανάγωγη, τότε η έννοια της πολλαπλότητας τομής ευθείας και καμπύλης έχει και πάλι νόημα εκτός αν η ευθεία είναι μια συνιστώσα της καμπύλης.

Μία ρητή συνάρτηση ορίζεται σε όλα (σχεδόν) τα σημεία της καμπύλης εκτός από το πολύ πεπερασμένου πλήθους. Η διαπίστωση αυτή είναι άμεση συνέπεια του ακόλουθου λήμματος:

Λήμμα XII.2.5. *Έστω $G, H \in K[x,y]$ πρώτα μεταξύ τους. Το σύνολο*

$$M = \{(\xi,\eta) \in K^2 : G(\xi,\eta) = H(\xi,\eta) = 0\}$$

είναι πεπερασμένο και περιέχεται στο $\overline{K} \times \overline{K}$.

Απόδειξη. Τα πολυώνυμα είναι πρώτα μεταξύ τους και στον $K(x)[y]$ υπάρχουν $a(x), b(x) \in K(x)$ τέτοια ώστε

$$a(x)G(x,y) + b(x)H(x,y) = 1.$$

Αν κάνουμε τα $a(x), b(x)$ ομώνυμα και πολλαπλασιάσουμε με τον κοινό παρονομαστή, τότε έχουμε

$$A(x)G(x,y) + B(x)H(x,y) = Q(x), A(x), B(x), Q(x) \in K[x] \text{ και } Q(x) \neq 0.$$

Συνεπώς για κάθε $(\xi,\eta) \in M(G,H)$ έχουμε $G(\xi,\eta) = H(\xi,\eta) = 0$ και επομένως $Q(\xi) = 0$.

Ανάλογα, αν εργαστούμε στον $K(y)[x]$, έχουμε ότι υπάρχει $R(y) \in K[y]$, $R(y) \neq 0$ τέτοιο ώστε $R(\eta) = 0$ για κάθε $(\xi,\eta) \in M(G,H)$. Τα Q και R όμως έχουν πεπερασμένο πλήθος ριζών, συνεπώς υπάρχουν πεπερασμένου πλήθους $(\xi,\eta) \in M(G,H)$.

Προφανώς, αφού ξ, η είναι ρίζες πολυωνύμων (των Q και R αντίστοιχα) με συντελεστές από το K τα $(\xi,\eta) \in M(G,H)$, $(\xi,\eta) \in \overline{K} \times \overline{K}$. □

Πόρισμα XII.2.6. *Αν $\phi \in K(C)$, τότε η ϕ δεν ορίζεται σε πεπερασμένο το πολύ πλήθος σημείων.*

Απόδειξη. Η ϕ θα έχει τη μορφή $\phi = G(\overline{x},\overline{y})/H(\overline{x},\overline{y})$ με $G, H \in K[x,y]$ και $\overline{x} = x + I$, $\overline{y} = y + I$, όπου $I = \langle F \rangle$ το ιδεώδες ορισμού της C και F το πολυώνυμο που ορίζει την C. Η ϕ δεν είναι ορισμένη στο (ξ,η) το πολύ για τα σημεία (ξ,η) για τα οποία να ισχύει $H(\xi,\eta) = 0$. Τα σημεία αυτά ανήκουν όλα στο σύνολο $M(F,H)$. Το σύνολο είναι πεπερασμένο, αφού F και H είναι πρώτα μεταξύ τους. (Αν δεν ήταν πρώτα μεταξύ τους, επειδη το F είναι ανάγωγο, θα είχαμε $F \mid H$, οπότε για κάθε $(x,y) \in C$ θα ίσχυε $H(x,y) = 0$ και η ϕ δεν θα υπήρχε, αφού δεν θα ήταν πουθενά ορισμένη). □

XII.2.2 Το προβολικό επίπεδο και προβολικές καμπύλες

Έστω K ένα σώμα και $\overline{K}$ μια αλγεβρική θήκη του K. Στον αφινικό χώρο

$$\mathbb{A}^3_K \setminus \{(0,0,0)\} = \{(x,y,z) \in \overline{K}, (x,y,z) \neq (0,0,0)\}$$

ορίζουμε μια σχέση ισοδυναμίας:

$$(x_1,y_1,z_1) \sim (x_2,y_2,z_2) \text{ όταν υπάρχει } \lambda \in \overline{K}^* \text{ τέτοιο ώστε } x_2 = \lambda x_1, y_2 = \lambda y_1, z_2 = \lambda z_1.$$

Η επαλήθευση ότι πρόκειται για μια σχέση ισοδυναμίας αφήνεται ως άσκηση. Το σύνολο των στοιχείων μιας κλάσης ισοδυναμίας

$$\{\lambda(x_1, y_1.z_1) : \lambda \in \overline{K}^*\}$$

θα το συμβολίζουμε με $[x_1 : y_1 : z_1]$. Το *προβολικό επίπεδο* $\mathbb{P}^2_K$ υπεράνω του σώματος K ορίζεται ως το σύνολο

$$\mathbb{P}^2_K = \{[x : y : z] : x, y, z \in \overline{K}\}.$$

Για κάθε επέκταση $L \supset K$ το σύνολο των L-ρητών σημείων του $\mathbb{P}^2_K$ ορίζεται ως εξής:

$$\mathbb{P}^2_K(L) = \{[x : y : z] \in \mathbb{P}^2_K : x, y, z \in L\}.$$

Οι ρητές συναρτήσεις του $\mathbb{P}^2_K$, ορίζονται ως πηλίκα ομογενών πολυωνύμων $F(x,y,z), G(x,y,z) \in K[x,y,z]$, ίδιου βαθμού. Η ρητή συνάρτηση F/G θα λέγεται ομαλή στο σημείο $P = [x : y : z] \in \mathbb{P}^2_K(L)$, όταν $G(x,y,z) \neq 0$. (Αφού το G είναι ομογενές, η σχέση $G(x,y,z) \neq 0$ είναι καλά ορισμένη).

Η ρητή συνάρτηση F/G επάγει μια συνάρτηση

$$(F/G)_L : \{P \in \mathbb{P}^2_K(L) : F/G \text{ ομαλή στο } P\} \longmapsto \frac{F(x,y,z)}{G(x,y,z)} \in L.$$

Προφανώς η συνάρτηση είναι καλά ορισμένη.

Παρατήρηση XII.2.7. Δεν υπάρχουν ομαλές, διάφορες της σταθεράς συναρτήσης, σε όλο το προβολικό επίπεδο, αφού ένα πολυώνυμο δεν μας δίνει μια καλά ορισμένη συνάρτηση (εκτός αν είναι σταθερή) και το πηλίκο F/G έχει πάντοτε σημεία στον $\mathbb{P}^2_K = \mathbb{P}^2_K(\overline{K})$ στα οποία μηδενίζεται η G.

Παρατήρηση XII.2.8. Ανάλογα ορίζεται η έννοια του n-διάστατου προβολικού χώρου $\mathbb{P}^n_K$ για κάθε $n \in \mathbb{N}$. Για $n = 1$ ο χώρος $\mathbb{P}^1_K$, ονομάζεται *προβολική ευθεία*.

Μπορούμε να εμφυτεύσουμε το

$$\begin{aligned} \mathbb{A}^2_K(L) &\hookrightarrow \mathbb{P}^2_K(L) \\ (x,y) &\mapsto [x : y : 1] \end{aligned}$$

Αντίστροφα, σε κάθε σημείο $[x : y : z] \in \mathbb{P}^2_K(L)$ με $z \neq 0$ μπορούμε να αντιστοιχίσουμε το σημείο του αφινικού επιπέδου $(x/z, y/z) \in \mathbb{A}^2_K(L)$.

Μπορούμε επομένως να θεωρήσουμε ότι το $\mathbb{P}^2_K$ προκύπτει από το αφινικό επίπεδο $\mathbb{A}^2_K$ με την προσθήκη όλων των σημείων της μορφής $[x : y : 0]$. Το σύνολο όλων αυτών των σημείων θα το αποκαλούμε *«επ' άπειρο ευθεία»*.

Ορισμός XII.2.9. Μια προβολική καμπύλη C βαθμού d υπεράνω του σώματος K, ορίζεται μέσω ενός ομογενούς πολυωνύμου $F(x,y,z) \in K$ βαθμού d, ως εξής:

$$C := C(F) = \{[x : y : z] \in \mathbb{P}^2_K : F(x,y,z) = 0\}.$$

1. Για κάθε επέκταση $L \supset K$ ορίζεται το σύνολο των L-ρητών σημείων της C

$$C(L) = \{[x : y : z] \in \mathbb{P}^2_K(L) : F(x,y,z) = 0\}.$$

2. Μια ρητή συνάρτηση επί της C είναι μια κλάση ισοδυναμίας ρητών συναρτήσεων G/H του $\mathbb{P}^2_K$ των οποίων ο παρονομαστής δεν έχει κανέναν κοινό διαιρέτη με το F, εκτός ίσως από κάποια σταθερά. Οι ρητές συναρτήσεις G_1/H_1 και G_2/H_2 είναι ισοδύναμες όταν $F \mid (G_1H_2 - G_2H_1)$. Μια ρητή συνάρτηση ϕ θα λέγεται ομαλή στο σημείο $P \in C(L)$, όταν έχει έναν αντιπρόσωπο G/H, για τον οποίο ισχύει $H(P) \neq 0$. Η ϕ ορίζει μια συνάρτηση

$$\begin{aligned} \phi_L : \{P \in C(L) : \phi \text{ ομαλή στο } P\} &\longrightarrow L \\ P = [x : y : z] &\longmapsto \frac{G(x,y,z)}{H(x,y,z)} \end{aligned}$$

3. Η C λέγεται ανάγωγη όταν το πολυώνυμο $F(x,y,z) \in K[x,y,z]$ είναι ανάγωγο πολυώνυμο. Η C λέγεται γεωμετρικά ανάγωγη όταν το πολυώνυμο $F(x,y,z)$ είναι απόλυτα ανάγωγο. Αν C είναι ανάγωγη, τότε το σύνολο των ρητών συναρτήσεων επί της C είναι ένα σώμα, το σώμα συναρτήσεων της C, $K(C)$.

Παραδείγματα XII.2.10. 1. Έστω η αφινική ευθεία $ax+by = c$. Η αντίστοιχη προβολική ευθεία (λέγεται και προβολική θήκη) είναι η $ax+by-cz = 0$. Αυτή έχει μοναδικό σημείο στο άπειρο το $[-b : a : 0] = 0$. Όλες οι προβολικές ευθείες προκύπτουν κατά τον ίδιο τρόπο, εκτός από την «επ' άπειρο ευθεία», $Z = 0$ (αποτελείται από το σύνολο των «επ' άπειρο σημείων»)

2. Η προβολική θήκη της $x^2 + y^2 = 1$ είναι $x^2 + y^2 - z^2 = 0$. Έχει τα «επ' άπειρο» L-ρητά σημεία $[1 : \pm 1 : 0]$, όταν το -1 είναι τέλειο τετράγωνο στο L, $i^2 = -1$. Αν η χαρακτηριστική του K είναι δύο, έχει μοναδικό επ' άπειρο σημείο το $[1 : 1 : 0]$.

3. Η προβολική θήκη της καμπύλης $y^2 = x^3 + ax + b$ είναι η $y^2z - x^3 - ax^2z - bz^3 = 0$. Έχει ακριβώς ένα (πάντοτε ρητό) σημείο το $[0, 1, 0]$ στο άπειρο.

XII.2.3 Σημεία τομής καμπύλης με ευθεία

Έστω $G : ax + by + cz = 0$, μια προβολική ευθεία και $C : F(x,y,z) = 0$ μια προβολική καμπύλη ορισμένες υπεράνω του σώματος K και $P = (\alpha, \beta, \gamma) \in \mathbb{P}^2_K(L)$. Υποθέτουμε ότι η ευθεία G δεν είναι συνιστώσα της C. Με $i(G, C; P)$ θα συμβολίζουμε την *πολλαπλότητα τομής* ευθείας και καμπύλης στο P, έννοια την οποία ορίζουμε ως εξής:

- Αν $P \notin C(L) \cap G(L)$, τότε $i(G, C; P) = 0$.
- Αν $P \in C(L) \cap G(L)$, τότε λύνουμε την εξίσωση ως προς μία μεταβλητή, για παράδειγμα

$$z = -\frac{a}{c}x - \frac{b}{c}y, \text{ αν } c \neq 0$$

και την τιμή αυτή αντικαθιστούμε στην $F(x,y,z)$. Προκύπτει ομογενές πολυώνυμο $H(x,y)$ δύο μεταβλητών το οποίο διαιρείται από το $\alpha y - \beta x$. Η πολλαπλότητα του παράγοντα αυτού στο πολυώνυμο $H(x,y)$ ορίζεται ως η πολλαπλότητα τομής $i(G, C; P)$.

Παράδειγμα XII.2.11. Θεωρούμε την καμπύλη

$$C : y^2z - x^3 + xz^2 = 0$$

Αν $G : y = 0$, τότε $H(x,z) = -x^3 + xz^2 = x(x+z)(-x+z)$. Επομένως τα σημεία τομής είναι τα $[0:0:1], [1:0:-1]$ και $[1:0:1]$ και έχουν όλα πολλαπλότητα ένα.

Έστω τώρα $G : x - z = 0$, επομένως $H(x,y) = xy^2$ και η πολλαπλότητα τομής στο $[0:-1:0]$ είναι 1, ενώ η πολλαπλότητα τομής στο $[1:0:1]$ είναι 2.

Έστω τέλος $G : z = 0$, επομένως $H(x,y) = -x^3$ συνεπώς το σημείο τομής είναι το $[0:1:0]$ και έχει πολλαπλότητα τομής 3.

Παρατηρούμε ότι μία προβολική ευθεία και μια κυβική καμπύλη έχουν, μετρώντας πολλαπλότητες, τρία σημεία τομής.

Θεώρημα XII.2.12. *Έστω $C : F(x,y,z) = 0$ μια προβολική καμπύλη υπεράνω του K βαθμού d και μία προβολική ευθεία $G : ax + by + cz = 0$ υπεράνω του K η οποία δεν είναι συνιστώσα της C. Ισχύει*

$$\sum_{P \in C(\overline{K}) \cap G(\overline{K})} i(G, C; P) = d.$$

Αν L επέκταση του K, για την οποία ισχύει

$$\sum_{P \in C(L) \cap G(L)} i(G, C; P) \geq d - 1,$$

τότε

$$\sum_{P \in C(L) \cap G(L)} i(G, C; P) = d.$$

Παρατήρηση XII.2.13. Το τελευταίο μέρος του παραπάνω θεωρήματος εξασφαλίζει ότι το τελευταίο σημείο τομής είναι L-ρητό αν όλα τα προηγούμενα είναι L-ρητά.

Απόδειξη. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $c \neq 0$. Θέτουμε $a' = -a/c$, $b' = -b/c$. Η εξίσωση της ευθείας γίνεται $z = a'x + b'y$. Αντικαθιστούμε το z στο $F(x,y,z)$ και έχουμε

$$H(x,y) = F(x,y,a'x + b'y).$$

Το $H(x,y)$ είναι ένα πολυώνυμο βαθμού d στον δακτύλιο $K[x,y]$. Στον δακτύλιο $\overline{K}[x,y]$ αναλύεται σε γινόμενο γραμμικών παραγόντων

$$H(x,y) = \alpha(\beta_1 x - \alpha_1 y)^{d_1}(\beta_2 x - \alpha_2 y)^{d_2} \cdots (\beta_k x - \alpha_k y)^{d_k}.$$

Το σημείο $P = [x:y:z] \in C(\overline{K}) \cap G(\overline{K})$ τότε και μόνο τότε όταν $H(x,y) = 0$ και $z = a'x + b'y$. Επομένως τα σημεία τομής είναι τα $P_i = [\alpha_i : \beta_i : a'\alpha_i + b'\beta_i]$, $i = 1, 2, \ldots, k$ και το καθένα εξ ορισμού έχει πολλαπλότητα $d_1, d_2, \ldots, d_k$ αντίστοιχα. Αλλά $d_1 + d_2 + \cdots + d_k = d$ και αποδείχθηκε το πρώτο μέρος.

Για το δεύτερο μέρος, παρατηρούμε ότι το πολυώνυμο $H(x,y)$ γράφεται ως γινόμενο d γραμμικών παραγόντων, εκ των οποίων οι $d-1$ έχουν συντελεστές στο L. Επομένως και αυτός που απέμεινε έχει συντελεστές στο L. □

Παρατηρούμε ότι ο βαθμός της ευθείας είναι 1 και ο βαθμός της καμπύλης είναι d και $d \cdot 1 = d$.

Κάπως πιο ντελικάτη είναι η έννοια της πολλαπλότητας τομής προβολικών καμπυλών. Ισχύει η γενίκευση της προηγούμενης πρότασης:

Θεώρημα XII.2.14 (Του Bezout). *Αν $C_1 : F(x,y,z) = 0$ και $C_2 : F_2(x,y,z) = 0$ δύο προβολικές (επίπεδες) καμπύλες υπεράνω του σώματος K, βαθμών m και n αντίστοιχα, οι οποίες δεν έχουν κοινή συνιστώσα, τότε ισχύει:*

$$\sum_{P \in C_1(\overline{K}) \cap C_2(\overline{K})} i(C_1, C_2; P) = m \cdot n.$$

Απόδειξη. [11, σελ. 112], [13, σελ. 182]. □

XII.2.4 Ιδιάζοντα σημεία προβολικών αλγεβρικών καμπυλών

Έστω ότι μια προβολική καμπύλη δίδεται μέσω του ομογενούς πολυωνύμου

$$F(x,y,z) \in K[x,y,z],$$

το σημείο $P \in \mathbb{P}^2_K(\overline{K})$ θα λέγεται ιδιάζον (singular) σημείο της καμπύλης αν και μόνο αν $F(P) = 0$ και οι τρεις μερικές παράγωγοι στο P μηδενίζονται, δηλαδή

$$F_x(P) = F_y(P) = F_z(P) = 0.$$

Παραδείγματα XII.2.15.

1. Έστω $f(x,y) = y^2 - x^3 \in K[x,y]$, η αφινική καμπύλη

$$V_f(\overline{K}) = \{(x,y) \in \overline{K} \times \overline{K} : y^2 = x^3\}.$$

Το ομογενές πολυώνυμο της προβολικής θήκης είναι το

$$F(x,y,z) = y^2z - x^3,$$

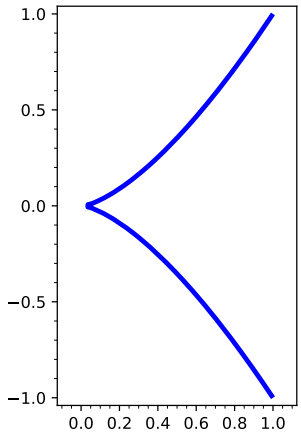
το οποίο έχει μερικές παραγώγους

$$F_x = -3x^2, F_y = 2yz, F_z = y^2.$$

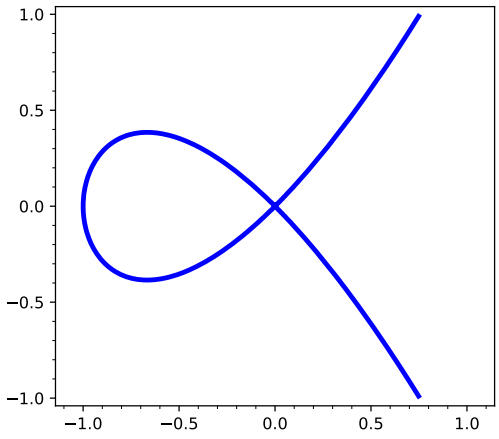
Το $P = [x : y : z]$ είναι ιδιάζον (εδώ η χαρακτηριστική του σώματος πρέπει να είναι διάφορη του $2, 3$) αν και μόνο αν

$$y^2z = x^3, x = 0, yz = 0, y = 0 \Leftrightarrow x = 0, y = 0 \text{ και } z \in K^* \Leftrightarrow P = [0 : 0 : 1].$$

Το αντίστοιχο αφινικό σημείο είναι το $(0,0)$. Εδώ η καμπύλη έχει κορυφή (cusp) στο $(0,0)$. Το γράφημά της έχει τη μορφή



2. Έστω $f(x,y) = y^2 - x^3 - x^2 \in K[x,y]$. Επομένως η προβολική θήκη ορίζεται από το ομογενές πολυώνυμο $F(x,y,z) = y^2z - x^3 - x^2z$. Η αντίστοιχη προβολική καμπύλη έχει επίσης το σημείο $P = [0 : 0 : 1]$ σαν μοναδικό ιδιάζον σημείο. Το αντίστοιχο αφινικό σημείο είναι το $(0,0)$. Η γραφική παράσταση αυτής είναι:



η οποία είναι κόμβος (node).

Παρατήρηση: Περνούμε πάντοτε στον προβολικό χώρο, διότι είναι δυνατόν η καμπύλη να έχει ιδιομορφία στα επ' άπειρον σημεία της.

3. Της κυβικής καμπύλης που ορίζεται από το ομογενές πολυώνυμο

$$F(x,y,z) = y^2z - x^3 - axz^2 - bz^3$$

το επ' άπειρο σημείο $P = [0:1:0]$ δεν είναι ποτέ ιδιάζον:

$$\begin{aligned} F_x(x,y,z) &= -3x^2 - az^2 \\ F_y(x,y,z) &= 2yz \\ F_z(x,y,z) &= y^2 - 2axz - 3bz^2. \end{aligned}$$

Για $P = [0:1:0]$, πάντοτε $F_z(P) = 1 \neq 0$, δηλαδή P όχι ιδιάζον. Συνεπώς τα ιδιάζοντα (singular) σημεία κυβικής καμπύλης της μορφής $f(x,y) = y^2 - x^3 - ax - b$ είναι έκεινα τα $P(x,y)$ για τα οποία $f(P) = f_x(P) = f_y(P) = 0$.

4. Μια κυβική καμπύλη δεν μπορεί να έχει περισσότερα από ένα ιδιάζοντα σημεία και αυτά θα είναι κορυφή ή κόμβος [11, σελ. 115].

Παρατήρηση XII.2.16. Όταν η πολλαπλότητα τομής της εφαπτομένης σε κάποιο μη-ιδιάζον σημείο P μιας επίπεδης προβολικής καμπύλης είναι ≥ 3, τότε το σημείο λέγεται σημείο καμπής (point of inflection ή flex point) της C.

Φυσικά αν η καμπύλη είναι κυβική, τότε τα σημεία καμπής είναι ακριβώς τα μη-ιδιάζοντα σημεία της καμπύλης στα οποία η εφαπτομένη έχει πολλαπλότητα ακριβώς 3.

XII.2.5 Ελλειπτικές καμπύλες

Ορισμός XII.2.17. Μια ελλειπτική καμπύλη υπεράνω του σώματος K είναι μια ομαλή προβολική καμπύλη E η οποία δίνεται μέσω μιας εξίσωσης της μορφής:

$$E|_K : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{XII.1}$$

με συντελεστές $a_1, a_2, a_3, a_4, a_6 \in K$

Παρατήρηση XII.2.18. Συχνά χρησιμοποιούμε το αφινικό μέρος αυτής

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

η οποία λέγεται γενική εξίσωση του Weierstrass. Ως μη-ιδιάζουσα προβολική καμπύλη βαθμού 3, έχει γένος $g(E_K) = 1$.

Παρατήρηση XII.2.19. Αν C είναι μια, μη-ιδιάζουσα (non-singular) προβολική καμπύλη ορισμένη από το $F(X,Y,Z) \in K[X,Y,Z]$ το γένος της καμπύλης είναι μια τοπολογική αναλλοίωτος $g = g(C)$. Στη συγκέκριμένη περίπτωση το γένος της καμπύλης δίνεται από τον τύπο

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

όπου $n = \deg F$.

Επίσης έχουμε ήδη δει ότι η καμπύλη έχει μοναδικό «επ' άπειρο» σημείο το $[0:1:0]$ το οποίο είναι και K-ρητό σημείο της καμπύλης. Για $z = 0$, έχουμε $x^3 = 0$. Συνεπώς, ως σημείο τομής της ελλειπτικής καμπύλης με την «επ' άπειρο» ευθεία έχει πολλαπλότητα 3, δηλαδή είναι σημείο καμπής. (Η πολλαπλότητα τομής είναι ≥ 2 και το «επ' άπειρο» σημείο $[0:1:0]$ είναι ομαλό σημείο της καμπύλης. Επομένως, η «επ' άπειρο» ευθεία είναι εφαπτομένη ευθεία της καμπύλης E στο σημείο $[0:1:0]$.)

Μάλιστα μπορεί να αποδειχθεί ότι μια προβολική κυβική καμπύλη C είναι της μορφής (XII.1) ακριβώς τότε όταν το επ' άπειρο σημείο $[0:1:0]$ της C είναι ομαλό σημείο αυτής, είναι σημείο καμπής και έχει την ευθεία $z = 0$ ως εφαπτομένη της C στο σημείο $[0:1:0]$.

Στη συνέχεια, επειδή θα ασχοληθούμε με ελλειπτικές καμπύλες υπεράνω του $\mathbb{Q}$, (όταν η χαρακτηριστική του σώματος K είναι διαφορετική του $2, 3$ αποδεικνύεται ότι η $E|_K$ είναι ισόμορφη προς την ελλειπτική καμπύλη

$$y^2z = x^3 + axz^2 + bz^3, a, b \in K$$

της οποίας το αφινικό μέρος ορίζεται από την (μικρή) εξίσωση του Weierstrass

$$y^2 = x^3 + ax + b, a, b \in K).$$

Αλλά πότε μια καμπύλη αυτής της μορφής είναι ελλειπτική, δηλαδή μη-ιδιάζουσα; Έστω

$$f(x) = x^3 + ax + b \in \mathbb{Q}[x].$$

Το σημείο $[0:a:1]$ είναι μη-ιδιάζον σημείο της καμπύλης ακριβώς τότε όταν το a είναι απλή ρίζα του $f(x)$. Πράγματι αν το σημείο $[x:y:z]$ είναι ιδιάζον, τότε και το $[x:-y:z]$ είναι ιδιάζον. Όμως μια ανάγωγη κυβική καμπύλη έχει το πολύ ένα ιδιάζον σημείο. Επομένως πρέπει $y = 0$, δηλαδή το σημείο θα είναι κατ' ανάγκη της μορφής $[x:0:z]$. Το επ' άπειρο σημείο της καμπύλης δεν είναι ιδιάζον. Επομένως ελέγχουμε το $P = [x:0:1]$. Αυτό είναι ιδιάζον, τότε και μόνο τότε όταν

$$\left.\frac{\partial F}{\partial x}\right|_P = 0 \text{ και } \left.\frac{\partial F}{\partial y}\right|_P = 0$$

όπου $F(x,y) = y^2 - x^3 - ax - b$. Πάντοτε ισχύει $\left.\frac{\partial F}{\partial y}\right|_P = 0$. Επομένως το $P = [x:0:1]$ είναι ιδιάζον αν και μόνο αν $\left.\frac{\partial F}{\partial x}\right|_P = 0$, αν και μόνο αν το x είναι πολλαπλή ρίζα του $f(x) = x^3 + ax + b$ και αν και μόνο αν $D(f) = 4a^3 + 27b^2 \neq 0$.

XII.2.6 Ρητά σημεία ελλειπτικών καμπυλών

Έστω τώρα K ένα σώμα χαρακτηριστικής $\mathrm{ch}(K) \neq 2, 3$ και $E|_K$ μια ελλειπτική καμπύλη που ορίζεται υπεράνω του K από την εξίσωση

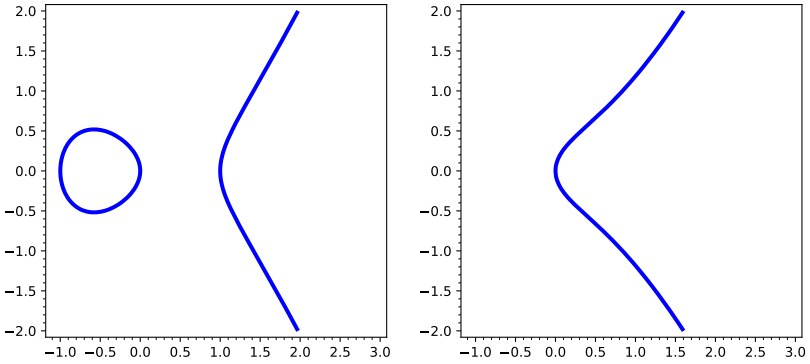
$$y^2 = x^3 + ax + b, a, b \in K$$

Για κάθε σώμα $L \supset K$ το σύνολο

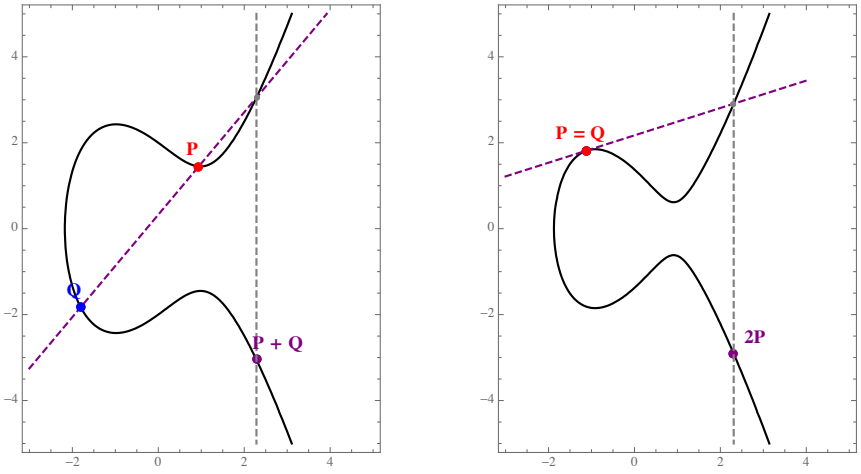
$$E(L) = \{(x,y) \in L \times L : y^2 = x^3 + ax + b\} \cup \{[0:1:0]\}$$

θα εφοδιαστεί με μια πράξη πρόσθεσης των στοιχείων του με την οποία γίνεται προσθετική αβελιανή ομάδα με ουδέτερο στοιχείο το επ' άπειρο σημείο $\mathcal{O} = [0 : 1 : 0]$. Η παρουσίαση θα γίνει γεωμετρικά.

Αν το $f(x) = x^3 + ax + b$, έχει ακριβώς μια πραγματική ρίζα, τότε το γράφημα της καμπύλης έχει μια συνεκτική συνιστώσα. Αν έχει τρεις πραγματικές ρίζες, το γράφημα έχει δύο συνεκτικές συνιστώσες.



Ορίζουμε την πρόσθεση δύο σημείων της ελλειπτικής καμπύλης ως εξής: Έστω τα σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$ επί της ελλειπτικής καμπύλης. Σχηματίζουμε την ευθεία L που ενώνει τα δύο αυτά σημεία. Η ευθεία τέμνει την ελλειπτική καμπύλη σε ένα τρίτο σημείο PQ. Από το σημείο PQ φέρνουμε την κάθετη ευθεία στον άξονα των x, η οποία τέμνει την ελλειπτική καμπύλη στο σημείο $P \oplus Q$. Το σημείο αυτό το ορίζουμε να είναι άθροισμα των σημείων P, Q.



Στην περίπτωση που θέλουμε να υπολογίσουμε το σημείο $P \oplus P$, αντί να θεωρήσουμε τη χορδή όπως στην προηγούμενη περίπτωση, θεωρούμε την εφαπτομένη στο σημείο αυτό.

Στην περίπτωση που ένας προσθετέος είναι το σημείο στο άπειρο, ισχύει $P \oplus \mathcal{O} = P$, δηλαδή το σημείο στο άπειρο είναι το ουδέτερο της πράξης.

Επίσης ισχύει, ότι τα τρία συνευθειακά σημεία έχουν άθροισμα $\mathcal{O}$.

Ας υποθέσουμε ότι $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$. Οι παραπάνω κανόνες πρόσθεσης μπορούν να εκφραστούν με τον εξής απλό τρόπο:

Ας υποθέσουμε ότι $P_1, P_2 \neq \mathcal{O}$.

- Αν $x_1 = x_2$ και $y_1 = -y_2$, τότε $P_1 + P_2 = \mathcal{O}$. Δηλαδή συμμετρικά σημεία ως προς τον άξονα των x έχουν άθροισμα $\mathcal{O}$.
- Διαφορετικά έχουμε

$$\lambda = (3x_1 + a)/(2y_1) \text{ αν } \quad P_1 = P_2$$

$$\lambda = (y_1 - y_2)/(x_1 - x_2) \text{ αν } \quad P_1 \neq P_2$$

Το σημείο $P_1 \oplus P_2$ έχει συντεταγμένες (x_3, y_3) που δίνονται από τους τύπους:

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - y_1 + \lambda x_1)$$

Ισχύουν οι παρακάτω ιδιότητες της πρόσθεσης σημείων όπως ορίστηκαν παραπάνω:

(i) $P \oplus Q = Q \oplus P$

(ii) $P \oplus \mathcal{O} = P$

(iii) Για κάθε P υπάρχει ένα σημείο R τέτοιο ώστε $P \oplus R = \mathcal{O}$

(iv) $P_1 \oplus (P_2 \oplus P_3) = (P_1 \oplus P_2) \oplus P_3$

Από τα παραπάνω τα (i) – (iii) είναι προφανή από τον γεωμετρικό ορισμό, ενώ το δύσκολο κομμάτι είναι η απόδειξη της προσεταιριστικής ιδιότητας, δηλαδή το (iv).

Για την απόδειξη χρησιμοποιείται το θεώρημα Bezout, ότι δύο προβολικές κυβικές καμπύλες, χωρίς κοινή συνιστώσα τέμνονται σε ακριβώς 9 σημεία και το

Θεώρημα XII.2.20. *Δύο προβολικές καμπύλες βαθμού n τέμνονται κατά Bezout σε ακριβώς n^2 σημεία. Αν ακριβώς mn από αυτά βρίσκονται σε μια ανάγωγη καμπύλη, τότε τα υπόλοιπα $n(n-m)$ βρίσκονται σε μία καμπύλη βαθμού $n - m$, [30].*

Ας περιοριστούμε τώρα σε ελλειπτικές καμπύλες E ορισμένες υπεράνω του $\mathbb{Q}$. Ότι το σύνολο των ρητών σημείων $E(\mathbb{Q})$ αποτελεί ομάδα το παρατήρησε ο Poincare το 1901. Το ερώτημά του ήταν, αν συνεχίσουμε με τη μέθοδο της χορδής και της εφαπτομένης θα πάρουμε όλα τα ρητά σημεία;

Στα 1922 ο Mordell απέδειξε το

Θεώρημα XII.2.21. *Η αβελιανή ομάδα $E(\mathbb{Q})$ μιάς ελλειπτικής καμπύλης $E|_{\mathbb{Q}} : y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$ είναι πεπερασμένα παραγόμενη*

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r,$$

όπου $E(\mathbb{Q})_{\text{tor}}$ είναι η ομάδα των ρητών σημείων πεπερασμένης τάξης και $r \in \mathbb{N}$.

Απόδειξη. Η ιδέα της απόδειξης βασίζεται και αυτή στη μέθοδο της καθόδου. Θα πρέπει να ορίσουμε ένα «μέτρο» για να μετρούμε τους ρητούς αριθμούς. Εδώ εισάγουμε την έννοια του «ύψους».

Ορισμός XII.2.22. Αν $Q = (x, y) \in \mathbb{Q}^2$ και $x = m/n$, $m, n \in \mathbb{Z}$ με Μ.Κ.Δ$(m, n) = 1$, τότε το ύψος του Q ορίζεται ως

$$h(Q) = \max(|m|, |n|).$$

Ξεκινούμε, λοιπόν από ένα ρητό σημείο Q και στη συνέχεια κατεβαίνουμε τα «σκαλιά» του ύψους, βρίσκοντας στη συνέχεια σημεία μικρότερου ύψους και τελικά πεπερασμένου πλήθους σημείων $P_1, P_2, \ldots, P_r$ των οποίων γραμμικός συνδυασμός με ακέραιους συντελεστές μας δίνει το τυχαίο αρχικό σημείο Q.

Κάπως πιο αναλυτικά η ιδέα απόδειξης του θεωρήματος;

1. Ισχύει $E(\mathbb{Q})/2E(\mathbb{Q})$ είναι πεπερασμένη ομάδα.
2. (i) Για κάθε $M \in \mathbb{R}$ το σύνολο $\{P \in E(\mathbb{Q}) : h(P) \le M\}$ είναι πεπερασμένο.
   (ii) Έστω P_0 ένα σταθερό σημείο της $E(\mathbb{Q})$ υπάρχει σταθερά $k_0 = k_0(a, b)$ τέτοια ώστε

$$h(P + P_0) \le 2h(P) + k_0, \text{ για κάθε } P \in E(\mathbb{Q}).$$

   (iii) Υπάρχει μια σταθερά $k = k(a, b)$ τέτοια ώστε

$$h(2P) \ge 4h(P) - k, \text{ για κάθε } P \in E(\mathbb{Q}).$$

Τώρα, έστω $Q_1, Q_2, \ldots, Q_n$ ένα πλήρες σύστημα αντιπροσώπων των κλάσεων $E(\mathbb{Q})/2E(\mathbb{Q})$. Για κάθε $P \in E(\mathbb{Q})$ υπάρχει $i_1 \in \{1, 2, \ldots, n\}$ τέτοιο ώστε $P - Q_{i_1} \in 2E(\mathbb{Q})$ συνεπώς υπάρχει $P_1 \in E(\mathbb{Q})$ ώστε $P - Q_{i_1} = 2P_1$ και ομοίως

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\cdots \\ P_m - Q_{i_m} &= 2P_m \end{aligned}$$

Επομένως το P γράφεται ως γραμμικός συνδυασμός

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Τα ύψη των P_i συνεχώς μικραίνουν λόγω των (2ii) και (2iii). Για αρκετά μεγάλο m το P_m έχει ύψος φραγμένο από κάποιο $M \in \mathbb{R}$, δηλαδή το σύνολο των P_m έχει πεπερασμένο πλήθος δυνατοτήτων. □

Ωραία! Αλλά τα ερωτήματα παραμένουν.

1. Δίδεται η $E : y^2 = x^3 + ax + b$. Ποια είναι η ομάδα $E(\mathbb{Q})_{\text{tor}}$.
2. Δίδεται η E. Πόσο είναι το r;

Το 1. είναι εύκολο. Το 2. είναι πάρα πολύ δύσκολο.

Θεώρημα XII.2.23 (Lutz,Nagell). *Έστω $E|_{\mathbb{Q}} : y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$. Αν το $P = (x, y) \in E(\mathbb{Q})_{\text{tor}}$, τότε*

1. $x, y \in \mathbb{Z}$
2. $y = 0$ *ή* $y^2 \mid \Delta = 4a^3 + 27b^2$.

Προσοχή! Δεν ισχύει το αντίστροφο. Αν $(x, y) \in \mathbb{Z}^2$ δεν ισχύει, κατ' ανάγκη, ότι (x, y) είναι σημείο στρέψης (torsion) της καμπύλης.

Παράδειγμα XII.2.24. Αν $y^2 = x^3 + x$, $a = 1, b = 0$ συνεπώς $\Delta = 4 \cdot 1^3 + 27 \cdot 0^2 = 4$. Αν $y \neq 0$, τότε $y \in \{\pm 1, \pm 2\}$. Καμμία από αυτές τις τιμές δεν δίνει ακέραιο x. Για παράδειγμα $x^3 + x = 1$, θέτουμε $f(x) = x^3 + x - 1$, $f(\pm 1) \neq 0$.

Επομένως, $E(\mathbb{Q}) = \{\mathcal{O}, (0, 0)\} \cong \mathbb{Z}/2\mathbb{Z}$.

Σημείωση XII.2.25. Τα σημεία τάξης 2 είναι ακριβώς αυτά για τα οποία το $y = 0$. Πράγματι, για $P = (x, 0)$ η εφαπτομένη του P τέμνει την ελλειπτική καμπύλη στο $\mathcal{O}$, και συνεπώς $2P + \mathcal{O} = \mathcal{O}$ και $2P = \mathcal{O}$.

Θεώρημα XII.2.26 (Mazur). *Έστω $E|_{\mathbb{Q}}$ ελλειπτική καμπύλη. Η ομάδα των ρητών σημείων πεπερασμένης τάξης της $E|_{\mathbb{Q}}$, έχει τις παρακάτω δυνατότητες:*

$$E(\mathbb{Q})_{\text{tor}} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 10 \text{ ή } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} & 1 \leq n \leq 4 \end{cases}$$

Σχετικά με το ερώτημα του προσδιορισμού του βαθμού (rank) r. Η ιδέα ότι αν μια ελλειπτική καμπύλη έχει πολλά ρητά σημεία θα έχει και πολλά σημεία modulo p αναγωγή της

$$E_{\mathbb{F}_p} : y^2 = x^3 + ax + b \mod p$$

για πολλούς πρώτους p, δηλαδή ένα είδος local-global-principle.

Θεωρούμε ένα πρώτο p, την εξίσωση της ελλειπτικής καμπύλης

$$E|_{\mathbb{Q}} : y^2 = x^3 + ax + b, a, b \in \mathbb{Z}$$

και στη συνέχεια την καμπύλη

$$E|_{\mathbb{F}_p} : y^2 = x^3 + \overline{a}x + \overline{b}, \overline{a} = a \mod p, \overline{b} = b \mod p.$$

Για τους πρώτους $p \mid 2\Delta$ η καμπύλη αυτή είναι κυβική αλλά ιδιάζουσα.

Για όλους τους υπόλοιπους πρώτους είναι μια ελλειπτική καμπύλη. Για την αναγωγή των ρητών της σημείων θα πρέπει να δουλέψουμε στο σώμα των p-αδικών $\mathbb{Q}_p \supset \mathbb{Q}$, το οποίο έχει δακτύλιο ακέραιων του $\mathbb{Z}_p$ και περιέχει τα στοιχεία

$$\mathbb{Z}_p \ni a = a_0 + a_1 p + a_2 p^2 + \cdots$$

$a_i \in \mathbb{Z}$, $0 \le a_i < p$. Η συνάρτηση αναγωγής $\mathbb{Z}_p \ni a \mapsto \overline{a} = a_0 \in \mathbb{F}_p$, η οποία είναι συμβατή με την πρόσθεση των στοιχείων της $E(\mathbb{Q}_p)$, δείτε την παράγραφο XIII.7.

Το

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + \overline{a}x + \overline{b}\} \cup \{\overline{\mathcal{O}}\}$$

είναι μια πεπερασμένη αβελιανή ομάδα. Πόσα στοιχεία περιέχει; Έστω $\mathcal{N}(p) = \#E(\mathbb{F}_p)$.

Παράδειγμα XII.2.27. Το πλήθος των σημείων της

$$y^2 = x^3 + 3x \text{ στο } \mathbb{F}_5$$

είναι $\mathcal{N}(5) = 10$, αφού τα σημεία της εν λόγω καμπύλης είναι τα

$$(0,0), (1,\pm 2), (2,\pm 2), (3,\pm 1), (4,\pm 1), \mathcal{O}$$

Γενικά στην $y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_p$ το x έχει p-δυνατότητες (από $0, 1, 2, \ldots, p-1$) και για κάθε τιμή του x αντιστοιχούν το πολύ 2-τιμές του y. Συνεπώς πάντοτε ισχύει (δεν ξεχνούμε και το σημείο στο άπειρο $\mathcal{O}$)

$$1 \le \mathcal{N}(p) \le 2p + 1$$

Μπορούμε να γράψουμε την ανισότητα ως εξής:

$$|p + 1 - \mathcal{N}(P)| \le p.$$

Βέβαια, δεν είναι για όλες τις τιμές του x, το πολυώνυμο x^3+ax+b τετραγωνικό υπόλοιπο modulo p. Αν δεχθούμε ότι η κατανομή σε τετραγωνικά υπόλοιπα και μη, είναι τυχαία, δηλαδή οι μισές τιμές του x δίνουν τετραγωνικά υπόλοιπα και οι άλλες μισές όχι, καταλήγουμε στο συμπέρασμα ότι $\mathcal{N}(P) \sim p + 1$. Πράγματι, ισχύει το θεώρημα του Hasse,

Θεώρημα XII.2.28.

$$|\mathcal{N}(p) - (p + 1)| \le 2\sqrt{p}.$$

Παρατήρηση XII.2.29.

1. Το φράγμα είναι best-possible, όταν αναφερόμαστε γενικά στις καμπύλες $E|_{\mathbb{F}_p}$. Μπορούμε φυσικά να θεωρήσουμε ειδικές κλάσεις, οπότε παίρνουμε για αυτές καλύτερα φράγματα.
2. Το θεώρημα γενικεύεται και για μη ελλειπτικές καμπύλες και έχει εφαρμογές στην κωδικοποίηση, [25].
3. Για κάθε ελλειπτική καμπύλη μπορεί να ορίσει κανείς την ζ-συνάρτηση αυτής. Μάλιστα υπάρχει έκφραση για την εικασία του Riemann της $\zeta_E(s)$. Στην περίπτωση αυτή η εικασία του Riemann έχει αποδειχθεί, δείτε και την εργασία του Μάριου Μαγιολαδίτη [32].

4. Για να μην εξαρτάται η τιμή του $\mathcal{N}(P)$ από το μοντέλο που έχουμε επιλέξει δεχόμαστε ότι το μοντέλο μας είναι (global) minimal model (με ό,τι και αν αυτό σημαίνει).
   Επομένως οι αριθμοί
   $$a(p) := p + 1 - \mathcal{N}(p)$$
   εξαρτώνται από την ελλειπτική καμπύλη και μόνο και όχι από την επιλογή της εξίσωσης του Weierstrass.

XII.2.7 Minimal διακρίνουσα

Έστω $E|_{\mathbb{Q}}$ η ελλειπτική καμπύλη

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + a_6 : \alpha_i \in \mathbb{Q}$$

Η εξίσωση δεν καθορίζει μονοσήμαντα την καμπύλη. Αποδεικνύεται ότι η E είναι ισομορφική με κάποια άλλη εξίσωση του Weierstrass μέσω μιας αμφίρρητης απεικόνισης υπεράνω του $\mathbb{Q}$ τότε και μόνο τότε όταν υπάρχει μια αμφίρρητη απεικόνιση ανάμεσά τους της μορφής

$$x = u^2 x' + r$$
$$y = u^3 y' + s u^2 x' + t$$

$u, r, s, t \in \mathbb{Q}$, $u \neq 0$, [24, Θεώρ. 3.1, σελ. 63]. Θέτουμε

$$b_2 = \alpha_1^2 + 4\alpha_2$$
$$b_4 = 2\alpha_4 + \alpha_1\alpha_3$$
$$b_6 = \alpha_3^2 + 4\alpha_6$$
$$b_8 = \alpha_1^2\alpha_6 + 4\alpha_2\alpha_6 - \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3^2 - \alpha_4^2$$
$$c_4 = b_2^3 - 24b_4$$
$$c_6 = b_2^3 + 36b_2b_4 - 216b_6$$

Ορισμός XII.2.30. Διακρίνουσα της $E|_{\mathbb{Q}}$ ορίζεται η ποσότητα

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^3 + 9b_2b_4b_6 = \frac{c_4^3 - c_6^2}{1728}.$$

Παρατήρηση XII.2.31. Η διακρίνουσα της

$$E|_{\mathbb{Q}} : y^2 = x^3 + a_4x + a_6$$

είναι $\Delta(E) = -16(4a_4^3 + 27a_6^2)$.

Με την αλλαγή των συντεταγμένων προκύπτει ότι

$$c_4 = u^4c_4', c_6 = u^6c_6', \Delta(E) = u^{12}\Delta'(E).$$

Αυτό σημαίνει, ότι είναι δυνατό δύο ελλειπτικές καμπύλες να είναι ισόμορφες και να έχουν διαφορετικές διακρίνουσες, οι όποιες διαφέρουν κατά δωδεκάτη δύναμη ενός $u \in \mathbb{Q}^*$.

Παράδειγμα XII.2.32. Η $E|_{\mathbb{Q}} : y^2 = x^3 + 1$, έχει διακρίνουσα $\Delta(E) = -2^4 \cdot 3^3$. Μέσω της αμφίρρητης, υπεράνω του $\mathbb{Q}$, απεικόνισης

$$x = x'/5^2, y = y'/5^3$$

προκύπτει η ισόμορφη ελλειπτική καμπύλη

$$E'|_{\mathbb{Q}} : (y')^2 = (x')^3 + 5^6$$

με διακρίνουσα $\Delta(E') = -2^4 \cdot 3^3 \cdot 5^2$.

Ορισμός XII.2.33. Η j-αναλλοίωτη της $E|_{\mathbb{Q}}$ ορίζεται

$$j(E) = \frac{c_4^3}{\Delta(E)}.$$

Εδώ αποδεικνύεται ότι αν

$$E \cong E', \text{ τότε } j(E) = j(E').$$

Αν η καμπύλη ορίζεται σε αλγεβρικά κλειστό σώμα, για παράδειγμα στο $\mathbb{C}$, τότε ισχύει και το αντίστροφο. Υπάρχει ταξινόμηση ισόμορφων ελλειπτικών καμπυλών σε οποιοδήποτε σώμα χαρακτηριστικής $\mathrm{chk} \neq 2, 3$.

Κάθε ελλειπτική καμπύλη $E|_{\mathbb{Q}}$ είναι ισόμορφη προς ελλειπτική καμπύλη με ακέραιους συντελεστές a_i. Από όλες τις εξισώσεις με ακέραιους συντελεστές της E μία έχει την ελάχιστη δυνατή δύναμη του p ως διαιρέτη της διακρίνουσας και θα λέγεται ελάχιστο μοντέλο της E στο p.

Συχνά εργαζόμαστε με τέτοια μοντέλα όταν εργαζόμαστε με την αναγωγή ελλειπτικών καμπυλών. Δείτε και την επόμενη υποπαράγραφο.

Αποδεικνύεται ότι για $E|_{\mathbb{Q}}$ υπάρχει ένα μοντέλο που είναι minimal για όλους τους πρώτους p, κάτι που δεν ισχύει για ελλειπτικές καμπύλες ορισμένες πάνω από αλγεβρικά σώματα αριθμών.

Το minimal μοντέλο για όλους τους πρώτους λέγεται global minimal μοντέλο. Είναι μοναδικό όταν $a_1 \in \{0, 1\}$ και $a_2 \in \{0, 1, 2\}$

Θεώρημα XII.2.34. *Έστω* $\mathrm{ch}(K) \neq 2, 3$, $j \in K$ *και*

$$E|_K : y^2 = x^3 + ax + b, a, b, \in K$$

μία ελλειπτική καμπύλη υπεράνω του σώματος K *με* $j(E) = j$.

1. *Αν* $j \neq 0, 1728$, *τότε οι* K*-κλάσεις ισομορφίας ελλειπτικών καμπυλών* E' *με* $j(E') = j$ *ταξινομούνται μέσω της ομάδας* $K^*/(K^*)^2$. *Όταν* $d \in K^*$ *είναι ένας αντιπρόσωπος της κλάσης, τότε η αντίστοιχη ελλειπτική καμπύλη ορίζεται από την εξίσωση*

$$y^2 = x^3 + d^2ax + d^3b.$$

2. *Αν* $j = 0$, *τότε* $a = 0$. *Οι* K*-κλάσεις ισομορφίας με* $j = 0$ *ταξινομούνται μέσω των στοιχείων της* $K^*/(K^*)^6$. *Αν* $d \in K^*$ *είναι ένας αντιπρόσωπος της κλάσης, η αντίστοιχη ελλειπτική καμπύλη είναι η*

$$y^2 = x^3 + db.$$

3. *Αν* $j = 1728$, *τότε* $a = b$. *Οι* K*-κλάσεις ισομορφίας με* $j = 1728$ *ταξινομούνται μέσω της* $K^*/(K^*)^4$. *Αν* $d \in K^*$ *αντιπρόσωπος μιας κλάσης, τότε η αντίστοιχη καμπύλης είναι*

$$y^2 = x^3 + dax.$$

XII.2.8 Ταξινόμηση της αναγωγής

Έστω $E|_{\mathbb{Q}}$ με συντελεστές και p είναι ένας πρώτος αριθμός. Υποθέτουμε ότι η E ορίζεται μέσω μιας ειδικής εξίσωσης που έχει minimal διακρίνουσα ως προς τον πρώτο p. Για $p > 3$ ένα ακέραιο μοντέλο είναι minimal ως προς τον πρώτο p, όταν η διακρίνουσα $\Delta(E)$ δεν διαιρείται από το p^{12}.

Αν $P = [x : y : z] \in \mathbb{P}^2(\mathbb{Q})$, πολλαπλασιάζουμε με κατάλληλο ακέραιο και έχουμε το σημείο P με ακέραιες συντεταγμένες, μία από τις οποίες δεν διαιρείται με p.

Η απεικόνιση

$$\begin{aligned} \mathbb{P}^2(\mathbb{Q}) &\longrightarrow \mathbb{P}^2(\mathbb{F}_p) \\ [x : y : z] &\longmapsto [\overline{x} : \overline{y} : \overline{z}] \end{aligned}$$

$\overline{x} \equiv x \mod p$, $\overline{y} \equiv y \mod p$, $\overline{z} \equiv z \mod p$ είναι καλά ορισμένη και λέγεται *απεικόνιση αναγωγής* modulo p.

Αν λοιπόν $E|_{\mathbb{Q}}$ είναι μια ελλειπτική καμπύλη στη μορφή Weierstrass, τότε θεωρούμε την καμπύλη $\overline{E}|_{\mathbb{F}_p}$ υπεράνω της $\mathbb{F}_p$ η οποία θα λέγεται αναγωγή της E modulo p.

Αν $p \nmid \Delta(E)$, τότε $\Delta(\overline{E}) \neq 0$, συνεπώς η $\overline{E}$ είναι μια ελλειπτική καμπύλη υπεράνω του $\mathbb{F}_p$. Αν $p \mid \Delta(E)$, τότε η $\overline{E}|_{\mathbb{F}_p}$, είναι μια ιδιάζουσα καμπύλη η οποία έχει μοναδικό ιδιάζον σημείο. Έστω $\overline{E}_{ns}$ το σύνολο των $\mathbb{F}_p$-ρητών *σημείων στα οποία η καμπύλη είναι μη-ιδιάζουσα.* Όπως και για τα σημεία $E(\mathbb{Q})$, έτσι και για τα σημεία $\overline{E}_{ns}$ ορίζεται πράξη πρόσθεσης με τη μέθοδο της χορδής και εφαπτομένης και το σύνολο $\overline{E}_{ns}$ έχει επίσης τη δομή πεπερασμένης αβελιανής ομάδας.

Θεώρημα XII.2.35. *Έστω $E|_{\mathbb{Q}}$ μια ελλειπτική καμπύλη ορισμένη μέσω εξίσωσης του Weierstrass η οποία είναι minimal ως προς το p.*

1. *Έστω ότι $p \nmid \Delta(E)$. Τότε η $\overline{E}|_{\mathbb{F}_p}$ είναι μια ελλειπτική καμπύλη. Θα λέμε ότι η $\overline{E}$ έχει καλή αναγωγή στο p. (Σ' αυτή την περίπτωση η ελλειπτική καμπύλη $\overline{E}$ είναι ανεξάρτητη κατά προσέγγιση ισομορφίας από την εκλογή της minimal εξίσωσης του Weierstrass της οποίας υπολογίσαμε την αναγωγή).*

2. *Η $\overline{E}$ είναι ιδιάζουσα και το μοναδικό ιδιάζον σημείο είναι κορυφή (cusp). Σ' αυτή την περίπτωση η $\overline{E}_{ns}$ είναι ισόμορφη προς την προσθετική ομάδα του σώματος $\mathbb{F}_p$ κάτι το οποίο σημαίνει ότι είναι κυκλική τάξης p. Σε αυτή την περίπτωση θα λέγεται ότι η E έχει προσθετική αναγωγή στο p ή μη ευσταθή αναγωγή.*

3. *Η $\overline{E}$ είναι ιδιάζουσα και έχει μοναδικό ιδιάζον σημείο κόμβο (node) του οποίου οι δύο εφαπτομένες είναι ορισμένες υπεράνω του $\mathbb{F}_p$. Σε αυτή την περίπτωση η $\overline{E}_{ns}$ είναι ισόμορφη με την πολλαπλασιαστική υποομάδα του σώματος $\mathbb{F}_p$. Αυτό σημαίνει ότι είναι κυκλική τάξης $p-1$. Σε αυτή την περίπτωση θα λέγεται ότι η E έχει split πολλαπλασιαστική ή ημι-ευσταθή αναγωγή στο p.*

4. *Η $\overline{E}$ είναι ιδιάζουσα και έχει μοναδικό ιδιάζον σημείο κόμβο (node) στο οποίο οι δύο εφαπτομένες δεν ορίζονται υπεράνω του $\mathbb{F}_p$. Όταν αυτό συμβαίνει η $\overline{E}_{ns}$, είναι κυκλική τάξης $p+1$. Σε αυτή την περίπτωση λέγεται ότι η E έχει non-split πολλαπλασιαστική ή non-split ημιευσταθή αναγωγή στο p.*

XII.2.9 Σημεία πεπερασμένης τάξης

Έστω $E|_{\mathbb{Q}}$ μια ελλειπτική καμπύλη

$$y^2 = x^3 + ax + b, a, b \in \mathbb{Z}.$$

Το σύνολο των σημείων

$$E(\overline{\mathbb{Q}}) = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\mathcal{O} = [0:1:0]\},$$

αποτελεί αβελιανή ομάδα. Για κάθε $N \in \mathbb{N}$

$$E[N] := \{P \in E(\overline{\mathbb{Q}}) : NP = \mathcal{O}\}.$$

Το $E[N]$ ως αβελιανή ομάδα είναι ισόμορφη

$$E[N] \cong \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}}.$$

Η ομάδα $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, είναι μια τοπολογική ομάδα, ως προς την τοπολογία του Krull, XIII.8.2 Είναι το αντίστροφο όριο όλων των ομάδων Galois

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{\substack{K, [K:\mathbb{Q}]<\infty \\ K/\mathbb{Q} \text{ Galois}}} \mathrm{Gal}(K/\mathbb{Q}).$$

Χοντρικά μιλώντας αυτό σημαίνει ότι η κατανόηση της ομάδας $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ αυτής είναι ισοδύναμη με την πλήρη κατανόηση όλων των ομάδων πηλίκων με τις πεπερασμένες υποομάδες Galois $\mathrm{Gal}(K/\mathbb{Q})$.

Τις ομάδες τις κατανοούμε μέσω των αναπαραστάσεών τους. Μια n-διάσταση αναπαράσταση της ομάδας $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ είναι ένας συνεχής ομομορφισμός ομάδων

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(K),$$

όπου K ένα τοπολογικό σώμα, συνήθως $K = \mathbb{C}$ ή $K = \mathbb{Q}_\ell$, $\ell \in \mathbb{P}$. Το σώμα $\mathbb{Q}_\ell$ αποτελεί την πλήρωση του $\mathbb{Q}$ ως προς την ℓ-αδική εκτίμηση εντελώς ανάλογα όπως το $\mathbb{R}$ αποτελεί την πλήρωση του $\mathbb{Q}$ ως προς την απόλυτη τιμή.

Ένα στοιχείο της ομάδας $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ είναι η μιγαδική συζυγία η οποία μαζί με την ταυτότητα είναι το μοναδικό στοιχείο της μυστήριας αυτής ομάδας που μπορούμε να γράψουμε επακριβώς.

Με $\overline{Z}$ θα συμβολίζουμε τον δακτύλιο των ακεραίων αλγεβρικών αριθμών. Έστω τώρα $p \in \mathbb{P}$ και P ένα μέγιστο ιδεώδες του $\overline{Z}$, $P \mid p$. Ανάλογα προς τις πεπερασμένες ομάδες επεκτάσεων Galois αλγεβρικών σωμάτων αριθμών, ορίζονται και στην $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ οι υποομάδες ανάλυσης, αδράνειας και διακλάδωσης και φυσικά και ο Frobenius Frob_p. Μάλιστα για κάθε πεπερασμένη Galois επέκταση $K/\mathbb{Q}$ ισχύει

$$\mathrm{Frob}_P|_K = \mathrm{Frob}_{P_K}, \text{ όπου } P_K = P \cap K.$$

Μονοδιάστατες αναπαραστάσεις της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Πρόκειται για την πιο κατανοητή περίπτωση. Μία μονοδιάστατη αναπαράσταση είναι της μορφής

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{C}^* = \mathrm{GL}_1(\mathbb{C}).$$

Μία τέτοια αναπαράσταση αντιστοιχεί σε έναν χαρακτήρα Dirichlet, δηλαδή έναν ομομορφισμό ομάδων

$$\chi : \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^* \longrightarrow \mathbb{C}^*.$$

Αυτό επιτυγχάνεται μέσω της ταύτισης της ομάδας Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ με την ομάδα $\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^*$.

Θεωρούμε το ακόλουθο διάγραμμα:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & & \\ \downarrow{\scriptstyle \pi_N} & & \\ \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) & \xrightarrow{\cong} & \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^* \\ & {\scriptstyle \rho_{\chi,N}} \searrow \quad \swarrow {\scriptstyle \chi} & \\ & \mathbb{C}^* & \end{array} \tag{XII.2}$$

Η απεικόνιση π_N είναι ο ομομορφισμός περιορισμού των στοιχείων της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ στην ομάδα $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Ο οριζόντιος ισομορφισμός είναι ο γνωστός, ενώ ο ομομορφισμός $\rho_{\chi,N}$ ορίζεται ώστε το διάγραμμα να είναι αντιμεταθετικό:

$$\rho_{\chi,N} \circ \pi_N(\sigma) = \chi(\mathrm{res}|_{\mathbb{Q}(\zeta_N)}\sigma).$$

Από το διάγραμμα γίνεται αμέσως φανερό ότι ο χαρακτήρας χ ορίζει έναν ομομορφισμό

$$\rho_\chi := \rho_{\chi,N} \circ \pi_N : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{C}^*.$$

Ιδιαίτερα, για $\sigma = \mathrm{conj}$ τη μιγαδική συζυγία έχουμε

$$\pi_N(\sigma)(\zeta_N) = \sigma|_{\mathbb{Q}(\zeta_N)} = \zeta_N^{-1}.$$

Επομένως $\rho_\chi(\mathrm{conj}) = \chi(-1)$. Επίσης για $p \in \mathbb{P}$, $p \nmid N$ ισχύει

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) &\xrightarrow{\cong} \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^* \\ \mathrm{Frob}_p &\longmapsto p \mod N \end{aligned}$$

και μαζί με το αντιμεταθετικό διάγραμμα έχουμε:

Αν P ένα απόλυτο στοιχείο Frobenius της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ώστε $P \mid p$, $p \in \mathbb{P}, p \nmid N$, τότε

$$\rho_\chi(\mathrm{Frob}_P) = \rho_{\chi,N}(\mathrm{Frob}_{P_{\mathbb{Q}(\zeta_N)}}) = \chi(p).$$

Μάλιστα ο ομομορφισμός ρ_χ είναι συνεχής συνάρτηση.

Αντίστροφα κάθε συνεχής ομομορφισμός

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{C}^*$$

έχει πεπερασμένη εικόνα, αφού παραγοντοποιείται μέσω ενός ομομορφισμού

$$\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathbb{C}^*$$

για κάποια αβελιανή επέκταση $K/\mathbb{Q}$. Το θεώρημα των Kronecker-Weber μας επιτρέπει να θεωρήσουμε το $K = \mathbb{Q}(\zeta_N)$ για κάποιο N. Συνεπώς η $\rho = \rho_\chi$ για κάποιο χαρακτήρα Dirichlet χ_ρ. Επιλέγουμε το ελάχιστο τέτοιο N. Για αυτό το N, ο χαρακτήρας είναι πρωταρχικός.

Επομένως, οι χαρακτήρες Dirichlet μας δίνουν την αναπαράσταση της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ συγκεκριμένου τύπου και όλοι αυτοί οι ομομορφισμοί (όλες αυτές οι αναπαραστάσεις) προκύπτουν από χαρακτήρες Dirichlet.

Παρατήρηση XII.2.36. Γενικότερα ισχύει το εξής; Κάθε συνεχής ομομορφισμός

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_d(\mathbb{C}),$$

έχει πεπερασμένη εικόνα. Αυτό σημαίνει ότι η πληροφορία που προσφέρει καλύπτει ένα πεπερασμένο μέρος της δομής της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Ωστόσο, η εικόνα ένος χαρακτήρα Dirichlet χ περιέχεται σε ένα αλγεβρικό σώμα αριθμών έστω K. Επομένως, περιέχεται και σε κάποιο τοπικό σώμα αριθμών $K_\mathcal{L}$ όπου $\mathcal{L}$ κάποιο πρώτο ιδεώδες του K, $\mathcal{L} \mid \ell$, $\ell \in \mathbb{P}$. Συνεπώς μπορούμε να αντικαταστήσουμε το $\mathbb{C}^*$ με το $K_\mathcal{L}^*$ στο προηγούμενο διάγραμμα. Και σε αυτή την περίπτωση η αναπαράσταση που αντιστοιχεί στον χ

$$\rho_\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow K_\mathcal{L}^*$$

είναι συνεχής.

Ορισμός XII.2.37. Έστω d θετικός ακέραιος και ℓ πρώτος. Μια ℓ-αδική Galois αναπαράσταση διάστασης d, είναι ένας συνεχής ομομορφισμός

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_d(L),$$

όπου L πεπερασμένη επέκταση του $\mathbb{Q}_\ell$. Αν

$$\rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_d(L),$$

κάποια άλλη αναπαράσταση και υπάρχει ένας πίνακας $M \in \mathrm{GL}_d(L)$ τέτοιος ώστε

$$\rho'(\sigma) = M^{-1}\rho(\sigma)M,$$

για όλα τα $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, τότε οι ρ και ρ' θα λέγονται ισοδύναμες και αυτό θα συμβολίζεται με $\rho \sim \rho'$.

Συνήθως, στο θέμα που μας απασχολεί θα έχουμε $L = \mathbb{Q}_\ell$, το σώμα των ℓ-αδικών αριθμών. Για μια εισαγωγή στους ℓ-αδικούς δείτε το παράρτημα XIII.7.

Για κάθε πρώτο ℓ υπάρχει μια κανονική εμφύτευση του $\mathbb{Q}$ στην πλήρωση $\mathbb{Q}_\ell$. Όταν όμως περάσουμε από την αλγεβρική θήκη $\overline{\mathbb{Q}}$ του $\mathbb{Q}$ στην αλγεβρική θήκη $\overline{\mathbb{Q}}_\ell$ του $\mathbb{Q}_\ell$ υπάρχουν αρκετές, διαφορετικές μεταξύ τους εμφυτεύσεις του $\overline{\mathbb{Q}}$ στο $\overline{\mathbb{Q}}_\ell$. (Αυτό ισοδύναμα θα το λέγαμε ότι υπάρχουν διαφορετικοί τρόποι επέκτασης της ℓ-αδικής εκτίμησης του $\mathbb{Q}$ στο $\overline{\mathbb{Q}}_\ell$). Αν επιλέξουμε μία από όλες, τότε έχουμε και μία εμφύτευση της ομάδας Galois

$$\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Αν αλλάξουμε την εμφύτευση του $\overline{\mathbb{Q}}$ στο $\overline{\mathbb{Q}}_\ell$ αλλάζει και η εμφύτευση των ομάδων Galois, μέσω μιας συζυγίας.

Στην απόλυτη ομάδα Galois, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ η μέγιστη αβελιανή ομάδα πηλίκο είναι η

$$\mathrm{Gal}^{\mathrm{ab}}(\overline{\mathbb{Q}}/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}),$$

όπου μ είναι η ομάδα όλων των ριζών της μονάδας στο $\overline{\mathbb{Q}}$. Αν περιοριστούμε στην ομάδα όλων των ριζών της μονάδας τάξεως δύναμης του ℓ, τότε ορίζεται ο ℓ-αδικός κυκλοτομικός χαρακτήρας της $\mathrm{Gal}(\mathbb{Q}/\mathbb{Q})$, χ_ℓ, ο οποίος ορίζεται

$$\begin{aligned} \chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) &\longrightarrow \mathbb{Q}_\ell^* \\ \sigma &\longmapsto (m_1, m_2, m_3, \ldots) \end{aligned}$$

Με $\mu_{\ell^n}^\sigma = \mu_{\ell^n}^{m_n}$, για κάθε n. Ο παραπάνω χαρακτήρας είναι μια Galois αναπαράσταση της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ και ισχύει $\chi_\ell(\mathrm{conj}) = -1$ και $\chi_\ell(\mathrm{Frob}_p) = p$ για κάθε $p \neq \ell$ και μάλιστα είναι ανεξάρτητος της επιλογής των P και Frob_p.

Αυτός ο τύπος δείχνει ότι ο κυκλοτομικός χαρακτήρας έχει άπειρη εικόνα και αυτό αποτελεί ένδειξη ότι οι *ℓ-αδικές αναπαραστάσεις* έχουν περισσότερο πλούσια δομή από αυτή των μιγαδικών.

Ορισμός XII.2.38. Έστω ρ μία Galois αναπαράσταση και p ένας πρώτος αριθμός. Η ρ θα λέγεται *μη-διακαδιζόμενη* στο p αν και μόνο αν

$$I_p = G_T(P/p) \subset \ker\rho$$

για κάθε μέγιστο ιδεώδες $P \subset \overline{\mathbb{Z}}$, $P \mid p$.

Παράδειγμα XII.2.39. Έστω $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ ένας πρωταρχικός χαρακτήρας Dirichlet p πρώτος, $p \nmid N$ και P ένα μέγιστο ιδεώδες του $\overline{\mathbb{Z}}$, $P \mid p$. Από το διαγραμμα (XII.2) έπεται ότι $\pi_N(I_p) = I_{P_N}$, όπου $P_N = P \cap \mathbb{Q}(\zeta_N)$. Αλλά $I_{P_N} = \{1\}$, αφού ο p δεν διακλαδίζεται στο $\mathbb{Q}(\zeta_N)$. Επομένως, $I_P \subset \ker\rho_\chi$, δηλαδή η ρ_χ είναι μη-διακλαδιζόμενη στο p.

XII.2.10 Galois αναπαραστάσεις και ελλειπτικές καμπύλες

Έστω $E|_{\mathbb{Q}}$ μια ελλειπτική καμπύλη και $N \in \mathbb{N}$, $N > 1$. Για τα σημεία $E(\overline{\mathbb{Q}})$ που έχουν τάξη N, έχουμε ήδη δει ότι

$$E[N] \cong \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}}.$$

Επιλέγουμε μια βάση (P_1, P_2) της $E[N]$. Αν $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, ο αυτομορφισμός σ δρα στην $E[N]$, αφού αν $[N]\cdot P = \mathcal{O} = [0:1:0]$, τότε και

$$[N]\cdot\sigma(P) = \sigma([N]\cdot P) = \sigma(\mathcal{O}) = \mathcal{O}$$

Στην παραπάνω δράση αν $P = (x, y)$, τότε $\sigma(P) = (\sigma(x), \sigma(y))$ ενώ το επ' άπειρο σημείο $\mathcal{O}$ παραμένει αναλλοίωτο.

Αν

$$\sigma(P_1) = a_\sigma P_1 \oplus c_\sigma P_2$$
$$\sigma(P_2) = b_\sigma P_1 \oplus d_\sigma P_2,$$

τότε ορίζεται μια δισδιάστατη αναπαράσταση

$$\rho_{E[N]} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Ο ισομορφισμός δεξιά εξαρτάται από την επιλογή της βάσης του $E[N]$.

Επειδή στην πρόσθεση σημείων ελλειπτικής καμπύλης οι συντεταγμένες δίνονται μέσω ρητών συναρτήσεων με συντελεστές ρητούς, έπεται ότι αν θεωρήσουμε το σώμα K_N υπεράνω του $\mathbb{Q}$ το οποίο παράγεται από όλες τις συνιστώσες όλων των σημείων της $E[N]$, η επέκταση $K_N/\mathbb{Q}$ είναι Galois και η αναπαράσταση $\rho_{E[N]}$ παραγοντοποιείται μέσω της ομάδας Galois $\mathrm{Gal}(K_N/\mathbb{Q})$:

$$\rho_{E[N]} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K_N/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Σύμφωνα με ένα πραγματικά δύσκολο θεώρημα του Serre [22], αυτή η Galois αναπαράσταση στα σημεία της $E[N]$ είναι συνήθως πολύ μεγάλη για όλα τα N τα οποία δεν διαιρούνται από ένα συγκεκριμένο σύνολο πεπερασμένου πλήθους πρώτων.

Θα γίνουμε σαφέστεροι. Η απεικόνιση «πολλαπλασιασμός με N» είναι ένας ενδομορφισμός της ελλειπτικής καμπύλης E. Επομένως, $\mathbb{Z} \subset \mathrm{End}(E)$. Αν $\mathbb{Z} \subsetneq \mathrm{End}(E)$, τότε η καμπύλη λέγεται ότι έχει μιγαδικό πολλαπλασιασμό (complex multiplication). Παρά το ότι οι ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό είναι αρκετά ειδικές, η θεωρία των ελλειπτικών καμπυλών με μιγαδικό πολλαπλασιασμό αποτελεί πλούσια πηγή ιδεών και μάλιστα είναι αρκετά χρήσιμη στη θεωρία κλάσεων σωμάτων των τετραγωνικών, μιγαδικών σωμάτων αριθμών.

Θεώρημα XII.2.40 (Serre)**.** *Αν η ελλειπτική καμπύλη $E|_{\mathbb{Q}}$ δεν έχει μιγαδικό πολλαπλασιασμό, τότε υπάρχει ένας ακέραιος M ώστε αν $(M, N) = 1$ η εικόνα της $\rho_{E[N]}$ είναι επιμορφισμός.*

Επειδή υπάρχει μια μη-ιδιάζουσα *συμπλεκτική δομή* στην $E[N]$, η οποία είναι συμβατή προς τη δράση της ομάδας $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, πρόκειται για τη σύζευξη του Weil (Weil-pairing), η οποία παίρνει τιμές στην ομάδα των N-ριζών της μονάδας, έπεται ότι το σώμα K_N περιέχει το κυκλοτομικό σώμα $\mathbb{Q}(\zeta_N)$ και η ομάδα $\mathrm{Gal}(K_N/\mathbb{Q}(\zeta_N))$ είναι υποομάδα της $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Από τα παραπάνω, γίνεται φανερό *το πόσο μεγάλο είναι το ενδιαφέρον* για την εύρεση ελλειπτικών καμπυλών για τις οποίες το σώμα K_p για κάποιο πρώτο αριθμό p είναι *μικρό*, για παράδειγμα αν $K_p = \mathbb{Q}(\zeta_p)$.

Ξεχωριστά για κάθε N αυτές οι αναπαραστάσεις δεν είναι εντελώς ικανοποιητικές. Αυτό επειδή είναι πολύ πιο εύκολο να ασχολούμαστε με αναπαραστάσεις των οποίων οι πίνακες έχουν στοιχεία δακτυλίου χαρακτηριστικής μηδέν. Θα κάνουμε το ίδιο που κάναμε και στις αναπαραστάσεις βαθμού ένα.

Ενοποιούμε τις αναπαραστάσεις για μεταβλητό N, ώστε να καταφέρουμε να έχουμε το επιθυμητό αποτέλεσμα. Το πρότυπο παράδειγμά μας είναι ο δακτύλιος των ℓ-αδικών ακεραίων $\mathbb{Z}_\ell$, XIII.7. Θεωρούμε γνωστό το ότι

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}.$$

Ορισμός XII.2.41. Έστω $E|_{\mathbb{Q}}$ ελλειπτική καμπύλη και $\ell \in \mathbb{P}$. Το ℓ-αδικό module του Tate ορίζεται ως

$$T_\ell(E) := \varprojlim_n E[\ell^n].$$

Η συνάρτηση συμβατότητας είναι

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Αφού κάθε $E[\ell^n]$ είναι ένα $\mathbb{Z}/\ell^n\mathbb{Z}$-module το $T_\ell(E)$ αποκτά, φυσική δομή, ως ένα $\mathbb{Z}_\ell$-module. Ισχύει ότι

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Η ομάδα $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ δρα στην $T_\ell(E)$ και η δράση είναι συνεχής. Επιλέγουμε βάση (P_n, Q_n) της $E[\ell^n]$, για κάθε $n \in \mathbb{N}$ με την ιδιότητα της συμβατότητος

$$[\ell]P_{n+1} = P_n \text{ και } [\ell]Q_{n+1} = Q_n \text{ για κάθε } n \in \mathbb{N}.$$

Κάθε βάση ορίζει έναν ισομορφισμό

$$E[\ell^n] \cong \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$$

Επομένως αν περάσουμε στο προβολικό (αντίστροφο) όριο, έχουμε $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Και πάλι, όπως και πριν, η απεικόνιση

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) &\longrightarrow \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}) \\ \sigma &\longmapsto \sigma|_{\mathbb{Q}(E[\ell^n])} \end{aligned}$$

είναι επιμορφισμός και η

$$\mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[\ell^n])$$

είναι μονομορφισμός. Συνεπώς το διάγραμμα

$$\begin{array}{ccc} & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \\ \swarrow & & \searrow \\ \mathrm{Aut}(E[\ell^n]) & \longleftarrow & \mathrm{Aut}(E[\ell^{n+1}]) \end{array}$$

είναι αντιμεταθετικό και το $T_\ell(E)$ γίνεται ένα $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module.

Κάθε βάση (P_n, Q_n) ορίζει έναν ισομορφισμό

$$\mathrm{Aut}(E[\ell^n]) \xrightarrow{\cong} \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

Περνούμε στο προβολικο (αντίστροφο) όριο και έχουμε

$$\mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Αφού η $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ δρα στο module του Tate $T_\ell(E)$ έχουμε έναν ομομορφισμό:

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell)$$

ο οποίος αποδεικνύεται ότι είναι και συνεχής απεικόνιση. Τελικά η $\rho_{E,\ell}$ είναι μια δισδιάστατη Galois αναπαράσταση της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ που αντιστοιχεί στην $E/\mathbb{Q}$.

Επιπλέον ισχύουν:

Έστω $E|_{\mathbb{Q}}$ ελλειπτική καμπύλη με οδηγό N, $\ell \in \mathbb{P}$

1. Η $\rho_{E,\ell}$ είναι μη-διακλαδιζόμενη για κάθε $p \nmid \ell N$.
2. Για κάθε $p \nmid \ell N$, έστω $P \in \mathbb{P}(\overline{\mathbb{Z}})$, ένα maximal ιδεώδες του $\overline{\mathbb{Z}}$ ώστε $P \mid p$. Η χαρακτηριστική εξίσωση του $\rho_{E,\ell}(\mathrm{Frob}_P)$ είναι η
$$x^2 - a_p(E)x + p = 0$$
3. Η Galois αναπαράσταση $\rho_{E,\ell}$ είναι *ανάγωγη*.
4. Η *ομάδα αδράνειας* $I_P \subset \ker\rho_{E,\ell}$, συνεπώς η $\rho_{E,\ell}$ είναι *μη διακλαδιζόμενη* στο p για κάθε $p \nmid \ell N$.
5. $\det \rho_{E,\ell}(\sigma) = \chi_\ell(\sigma)$ όπου χ_ℓ ο κυκλοτομικός χαρακτήρας.
6. $\det \rho_{E,\ell}(\mathrm{Frob}_p) = p$
7. $\mathrm{Tr}\rho_{E,\ell}(\mathrm{Frob}_p)) = a_p(E)$.

XII.2.11 Η L-σειρά ελλειπτικής καμπύλης

Η $E|_{\mathbb{Q}}$ ελλειπτική καμπύλη. Ορίζουμε τον παράγοντα Euler για κάθε $p \in \mathbb{P}$

$$L_p(t) = \begin{cases} \frac{1}{1-a(p)t+pt^2}, & \text{όταν } p \nmid \Delta \\ \frac{1}{1-a(p)t}, & \text{όταν } p \mid \Delta \end{cases}$$

Ο ορισμός αυτός σχετίζεται με τον ορισμό της ζ_E, για $p \nmid \Delta$ είναι το αντίστροφο του αριθμητή της ζ_E. Άμεση συνέπεια του Θεωρήματος του Hasse είναι το

Θεώρημα XII.2.42. *Η* L*-σειρά της* $E|_{\mathbb{Q}}$

$$L(E,s) := \prod_{p\in\mathbb{P}} L_p(p^{-s}) = \prod_{p|\Delta} \frac{1}{1-a(p)p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1-a(p)p^{-s}+p^{1-2s}}$$

συγκλίνει απόλυτα για κάθε $s \in \mathbb{C}$ *με* $\mathrm{Re}(s) > 3/2$.

Κατ' αναλογία προς τις ζήτα συναρτήσεις των Riemann, Dedekind, Artin, ο Hasse διατύπωσε την ακόλουθη εικασία:

Εικασία XII.2.43 (Hasse)**.** Έστω $E|_{\mathbb{Q}}$. Η L-σειρά της $L(E,s)$ επεκτείνεται *αναλυτικά* σε όλο το μιγαδικό επίπεδο και πληροί την ακόλουθη συναρτησιακή εξίσωση για κατάλληλο $N \in \mathbb{N}$

$$\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

$$\Lambda(E,s-2) = \pm\Lambda(E,s).$$

Ο άξονας συμμετρίας είναι ο $s = 1$.

Ορισμός XII.2.44. Ο αριθμός N λέγεται αναλυτικός οδηγός της E και είναι γινόμενο πρώτων που διαιρούν τη διακρίνουσα $\Delta(E)$.

Στη δεκατετία του '60 οι Birch και Swinnerton-Dyer υπολόγισαν τιμές της $L(E,s)$ και διατύπωσαν την εικασία

Εικασία XII.2.45. Δεχόμαστε την αλήθεια της εικασίας του Hasse.

$$r = \mathrm{rank}(E(\mathbb{Q})) \Leftrightarrow \text{ Η } L(E,s) \text{ έχει στο } s = 1 \text{ ρίζα πολλαπλότητας } r.$$

Προβλήματα:

1. Πώς θα αποδείξουμε την εικασία του Hasse;
2. Πώς θα αποδείξουμε την εικασία των Birch-Swinnerton-Dyer;

XII.3 Modular συναρτήσεις και μορφές και η «ευτυχής συγκυρία»

Ας θεωρήσουμε την ελλειπτική καμπύλη

$$E|_{\mathbb{Q}} : y^2 + y = x^3 - x^2$$

με $\Delta(E) = -11$. Στη μορφή του Weierstrass η καμπύλη γράφεται

$$y^2 = x^3 - 4x^2 + 16$$

Υπολογίζουμε τα $a(p) = p + 1 - \mathcal{N}(p)$

p	3	5	7	11	13	17	19	23	29	31	$\cdots$
m	-1	1	-2	1	4	-2	0	-1	0	7	$\cdots$

Κανείς δεν μπορεί «με το μάτι» να παρατηρήσει κάποια κανονικότητα στους συντελεστές.

Ο Martin Eichler παρατήρησε ότι οι συντελεστές αυτοί συμπίπτουν, για δυνάμεις πρώτου αριθμού, με τους συντελεστές της συνάρτησης

$$\begin{aligned} f(q) &= q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 - 2q^7 - 2q^9 - 2q^{10} + q^{11} \\ &\quad - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + \cdots \end{aligned}$$

Θεώρημα XII.3.1 (Eichler). *Ισχύει ότι τα* $a(p)$ *της ελλειπτικής καμπύλης είναι ίσα με τα* a_p *της συνάρτησης* $f(q)$ *για κάθε* $p \geq 3$.

Γράφουμε $q = e^{2\pi i z}$, $z \in \mathbb{C}$ και $\mathrm{Im} z > 0$, συνεπώς $|q| < 1$. Σαν συνάρτηση του z αποδεικνύεται ότι ισχύει

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z),$$

για κάθε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \text{ με } ad - bc = 1 \text{ και } 11 \mid c$$

Η f λέγεται modular μορφή βάρους 2 και level $N = 11$.

Παρατήρηση XII.3.2. Στην modular συνάρτηση του παραδείγματός μας το επίπεδο (level) της f είναι N, δηλαδή συμπίπτει με τον οδηγό (conductor) της $E|_{\mathbb{Q}}$

Ορισμός XII.3.3. Μια ελλειπτική καμπύλη $E|_{\mathbb{Q}}$ με οδηγό $N \in \mathbb{N}$ θα λέγεται modular, όταν υπάρχει modular μορφή $f(z)$ βάρους 2 και επιπέδου N τέτοια ώστε

$$L(E,s) = L(f,s)$$

Εδώ αν το ανάπτυγμα Fourier της f είναι

$$f(q) = \sum_{n=0}^{\infty} a_n q^n$$

η L-σειρά αυτής ορίζεται η

$$L(f,s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Αλλά για τις modular μορφές η αναλυτική επέκταση και η συναρτησιακή εξίσωση της $L(f,s)$ ήταν ήδη γνωστή. Η παραπάνω σχέση μεταφέρει αυτές τις όμορφες ιδιότητες και στην L-σειρά της αντίστοιχης ελλειπτικής καμπύλης.

Μετά το αποτέλεσμα του Eichler (1954) διατυπώθηκε η εικασία Shimura-Taniyama ότι κάθε ελλειπτική καμπύλη $E|_{\mathbb{Q}}$ είναι modular.

XII.4 Ελλειπτικές καμπύλες και η Εικασία του Fermat

Μια σύντομη παράσταση σε τέσσερις πράξεις.

XII.4.1 Το θεώρημα του Frey

Η ιδέα είναι να μεταφερθεί το πρόβλημα στο «πλούσιο λιβάδι» της θεωρίας των ελλειπτικών καμπυλών.

Υποθέτουμε ότι η εξίσωση του Fermat για κάποιο πρώτο p, $p \geq 5$, έχει μια πρωταρχική λύση $(a, b, c) \in \mathbb{Z}^3$ με $abc \neq 0$ και $(a, b, c) = 1$. Θα μελετήσουμε την ελλειπτική καμπύλη

$$E^{(p)}_{a,b,c} : y^2 = x(x - a^p)(y - c^p) = x^3 - (a^p + c^p)x^2 + a^p c^p x.$$

Τελικά θα αποδείξουμε ότι η $E_{a,b,c}$ έχει πολλές και εξαιρετικές ιδιότητες που στην πραγματικότητα δεν υπάρχει.

Σημείωση XII.4.1. Όταν η ελλειπτική καμπύλη έχει τη μορφή

$$E : y^2 = x^3 + Ax^2 + Bx + C,$$

τότε η διακρίνουσα είναι

$$\Delta(E) = -4A^3C + A^2B^2 + 18ABC - 4B^3 - 27C^2$$

[1, σελ. 39, ασκ. 15]. Στην περίπτωσή μας

$$\begin{aligned} A &= -(a^p + c^p) \\ B &= a^p c^p \\ C &= 0 \end{aligned}$$

Επομένως $\Delta(E^{(p)}_{a,b,c}) = B^2(A^2 - 4B) = (abc)^{2p}$. Αποδεικνύεται ότι ο οδηγός της $E^{(p)}_{a,b,c}$ είναι

$$N := \prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p$$

Από τη σχέση $a^p + b^p = c^p$, έπεται ότι ένας το πολύ από τους a, b, c είναι άρτιος.

- Αν είναι ο a γράφουμε $b^p + (-c)^p = (-a)^p$.
- Αν είναι ο b γράφουμε $a^p + (-c^p) = (-b)^p$
- Αν δεν είναι ούτε ο a ούτε ο b, τότε αναγκαστικά είναι ο c

Επομένως χωρίς βλάβη της γενικότητας *υποθέτουμε ότι* c *άρτιος*. Επειδή $p \geq 5$, έχουμε ότι

$$c^p \equiv 0 \mod 32.$$

Το $a^p + b^p \equiv 0 \mod 4$ δίνει ότι $b^p \equiv -a^p \mod 4$. Επομένως ένας από τους δύο a^p και b^p είναι ισότιμος προς το $1 \mod 4$. Λόγω συμμετρίας των a^p και b^p μπορούμε να υποθέσουμε ότι $a^p \equiv 1 \mod 4$. Επομένως $a \equiv 1 \mod 4$ και $b \equiv 3 \mod 4$. Μέσω του αφινικού μετασχηματισμού $x = 4\phi$ και $y = 4\phi + 8\omega$ η αρχική εξίσωση μετασχηματίζεται στην ισόμορφή της:

$$\omega^2 + \phi\omega = \phi^3 + \frac{1}{4}(1 - a^p - c^p)\phi^2 + \frac{1}{16}a^p c^p \phi.$$

Λόγω των υποθέσεων για τα a^p και c^p προκύπτει ότι η εξίσωση

$$Y^2 + YX = X^3 + AX^2 + BX,$$

με $A = \frac{1}{4}(1 - a^p - c^p)$, $B = \frac{1}{16}a^p c^p$ έχει ακέραιους συντελεστές και διακρίνουσα $\frac{(abc)^{2p}}{2^8}$.

Η παραπάνω εξίσωση αποτελεί ένα γενικό ελαχιστικό μοντέλο (global minimal model) υπεράνω του $\mathbb{Q}$, αφού ο οδηγός της είναι ελεύθερος τετραγώνου.

Αν $q \in \mathbb{P}$, $q \mid abc$, τότε

- Αν $q \mid ac$ η
$$E^{(p)}_{a,b,c}|_{\mathbb{F}_q} : Y^2 = X^3 - a^p X^2 \text{ ή } E^{(p)}_{a,b,c}|_{\mathbb{F}_q} : Y^2 = X^3 - c^p X^2$$
και έχει *κόμβο* στο $(0,0)$.
- Αν $q \mid b$, τότε
$$E^{(p)}_{a,b,c}|_{\mathbb{F}_q} : Y^2 = X^3 - (a^p + c^p)X^2 + a^p c^p X = X^3 - 2a^p X^2 + a^{2p^i} X,$$
αφού $c^p \equiv a^p \mod q$. Το σημείο $(a^p, 0)$ είναι σημείο της καμπύλης $a^{3p} - 2a^p a^{2p} + a^{2p} a^p = 0$ και η καμπύλη έχει επίσης *κόμβο* στο $(a^p, 0)$.

Τέλος η ισόμορφη καμπύλη είναι επίσης global minimal model και για $q = 2$ γίνεται

$$E|_{\mathbb{F}_2} Y^2 + YX = \begin{cases} X^3, & \text{αν } 8 \mid (1 - a^p - c^p) \\ X^3 + X^2, & \text{διαφορετικά} \end{cases}$$

Στην περίπτωση αυτή το ιδιάζον σημείο είναι το $(0,0)$ και είναι *κόμβος*. Επομένως:

1. Η ελλειπτική καμπύλη $E^{(p)}_{a,b,c}$ είναι ημιευσταθής (semi-stable) για όλους τους πρώτους αριθμούς q. Έστω K_p το σώμα που προκύπτει με επισύναψη των συντεταγμένων των σημείων τάξης p της ελλειπτικής καμπύλης $E^{(p)}_{a,b,c}$ υπεράνω του $\mathbb{Q}$. Ο G. Frey απέδειξε ότι η επέκταση $K_p/\mathbb{Q}$ έχει ελάχιστη διακλάδωση.
2. Συγκεκριμένα, η επέκταση $K_p/\mathbb{Q}$ είναι μη-διακλαδιζόμενη για όλα τα πρώτα ιδεώδη P του K_p, $P \nmid 2p$.
3. Το K_p διακλαδίζεται ελαφρά στα πρώτα ιδεώδη P, $P \mid p$. Αυτό σημαίνει ότι η πλήρωση του K, ως προς το P προκύπτει ως ομαλά διακλαδιζόμενη επέκταση του $\mathbb{Q}_p$ στην οποία ακολουθεί επέκταση του Kummer βαθμού p και όπου τα ριζικά της επέκτασης Kummer είναι P-μονάδες.
4. Η ομάδα Galois $\mathrm{Gal}(K_p/\mathbb{Q})$ είναι ισόμορφη προς την $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$.

Επομένως, η ύπαρξη μιας λύσης της εξίσωσης του Fermat συνεπάγεται την ύπαρξη μιας σχεδόν μη-διακλαδιζομένης επέκτασης του $\mathbb{Q}$ με ομάδα Galois $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ η οποία περιέχει τις p-ρίζες της μονάδας.

Για να αποδείξουμε λοιπόν την εικασία του Fermat, αρκεί να αποδείξουμε ότι δεν υπάρχουν τέτοιες επεκτάσεις. Αναλυτικά παραπέμπουμε στη μεταπτυχιακή του εργασία του Α. Κοντογεώργη [31].

XII.4.2 Η εικασία του Serre

Ο Serre μελέτησε αναπαραστάσεις της ομάδας $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ως προς πεπερασμένα σώματα. Αν $\ell \in \mathbb{P}$ μας ενδιαφέρουν κυρίως δισδιάστατες αναπαραστάσεις. Εξ ορισμού ως αναπαραστάσεις μιας ομάδας ως προς ένα σώμα με θετική χαρακτηριστική είναι «modular». Είναι όμως modular και με εντελώς διαφορετικό και πολύ πιο βαθύ τρόπο. Προκύπτει από μία modular μορφή!

Αν η ελλειπτική καμπύλη είναι modular με οδηγό N_E, τότε υπάρχει μια modular μορφή (νέα μορφή, με ό,τι και αν σημαίνει αυτό)

$$f(q) = \sum_{n=0}^{\infty} c_p q^n, q = e^{2\pi i z}$$

βάρους 2 ως προς την $\Gamma_0(N)$ και την ιδιότητα

$$a_p(E) = c_p(E),$$

για όλους τους πρώτους p, $p \nmid N_E$. Η αντίστοιχη αναπαράσταση ρ_ℓ συνδέεται με την modular μορφή, μέσω της σχέσης

$$\mathrm{Tr}(\rho_\ell(\mathrm{Frob}_p)) \equiv c_p \mod \ell$$

για όλους τους πρώτους p εκτός από πεπερασμένο πλήθος.

Η εικασία του Serre αφορά αναπαραστάσεις της μορφής

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell),$$

όπου $\overline{\mathbb{F}}_\ell$ η αλγεβρική θήκη του πεπερασμένου σώματος $\mathbb{F}_\ell$. Οι αναπαραστάσεις αυτές όπως και οι προηγούμενες είναι και συνεχείς συναρτήσεις ως προς την τοπολογία του Krull και τη διακριτή τοπολογία αντίστοιχα. Αυτό σημαίνει ότι $\ker\rho$ είναι ανοιχτό σύνολο. Επομένως αντιστοιχεί σε μια πεπερασμένη επέκταση Galois $K/\mathbb{Q}$. Συνεπώς ο περιορισμός της ρ στην $\mathrm{Gal}(K/\mathbb{Q})$ απεικονίζεται στην $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. Επειδή $K/\mathbb{Q}$ πεπερασμένη, έπεται ότι η εικόνα $\mathrm{Im}\rho(\mathrm{Gal}(K/\mathbb{Q}))$ περιέχεται σε μια ομάδα $\mathrm{GL}_2(\mathbb{F})$, όπου $\mathbb{F}$ κάποιο πεπερασμένο σώμα $\mathbb{F}$.

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & & \\ \downarrow & \searrow^{\rho} & \\ \mathrm{Gal}(K/\mathbb{Q}) & \hookrightarrow & \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \end{array}$$

Η εικασία του Serre δηλώνει ότι κάθε συνεχής ανάγωγη αναπαράσταση,

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

για την οποία ισχύει μία επιπλέον συνθήκη, προκύπτει από μια κατάλληλη modular μορφή modulo ℓ.

Παράδειγμα XII.4.2. Προκειται για το πρώτο παράδειγμα που μελέτησε ο Serre. Η

$$\Delta(z) := \sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{n=1}^{\infty} (1-q^n)^{24}, q = e^{2\pi i z}, \mathrm{Im}(z) > 0$$

συνάρτηση είναι γνωστό ότι είναι η μοναδική κανονικοποιημένη μορφή κορυφών (cusp form), δηλαδή $\tau(0) = 0$ και $\tau(1) = 1$ βάρους 12 ως προς την ομάδα $\mathrm{SL}_2(\mathbb{Z})$. Ο Serre διατύπωσε την εικασία ότι υπάρχει μια οικογένεια «αυστηρά συμβατών» ℓ-αδικών αναπαραστάσεων της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ των οποίων η αντίστοιχη L-σειρά συμπίπτει με την L-σειρά της $\Delta(z)$ η οποία είναι

$$L(\Delta, s) = \sum_{n=1}^{\infty} \tau(n) n^{-s} = \prod_p \left(1 - \tau(p)p^{-s} + p^{11-2s}\right)^{-1}.$$

Το p διατρέχει όλους τους πρώτους αριθμούς. Πολύ σύντομα, μετά τη διατύπωση της εικασίας, ο Deligne κατασκεύασε για κάθε πρώτο ℓ, μια αναπαράσταση ρ_{ℓ^∞}

$$\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

μη-διακλαδιζόμενη έξω από το ℓ, τέτοια ώστε για όλους τους πρώτους $p \neq \ell$ να ισχύει

$$\mathrm{tr}(\rho_{\ell^\infty}(\mathrm{Frob}_p)) = \tau(p) \text{ και } \det(\rho_{\ell^\infty}(\mathrm{Frob}_p)) = p^{11}.$$

Επομένως, αν αναλύσουμε την $\rho_{\ell^\infty} \mod \ell$ έχουμε μία αναπαράσταση

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

με ανάλογες ιδιότητες. Εδώ οι παραπάνω ισότητες αντικαθίστανται από ισοτιμίες modulo ℓ, δηλαδή η αναπαράσταση ρ_ℓ είναι για τη διακρίνουσα $\Delta(z)$ ακριβώς ότι η ρ_ℓ για μια ελλειπτική

καμπύλη E. Η μόνη διαφορά είναι ότι οι ακέραιοι $a_p(E)$ αντικαθίστανται από τις αντίστοιχες τιμές της συνάρτησης του Ramanujan $\tau(p)$. Η ορίζουσα της ρ_ℓ είναι η 11η δύναμη του κυκλοτομικού χαρακτήρα $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^*$ modulo ℓ. Πρόκειται για τον χαρακτήρα που μας δίνει τη δράση της ομάδας $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ στις ℓ-στές ρίζες της μονάδας στο $\overline{\mathbb{Q}}$.

Γενικότερα, αν θεωρήσουμε κάποιο βάρος modular μορφών $k \geq 2$ και υποθέσουμε ότι η $f = \sum_{n=1}^{\infty} c_n q^n$ είναι μια, μη-μηδενική, μορφή κορυφών (cusp-form), βάρους k ως προς την ομάδα $\mathrm{SL}_2(\mathbb{Z})$ η οποία είναι Hecke ιδιομορφή, δηλαδή $f|T_n = c_n f$ για όλους τους τελεστές του Hecke. Τότε οι κατ'αρχήν μιγαδικοί αριθμοί c_n, αποδεικνύεται ότι είναι ακέραιοι αλγεβρικοί και παράγουν μια πεπερασμένη επέκταση E υπεράνω του $\mathbb{Q}$. Το σώμα E είναι πλήρως πραγματικό. Επομένως οι συντελεστές c_n ανήκουν στον δακτύλιο των ακεραίων αλγεβρικών R_E του σώματος E. Για κάθε ομομορφισμό δακτυλίων

$$\phi : R_E \longrightarrow \overline{\mathbb{F}}_\ell$$

μπορεί κανείς να ορίσει μία αναπαράσταση

$$\rho_\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longmapsto \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

η οποία δεν διακλαδίζεται για κανέναν πρώτο, διάφορο του ℓ, έτσι ώστε

$$\mathrm{tr}(\rho(\mathrm{Frob}_p)) = \phi(c_p), \det(\rho(\mathrm{Frob}_p)) = p^{k-1}$$

για κάθε πρώτο $p \neq \ell$. Ισχύει $\det \rho = \chi^{k-1}$. Επειδή δε ο k είναι άρτιος, δεν υπάρχουν modular μορφές περιττού βάρους ως προς την ομάδα $\mathrm{SL}_2(\mathbb{Z})$, έπεται ότι η ορίζουσα είναι μια περιττή δύναμη του κυκλοτομικού χαρακτήρα χ. Επομένως η ορίζουσα

$$\det \rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^*,$$

δεν διακλαδίζεται για πρώτους p, $p \neq \ell$ και παίρνει την τιμή $-1 \in \overline{\mathbb{F}}_\ell$ για τον μιγαδικό συζυγή αυτομορφισμό $\mathrm{conj} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Η αναπαράσταση λέγεται περιττή.

Εικασία XII.4.3 (Serre)**.**

1. Ασθενής εικασία. Έστω
$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell).$$
Η ρ είναι modular. Αυτό σημαίνει ότι υπάρχουν ακέραιοι N και k έτσι ώστε η ρ να προκύπτει από μία μορφή κορυφών $f \in S_k(\Gamma_1(N))$. (Η ομάδα $\Gamma_1(N)$ ορίζεται ως εξής:
$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}).$$
2. Ισχυρή εικασία. Εδώ μας δίνεται η «συνταγή» για τους ακέραιους $N = N(\rho)$ και $k = k(\rho)$ και η αναπαράσταση ρ προκύπτει από κάποια μορφή κορυφών $f \in S_{k(\rho)}(\Gamma_1(N(\rho)))$. Ο Serre μάλιστα περιέγραψε μια συνταγή για την εύρεση του ελάχιστου level $N(\rho)$.

Ήταν ήδη σαφές στον Frey ότι η ύπαρξη μιας τέτοιας καμπύλης, όπως αυτή προέκυψε από την υπόθεση της ύπαρξης ακέραιας λύσης της εικασίας του Fermat ερχόταν σε αντίφαση με την εικασία Shimura-Taniyama, αλλά δεν τα κατάφερε να δώσει μια πλήρη απόδειξη.

Αυτό έδωσε αφορμή στον Serre, ο οποίος ασχολήθηκε με το θέμα, παρουσίασε τις ιδέες του σε μια επιστολή του στον J.F. Mestre (1987) [21], επέστρεψε στα σημαντικά αποτελέσματα του έτους 1972 και δημοσίευσε την επίσης εξαιρετική εργασία *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ [23] στην οποία διατύπωσε τη σχετική εικασία.

Η εικασία του Serre, αποδείχθηκε τελικά από τους K. Chandrashekhar και J. P. Wintenberger, [14], [15]. Αλλά αφού η πλήρης απόδειξη της εικασίας του Serre δόθηκε το 2009, ποιος είναι ο ρόλος που έπαιξε η εικασία του Serre στην απόδειξη της εικασίας του Fermat ώστε να θεωρείται ένας από τους τέσσερις σημαντικούς πυλώνες της απόδειξης;

Αλλά νομίζουμε ότι είναι καιρός να προχωρήσουμε στην τρίτη πράξη.

XII.4.3 Το θεώρημα του Ribet

Το θεώρημα αναφέρεται στη βελτιστοποίηση του βάρους των modular μορφών.

Θεώρημα XII.4.4. *Υποθέτουμε ότι η* $E|_{\mathbb{Q}}$ *είναι μια modular ελλειπτική καμπύλη με εξίσωση η οποία είναι ένα minimal global μοντέλο, διακρίνουσα* $\Delta(E)$ *και οδηγό* $N(E)$*. Το ότι η* $E|_{\mathbb{Q}}$ *είναι modular, έπεται ότι υπάρχει μια modular μορφή* $f(z) \in S_2(\Gamma_0(N))$ *τέτοια ώστε*

$$L(E,s) = L(E,f).$$

Για κάθε πρώτο ℓ, $\ell \mid N(E)$ *υπάρχει* $f_1(z) \in S_2(\Gamma_0(N_1))$ $N_1 = N/\ell$ *για την οποία ισχύει*

$$L(E,s) = L(E,f_1)$$

και μάλιστα αν

$$f(z) = \sum_{n=1}^{\infty} c_n q^n, c_1 = 1, c_n \in \mathbb{Z}$$

και

$$f_1(z) = \sum_{n=1}^{\infty} d_n q^n, d_1 = 1, d_n \in \mathbb{Z}$$

ισχύει $c_n \equiv d_n \mod \ell$*, για* $1 \leq n < \infty$.

Το θεώρημα του Ribet δεν είχε την αναλυτική έκφραση, όπως το αναφέραμε, αλλά αποδείχθηκε μέσω της ισοδύναμης μορφής της modularity των Galois αναπαραστάσεων της ομάδας $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Κατά την προσέγγιση αυτή απέδειξε και μέρος της εικασίας του Serre. Συγκεκριμένα:

Θεώρημα XII.4.5 (Ribet)**.** *Έστω* $\ell \in \mathbb{P}, \ell \geq 3$ *και έστω*

$$\overline{\rho}_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

ανάγωγη ℓ*-αδική αναπαράσταση της* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*. Υποθέτουμε ότι η* $\overline{\rho}_\ell$ *είναι modular επιπέδου* $N := N(\overline{\rho}_\ell)$ *ελευθέρου τετραγώνου και ότι υπάρχει ένας πρώτος* q, $q \mid N$, $q \neq \ell$*, για τον οποίο η* $\overline{\rho}_\ell$ *δεν είναι πεπερασμένη. Έστω τώρα* $p \in \mathbb{P}$, $p \mid N$ *για τον οποίο η* $\overline{\rho}_\ell$ *είναι πεπερασμένη. Τότε η* $\overline{\rho}_\ell$ *είναι modular με level* N/p.

Πόρισμα XII.4.6. *Η ελλειπτική καμπύλη του Frey* $E^{(\ell)}_{a,b,c}|_{\mathbb{Q}}$ *δεν είναι modular, για* $\ell \geq 5$.

Απόδειξη. Ότι η εικασία του Fermat είναι αληθής για τον $\ell = 3$ είναι γνωστό. Ας υποθέσουμε λοιπόν ότι $\ell \geq 5$. Αν ήταν modular, τότε η αντίστοιχη αναπαράσταση $\overline{\rho}_\ell$ θα ήταν modular με level έστω N.

Η $E_{a,b,c}$ είναι ημι-ευσταθής (semi-stable). Επομένως ο οδηγός της $N = \prod_{p|abc} p$ είναι ελεύθερος τετραγώνου. Η διακρίνουσα $\Delta(E^{(\ell)}_{a,b,c}) = \frac{(abc)^{2\ell}}{2^8}$ είναι minimal διακρίνουσα της $E^{(\ell)}_{a,b,c}$. Η αναπαράσταση $\overline{\rho}_\ell$ είναι ανάγωγη για κάθε $\ell \geq 5$ [23]. Αυτό προέκυψε ως πόρισμα του θεωρήματος του Mazur. Αν $p \neq \ell$ και η $\overline{\rho}_\ell$ είναι μη-διακλαδιζόμενη στο p, τότε λέγεται πεπερασμένη στο p.

Αλλά, αν $E/\mathbb{Q}$ ελλειπτική καμπύλη, $\Delta(E)$ minimal διακρίνουσα της E, ℓ και p πρώτοι αριθμοί (δεν αποκλείεται η ισότητα $p = \ell$), τότε η αναπαράσταση

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(E[\ell])$$

είναι άπειρη στο p αν και μόνο αν $\nu_p(\Delta(E)) \equiv 0 \mod \ell$, όπου ν_p είναι η p-αδική εκτίμηση, [23]. Η minimal διακρίνουσα της ελλειπτικής καμπύλης του Frey $E^{(\ell)}_{a,b,c}|_{\mathbb{Q}}$ είναι $\Delta(E^{(\ell)}_{a,b,c}) = \frac{(abc)^{2\ell}}{2^8}$.

Επομένως

$$\nu_p(\Delta(E^{(\ell)}_{a,b,c})) \equiv 0 \mod \ell, \text{ για } p \neq 2$$
$$\nu_2(\Delta(E^{(\ell)}_{a,b,c})) \not\equiv 0 \mod \ell.$$

Συνεπώς η $\overline{\rho}_\ell$ είναι πεπερασμένη σε όλους τους περιττούς πρώτους, αλλά όχι στο $q = 2$. Άρα μπορούμε να εφαρμόσουμε το θεώρημα του Ribet για $q = 2$.

Αυτό μας επιτρέπει να «σκοτώσουμε» διαδοχικά όλους τους περιττούς πρώτους του N. Έτσι καταλήγουμε στο συμπέρασμα η $\overline{\rho}_\ell$ είναι modular επιπέδου 2, δηλαδή υπάρχει μια κανονικοποιημένη μορφή κορυφής $f \in S_2(\Gamma_0(2))$ της οποίας η αντίστοιχη αναπαράσταση είναι ισοδύναμη προς την $\widetilde{\rho}_\ell$. Αυτό όμως είναι αδύνατο, αφού

$$\dim_{\mathbb{C}} S_2(\Gamma_0(N)) = 0.$$

□

Ακολουθεί η «κάθαρση» της παράστασής μας!

XII.4.4 Το θεώρημα του Wiles

Εικασία XII.4.7 (Shimura-Taniyama)**.** Κάθε ελλειπτική καμπύλη $E|_{\mathbb{Q}}$ είναι modular.

Θεώρημα XII.4.8 (Wiles 1994)**.** *Κάθε ημι-ευσταθής ελλειπτική καμπύλη $E|_{\mathbb{Q}}$ είναι modular*

Πόρισμα XII.4.9. *Η εικασία του Fermat είναι αληθής.*

Απόδειξη. Έστω $\ell \in \mathbb{P}, \ell \geq 5$. Αν η εξίσωση του Fermat έχει κάποια ακέραια, μη-τετριμμένη λύση για κάποιο ℓ, αυτό σημαίνει ότι υπάρχει η ελλειπτική καμπύλη του Frey $E^{(\ell)}_{a,b,c}$. Είναι ημιευσταθής, αλλά αποδείξαμε ότι δεν είναι modular, κάτι που έρχεται σε αντίφαση προς το θεώρημα του Wiles. Συνεπώς, δεν υπάρχουν ακέραιες, μη τετριμμένες λύσεις της εξίσωσης Fermat. □

XII.4.5 Η στρατηγική της απόδειξης του Wiles

Υπάρχουν διάφοροι, ισοδύναμοι μεταξύ τους, χαρακτηρισμοί των modular ελλειπτικών καμπυλών $E|_{\mathbb{Q}}$, δείτε για παράδειγμα [10], [9].

Και ο A. Wiles, ακολουθεί τον ισοδύναμο χαρακτηρισμό μέσω της θεωρίας των Galois αναπαραστάσεων της ομάδας $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Η ομάδα αυτή δρα φυσιολογικά, μέσω μεταθέσεων στις ρίζες των πολυωνύμων με ρητούς συντελεστές. Αν μας δοθεί ένα πεπερασμένο σύνολο S πρώτων αριθμών, μπορούμε να θεωρήσουμε μόνο τα μονικά πολυώνυμα με ακέραιους συντελεστές των οποίων η διακρίνουσα διαιρείται μόνο από πρώτους $\ell \in S$. Η ομάδα $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ δρα στις ρίζες τέτοιων πολυωνύμων μέσω ένας πηλίκου και συγκεκριμένα της ομάδας $\mathrm{Gal}_S(\overline{\mathbb{Q}}/\mathbb{Q})$ των αυτομορφισμών της maximal αλγεβρικής επέκτασης του $\mathbb{Q}$ η οποία είναι μη-διακλαδιζόμενη για όλους τους πρώτους που δεν ανήκουν στο S.

Επιπρόσθετα, έχουμε ήδη δει (γραμμικές) αναπαραστάσεις της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ στην ομάδα $\mathrm{GL}_n(L)$, όπου L είναι το $\mathbb{C}$ ή το πεπερασμένο σώμα $\mathbb{F}_{\ell^r}$ ή κάποια πεπερασμένη επέκταση του σώματος $\mathbb{Q}_\ell$ των ℓ-αδικών αριθμών. Ανάλογα ισχύουν και για τις αναπαραστάσεις της ομάδας $\mathrm{Gal}_S(\overline{\mathbb{Q}}/\mathbb{Q})$.

Αν μας δοθεί τώρα μια Galois αναπαράσταση

$$\rho : \mathrm{Gal}_S(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{Z}_\ell),$$

όπου $\mathbb{Z}_\ell$ είναι ο δακτύλιος των ακεραίων ℓ-αδικών αριθμών, μπορούμε να θεωρήσουμε την αντίστοιχη modulo ℓ αναπαράσταση

$$\overline{\rho} : \mathrm{Gal}_S(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{F}_\ell).$$

Σε πρώτο και σημαντικό βήμα ο Wiles απέδειξε το περίφημο θεώρημα της ανόδου της modularity σύμφωνα με το οποίο αν

$$\rho : \mathrm{Gal}_s(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

ανάγωγη αναπαράσταση, τότε κάτω από συγκεκριμένες συνθήκες, στις οποίες δεν θα αναφερθούμε εδώ, αν η $\overline{\rho}$ είναι modular και ανάγωγη, τότε είναι και η ρ.

Αν λοιπόν $E|_{\mathbb{Q}}$ μια ελλειπτική καμπύλη, θεωρούμε τις ομάδες

$$E[3^n] = \{P \in E(\overline{\mathbb{Q}}) : 3^n P = \mathcal{O}\}$$

και

$$T_3[E] = \lim_{\leftarrow n} E[3^n]$$

και τις αναπαραστάσεις Galois

$$\widetilde{\rho}_{E,3} : \mathrm{Gal}_S(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[3]) \cong \mathrm{GL}_2(\mathbb{F}_3)$$

και

$$\rho_{E,3} : \mathrm{Gal}_S(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_3).$$

Η εικασία του Artin, αφορά στην modularity όλων των περιττών 2-διάστατων Galois αναπαραστάσεων

$$\rho : \mathrm{Gal}_S(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{C}).$$

Η εικασία διατυπώθηκε το 1923. Η εικόνα της ρ modulo scalar πίνακες είναι ισόμορφη προς μία διεδρική ομάδα ή την A_4 ή την S_4 ή την A_5. Η περίπτωση που η εικόνα είναι διεδρική αποδείχθηκε από τον Hecke. Για την περίπτωση που η εικόνα είναι A_4 ή S_4 δηλαδή μια επιλύσιμη ομάδα αποδείχθηκε από τους Langlands [17] και Tunnell [27].

Όταν λοιπόν η $E|_{\mathbb{Q}}$ είναι ημι-ευσταθής, ο Wiles κατάφερε να ελέγξει τις προϋποθέσεις του Modularity lifting θεωρήματος για τις αναπαραστάσεις $\rho_{E,3}$ και $\overline{\rho}_{E,3}$, υπό την προϋπόθεση ότι η $\overline{\rho}_{E,3}$ είναι ανάγωγη και κατέληξε στο συμπέρασμα ότι η $\rho_{E,3}$ είναι modular, κάτι από το οποίο συνεπάγεται ότι και η $E|_{\mathbb{Q}}$ είναι modular.

Στη συνέχεια, στην περίπτωση που η $\overline{\rho}_{E,3}$ δεν είναι ανάγωγη, εργάστηκε με τον πρώτο $\ell = 5$. Η Galois αναπαράσταση $\overline{\rho}_{E,5}$ είναι πάντοτε ανάγωγη, αφού σύμφωνα με το θεώρημα του Mazur, δεν υπάρχει ελλειπτική καμπύλη $E|_{\mathbb{Q}}$ να έχει υποομάδα ρητών σημείων τάξεως 15.

Όμως η Galois αναπαράσταση της $E[5]$ δεν ήταν εκ των προτέρων γνωστή. Για να το πετύχει αυτό ο Wiles θεώρησε μια βοηθητική ημιευσταθή ελλειπτική καμπύλη E' για την οποία ισχύουν ότι $\widetilde{\rho}_{E',5} = \widetilde{\rho}_{E,5}$ και $\widetilde{\rho}_{E',3}$ είναι ανάγωγη. Από το προηγούμενο επιχείρημα του Wiles για $\ell = 3$, έπεται ότι η E' είναι modular, οπότε και η $E'[5] = E[5]$ είναι επίσης modular και με εφαρμογή του lifting modularity θεωρήματος απέδειξε ότι και η ημι-ευσταθής $E|_{\mathbb{Q}}$ είναι modular. Το τέχνασμα της απόδειξης του Wiles ονομάστηκε «3-5-switch».

Ο Henry Darmon στο [6] αναφέρει:

> *«It is a dramatic illustration for the unity and historical continuity of mathematics that the solution in radicals of the general quartic equation, one of the great feats of the algebraists of the Italian Renaissance, is precisely what allowed Langlands, Tunnell, and Wiles to prove their modularity results more than five centuries later.»*

Η modularity όλων των ελλειπτικών καμπυλών $E|_{\mathbb{Q}}$, όχι μόνο των ημι-ευσταθών, ολοκληρώθηκε το 2001 από τους C. Breuil, B. Conrad, F. Diamond, και R. Taylor, [3].

Στον A. Wiles, δεν ήταν δυνατόν να απονεμηθεί το Fields Medall, αφού όταν έγινε το Παγκόσμιο Συνέδριο Μαθηματικών το 1998 στο Βερολίνο είχε ήδη κλείσει την ηλικία των 40 ετών. Του απονεμήθηκε ένα έξτρα τιμητικό δίπλωμα στο εν λόγω συνέδριο. Του απονεμήθηκε όμως το βραβείο Abel το 2016 [1].

[1] Στο link που ακολουθεί μπορεί κανείς να παρακολουθήσει την διάλεξη του Wiles κατά την απονομή του βραβείου Abel `https://www.youtube.com/watch?v=WNVq4nK3ir0`

Βιβλιογραφία

[1] Alaca, Ş. & Williams, K. S. *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, 2004, pp. xviii+428. ISBN: 0-521; 0-521-54011-9.

[2] Ash, A. & Gross, R. *Fearless symmetry*. Exposing the hidden patterns of numbers, With a foreword by Barry Mazur. Princeton University Press, Princeton, NJ, 2006, pp. xx+272. ISBN: 0-691-12492-2; 978-0-691-12492-6.

[3] Breuil, C. et al. *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*. *J. Amer. Math. Soc.* 14.4 (2001), pp. 843–939. ISSN: 0894-0347. URL: https://doi.org/10.1090/S0894-0347-01-00370-8.

[4] Conrad, B. & Rubin, K., eds. *Arithmetic Algebraic Geometry*. Vol. 9. IAS/Park City Mathematics Series. Including papers from the Graduate Summer School of the Institute for Advanced Study/Park City Mathematics Institute held in Park City, UT, June 20–July 10, 1999. American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2001, pp. xiv+569. ISBN: 0-8218-2173-3.

[5] Cornell, G., Joseph, S. & Glenn, S. *Modular Forms and Fermat's Last Theorem*. Springer New York, 1997. ISBN: 9780387946092. URL: https://books.google.gr/books?id=VaquzVwtMsC.

[6] Darmon, H. *Andrew Wiles's marvelous proof*. *Notices Amer. Math. Soc.* 64.3 (2017), pp. 209–216. ISSN: 0002-9920.

[7] Darmon, H., Diamond, F. & Taylor, R. *Fermat's Last Theorem*. *Current developments in mathematics, 1995 (Cambridge, MA)*. Int. Press, Cambridge, MA, 1994, pp. 1–154.

[8] Darmon, H., Diamond, F. & Taylor, R. *Fermat's Last Theorem*. *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*. Int. Press, Cambridge, MA, 1997, pp. 2–140.

[9] Diamond, F. & Shurman, J. *A First Course in Modular Forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, pp. xvi+436. ISBN: 0-387-23229-X.

[10] Frey, G. *The Way to the Proof of Fermat's Last Theorem*. *Ann. Fac. Sci. Toulouse Math. (6)* 18.Fascicule Spécial (2009), pp. 5–23. ISSN: 0240-2963. URL: http://afst.cedram.org/item?id=AFST_2009_6_18__5_0.

[11] Fulton, W. *Algebraic Curves*. Advanced Book Classics. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989, pp. xxii+226. ISBN: 0-201-51010-3.

[12] Gouvêa, F. Q. *"A marvelous proof"*. *Amer. Math. Monthly* 101.3 (1994), pp. 203–222. ISSN: 0002-9890. URL: https://doi.org/10.2307/2975598.

[13] Hulek, K. *Elementary Algebraic Geometry*. Vol. 20. Student Mathematical Library. Translated from the 2000 German original by Helena Verrill. American Mathematical Society, Providence, RI, 2003, pp. viii+213. ISBN: 0-8218-2952-1. URL: https://doi.org/10.1090/stml/020.

[14] Khare, C. & Wintenberger, J.-P. *Serre's modularity conjecture. I*. *Invent. Math.* 178.3 (2009), pp. 485–504. ISSN: 0020-9910. URL: https://doi.org/10.1007/s00222-009-0205-7.

[15] Khare, C. & Wintenberger, J.-P. *Serre's modularity conjecture. II*. *Invent. Math.* 178.3 (2009), pp. 505–586. ISSN: 0020-9910. URL: https://doi.org/10.1007/s00222-009-0206-6.

[16] Lang, S. *Introduction to modular forms*. Vol. 222. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original. Springer-Verlag, Berlin, 1995, pp. x+261. ISBN: 3-540-07833-9.

[17] Langlands, R. P. *Base Change for* $\mathrm{GL}(2)$. Vol. 96. Annals of Mathematics Studies. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1980, pp. vii+237. ISBN: 0-691-08263-4; 0-691-08272-3.

[18] Rubin, K. & Silverberg, A. *A report on Wiles' Cambridge lectures*. *Bull. Amer. Math. Soc. (N.S.)* 31.1 (1994), pp. 15–38. ISSN: 0273-0979. URL: https://doi.org/10.1090/S0273-0979-1994-00512-9.

[19] Saito, T. *Fermat's Last Theorem*. Vol. 245. Translations of Mathematical Monographs. The proof, Translated from the 2009 Japanese original by Masato Kuwata, Iwanami Series in Modern Mathematics. American Mathematical Society, Providence, RI, 2014, pp. xvi+222. ISBN: 978-0-8218-9849-9. URL: https://doi.org/10.1090/mmono/245.

[20] Saito, T. *Fermat's last theorem*. Vol. 243. Translations of Mathematical Monographs. Basic tools, Translated from the Japanese original by Masato Kuwata. American Mathematical Society, Providence, RI, 2013, pp. xiv+200. ISBN: 978-0-8218-9848-2. URL: https://doi.org/10.1090/mmono/243.

[21] Serre, J.-P. *Lettre à J.-F. Mestre. Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*. Vol. 67. Contemp. Math. Amer. Math. Soc., Providence, RI, 1987, pp. 263–268. URL: https://doi.org/10.1090/conm/067/902597.

[22] Serre, J.-P. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. *Invent. Math.* 15.4 (1972), pp. 259–331. ISSN: 0020-9910. URL: https://doi.org/10.1007/BF01405086.

[23] Serre, J.-P. *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.* 54.1 (1987), pp. 179–230. ISSN: 0012-7094. URL: https://doi.org/10.1215/S0012-7094-87-05413-5.

[24] Silverman, J. H. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. URL: https://doi.org/10.1007/978-0-387-09494-6.

[25] Stichtenoth, H. *Algebraic function fields and codes*. Second. Vol. 254. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 2009, pp. xiv+355. ISBN: 978-3-540-76877-7.

[26] Taylor, R. & Wiles, A. *Ring-theoretic properties of certain Hecke algebras*. *Ann. of Math. (2)* 141.3 (1995), pp. 553–572. ISSN: 0003-486X. URL: https://doi.org/10.2307/2118560.

[27] Tunnell, J. *Artin's conjecture for representations of octahedral type*. *Bull. Amer. Math. Soc. (N.S.)* 5.2 (1981), pp. 173–175. ISSN: 0273-0979. URL: https://doi.org/10.1090/S0273-0979-1981-14936-3.

[28] Washington, L. C. *Elliptic Curves*. Discrete Mathematics and its Applications (Boca Raton). Number theory and cryptography. Chapman & Hall/CRC, Boca Raton, FL, 2003, pp. xii+428. ISBN: 1-58488-365-0.

[29] Wiles, A. *Modular Elliptic Curves and Fermat's Last Theorem*. *Ann. of Math. (2)* 141.3 (1995), pp. 443–551. ISSN: 0003-486X. URL: https://doi.org/10.2307/2118559.

[30] Αντωνιάδης, Ι. Α. *Ελλειπτικές Καμπύλες*. Ηράκλειο: Πανεπιστήμιο Κρήτης, 1999.

[31] Κοντογεώργης, Α. *Ημιευσταθείς Ελλειπτικές Καμπύλες και το τελευταίο θεώρημα του Fermat*. MA thesis. Πανεπιστήμιο Κρήτης, 1994.

[32] Μαγιολαδίτης, Μ. *Αλγεβρικές καμπύλες, εικασία του Riemann και κωδικοποίηση*. MA thesis. Πανεπιστήμιο Κρήτης, 2001. URL: https://www.researchgate.net/publication/32952663_Algebrikes_Kampyles_eikasia_tou_Riemann_kai_kodikopoiese.

XIII

Παράρτημα - Δακτύλιοι και modules

Στο κεφάλαιο αυτό αναφέρονται βασικές έννοιες και αποτελέσματα θεωρίας δακτυλίων και modules (προτύπων) χρήσιμα για την κατανόηση της ύλης του βιβλίου.

XIII.1 Ακέραιες περιοχές

Ορισμός XIII.1.1. Μια *ακέραια περιοχή* είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο χωρίς διαιρέτες του μηδενός.

Παράδειγμα XIII.1.2. Οι παρακάτω δακτύλιοι είναι ακέραιες περιοχές:

- $\mathbb{Z}$
- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ όπου ω μια πρωταρχικη 3-ρίζα της μονάδας.
- $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$, όπου m ακέραιος, θετικός ή αρνητικός όχι τέλειο τετράγωνο.
- $\mathbb{Z}[X]$ ο δακτύλιος των πολυωνύμων μιας μεταβλητής με συντελεστές ακεραίους.
- $\mathbb{Z}[\theta] = \{a + b\theta + c\theta^2 : a, b, \nu \in \mathbb{Z}\}$, όπου θ μια ρίζα της κυβικής εξίσωσης $X^3 + X + 1 = 0$.
- Ο δακτύλιος $\mathbb{Z}_m$ των κλάσεων υπολοίπων modulo $m \in \mathbb{N}$, $m \geq 2$. Ο $\mathbb{Z}_m$ είναι ακέραια περιοχή (στην προκειμένη περίπτωση σώμα) αν και μόνο αν ο m είναι πρώτος αριθμός.

Σε μία ακέραια περιοχή ορίζεται η έννοια της διαιρετότητας των στοιχείων αυτής.

Ορισμός XIII.1.3. Έστω R μια ακέραια περιοχή και $a, b \in R$. Το a διαιρεί το b (συμβολισμός $a \mid b$) όταν υπάρχει $c \in R$, ώστε $b = ac$.

Παράδειγμα XIII.1.4.

- Στην ακέραια περιοχή $\mathbb{Z}[i]$ το $1 + i \mid 2$ αφού $2 = (1 + i)(1 - i)$.
- Στην ακέραια περιοχή $\mathbb{Z}[\omega]$ το $(1 - \omega)^2 \mid 3$ αφού $3 = (1 - \omega)^2(1 + \omega)$
- Στην ακέραια περιοχή $\mathbb{Z}[\theta]$ το $(1 + \theta - \theta^2) \mid (-\theta - 2\theta^2)$ αφού $-\theta - 2\theta^2 = (1 + \theta - \theta^2)(1 - \theta)$.
- Στην ακέραια περιοχή $\mathbb{Z}[\sqrt{2}]$ το $(2 + \sqrt{2}) \nmid 5$ αφού $\frac{5}{2+\sqrt{2}} = 5 - \frac{5}{2}\sqrt{2}$ και $\frac{5}{2} \notin \mathbb{Z}$.

Ορισμός XIII.1.5. Ένα στοιχείο $a \in R$, R ακεραία περιοχή θα λέγεται *μονάδα* του R όταν $a \mid 1$

Πρόταση XIII.1.6. *Το σύνολο των μονάδων* $E(R)$ *ή* R^* *της ακέραιας περιοχής* R. *αποτελεί αβελιανή πολλαπλασιαστική ομάδα (άσκηση).*

Ορισμός XIII.1.7. Δύο στοιχεία a, b μιας ακεραίας περιοχής R θα λέγονται *συνεταιρικά* όταν $a \mid b$ και $b \mid a$. Συμβολισμός $a \sim b$.

Παράδειγμα XIII.1.8. Στην ακέραια περιοχή $\mathbb{Z}[\sqrt{2}]$ τα $1+3\sqrt{2}$ και $5-2\sqrt{2}$ είναι συνεταιρικά αφού

$$\frac{1+3\sqrt{2}}{5-2\sqrt{2}} = 1+\sqrt{2} \in \mathsf{E}(\mathbb{Z}[\sqrt{2}]).$$

Είναι γνωστό ότι στο $\mathbb{Z}$ ένας ακέραιος ≥ 2 λέγεται πρώτος όταν οι μοναδικοί θετικοί διαιρέτες αυτού είναι το 1 και ο εαυτός του. Επίσης γνωρίζουμε ότι για κάθε πρώτο ακέραιο p ισχύουν οι ακόλουθες δύο ιδιότητες:

1. Αν $p = ab,\ a,b \in \mathbb{Z} \Rightarrow a$ ή $b = \pm 1$.
2. Αν $p \mid ab,\ a,b \in \mathbb{Z} \Rightarrow p \mid a$ είτε $p \mid b$.

Κατ' αναλογία προς το $\mathbb{Z}$ μπορούμε να ορίσουμε

Ορισμός XIII.1.9. Έστω R μια ακέραια περιοχή.

1. Ένα στοιχείο $a \in R,\ a \neq 0,\ a \notin \mathsf{E}(R)$ θα λέγεται *ανάγωγο στοιχείο* της R όταν
$$\text{Αν } a = bc, b, c \in R \Rightarrow b \text{ ή } c \in \mathsf{E}(R).$$
2. Το στοιχείο $p \in R,\ p \neq 0,\ p \notin \mathsf{E}(R)$ θα λέγεται πρώτο στοιχείο του R όταν
$$\text{Αν } p \mid ab, a, b \in R \Rightarrow p \mid a \text{ είτε } p \mid b.$$

Παράδειγμα XIII.1.10.
- Το 2 είναι ανάγωγο στην ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$.
- Το $7+\sqrt{-5}$ δεν είναι ανάγωγο στην ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$ αφού $7+\sqrt{-5} = (1+\sqrt{-5})(2-\sqrt{-5})$
- Το 2 είναι πρώτο στοιχείο της $\mathbb{Z}$
- Το 2 δεν είναι πρώτο στοιχείο της $\mathbb{Z}[\sqrt{-5}]$ αφού το $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ ενώ $2 \nmid 1 \pm \sqrt{-5}$.

Πρόταση XIII.1.11. *Αν R ακέραια περιοχή, τότε κάθε πρώτο στοιχείο αυτής είναι ανάγωγο (άσκηση).*

XIII.2 Ευκλείδειες περιοχές

Η πρώτη σημαντική ιδιότητα του $\mathbb{Z}$ είναι η ύπαρξη ευκλείδειας διαίρεσης. Γενικεύουμε αυτή την έννοια.

Ορισμός XIII.2.1. Έστω R μια ακέραια περιοχή. Μια συνάρτηση $\phi : R \to \mathbb{Z}$ θα λέγεται *ευκλείδεια συνάρτηση* όταν

1. Για όλα τα $a, b \in R,\ b \neq 0$, ισχύει $\phi(ab) \geq \phi(a)$ και
2. Αν $a, b \in R,\ b \neq 0$ υπάρχουν $\pi, \upsilon \in R$ ώστε $a = b\pi + \upsilon$ και $\phi(\upsilon) < \phi(b)$.

Ορισμός XIII.2.2. Αν R είναι μία ακέραια περιοχή εφοδιασμένη με μία ευκλείδεια συνάρτηση ϕ, τότε η R λέγεται ευκλείδεια περιοχή ως προς την ϕ.

Παράδειγμα XIII.2.3.
1. $(\mathbb{Z}, \phi)$, όπου $\phi(a) = |a|$ για κάθε $a \in \mathbb{Z}$
2. $(\mathbb{Z}[i], \phi)$, όπου $\phi(a+bi) = a^2 + b^2$
3. $(\mathbb{Z}[\sqrt{-2}])$, όπου $\phi(a+b\sqrt{-2}) = a^2 + 2b^2$
4. $(\mathbb{Z}[\sqrt{2}])$, όπου $\phi(a+b\sqrt{2}) = |a^2 - 2b^2|$
5. $(K[X], \phi)$, όπου K σώμα και
$$\phi(f(X)) = \begin{cases} \deg f(x), & \text{αν } f(x) \neq 0 \\ -1, & \text{αν } f(x) = 0 \end{cases}$$

(Άσκηση)

Έστω τώρα m ακέραιος ελεύθερος τετραγώνου. Ορίζουμε τη συνάρτηση, απόλυτη τιμή της norm στοιχείων του σώματος K

$$\begin{aligned}\phi_m : \mathbb{Q}(\sqrt{m}) &\longrightarrow \mathbb{Z}\\ (\kappa + \lambda\sqrt{m}) &\longmapsto |\kappa^2 - \lambda^2 m|\end{aligned}$$

Το ερώτημα είναι για ποια $m \equiv 2,3 \mod 4$ η ακέραια περιοχή $\mathbb{Z}[\sqrt{m}]$ και για ποια $m \equiv 1 \mod 4$ η ακέραια περιοχή $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ είναι ως προς την ϕ_m ευκλείδεια περιοχή ή όπως αλλιώς λέγονται *norm ευκλείδεια περιοχή*.

Αποδεικνύεται ότι για $m = 2,3 \mod 4$, $m < 0$ η ακέραια περιοχή $\mathbb{Z}[m]$ είναι norm ευκλείδεια αν και μόνο αν $m = -1, -2$. Επίσης στην περίπτωση που $m \equiv 1 \mod 4$, $m < 0$ αποδεικνύεται ότι η $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ είναι norm ευκλείδεια αν και μόνο αν $m = -3, -7, -11$.

Εντελώς φυσιολογικά εγείρεται το ερώτημα τι γίνεται με αυθαίρετες ευκλείδειες συναρτήσεις όχι κατ' ανάγκη norm-ευκλείδειες. Αν $K = \mathbb{Q}(\sqrt{m})$ μιγαδικό ($m < 0$) τετραγωνικό σώμα αριθμών και η περιοχή των ακεραίων αλγεβρικών αριθμών αυτού

$$R_K = \begin{cases}\mathbb{Z}[\sqrt{m}] & \text{αν } m \equiv 2,3 \mod 4\\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{αν } 1 \mod 4\end{cases}$$

είναι ευκλείδεια ως προς κάποια ευκλείδεια συνάρτηση, τότε είναι και norm ευκλείδεια, [12].

Αν τώρα $K = \mathbb{Q}(\sqrt{m})$ πραγματικό ($m > 0$) τετραγωνικό σώμα αριθμών, τότε γνωρίζουμε ότι η ακέραια περιοχή των ακεραίων αλγεβρικών αριθμών του σώματος K είναι norm-ευκλείδειες αν και μόνο αν $m = 2,3,5,6,7,11,13,17,19,21,23,29,37,41,57,73$, [4].

Αλλά τι γίνεται αν επιτρέψουμε οποιαδήποτε ευκλείδεια συνάρτηση; Το 1994 ο D.A. Clark απέδειξε ότι η ακέραια περιοχή των ακεραίων αλγεβρικών αριθμών $R_K = \mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ του σώματος $K = \mathbb{Q}(\sqrt{69})$ είναι ευκλείδεια περιοχή αλλά όχι norm-ευκλείδεια, [5]. Η συνάρτηση του Clark είναι η

$$\phi(a + b\frac{1+\sqrt{69}}{2}) = \begin{cases}|a^2 + ab - 17b^2| & \text{όταν } (a,b) \neq (10,3)\\ 26 & \text{όταν } (a,b) = (10,3)\end{cases}$$

Σημείωση XIII.2.4. Αφού το 26 μπορεί να αντικατασταθεί από οποιονδήποτε ακέραιο > 25 υπάρχουν άπειρες ϕ ώστε η $(\mathbb{Z}[\frac{1+\sqrt{69}}{2}], \phi)$ να είναι ευκλείδεια.

Ο Samuel [15] εικάζει ότι ίσως η ακέραια περιοχή $\mathbb{Z}[\sqrt{14}]$ είναι ευκλείδεια αλλά όχι norm ευκλείδεια. Αυτό αποδείχθηκε από τον H.Harper [8], [9].

Τέλος αξίζει νομίζουμε να αναφέρουμε και το αποτέλεσμα του W. Narkiewicz [13] ότι υπάρχουν το πολύ δύο πραγματικά τετραγωνικά σώματα αριθμών $K = \mathbb{Q}(\sqrt{m})$ για τα οποία η ακέραια περιοχή των ακέραιων αλγεβρικών αριθμών R_K είναι περιοχή μοναδικής (μονοσήμαντης) ανάλυσης αλλά όχι ευκλείδεια περιοχή.

XIII.3 Περιοχές κυρίων ιδεωδών

Στην αρχή θα ορίσουμε την έννοια του ιδεώδους μιας ακέραιας περιοχής και θα περιγράψουμε βασικές ιδιότητες αυτών.

Ορισμός XIII.3.1. Ένα μη-κενό σύνολο A ακέραιας περιοχής R λέγεται *ιδεώδες* όταν:

1. Αν $a \in A, b \in A \Rightarrow a + b \in A$
2. Αν $a \in A$ και $r \in R \Rightarrow ra \in A$

Αν $\{a_1, a_2, \ldots, a_n\}$ είναι ένα σύνολο στοιχείων της R, τότε το σύνολο όλων των πεπερασμένων γραμμικών συνδυασμών των $a_1, \ldots, a_n$

$$\mathcal{A} = \{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_i \in R, i = 1, 2, \ldots, n\}$$

είναι ιδεώδες της R. Λέγεται το ιδεώδες που παράγεται από το σύνολο $\{a_1, a_2, \ldots, a_n\}$ και συμβολίζεται με $\langle a_1, a_2, \ldots, a_n\rangle$. Ειδικότερα, ένα ιδεώδες A της R θα λέγεται *κύριο* όταν παράγεται από ένα στοιχείο, $A = \langle a\rangle = Ra$.

Ορισμός XIII.3.2. Μια ακέραια περιοχή R θα λέγεται *περιοχή κυρίων ιδεωδών* (ΠΚΙ) όταν όλα της τα ιδεώδη είναι κύρια.

Παράδειγμα XIII.3.3. Οι δακτύλιοι $\mathbb{Z}, K[X]$ είναι ΠΚΙ, όπου K σώμα.

Στα ιδεώδη μπορούμε να ορίσουμε πράξεις πρόσθεσης και πολλαπλασιασμού. Έτσι έχουμε:

Ορισμός XIII.3.4. Έστω A, B ιδεώδη της ακέραιας περιοχής R. Το άθροισμα των A, B ορίζεται ως το σύνολο

$$A + B = \{a + b : a \in A, b \in B\}.$$

Το παραπάνω σύνολο είναι ιδεώδες του R και μάλιστα είναι το ελάχιστο ιδεώδες του R που περιέχει τα A και B.

Το γινόμενο $A \cdot B$ είναι το σύνολο όλων των πεπερασμένων αθροισμάτων της μορφής

$$A \cdot B = \{a_1b_1 + \cdots + a_nb_n : \text{για κάποιο φυσικό } n, a_i \in A, b_i \in B\}.$$

Και το γινόμενο είναι ιδεώδες της R και περιέχεται στην τομή $A \cap B$.

Μπορούμε ακόμη να ορίσουμε διαιρετότητα ιδεωδών.

Ορισμός XIII.3.5. Έστω A και B ιδεώδη της ακέραιας περιοχής R. Θα λέμε ότι το A διαιρεί το B (συμβολισμός $A \mid B$) όταν $B \subset A$.

Πρόταση XIII.3.6. *Αν* R *ακεραία περιοχή,* $\epsilon \in E(R)$ *και* A *ένα ιδεώδες αυτής, τότε ισχύουν (άσκηση)*

1. $\langle\epsilon\rangle = R$
2. $\langle a\rangle \mid \langle b\rangle \Leftrightarrow a \mid b$
3. $\langle a\rangle = \langle b\rangle \Leftrightarrow a/b \in E(R)$

Πρόταση XIII.3.7. *Αν* R *είναι περιοχή κυριών ιδεωδών, τότε κάθε ανάγωγο στοιχείο αυτής είναι και πρώτο.*

Παρατήρηση XIII.3.8. Απο τις προτάσεις XIII.1.11 και XIII.3.6 έπεται ότι σε περιοχές κυρίων ιδεωδών οι έννοιες ανάγωγο και πρώτο στοιχείο συμπίπτουν.

Ορισμός XIII.3.9. Ένα γνήσιο ιδεώδες M ($M \neq \langle 0\rangle, \langle 1\rangle = R$) μιας ακέραιας περιοχής R θα λέγεται *maximal (μέγιστο)*, όταν για οποιοδήποτε ιδεώδες A της R, $M \subset A \subset R$ έπεται ότι κατ' ανάγκη $A = M$ ή $A = R$.

Πρόταση XIII.3.10. *Έστω* R *ακέραια περιοχή και*

$$a \in R, a \neq 0, a \notin E(R).$$

Αν το ιδεώδες $\langle a\rangle$ *είναι maximal ιδεώδες της* R*, τότε το* a *είναι ανάγωγο στοιχείο της* R*. Ιδιαίτερα, αν η* R *είναι περιοχή κυρίων ιδεωδών και* $a \in R, a \neq 0, a \notin E(R)$*, τότε*

$$\langle a\rangle \textit{ maximal} \Leftrightarrow a \textit{ πρώτο στοιχείο της } R$$

Απόδειξη. Άσκηση □

Ορισμός XIII.3.11. Ένα ιδεώδες $P, P \neq R$ μίας ακέραιας περιοχής R θα λέγεται *πρώτο*, όταν

$$a, b \in R, ab \in P \Rightarrow a \in P \text{ είτε } b \in P.$$

Σημείωση XIII.3.12. Είναι γνωστό ότι αν R ακέραια περιοχή, τότε το $\langle 0 \rangle$ είναι πρώτο. Στην αλγεβρική θεωρία αριθμών όμως το $\langle 0 \rangle$ δεν το θεωρούμε ως ιδεώδες. Πρόκειται για έναν τεχνικό περιορισμό.

Πρόταση XIII.3.13. *Έστω R ακέραια περιοχή*

1. *Αν $a \in R, a \neq 0, a \notin E(R)$, τότε*

$$\big(\langle a \rangle \textit{ πρώτο ιδεώδες της } R\big) \Leftrightarrow \big(a \textit{ πρώτο στοιχείο της } R\big)$$

2. *Αν M maximal ιδεώδες της R, τότε το M πρώτο ιδεώδες αυτής.*

3. *Αν η R είναι περιοχή κυρίων ιδεωδών και A ένα γνήσιο ($A \neq \langle 0 \rangle, \langle 1 \rangle = R$) ιδεώδες της R, τότε*

$$A \textit{ maximal} \Leftrightarrow A \textit{ πρώτο}$$

4. *Αν $P \neq R$, ιδεώδες της ακέραιας περιοχής R, τότε*

$$(P \textit{ πρώτο ιδεώδες της } R) \Leftrightarrow (\textit{ αν } P \mid AB \Rightarrow P \mid A \textit{ είτε } P \mid B)$$

Πρόταση XIII.3.14. *Κάθε ευκλείδεια περιοχή είναι και περιοχή κυρίων ιδεωδών.*

Απόδειξη. Άσκηση □

Παρατήρηση XIII.3.15. Το αντίστροφο δεν ισχύει. Η ακέραια περιοχή $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ είναι περιοχή κυρίων ιδεωδών αλλά δεν είναι ευκλείδεια περιοχή.

XIII.4 Περιοχές μονοσήμαντης ανάλυσης

Είναι γνωστό ότι κάθε ακέραιος $a \in \mathbb{Z}$, $a \neq 0, a \neq \pm 1$ αναλύεται σε γινόμενο αναγώγων (πρώτων) παραγόντων και μάλιστα η ανάλυση αυτή είναι μοναδική. Τις δύο αυτές ιδιότητες θα μελετήσουμε τώρα σε ακέραιες περιοχές.

Ορισμός XIII.4.1. Έστω R ακέραια περιοχή και $a \in R, a \neq 0, a \notin E(R)$. Μια *παραγοντοποίηση* του a είναι ένα πεπερασμένο σύνολο π_i, $i = 1, 2, \ldots, n$ αναγώγων στοιχείων του R για το οποίο ισχύει

$$a = \prod_{i=1}^{n} \pi_i$$

Ο R θα λέγεται *περιοχή ανάλυσης*, όταν κάθε $a \in R, a \neq 0, a \notin E(R)$ έχει μία τουλάχιστον παραγοντοποίηση.

Το ερώτημα είναι, πότε μια ακέραια περιοχή είναι περιοχή ανάλυσης; Μια ικανή συνθήκη είναι η ακόλουθη:

Πρόταση XIII.4.2. *Αν δεν υπάρχει άπειρη ακολουθία $(a_i)_{i \in \mathbb{N}}$ στοιχείων της R για την οποία το a_{i+1} να είναι γνήσιος διαιρέτης του a_i για κάθε φυσικό i, τότε ο R είναι περιοχή ανάλυσης.*

Πόρισμα XIII.4.3. *Έστω* R *ακέραια περιοχή. Αν κάθε αύξουσα ακολουθία κυρίων ιδεωδών της* R *γίνεται τελικά σταθερή, τότε η* R *είναι περιοχή ανάλυσης.*

Ένα εξαιρετικά σημαντικό αποτέλεσμα είναι το

Θεώρημα XIII.4.4. *Έστω* R *ακέραια περιοχή. Οι ακόλουθες προτάσεις είναι μεταξύ τους ισοδύναμες:*

Κάθε αύξουσα ακολουθία ιδεωδών της R

$$A_0 \leq A_1 \leq A_2 \leq \cdots$$

γίνεται τελικά σταθερή, δηλαδή υπάρχει φυσικός n *για τον οποίο* $A_n = A_{n+1} = A_{n+2} = \cdots$

Κάθε διάφορο του κενού σύνολο ιδεωδών του R *έχει maximal στοιχείο*

Κάθε ιδεώδες A *της* R *είναι πεπερασμένα παραγόμενο, δηλαδή υπάρχουν* $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ *για τα οποία ισχύει*

$$A = R\alpha_1 + R\alpha_2 + \cdots + R\alpha_n = \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle.$$

Απόδειξη. Αποδεικνύεται αμέσως μετά τον ορισμό III.2.2. □

Παρατήρηση XIII.4.5. Το θεώρημα ισχύει γενικότερα για αντιμεταθετικούς δακτυλίους, αλλά εμείς το χρειαζόμαστε εδώ ειδικά για ακέραιες περιοχές.

Ορισμός XIII.4.6. Μία ακέραια περιοχή στην οποία ισχύει μια οποιαδήποτε από τις τρεις παραπάνω προτάσεις (και συνεπώς και οι τρεις) του θεωρήματος, λέγεται *περιοχή της Noether*.

Παρατήρηση XIII.4.7. Κάθε περιοχή της Noether είναι και περιοχή ανάλυσης.

Άμεση συνέπεια του θεωρήματος είναι τα ακόλουθα πορίσματα:

Πόρισμα XIII.4.8. *Κάθε περιοχή κυρίων ιδεωδών είναι περιοχή της Noether.*

Πόρισμα XIII.4.9. *Κάθε ευκλείδεια περιοχή είναι περιοχή της Noether. Ειδικά, οι ακέραιες περιοχές* $\mathbb{Z}$ *και* $K[X]$ *είναι περιοχές της Noether.*

Θεώρημα XIII.4.10 (Θεώρημα βάσης του Hilbert)**.** *Αν* R *είναι περιοχή της Noether, τότε και ο δακτύλιος των πολυωνύμων* $R[x]$ *είναι επίσης περιοχή της Noether.*

Απόδειξη. Πράγματι, αν υποθέσουμε ότι ο δακτύλιος R είναι δακτύλιος της Noether και έστω ένα ιδεώδες $A \triangleleft R[x]$. Ας υποθέσουμε ότι δεν είναι πεπερασμένα παραγόμενο, συνεπώς υπάρχει ακολουθία στοιχείων

$$\{f_0, f_1, \ldots, f_m \ldots\},$$

όπου $B_n = \langle f_0, \ldots, f_{n-1}$ και $f_n \in a \backslash B_n$, την οποία μπορούμε να την επιλέξουμε με τέτοιο τρόπο ώστε το στοιχείο f_n να είναι ελάχιστου βαθμού στο σύνολο $A \backslash B_n$. Είναι σαφές ότι για κάθε $n \in \mathbb{N}$

$$\deg f_n \leq \deg f_{n+1}.$$

Θεωρούμε τους leading terms $a_n = \mathrm{Lead}(f_n)$ των πολυωνύμων $f_n \in R[x]$, και σχηματίζουμε την ακολουθία ιδεωδών του δακτυλίου R

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \cdots \subset \langle a_0, a_1, \ldots, a_s \rangle \subset$$

η οποία είναι τελικά σταθερή, αφού ο R είναι δακτύλιος της Noether. Θεωρούμε το σταθερό ιδεώδες της ακολουθίας $B = \langle a_0, a_1, \ldots, a_{N-1} \rangle$ και έχουμε ότι $a_N \in B$, δηλαδή

$$a_N = \sum_{i<N} u_i a_i, u_i \in R.$$

Θεωρούμε το στοιχείο

$$g = \sum_{i<N} u_i x^{\deg f_N - \deg f_i} f_i,$$

το οποίο έχει leading term ίσο με αυτό του f_N. Προφανώς $g \in B_N$, $f_N \notin B_N$ συνεπώς $f_N - g \notin B_N$. Όμως $\deg(f_N - g) < \deg f_N$, άτοπο από τον τρόπο επιλογής του f_N. □

Παρατήρηση XIII.4.11. Αφού $\mathbb{Z}$ περιοχή της Noether και η ακέραια περιοχή $\mathbb{Z}[x]$ είναι επίσης περιοχή της Noether.

Πρόταση XIII.4.12. *Η ομομορφική εικόνα μίας περιοχής Noether είναι επίσης περιοχή Noether.*

Παράδειγμα XIII.4.13. Η απεικόνιση $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-5}]$ είναι επιμορφισμός δατυλίων. Αφού $\mathbb{Z}[x]$ περιοχή της Noether και η $\mathbb{Z}[\sqrt{-5}]$ είναι περιοχή της Noether και συνεπώς περιοχή ανάλυσης.

Πολύ πιο σπουδαίο είναι να έχουμε μονοσήμαντη (μονότροπη) ανάλυση.

Ορισμός XIII.4.14. Μια ακέραια περιοχή R λέγεται *περιοχή μονοσήμαντης ανάλυσης*, όταν

1. Κάθε $a \in R, a \neq 0, a \in E(R)$ αναλύεται σε γινόμενο αναγώγων στοιχείων και
2. Η ανάλυση αυτή είναι μονοσήμαντη (μονότροπη). Αυτό θα πει ότι δύο αναλύσεις της μορφής

$$a = \prod_{i=1}^{n} p_i = \prod_{i=1}^{n} (\epsilon_i p_i)$$

με $\epsilon_i \in E(R), \prod_{i=1}^{n} \epsilon_i = 1$ δεν θεωρούνται διαφορετικές, καθώς και ότι η σειρά των αναγώγων παραγόντων δεν λαμβάνεται υπόψη.

Αλλά πότε μια ακέραια περιοχή είναι περιοχή μονοσήμαντης ανάλυσης;

Θεώρημα XIII.4.15. *Υποθέτουμε ότι η ακέραια περιοχή είναι περιοχή ανάλυσης. Ισχύει η ισοδυναμία:*

(*Η R είναι περιοχή μονοσήμαντης ανάλυσης*) ⇔ (*Κάθε ανάγωγο στοιχείο του R είναι και πρώτο*)

Στο κύριο μέρος του βιβλίου θα αποδείξουμε ότι το σώμα $K = \mathbb{Q}(\sqrt{-5})$ έχει ως δακτύλιο των ακεραίων αλγεβρικών την ακεραία περιοχή $\mathbb{Z}[\sqrt{-5}]$ και έχει αριθμό κλάσεων 2. Συνεπώς η $\mathbb{Z}[\sqrt{-5}]$ είναι περιοχή ανάλυσης - αλλά όχι περιοχή μονοσήμαντης ανάλυσης.

Παρατήρηση XIII.4.16. Έχουμε αποδείξει ότι

$$(\mathbb{Z} \text{ Π.Κ.Ι}) \Longrightarrow (\mathbb{Z} \text{ Π.Μ.Α. }) \xRightarrow{\text{Θ. Βάσης Hilbert}} (\mathbb{Z}[x] \text{ Π. Μ. Α.})$$

Όμως δεν ισχύει, αν R περιοχή κυρίων ιδεωδών, τότε και ο $R[X]$ περιοχή κυριών ιδεώδων. Πράγματι, στον $\mathbb{Z}[x]$ το ιδεώδες $A = \langle 2, x \rangle$ δεν είναι κύριο ιδεώδες.

XIII.5 Η αριθμητική της περιοχής του Gauss

Αν $\alpha = x+iy$ οποιοσδήποτε μιγαδικός, ο *συζυγής* του θα είναι ο $\alpha' = x-iy$. Ορίζουμε την *norm* του α, $N(\alpha) = \alpha\cdot\alpha'$.

Ισχύουν:

(i) Η $N(\alpha)$ είναι μη-αρνητικός πραγματικός αριθμός.

(ii) $N(\alpha) = 0$, τότε και μόνο τότε όταν $\alpha = 0$.

(iii) Ισχύει $N(\alpha\beta) = N(\alpha)N(\beta)$, για κάθε $\alpha, \beta \in \mathbb{Z}[i]$.

(iv) Αν $\alpha \in \mathbb{Z}[i]$, τότε $N(\alpha) \in \mathbb{Z}$.

(v) Αν $\alpha \in \mathbb{Z}[i]$, τότε ο α είναι *μονάδα* του $\mathbb{Z}[i]$, αν και μόνο αν $N(\alpha) = 1$.

(vi) Η ομάδα των μονάδων του $\mathbb{Z}[i]$ είναι $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ (άσκηση).

Θα προσπαθήσουμε τώρα να κατασκευάσουμε μία θεωρία διαιρετότητας και μονοσήμαντης ανάλυσης στην περιοχή του Gauss εντελώς ανάλογης μ' εκείνη των ακεραίων.

Έστω $\alpha, \beta \in \mathbb{Z}[i]$. Θα λέμε ότι ο α *διαιρεί* τον β ($\alpha|\beta$) αν και μόνο αν υπάρχει $\gamma \in \mathbb{Z}[i]$ τέτοιος ώστε $\beta = \alpha\gamma$, αλλιώς θα λέμε ότι ο α δεν διαιρεί τον β ($\alpha \nmid \beta$) π.χ. $2+i|7+i$.

Το μέγεθος ενός ακεραίου του Gauss μετριέται μέσω της norm του. Το ανάλογο του αλγόριθμου της διαίρεσης με υπόλοιπο θα είναι:

Έστω $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Υπάρχουν $\gamma, \delta \in \mathbb{Z}[i]$ τέτοιοι ώστε

$$\alpha = \beta\gamma + \delta, \text{ και } 0 \leq N(\delta) < N(\beta).$$

Απόδειξη: Έχουμε $\alpha = a+bi$, $\beta = c+di$, όπου $a, b, c, d \in \mathbb{Z}$.

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di}\cdot\frac{c-di}{c-di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i = e+fi$$

όπου $e, f \in \mathbb{Q}$

$$e = \frac{ac+bd}{c^2+d^2},\ f = \frac{bc-ad}{c^2+d^2}.$$

Υπάρχουν $g, h \in \mathbb{Z}$ τέτοια ώστε $|g-e| \leq \frac{1}{2}$, $|h-f| \leq \frac{1}{2}$. Θέτουμε $\gamma = g+hi$ και βρίσκουμε

$$\frac{\alpha}{\beta} = \gamma + (e-g) + (f-h)i \Longrightarrow \alpha = \beta\gamma + \{(e-g)+(f-h)i\}\beta.$$

Έστω $\delta := \{(e-g)+(f-h)i\}\beta$. Τότε $\alpha = \beta\gamma + \delta$. Επειδή $\gamma \in \mathbb{Z}[i]$, έχουμε $\delta = \alpha - \beta\gamma \in \mathbb{Z}[i]$. Τώρα:

$$N(\delta) = N((e-g)+(f-h)i)N(\beta) = N(\beta)\cdot\{(e-g)^2+(f-h)^2\}$$

$$\leq N(\beta\{\frac{1}{4}+\frac{1}{4}\} = \frac{1}{2}N(\beta) < N(\beta)$$

διότι $N(\beta) \neq 0$ καθ' όσον $\beta \neq 0$. □

Ορίζουμε τώρα, εντελώς ανάλογα, τον μέγιστο κοινό διαιρέτη των ακεραίων του Gauss α και β ως εξής: $\gamma = (\alpha, \beta)$ αν και μόνο αν

- $\gamma|\alpha$ και $\gamma|\beta$
- Αν $\delta \in \mathbb{Z}[i]$, και $\delta|\alpha$, $\delta|\beta$, τότε $\delta|\gamma$.

Η διαφορά με τον μέγιστο κοινό διαιρέτη των ακεραίων είναι ότι ζητούμε ο μέγιστος κοινός διαιρέτης στο $\mathbb{Z}$ να είναι θετικός. Αυτό δεν μπορούμε να το κάνουμε στο $\mathbb{Z}[i]$ και αυτό έχει ως συνέπεια ο μέγιστος κοινός διαιρέτης στο $\mathbb{Z}[i]$ να *μην* είναι *μοναδικός*.

Δύο ακέραιοι του Gauss α, β, θα λέγονται *συνεταιρικοί*, αν και μόνο εάν υπάρχει $\varepsilon \in E(\mathbb{Z}[i])$ έτσι ώστε $\alpha = \varepsilon\beta$, δηλαδή ο α και β είναι συνεταιρικοί, συνεπώς αν και μόνο αν ο α είναι κάποιος από τους $\beta, -\beta, i\beta, -i\beta$.

Αν πάλι $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha\beta \neq 0$, τότε οποιοιδήποτε μέγιστοι κοινοί διαιρέτες των α, β είναι μεταξύ τους συνεταιρικοί.

Απόδειξη: Έστω $\alpha \neq 0$ και γ_1, γ_2 δύο μέγιστοι κοινοί διαιρέτες των α και β. Εξ ορισμού του μέγιστου κοινού διαιρέτη έχουμε

$$\gamma_1|\alpha,\ \gamma_1|\beta,\ \gamma_2|\alpha,\ \gamma_2|\beta$$

καθώς και $\gamma_1|\gamma_2,\ \gamma_2|\gamma_1$. Επειδή $\alpha \neq 0$, έχουμε

$$\gamma_1 \neq 0,\ \gamma_2 = \eta\gamma_1,\ \gamma_1 = \lambda\gamma_2,\ \eta, \lambda \in \mathbb{Z}[i].$$

Συνεπώς $\gamma_1 = \eta\lambda\gamma_1$, δηλαδή $\eta\lambda = 1 \Rightarrow \lambda = \dfrac{1}{\eta} \in \mathbb{Z}[i]$. Επομένως $\lambda, \eta, \in E(\mathbb{Z}[i])$, δηλαδή τα γ_1, γ_2 είναι συνεταιρικά. □

Στη συνέχεια θα αποδείξουμε την ύπαρξη του μέγιστου κοινού διαιρέτη.

Έστω $\alpha, \beta \in \mathbb{Z}[i],\ \alpha, \beta \neq 0$ και

$$S = \{\alpha\lambda + \beta\eta \mid \lambda, \eta \in \mathbb{Z}[i]\}.$$

Επειδή $\alpha = \alpha \cdot 1 + \beta \cdot 0$ και $\beta = \alpha \cdot 0 + \beta \cdot 1 \in S$, έπεται ότι το S περιέχει μη-μηδενικούς αριθμούς. Διαλέγουμε $\gamma \in S$ τέτοιο ώστε $N(\gamma)$ να είναι ο ελάχιστος φυσικός (γιατί μπορούμε να βρούμε τον γ;). Ισχυρίζομαι ότι ο γ είναι ένας μέγιστος κοινός διαιρέτης των α και β.

Πράγματι, το γεγονός ότι $\gamma \in S$, συνεπάγεται ότι υπάρχουν $\lambda_0, \nu_0 \in \mathbb{Z}[i]$ τέτοιοι ώστε $\gamma = \alpha\lambda_0 + \beta\nu_0$.

Αν λοιπόν $\delta|\alpha$ και $\delta|\beta$, έχουμε $\alpha = \delta\theta,\ \beta = \gamma\zeta$, οπότε $\gamma = \delta(\theta\lambda_0 + \zeta\nu_0)$, συνεπώς $\delta|\gamma$.

Θα δείξουμε τώρα ότι κάθε στοιχείο του S (και συνεπώς και τα α, β) είναι πολλαπλάσιο του γ.

Κατ' αρχήν παρατηρούμε ότι αν $\varepsilon, \rho \in S$ και $\theta \in \mathbb{Z}[i]$, τότε $\varepsilon - \theta\rho \in S$.

Πράγματι: Έστω $\varepsilon = \alpha\lambda_1 + \beta\nu_1,\ \rho = \alpha\lambda_2 + \beta\nu_2$. Τότε

$$\varepsilon - \theta\rho = \alpha(\lambda_1 - \theta\lambda_2) + \beta(\nu_1 - \theta\nu_2) \in S.$$

Έστω τώρα ω τυχαίο στοιχείο του S. Γράφουμε $\omega = \gamma\zeta + \rho$, $\zeta, \rho \in \mathbb{Z}[i]$, $0 \leq N(\rho) < N(\gamma)$. Επειδή ω και $\gamma \in S$, έπεται ότι $\omega - \gamma\zeta \in S$, δηλαδή $\rho \in S$ οπότε, λόγω της εκλογής του γ, $N(\rho) = 0$ συνεπώς $\rho = 0$. Άρα $\omega = \gamma\zeta$, το οποίο σημαίνει (εξ ορισμού) ότι $\gamma|\omega$.

Άμεση συνέπεια των παραπάνω είναι ότι αν $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha\beta \neq 0$ και γ ένας μέγιστος κοινός διαιρέτης των α και β, υπάρχουν ν και $\lambda \in \mathbb{Z}[i]$ τέτοιοι ώστε

$$\gamma = \alpha\nu + \beta\lambda.$$

Στη συνέχεια θα ορίσουμε *πρώτους* αριθμούς στην περιοχή του Gauss. Κατ' αρχάς παρατηρούμε ότι κάθε ακέραιος του Gauss γ διαιρείται από τις μονάδες $\pm 1, \pm i$ και τους συνεταιρικούς του $\pm\gamma, \pm i\gamma$.

- Ένας ακέραιος του Gauss π θα λέγεται *πρώτος*, αν και μόνο αν δεν είναι μονάδα και οι μόνοι διαιρέτες του είναι οι μονάδες του δακτυλίου $\mathbb{Z}[i]$ και οι συνεταιρικοί του π.
- Έστω π ακέραιος του Gauss τέτοιος ώστε $N(\pi) = p$, όπου p πρώτος αριθμός. Εύκολα διαπιστώνεται ότι ο π είναι *πρώτος*.

Πράγματι, έστω $\delta|\pi$. Τότε $\pi = \delta\gamma$, όπου $\gamma \in \mathbb{Z}[i]$. Συνεπώς

$$N(\pi) = N(\delta)N(\gamma) \Longrightarrow p = N(\delta)N(\gamma) \Longrightarrow N(\gamma) = 1, \text{ ή } N(\delta) = 1.$$

Επομένως γ ή δ είναι μονάδα, δηλαδή $\delta = \pm\pi, \pm i\pi, \pm 1, \pm i$.

Τώρα θα δείξουμε ότι:

Αν π πρώτος του $\mathbb{Z}[i]$ και α, β ακέραιοι του Gauss, τότε

$$(\pi|\alpha\beta \implies \pi|a \quad \text{είτε} \quad \pi|\beta).$$

Πράγματι, έστω ότι $\pi|\alpha\beta$, αλλά $\pi \nmid \beta$. Θα δείξουμε ότι $\pi|\alpha$. Οι μόνοι διαιρέτες του π είναι $\pm 1, \pm i, \pm\pi$ και $\pm i\pi$. Επειδή $\pi \nmid \beta$, έπεται ότι ένας μέγιστος κοινός διαιρέτης (π, β) είναι μία μονάδα του $\mathbb{Z}[i]$, δηλαδή ένας μέγιστος κοινός διαιρέτης $(\pi, \beta) = 1$, οπότε υπάρχουν $\nu, \lambda \in \mathbb{Z}[i]$ τέτοιοι ώστε $1 = \pi\nu + \beta\lambda$, δηλαδή $\alpha = \pi(\nu\alpha) + (\alpha\beta)\lambda$. Επειδή $\pi|\alpha\beta$, έπεται ότι $\pi|\alpha$. □

Ας προσπαθήσουμε τώρα να παραγοντοποιήσουμε ακεραίους του Gauss σε γινόμενο πρώτων. Όπως δεν παραγοντοποιούμε το $0, \pm 1$ στο $\mathbb{Z}$, έτσι δεν παραγοντοποιούμε $0, \pm 1, \pm i$ στον $\mathbb{Z}[i]$. Θα αποδείξουμε ότι

Κάθε ακέραιος του Gauss $\gamma \neq 0, \pm 1, \pm i$ αναλύεται σε γινόμενο πρώτων παραγόντων.

Πράγματι, θα το αποδείξουμε επαγωγικά ως προς την $N(\gamma)$. Προφανώς $N(\gamma) \geq 2$. Αν $N(\gamma) = 2$, τότε (σύμφωνα με την προηγούμενη παρατήρηση) ο γ είναι πρώτος.

Υποθέτουμε τώρα ότι $N(\gamma) > 2$ και ότι κάθε ακέραιος του Gauss που έχει norm μικρότερη της norm του γ, αναλύεται σε γινόμενο πρώτων παραγόντων. Αν ο γ είναι πρώτος, τελειώσαμε. Έστω ότι ο γ δεν είναι πρώτος. Τότε υπάρχουν $\alpha, \beta \in \mathbb{Z}[i]$ όχι μονάδες τέτοιοι ώστε $\gamma = \alpha\beta$. Τότε $1 < N(\alpha),\ N(\beta) < N(\gamma)$ και, λόγω της υπόθεσης της μαθηματικής επαγωγής,

$$\alpha = \pi_1\pi_2\cdots\pi_s, \quad \beta = \nu_1\nu_2\cdots\nu_t$$

όπου π_i, ν_j πρώτοι του $\mathbb{Z}[i]$. Συνεπώς

$$\gamma = \alpha\beta = \pi_1\pi_2\cdots\pi_s\nu_1\nu_2\cdots\pi_t.$$

□

Στη συνέχεια θα εξετάσουμε αν η ανάλυση αυτή είναι μονοσήμαντη (μοναδική). Βέβαια, αν έχουμε μία ανάλυση μπορούμε να βάλουμε μονάδες μέσα στο γινόμενο, αλλά αυτήν την ανάλυση δεν θα τη θεωρούμε διαφορετική. Επίσης, δεν ζητούμε η σειρά των πρώτων παραγόντων να είναι η ίδια. Θα αποδείξουμε λοιπόν ότι:

Έστω γ ακέραιος του Gauss διαφορετικός των $0, \pm 1, \pm i$.

Ο γ γράφεται ως γινόμενο πρώτων. Αν

$$\gamma = \pi_1\pi_2\cdots\pi_s = \nu_1\nu_2\cdots\nu_t$$

δύο αναλύσεις του γ σε γινόμενο πρώτων, τότε $s = t$ και, αλλάζοντας ίσως τη σειρά των $\nu_1, \nu_2, \cdots, \nu_s$, έχουμε π_1, ν_1 είναι συνεταιρικοί, π_2, ν_2 είναι συνεταιρικοί, $\cdots$, π_s, ν_s είναι συνεταιρικοί.

Απόδειξη: Επαγωγή ως προς την $N(\gamma)$. Έστω $\gamma \neq 0, \pm 1, \pm i$. Τότε $N(\gamma) \geq 2$. Αν $N(\gamma) = 2$, τότε ο γ είναι πρώτος, οπότε $\gamma = \pi_1 = \nu_1$, ισχύει. Υποθέτουμε ότι $N(\gamma) > 2$ και ότι η πρόταση είναι αληθής για όλους τους ακεραίους του Gauss με norm μικρότερη της $N(\gamma)$. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $s > 1$. Τότε $\pi_1|\pi_1\pi_2\cdots\pi_s \Rightarrow \pi_1|\nu_1\nu_2\cdots\nu_t$, δηλαδή $\pi_1|\nu_j$ για κάποιο j. Ας το ονομάσουμε αυτό ν_1, δηλαδή $\pi_1|\nu_1$. Επειδή ν_1 πρώτος συνεπάγεται ότι $\nu_1 = \pi_1\varepsilon$, ε μονάδα του $\mathbb{Z}[i]$, δηλαδή π_1, ν_1 είναι συνεταιρικά. Η σχέση $\gamma = \pi_1\pi_2\cdots\pi_s = \nu_1\nu_2\cdots\nu_t$ γράφεται

$$\pi_2\pi_3\cdots\pi_s = (\varepsilon\nu_2)\nu_3\cdots\nu_t.$$

Επειδή $N(\pi_1) \geq 2$ και $s > 1$ έπεται

$$1 < N(\pi_2\pi_3\cdots\pi_s) < N(\pi_1\pi_2\cdots\pi_s) = N(\gamma).$$

Λόγω της υπόθεσης της μαθηματικής επαγωγής έχουμε $s - 1 = t - 1$ και, αλλάζοντας ίσως τη θέση, $(\pi_2, \nu_2), \ldots, (\pi_s, \nu_s)$ συνεταιρικά. □

Θα δώσουμε τώρα μία καινούργια απόδειξη του προβλήματος, ποιοι φυσικοί μπορούν να γραφούν ως άθροισμα δύο τετραγώνων ακεραίων αριθμών.

Έστω $x^2 + y^2 = n$. Τότε $(x + iy)(x - iy) = n$, οπότε το πρόβλημα γίνεται:

Να βρεθούν όλοι οι ακέραιοι του Gauss με

$$N(x+iy) = x^2 + y^2 = n.$$

Για να λύσουμε αυτό το πρόβλημα θα πρέπει να περιγράψουμε επακριβώς όλους τους πρώτους του $\mathbb{Z}[i]$. Επειδή κάθε συνεταιρικός πρώτου είναι επίσης πρώτος, θα μελετήσουμε τους πρώτους κατά προσέγγιση συνεταιρικών.

Έστω π πρώτος του $\mathbb{Z}[i]$. Τότε υπάρχει *ακριβώς* ένας πρώτος του $\mathbb{Z}$, p τέτοιος ώστε $\pi|p$.

Απόδειξη: Έχουμε $N(\pi) \in \mathbb{Z}$ συνεπώς $N(\pi) = p_1 p_2 \cdots p_t$, $p_i \in \mathbb{Z}$, πρώτοι. Επειδή $N(\pi) = \pi\pi'$ έπεται $\pi|p_1 p_2 \cdots p_t$ δηλαδή $\pi|p_i$ για κάποιο i. Δεν μπορεί να διαιρεί κανέναν άλλο, διότι αν $\pi|p$ και $\pi|q$ με $p \neq q$, τότε $1 = px + qy$ συνεπώς $\pi|px + qy = 1$ επομένως $\pi\nu = 1$ άρα $\nu = \dfrac{1}{\pi}$ είναι ακέραιος του Gauss, που σημαίνει ότι ο π είναι μονάδα, άτοπο. □

Αρκεί λοιπόν να παραγοντοποιήσουμε όλους τους ακεραίους στον $\mathbb{Z}[i]$. Αν $p = 2$, τότε $2 = -i(1+i)^2$ και $1+i$ είναι πρώτος του $\mathbb{Z}[i]$, διότι $N(1+i) = 2$. Δηλαδή όλοι οι πρώτοι του $\mathbb{Z}[i]$, $\pi|2$ είναι συνεταιρικοί του $1+i$.
Έστω τώρα p περιττός πρώτος και έστω $\pi = x + iy|p$, δηλαδή ο p γράφεται $p = \pi\nu$, $\nu \in \mathbb{Z}[i]$. Επομένως

$$p^2 = N(p) = N(\pi)N(\nu) \Longrightarrow N(\pi) = p \quad \text{ή} \quad p^2.$$

Επειδή $x^2 + y^2 \equiv 0, 1, 2 \pmod{p}$, δεν μπορεί να ισχύει $x^2 + y^2 = p$ όταν $p \equiv 3 \pmod{4}$. Σ' αυτή την περίπτωση θα πρέπει να ισχύει $x^2 + y^2 = p^2$, επομένως

$$p^2 = N(p) = N(\pi)N(\nu) = p^2 N(\nu) \Longrightarrow N(\nu) = 1$$

δηλαδή ν μονάδα του $\mathbb{Z}[i]$. Επομένως, αν $p \equiv 3 \pmod{4}$, τότε π και p είναι συνεταιρικά.

Έστω τώρα $p \equiv 1 \pmod{4}$. Η ισοδυναμία $z^2 \equiv -1 \pmod{p}$ (1) έχει λύση. Έστω z_0 μία λύση της (1). Τότε

$$p|z_0^2 + 1 \Rightarrow \pi|z_0^2 + 1 \Rightarrow \pi|(z_0 - i)(z_0 + i) \Rightarrow \pi|z_0 - i \text{ ή } \pi|z_0 + i.$$

Σημειώνουμε τώρα ότι $p \nmid z - i$ και $p \nmid z + i$ διότι $\dfrac{1}{p}z \pm \dfrac{1}{p}i \notin \mathbb{Z}[i]$. Αυτό σημαίνει ότι στην περίπτωση $p \equiv 1 \pmod{4}$ οι π και p *δεν* είναι συνεταιρικοί. Επομένως $N(\pi) \neq N(p) = p^2$ δηλαδή $N(\pi) = p$ άρα $\pi\pi' = p$ και συνεπώς ο p διαιρείται από τους π και π'. Για να προσδιορίσουμε πλήρως όλους τους πρώτους του $\mathbb{Z}[i]$, θα πρέπει να δούμε πότε οι π και π' είναι συνεταιρικοί. Έστω λοιπόν $\pi = x + iy$ τέτοιος ώστε $N(\pi) = x^2 + y^2 = p$. Υποθέτουμε ότι π και π' είναι συνεταιρικά, δηλαδή $\pi = \varepsilon\pi'$, $\varepsilon = \pm 1, \pm i$, $\pi' = x - iy$.

Αν $\varepsilon = 1$, τότε $x + iy = x - iy$, δηλαδή $y = 0$ τότε $x^2 = p$, άτοπο. Όμοια αν $\varepsilon = -1$, $x = 0$ και $y^2 = p$, άτοπο.
Αν $\varepsilon = i$, τότε $x + iy = i(x - iy) = y + ix$, δηλαδή $x = y$ και $p = x^2 + x^2 = 2x^2$, άτοπο. Αν $\varepsilon = -i$, τότε $x = -y$ οπότε $2x^2 = p$, άτοπο.

Αποδείξαμε λοιπόν το εξής:

Θεώρημα XIII.5.1. *Έστω p πρώτος αριθμός. Η ανάλυση του p στην περιοχή του Gauss είναι:*

- *Αν $p = 2$, τότε $p = -i\pi^2$, όπου π πρώτος του $\mathbb{Z}[i]$ και $N(\pi) = 2$.*
- *Αν $p \equiv 3 \pmod{4}$, τότε $p = \pi$ είναι πρώτος και $N(\pi) = p^2$.*
- *Αν $p \equiv 1 \pmod{4}$, τότε $p = \pi\pi'$, όπου π και π' πρώτοι μη-συνεταιρικοί και $N(\pi) = N(\pi') = p$.*

Ξαναγυρίζουμε τώρα στο πρόβλημα του καθορισμού των θετικών ακεραίων αριθμών που είναι norm ακεραίων του δακτυλίου του Gauss. Έστω $\alpha \neq 0, \pm 1, \pm i$. Αναλύουμε τον α σε γινόμενο πρώτων στοιχείων του $\mathbb{Z}[i]$. Έστω $\alpha = \pi_1 \pi_2 \cdots \pi_s$, όπου π_i πρώτοι του $\mathbb{Z}[i]$. Τότε $N(\alpha) =$

$N(\pi_1)N(\pi_2)\cdots N(\pi_s)$. Υποθέτουμε ότι $\pi_i | p_i,\ i = 1, 2, \cdots, s,\ p_i$ πρώτος ακέραιος. Τότε $N(\alpha) = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, όπου

$$\left\{ \begin{array}{lllll} a_i = 2, & \text{αν} & p_i \equiv 3 & (\mathrm{mod}\ 4) & \\ a_i = 1, & \text{αν} & p_i = 2 & \text{ή} \quad p_i \equiv 1 & (\mathrm{mod}\ 4) \end{array} \right\}$$

Βλέπουμε λοιπόν ότι $N(\alpha) = m^2 q_1 q_2 \cdots q_t,\ m \in \mathbb{Z}$ και $q_1, q_2, \cdots, q_t$ πρώτοι αριθμοί διακεκριμένοι μεταξύ τους και ίσοι με 2 ή ισοδύναμοι με $1 \pmod 4$.

Ισχύει και το αντίστροφο, ότι δηλαδή κάθε τέτοιος φυσικός αριθμός γράφεται σαν άθροισμα δυο τετραγώνων. Εκμεταλλευόμενοι την αριθμητική της περιοχής του Gauss, δώσαμε επομένως μία απόδειξη του θεωρήματος:

Θεώρημα XIII.5.2. *Ένας θετικός ακέραιος n μπορεί να παρασταθεί ως άθροισμα δύο τετραγώνων αν και μόνο αν κάθε πρώτος παράγοντας p του n της μορφής $p \equiv 3 \mod 4$ εμφανίζεται στην ανάλυση του n σε γινόμενο πρώτων παραγόντων με άρτιο εκθέτη.*

XIII.6 Modules

XIII.6.1 Ορισμός και βασικές ιδιότητες

Η έννοια του module γενικεύει αυτή του K-διανυσματικού χώρου, όταν το σύνολο των scalars δεν είναι πλέον σώμα, αλλά ένας δακτύλιος R. Συμπεριλαμβάνει, όπως θα δούμε σε λίγο και τις αβελιανές ομάδες ως $\mathbb{Z}$-modules.

Όμως η έννοια εμφανίζεται για πρώτη φορά στην Αλγεβρική Θεωρία Αριθμών κατά τη μελέτη υποσυνόλων των δακτυλίων των αλγεβρικών αριθμών. Η σημασία της αναγνωρίστηκε στα τέλη της δεκαετίας του 1920 κυρίως λόγω των ερευνητικών αποτελεσμάτων της E. Noether, η οποία ήταν η πρώτη που αναγνώρισε τη σημασία της έννοιας ως γέφυρας σύνδεσης της θεωρίας αναπαραστάσεων πεπερασμένων ομάδων και της θεωρίας δομής των αλγεβρών.

Θα περιοριστούμε κατ' αρχή στην περίπτωση που ο δακτύλιος R είναι αντιμεταθετικός με μοναδιαίο και αργότερα σε περιοχές κυρίων ιδεωδών. Έστω λοιπόν R αντιμεταθετικός δακτύλιος με μοναδιαίο.

Ορισμός XIII.6.1. Ένα σύνολο $M, M \neq \varnothing$ θα λέγεται R-*module* όταν

1. Το σύνολο M είναι εφοδιασμένο με μία πράξη (πρόσθεση) και $(M, +)$ είναι αβελιανή ομάδα.
2. Ο R δρα στην ομάδα M,

$$\begin{aligned} R \times M &\longrightarrow M \\ (r, m) &\longmapsto r \cdot m \end{aligned}$$

και ισχύουν οι ακόλουθες ιδιότητες:

(α') $r(m_1 + m_2) = rm_1 + rm_2$ για κάθε $r \in R$ και κάθε $m_1, m_2 \in M$

(β') $(r_1 + r_2)m = rm_1 + rm_2$ για κάθε $r_1, r_2 \in R$ και $m \in M$

(γ') $(r_1 r_2)m = r_1(r_2 m)$ για κάθε $r_1, r_2 \in R$ και $m \in M$

(δ') $1 \cdot m = m$ για κάθε $m \in M$

Παράδειγμα XIII.6.2. 1. Κάθε K-διανυσματικός χώρος M είναι K-module.

2. Το σύνολο R^n $(n \geq 1)$ των n-άδων του R με πράξεις την πρόσθεση n-άδων και πολλαπλασιασμό κατά συνιστώσες είναι επίσης ένα R-module.

3. Κάθε ιδεώδες A του R, είναι R-module με πράξη

$$\begin{aligned} R \times A &\longrightarrow A \\ (r, a) &\longmapsto ra \end{aligned}$$

4. Αν A ιδεώδες του R, ο δακτύλιος πηλίκων R/A είναι επίσης ένα R-module με εξωτερική πράξη

$$\begin{aligned} R \times R/A &\longrightarrow R/A \\ (r, a + A) &\longmapsto ra + A \end{aligned}$$

5. Αν $(M, +)$ αβελιανή ομάδα, η δράση του $\mathbb{Z}$, $m \in M$

$$n \cdot m = \begin{cases} \underbrace{m + \cdots + m}_{n-\text{φορές}} & \text{αν } n > 0 \\ 0 & \text{αν } n = 0 \\ \underbrace{(-m) + \cdots + (-m)}_{n-\text{φορές}} & \text{αν } n < 0 \end{cases}$$

εφοδιάζει το M τη δομή ενός $\mathbb{Z}$-module.
Ισχύει και το αντίστροφο. Αν M ένα $\mathbb{Z}$-module, τότε αποδεικνύεται ότι η πράξη

$$\begin{aligned} \mathbb{Z} \times M &\longrightarrow M \\ (n, x) &\longmapsto mx \end{aligned}$$

ταυτίζεται με τη δράση του $\mathbb{Z}$ στην ομάδα $(M, +)$. Συνεπώς οι έννοιες $\mathbb{Z}$-module και αβελιανή ομάδα ταυτίζονται.

6. Ο $R[x]$ είναι επίσης R-module με τις συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού με το R.
7. Έστω K-διανυσματικός χώρος V και $T \in \mathrm{End}(V)$. Ο V γίνεται ένα $K[x]$-module με τη δράση

$$\begin{aligned} K[x] \times V &\longrightarrow V \\ (f(x), v) &\longmapsto f(x)v = f(T)v \end{aligned}$$

Η θεωρία των κανονικών μορφών Jordan προκύπτει από την ταξινόμηση των πρώτων ιδεωδών του δακτυλίου $K[x]$.

Ορισμός XIII.6.3. Έστω M ένα R-module. Ένας R-*γραμμικός συνδυασμός* των στοιχείων $m_1, \ldots, m_k$ του M είναι ένα στοιχείο της μορφής

$$r_1 m_1 + r_2 m_2 + \cdots + r_k m_k : r_i \in R.$$

Αν κάθε στοιχείο του M είναι ένας γραμμικός συνδυσμός των $m_1, m_2, \ldots, m_k$, τότε λέμε ότι το M παράγεται από το σύνολο $\{m_1, \ldots, m_k\}$ και το συμβολίζουμε με

$$M = \langle m_1, m_2, \ldots, m_k \rangle.$$

Ένα πεπερασμένα παραγόμενο ιδεώδες του R είναι ένας R-γραμμικός συνδυασμός ενός πεπερασμένου συνόλου στοιχείων του R.

Παράδειγμα XIII.6.4. Το ιδεώδες $A = \langle 1 + 2i \rangle$ του $\mathbb{Z}[i]$ είναι $\mathbb{Z}[i]$-module και $\mathbb{Z}$-module.
Ως $\mathbb{Z}[i]$-module παράγεται από το στοιχείο $1 + 2i$, $A = \mathbb{Z}[i](1 + 2i)$.
Ως $\mathbb{Z}$-module, το A παράγεται από τα στοιχεία $1 + 2i$ και $i(1 + 2i) = -2 + i$, δηλαδή

$$A = \langle 1 + 2i, -2 + i \rangle = \mathbb{Z}(1 + 2i) + \mathbb{Z}(-2 + i).$$

Ορισμός XIII.6.5. Ένα *παράγον σύνολο* ή *σύνολο γεννητόρων* ενός R-module M είναι ένα υποσύνολο $\{m_i\}_{i \in I}$ του M ώστε κάθε $m \in M$ είναι πεπερασμένος R-γραμμικός συνδυασμοός στοιχείων του $\{m_i\}_{i \in I}$,

$$m = \sum_{i \in I} r_i m_i,$$

και για όλα εκτός από πεπερασμένα r_i, $r_i = 0$.

Παράδειγμα XIII.6.6. Το R-module $R[x]$ έχει ως σύνολο γεννητόρων το άπειρο σύνολο $\{1, x, x^2, x^3, \ldots\}$. Ως $R[x]$-module το $R[x]$ παράγεται από το μοναδιαίο στοιχείο του R αφού:

$$f(x) = 1 \cdot f(x) \text{ για κάθε } f(x) \in R[x].$$

Ορισμός XIII.6.7. Όταν ένα R-module παράγεται μόνο από ένα στοιχείο λέγεται *κυκλικό* R-module.

Ορισμός XIII.6.8. Έστω M και N R-modules. Μία συνάρτηση $\phi : M \to N$ θα λέγεται R-*γραμμικός μετασχηματισμός* (από το M στο N), όταν

1. $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$ για όλα τα $m_1, m_2 \in R$ και
2. $\phi(rm) = r\phi(m)$ για όλα τα $r \in R$ και $m \in M$.

Παράδειγμα XIII.6.9. Έστω $\alpha \in \mathbb{Z}[\sqrt{2}]$. Ορίζουμε

$$\begin{aligned} m_\alpha : \mathbb{Z}[\sqrt{2}] &\longrightarrow \mathbb{Z}[\sqrt{2}] \\ x &\longmapsto m_\alpha(x) = \alpha x \end{aligned}$$

ο οποίος είναι ένας $\mathbb{Z}[\sqrt{2}]$-γραμμικός μετασχηματισμός του $\mathbb{Z}[\sqrt{2}]$.

Ορισμός XIII.6.10. Ένας *ισομορφισμός* των R-modules M και N είναι μία αμφιμονοσήμαντη R-γραμμική απεικόνιση $\phi : M \to N$. Αν υπάρχει μια τέτοια, τα M, N λέγονται ισόμορφα και το συμβολίζουμε με $M \cong N$.

Παράδειγμα XIII.6.11. Έστω $M = \mathbb{Z}[i]$ και $N = \mathbb{Z}[\sqrt{2}]$. Τα M, N έχουν και τη δομή δακτυλίου, και τη δομή $\mathbb{Z}$-module.

Ως δακτύλιοι δεν είναι ισόμορφοι, αφού δύο ισόμορφοι δακτύλιοι έχουν ισόμορφες ομάδες μονάδων, ενώ

$$E(\mathbb{Z}[i]) = \{\pm 1, \pm i\} \text{ και } E(\mathbb{Z}[\sqrt{2}]) = \langle \pm \rangle \times \langle 1 + \sqrt{2} \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \text{ άπειρη κυκλική ομάδα}$$

Ως $\mathbb{Z}$-modules όμως είναι και τα δύο ισόμορφα προς το $\mathbb{Z}^2$

$$\begin{aligned} \mathbb{Z}^2 &\longrightarrow \mathbb{Z}[i] & \qquad \mathbb{Z}^2 &\longrightarrow \mathbb{Z}[\sqrt{2}] \\ (a, b) &\longmapsto a + bi & \qquad (a, b) &\longmapsto a + b\sqrt{2} \end{aligned}$$

Ορισμός XIII.6.12. Έστω $\phi : M \to N$, R-γραμμικός μετασχηματισμός των R-modules M, N.

- Ο *πυρήνας* της ϕ, $\ker\phi = \{m \in M : \phi(m) = 0\}$ και
- *Η εικόνα* της ϕ, $\mathrm{Im}\phi = \{n \in N : \exists m \in M : \phi(m) = n\}$.

Ορισμός XIII.6.13. Έστω M ένα R-module και $\varnothing \neq N \subset M$. Το N θα λέγεται R-υποmodule του M όταν και το N είναι ένα R-module ως προς τους περιορισμούς των πράξεων του M. Το N είναι R-υποmodule ακριβώς τότε όταν

1. Αν $n_1, n_2 \in N \Rightarrow n_1 - n_2 \in N$ και
2. Αν $r \in R$ και $n \in N \Rightarrow rn \in N$.

Παράδειγμα XIII.6.14. Αν θεωρήσουμε τον R ως R-module, τότε τα R-υποmodule του R είναι ακριβώς τα ιδεώδη αυτού.

Παράδειγμα XIII.6.15. Ο δακτύλιος $\mathbb{Z}[i]$ είναι περιοχή κυρίων ιδεωδών, συνεπώς κάθε $\mathbb{Z}[i]$-υποmodule του είναι ένα ιδεώδες αυτού της μορφής $\mathbb{Z}[i]\alpha$, $\alpha \in \mathbb{Z}[i]$. Αλλά τα ιδεώδη του $\mathbb{Z}[i]$ είναι και $\mathbb{Z}$-υποmodules. Όμως *υπάρχουν και άλλα* $\mathbb{Z}$*-υποmodules πέραν των ιδεωδών*. Για παράδειγμα το $\mathbb{Z}[2i]$ είναι $\mathbb{Z}$-υποmodule του $\mathbb{Z}[i]$ αλλά δεν είναι ιδεώδες του $\mathbb{Z}[i]$ αφού $i(a+b2i) = -2b + ia \notin \mathbb{Z}[2i]$ για a περιττό.

Έστω τώρα ένα R-module M και ένα R-υποmodule αυτού N. Ως αβελιανές ομάδες ορίζουν την ομάδα πηλίκου M/N. Η αβελιανή ομάδα M/N γίνεται ένα R-module με πράξη

$$R \times M/N \longrightarrow M/N$$
$$(r, m + N) \longmapsto rm + N$$

Αυτός είναι ο ορισμός του R-*module πηλίκο* του M δια του N. Ανάλογα αν $B \subset A \subset R$ ιδεώδη του R, τα οποία τα θεωρούμε ως R-modules, δηλαδή το A είναι R-module και το B είναι R-υποmodule του A. Συνεπώς το A/B είναι R-module, το R-module πηλίκο του A δια του B. Αυτό είναι ένα ιδεώδες του R/B.

Αν $\phi : M \to N$ κάποιος R-γραμμικός μετασχηματισμός από R-modules, τότε ο πυρήνας $\ker\phi$ είναι R-υποmodule του M και η εικόνα επίσης. Ισχύει

$$\frac{M}{\ker\phi} \cong \mathrm{Im}\phi.$$

Ορισμός XIII.6.16. Έστω M_1, M_2 R-υποmodules του R-module M. Το R-module

$$M_1 + M_2 := \{m_1 + m_2 : m_1 \in M_1, m_2 \in M_2\}$$

λέγεται *άθροισμα* των R-υποmodules M_1 και M_2. Προφανώς και η τομή $M_1 \cap M_2$ δύο R-υποmodules είναι επίσης R-υποmodule του M.

Πρόταση XIII.6.17. *Έστω M_1 και M_2 δύο R-υποmodules του R-module M. Ισχύει $M_1 \cap M_2 = \{0\}$ αν και μόνο αν κάθε στοιχείο $z \in M_1 + M_2$ γράφεται μονοσήμαντα στη μορφή $z = m_1 + m_2$, $m_i \in M_i$ (άσκηση).*

Ορισμός XIII.6.18. Το άθροισμα $M_1 + M_2$ θα λέγεται *ευθύ* αν και μόνο αν κάθε στοιχείο $z \in M_1 + M_2$ γράφεται μονοσήμαντα στη μορφή $z = m_1 + m_2$, $m_i \in M_i$. Θα το συμβολίζουμε ως $M_1 \oplus M_2$.

Ορισμός XIII.6.19. Το R-υποmodule N του R-module M θα λέγεται *ευθύς προσθετέος* του M αν και μόνο αν υπάρχει R-υποmodule N′ του M για το οποίο ισχύει $M = N \oplus N'$. Το N′ θα λέγεται συμπλήρωμα του N.

Παρατήρηση XIII.6.20. Δεν είναι κάθε υποmodule ευθύς προσθετέος, αλλά και αν είναι ευθύς προσθετέος, το συμπλήρωμα δεν είναι κατ' ανάγκη μοναδικό.

Παράδειγμα XIII.6.21.

1. Το $\mathbb{Z}$ ως $\mathbb{Z}$-module. Έστω $m \in \mathbb{N}$. Το $\langle m\rangle = \mathbb{Z}m$ είναι ένα ιδεώδες του $\mathbb{Z}$, επομένως είναι ένα $\mathbb{Z}$-υποmodule του $\mathbb{Z}$. Το $m\mathbb{Z}$ δεν είναι ένας ευθύς προσθετέος, αφού ένα συμπλήρωμά του θα ήταν κατ' ανάγκη ένα ιδεώδες του $\mathbb{Z}$, δηλαδή ένα $\mathbb{Z}$-module της μορφής $\langle n\rangle = \mathbb{Z}n$. Άλλα αν $\mathbb{Z}m \oplus A = \mathbb{Z}$, τότε $A \cong \mathbb{Z}/m\mathbb{Z}$ πεπερασμένο σύνολο και είναι αδύνατο να είναι ισόμορφο με το $\langle n\rangle = \mathbb{Z}n$ που είναι άπειρο σύνολο.
2. Έστω ο $\mathbb{R}$-διανυσματικός χώρος $\mathbb{R}^2$ και L μια ευθεία που περνάει από την αρχή των αξόνων. Κάθε άλλη ευθεία που περνάει από την αρχή των αξόνων είναι ευθύ συμπλήρωμα της L.

XIII.6.2 Ελεύθερα modules

Έχουμε ήδη ορίσει την έννοια «παράγον σύνολο» ή σύνολο γεννητόρων ενός R-module. Στη συνέχεια θα ορίσουμε και τη γραμμική ανεξαρτησία.

Ορισμός XIII.6.22. Έστω M ένα R-module. Ένα υποσύνολο $B \subset M$ θα λέγεται R-*γραμμικά ανεξάρτητο* αν και μόνο αν για κάθε πεπερασμένο υποσύνολο $\{b_1, b_2, \ldots, b_k\}$ του B η σχέση

$$\sum_{i=1}^{k} r_i b_i = 0 \Rightarrow r_i = 0 \text{ για } i = 1, 2, \ldots, k.$$

Αλλιώς το σύνολο λέγεται γραμμικά εξαρτημένο.

Ορισμός XIII.6.23. Ένα R-module θα λέγεται *ελεύθερο* όταν έχει μία βάση B, δηλαδή υπάρχει ένα γραμμικά ανεξάρτητο υποσύνολο $B \subset M$ το οποίο είναι παράγον σύνολο του M.

Παράδειγμα XIII.6.24.
1. Το R-module R^n είναι ελεύθερο. Μια βάση αυτού είναι το σύνολο $B = \{e_1, e_2, \dots, e_n\}$, $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ όπου η μονάδα είναι στην i-θέση.
2. Το R-module $R[x]$ είναι ελεύθερο. Μια βάση αυτού είναι το σύνολο $B = \{x^n : n \in \mathbb{N}\}$.
3. Το ευθύ άθροισμα από ελεύθερα R-modules είναι επίσης ελεύθερο.
4. Το ιδεώδες $P = \langle 2, 1 + \sqrt{-5} \rangle$ του $\mathbb{Z}[\sqrt{-5}]$ μπορεί να θεωρηθεί ως $\mathbb{Z}[\sqrt{-5}]$-module και ως $\mathbb{Z}$-module. Το σύνολο $\{2, 1 + \sqrt{-5}\}$ είναι γραμμικά εξαρτημένο ως προς τον $\mathbb{Z}[\sqrt{-5}]$, αφού ισχύει
$$r_1 2 + r_2(1 + \sqrt{-5}) = 0$$
με $r_1 = 1 + \sqrt{-5}$ και $r_2 = -2$. Ως προς τον $\mathbb{Z}$ όμως είναι γραμμικά ανεξάρτητο και μάλιστα ελεύθερο $\mathbb{Z}$-module, αφού το παραπάνω σύνολο είναι και βάση του P.

Παρατήρηση XIII.6.25. Ενώ η έννοια του ελεύθερου R-module μοιάζει με αυτή του K-διανυσματικού χώρου, χρειάζεται προσοχή γιατί υπάρχουν και σημαντικές διαφορές.

Από τη γραμμική άλγεβρα τα παρακάτω είναι γνωστά:
1. Κάθε K-διανυσμάτικός χώρος V είναι ένα ελεύθερο K-module.
2. Αν $X \subset V$, K-γραμμικά ανεξάρτητο, τότε αυτό επεκτείνεται σε μία βάση του V.
3. Αν X παράγον σύνολο του V, $V = \langle X \rangle$, τότε υπάρχει $B \subset X$ το οποίο είναι βάση του V.

Οι ιδιότητες αυτές δεν ισχύουν για οποιοδήποτε R-module.

Αντιπαραδείγματα XIII.6.26.
1. Κάθε πεπερασμένη αβελιανή ομάδα δεν είναι ελεύθερο $\mathbb{Z}$-module. (Άσκηση)
2. Ελεύθερο R-module στο οποίο ένα γραμμικά ανεξάρτητο υποσύνολο δεν επεκτείνεται σε βάση.
   Έστω το $\mathbb{Z}$-module $M = \mathbb{Z}$. Αυτό είναι ελεύθερο $\mathbb{Z}$-module με βάση το $\{1\}$. Θεωρούμε το σύνολο $\{2\}$. Είναι $\mathbb{Z}$-γραμμικά ανεξάρτητο, αφού αν $m2 = 0$, τότε το $m = 0$. Το $\{2\}$ δεν παράγει το $\mathbb{Z}$, αφού $2\mathbb{Z} \subsetneq \mathbb{Z}$. Αν υποθέσουμε ότι επεκτείνεται σε κάποια βάση, δηλαδή ότι υπάρχει βάση B τέτοια ώστε $2 \in B$, τότε το B θα περιέχει ένα τουλάχιστον ακόμη στοιχείο $b \in \mathbb{Z}$ με $b \neq 2$. Τότε όμως το $\{2, b\} \subset B$ και είναι $\mathbb{Z}$ εξαρτημένο, αφού $2b - 2b = 0$, άτοπο.
3. Ελεύθερο R-module M για το οποίο υπάρχει $X \subset M$, $M = \langle X \rangle$ αλλά δεν περιέχει βάση. Θεωρούμε και πάλι το $\mathbb{Z}$-module $M = \mathbb{Z}$ και $X = \{m, n\}$ $m \neq \pm 1, n \neq \pm 1$ και $(m, n) = 1$ για παράδειγμα $X = \{2, 3\}$. Υπάρχουν $a, b \in \mathbb{Z}$ ώστε $1 = am + bn$ οπότε για κάθε $x \in \mathbb{Z}$, $x = x1 = xam + xbn$, συνεπώς
$$\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}.$$
   Το X δεν είναι $\mathbb{Z}$-γραμμικά ανεξάρτητο αφού $mn - nm = 0$. Συνεπώς δεν είναι $\mathbb{Z}$-βάση του $M = \mathbb{Z}$. Είναι φανερό ότι $m\mathbb{Z} \subsetneq \mathbb{Z}$ και $n\mathbb{Z} \subsetneq Z$. Επομένως το X δεν περιέχει βάση του $\mathbb{Z}$-module $\mathbb{Z}$.

Πρόταση XIII.6.27. *Έστω M ένα ελεύθερο R-module, $R \neq \{0\}$. Υποθέτουμε ότι το M έχει μια πεπερασμένη βάση με n-στοιχεία. Τότε οποιαδήποτε άλλη βάση έχει επίσης n-στοιχεία.*

Απόδειξη. Αφού R αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο περιέχει μέγιστα ιδεώδη [20, Θεωρ. 9.7]. Έστω m ένα από αυτά. Έστω A ένα ιδεώδες του R. Το σύνολο AM είναι το υπομodule του R-module M που παράγεται από το σύνολο $\{am | a \in A, m \in M\}$. Το module πηλίκο M/AM γίνεται R/A-module με πράξη
$$R/A \times M/AM \longrightarrow M/AM$$
$$(r + A, m + AM) \longmapsto (r + A)(m + AM) = rm + AM.$$

Επομένως το $M/\mathfrak{m}M$ είνα ένα $R/\mathfrak{m}R$-module. Το $\mathfrak{m}$ είναι maximal, άρα το $R/\mathfrak{m}$ είναι σώμα. Συνεπώς το $M/\mathfrak{m}M$ είναι ένας $R/\mathfrak{m}$-διανυσματικός χώρος.

Αν $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ μια βάση του M, τότε το σύνολο $\{\alpha_1 + \mathfrak{m}M, \alpha_2 + \mathfrak{m}M, \ldots, \alpha_n + \mathfrak{m}M\}$ είναι μια βάση του διανυσματικού χώρου $M/\mathfrak{m}M$ (άσκηση). Όλες οι βάσεις ενός διανυσματικού χώρου έχουν το ίδιο πλήθος στοιχείων, συνεπώς το ίδιο ισχύει και για το M. □

Είμαστε πλέον σε θέση να δώσουμε τον ακόλουθο:

Ορισμός XIII.6.28. Έστω M κάποιο ελεύθερο R-module $R \neq \{0\}$. Ο πληθάριθμος μια πεπερασμένης βάσης του λέγεται *βαθμός (rank)* του M.

Τώρα αν το M είναι ελεύθερο R-module και N ένα R-υποmodule αυτού, είναι και αυτό ελεύθερο; Η απάντηση γενικά είναι όχι.

Παράδειγμα XIII.6.29. Το ιδεώδες $A = \langle x, y\rangle$ του δακτυλίου $K[x, y]$, όπου K σώμα δεν είναι ως $K[X, Y]$-module ελεύθερο (γιατί;).

Χάθηκε λοιπόν μια καταπληκτική ιδιότητα των διανυσματικών χώρων πεπερασμένης διάστασης. Μπορούμε να την ξανακερδίσουμε; Ναι, αν περιορίσουμε την κλάση των δακτυλίων R.

Πρόταση XIII.6.30. *Ένα R-module M είναι ελεύθερο R-module αν και μόνο αν $M \cong \bigoplus_{t\in I} R_t$, όπου $R_t = R$ για κάθε $t \in I$.*

Απόδειξη. "⇒" Έστω $\{e_i : i \in I\}$ μια βάση του M. Η απεικόνιση

$$M \ni m = \sum_{i\in I} r_i e_i \to (r_i)_{i\in I} \in \bigoplus_{t\in I} R_t$$

είναι R-ισομορφισμός. Στο $\sum_{i\in I} r_i e_i$ όλα εκτός από πεπερασμένα r_i είναι 0.

"⇐" Αν $M \cong \bigoplus_{t\in I} R_t$, το $\bigoplus_{t\in I} R_t$ ειναι ελεύθερο R-module συνεπώς και το M. □

Πόρισμα XIII.6.31. *Κάθε R-module είναι ομομορφική εικόνα ενός ελεύθερου R-module.*

Απόδειξη. Αν I ένα σύνολο γεννητόρων του M, για παράδειγμα $I = M$, τότε η απεικόνιση

$$\bigoplus_{t\in I} R_t \longrightarrow M$$
$$(r_t)_{t\in I} \longmapsto \sum r_t t \in M$$

είναι επιμορφισμός από R-modules. □

XIII.6.3 R-modules με R περιοχή κυρίων ιδεωδών

Στην παράγραφο αυτή θα περιγράψουμε εν συντομία τα αποτελέσματα.

Ορισμός XIII.6.32. Έστω M ένα R-module (εδώ αρκεί ο R να είναι ακεραία περιοχή). Ένα στοιχείο $m \in M$ για το οποίο υπάρχει $r \in R, r \neq 0$ τέτοιο ώστε $rm = 0$ θα λέγεται *στοιχείο στρέψης* του M.

Πρόταση XIII.6.33. *Έστω M ένα R-module, R ακέραια περιοχή. Το σύνολο*

$$T = \{m \in M : m \text{ στοιχείο στρέψης του } M\} \text{ αποτελεί ένα } R - \text{υποmodule του } M.$$

Σημείωση XIII.6.34. Η έννοια στρέψης (torsion) προέρχεται από την αλγεβρική τοπολογία.

Αν $T = \{0\}$, τότε το M λέγεται *ελεύθερο στρέψης (torsion free)*. Αν το $T = M$, τότε το M λέγεται *module στρέψης*.

Για παράδειγμα είναι κάθε ελεύθερο R-module ελεύθερο στρέψης και κάθε πεπερασμένη αβελιανή ομάδα είναι ως $\mathbb{Z}$-module ένα module στρέψης.

Από εδώ και κάτω υποθέτουμε ότι ο R είναι περιοχή κυρίων ιδεωδών.

Θεώρημα XIII.6.35. *Έστω M ένα ελεύθερο R-module βαθμού (rank) n. Κάθε R-υποmodule του M είναι πεπερασμένα παραγόμενο R-module με το πολύ n-γεννήτορες.*

Θεώρημα XIII.6.36. *Κάθε υποmodule ενός ελεύθερου R-module M βαθμου n είναι ελεύθερο R-module βαθμού $\leq n$.*

Παρατήρηση XIII.6.37.

1. Αν ο R δεν είναι περιοχή κυρίων ιδεωδών, τότε είτε δεν είναι ακέραια περιοχή είτε έχει μη-κύριο ιδεώδες. Αν δεν είναι ακέραια περιοχή, τότε έχουμε $xy = 0$ με $x \in R\backslash\{0\}$ και $y \in R\backslash\{0\}$. Αυτό σημαίνει ότι το ιδεώδες Rx του R δεν είναι ελεύθερο R-module.

   Αν πάλι έχει ένα μη κύριο ιδεώδες, τότε αυτό δεν είναι ελεύθερο R-module.
2. Το θεώρημα ισχύει γενικότερα. Κάθε υποmodule ενός ελεύθερου R-module, όπου R περιοχή κυρίων ιδεωδών, είναι επίσης ελεύθερο.
3. Ο όρος «ελεύθερο» στο «ελεύθερο στρέψης» και «ελεύθερο» module έχει διαφορετική σημασία. Ένα «ελεύθερο στρέψης» module σημαίνει ότι δεν έχει, μη-μηδενικά στοιχεία στρέψης, ενώ «ελεύθερο module» σημαίνει ότι έχει μια βάση.

Από το θεώρημα XIII.6.36 προκύπτει το

Πόρισμα XIII.6.38. *Κάθε πεπερασμένα παραγόμενο ελεύθερο στρέψης R-module με R περιοχή κυρίων ιδεωδών είναι ένα ελεύθερο R-module πεπερασμένης τάξης.*

Παρατήρηση XIII.6.39. Το πόρισμα είναι λάθος χωρίς την υπόθεση του πεπερασμένα παραγόμενου. Πράγματι το σώμα των ρητών είναι μια αβελιανή ομάδα ($\mathbb{Z}$-module), αλλά όχι πεπερασμένα παραγόμενο $\mathbb{Z}$-module και δεν έχει βάση, δηλαδή δεν είναι ελεύθερο $\mathbb{Z}$-module.

Πόρισμα XIII.6.40. *Αν έχουμε ένα πύργο $M_3 \subset M_2 \subset M_1$ από R-modules και $M_1 \cong R^n$ και $M_3 \cong R^n$, τότε και $M_2 \cong R^n$.*

Σημείωση XIII.6.41. Και αυτό δεν ισχύει, αν ο R δεν είναι περιοχή κυρίων ιδεωδών.

Θεώρημα XIII.6.42. *Αν M πεπερασμένα παραγόμενο R-module, τότε*

$$M = M_t \oplus M_f$$

όπου το M_t είναι το υποmodule στρέψεως του M και το M_f είναι ένα ελεύθερο R-module πεπερασμένου βαθμού.

Παρατήρηση XIII.6.43. Αν $\operatorname{rank} M_f = r$, τότε $M = M_t \oplus R^r$. Ιδιαίτερα αν A πεπερασμένα παραγόμενη αβελιανή ομάδα, τότε

$$A = A_t \oplus \mathbb{Z}^r.$$

Εννοείται ότι από το θεμελιώδες θεώρημα των πεπερασμένων (προσθετικών) ομάδων η A_t είναι ένα ευθύ άθροισμα p-ομάδων.

Τέλος αναφέρουμε το θεώρημα των στοιχειωδών διαιρετών (Elementarteilersatz)

Θεώρημα XIII.6.44. *Έστω* F *ένα ελεύθερο* R*-module πεπερασμένου βαθμού* n *και ένα* R*-υποmodule* M *του* F.

1. *Τότε και το* M *είναι ένα ελεύθερο* R*-module βαθμού* $d \leq n$.
2. *Υπάρχουν στοιχεία* $x_1, x_2, \ldots, x_d \in M$ *και* $\epsilon_1, \epsilon_2 \ldots, \epsilon_d \in R\backslash\{0\}$ *τέτοια ώστε*
   (α') *Το συνολο* $\{\epsilon_1 x_1, \epsilon_2 x_2, \ldots, \epsilon_d x_d\}$ *είναι βάση του* R*-module* M.
   (β') $\epsilon_i \mid \epsilon_{i+1}$ *για* $1 \leq i < d$.

Τα στοιχεία $\epsilon_1, \epsilon_2, \ldots, \epsilon_d$ *είναι modulo συνεταιρικά μονοσήματα καθορισμένα από το* M*, ανεξάρτητα της επιλογής των* $x_1, x_2, \ldots, x_d$ *και λέγονται στοιχειώδεις διαιρέτες του* $M \subset F$.

Παρατήρηση XIII.6.45. Το Θεώρημα αυτό έχει αποδειχθεί εν μέρει στο κύριο μέρος του βιβλίου στη σελίδα 54.

XIII.7 Απόλυτες τιμές σε σώματα αριθμών

Ορισμός XIII.7.1. Μία *απόλυτη τιμή* $\|\cdot\|_K$ σε ένα σώμα K είναι μία συνάρτηση

$$\begin{aligned} K &\to \mathbb{R}^+, \\ x &\mapsto \|x\|_K \end{aligned}$$

έτσι ώστε

1. $\|x\|_K \geq 0$,
2. $x = 0 \Leftrightarrow \|x\|_K = 0$,
3. $\|x + y\|_K \leq \|x\|_K + \|y\|_K$

Αν επιπλέον ισχύει $\|x \cdot y\|_K = \|x\|_K \cdot \|y\|_K$, τότε η απόλυτη τιμή λέγεται *πολλαπλασιαστική*.

Ορισμός XIII.7.2. Μία ακολουθία $(a_n)_{n\in\mathbb{N}}$ θα λέγεται *ακολουθία Cauchy*, αν και μόνο αν

$$\text{για κάθε } \epsilon > 0, \text{ υπάρχει } n_0 \in \mathbb{N}, \text{ ώστε } n, m \geq n_0 \Rightarrow \|a_n - a_m\|_K < \epsilon.$$

Ορισμός XIII.7.3. Μία ακολουθία $(a_n)_{n\in\mathbb{N}}$ θα λέγεται *συγκλίνουσα* στο K, αν υπάρχει $\ell \in K$ ώστε

$$\text{για κάθε } \epsilon > 0, \text{ υπάρχει } n_0 \in \mathbb{N}, \text{ ώστε } n \geq n_0 \Rightarrow \|a_n - \ell\|_K < \epsilon.$$

Όπως και στις ακολουθίες στο σώμα $\mathbb{R}$, εφοδιασμένο με τη συνηθισμένη μετρική, μπορούμε να αποδείξουμε ότι κάθε συγκλίνουσα ακολουθία είναι Cauchy.

Το αντίστροφο δεν συμβαίνει πάντα, για παράδειγμα στο σώμα των ρητών αριθμών εφοδιασμένο με τη συνηθισμένη μετρική, η ακολουθία των δεκαδικών προσεγγίσεων του $\sqrt{2}$ είναι Cauchy χωρίς να είναι συγκλίνουσα.

Ορισμός XIII.7.4. Ένα σώμα K θα λέγεται *πλήρες* ως προς μία απόλυτη τιμή, αν και μόνο αν κάθε ακολουθία Cauchy είναι συγκλίνουσα.

Παράδειγμα XIII.7.5. Το $\mathbb{R}$ εφοδιασμένο με τη συνηθισμένη απόλυτη τιμή είναι πλήρες. Το $\mathbb{C}$ εφοδιασμένο με τη συνηθισμένη απόλυτη τιμή είναι πλήρες. Το $\mathbb{Q}$ εφοδιασμένο με τη συνηθισμένη μετρική δεν είναι πλήρες.

Μπορούμε να αποδείξουμε ότι για κάθε σώμα K εφοδιασμένο με μία απόλυτη τιμή μπορεί να οριστεί μια επέκταση του $\widetilde{K}$ με μια απολυτή τιμή, η οποία είναι επέκταση της αρχικής, και το $\widetilde{K}$ να είναι πλήρες. Η κατασκευή η οποία έχει αρκετές τεχνικές λεπτομέρειες γίνεται ως εξής: Θεωρούμε το σύνολο των ακολουθιών Cauchy του K το οποίο το μετατρέπουμε σε δακτύλιο

με πράξεις τις συνηθισμένες πράξεις πρόσθεσης και πολλ/σμού ακολουθιών. Μπορούμε να αποδείξουμε ότι οι ακολουθίες που συγκλίνουν στο μηδέν αποτελούν ένα μέγιστο ιδεώδες του παραπάνω αυτού δακτυλίου, οπότε ορίζουμε ως πλήρωση του K ως προς τη μετρική $\|\cdot\|$ το σώμα

$$\widetilde{K} := \frac{\text{ακολουθίες Cauchy με στοιχεία από το } K}{\text{ακολουθίες που συγκλίνουν στο } 0}.$$

Για όλες τις τεχνικές λεπτομέρειες της κατασκευής αυτής παραπέμπουμε στις διδακτικές σημειώσεις του προπτυχιακού μαθήματος [18].

Το σώμα K μπορούμε να το θεωρήσουμε ως υπόσωμα του $\widetilde{K}$ με τη βοήθεια του μονομορφισμού:

$$K \hookrightarrow \widetilde{K}$$
$$x \mapsto (a_n), a_n = x, \text{ σταθερή ακολουθία}$$

Ορισμός XIII.7.6. Θα λέμε ότι δύο απόλυτες τιμές $\|\cdot\|_1, \|\cdot\|_2$ του σώματος K είναι *ισοδύναμες* αν και μόνο αν υπάρχουν θετικοί πραγματικοί αριθμοί c_1, c_2 ώστε για κάθε $x \in K$

$$c_1\|x\|_1 \leq \|x\|_2 \leq c_2\|x\|_2.$$

Είναι σαφές ότι ισοδύναμες μετρικές επάγουν την ίδια τοπολογία στο K.

Άσκηση: Αποδείξτε ότι αν οι μετρικές $\|\cdot\|_1, \|\cdot\|_2$ είναι ισοδύναμες και (a_n) είναι ακολουθία στοιχείων του K, τότε $a_n \xrightarrow{\|\cdot\|_1} \ell$ αν και μόνο αν $a_n \xrightarrow{\|\cdot\|_2} \ell$.

Παράδειγμα XIII.7.7. Θεωρούμε το σώμα των ρητών αριθμών $\mathbb{Q}$. Το σώμα αυτό είναι εφοδιασμένο με τη γνωστή απόλυτη τιμή $|\cdot|$ την οποία θα τη συμβολίζουμε με $\|\cdot\|_\infty$. Αν πληρώσουμε το $\mathbb{Q}$ με την απόλυτη τιμή $\|\cdot\|_\infty$, τότε καταλήγουμε στο σώμα των πραγματικών αριθμών.

Μπορούμε όμως να ορίσουμε και άλλες απόλυτες τιμές στο σώμα των ρητών αριθμών τις p-*αδικές*, όπου p-πρώτος. Είναι σαφές ότι κάθε ακέραιος αριθμός x μπορεί να γραφεί στη μορφή

$$x = p^{\nu_p(x)}a, (a, p) = 1$$

όπου το $\nu_p(x) \in \mathbb{Z}$ είναι ο μη αρνητικός αριθμός που εκφράζει τη δύναμη με την οποία βρίσκεται ο πρώτος αριθμός p στην ανάλυση του x σε πρώτους παράγοντες.

Ορίζουμε λοιπόν ότι

$$\|x\|_p = \left(\frac{1}{p}\right)^{\nu_p(x)},$$

και έχουμε μία συνάρτηση από το $\mathbb{Z} \to \mathbb{R}$.

Τη συνάρτηση αυτή μπορούμε να την επεκτείνουμε σε μία συνάρτηση

$$\|\cdot\|_p : \mathbb{Q} \to \mathbb{R},$$

ορίζοντας ως

$$\|\frac{a}{b}\|_p = \frac{\|a\|_p}{\|b\|_p}.$$

Μπορούμε να δούμε ότι η παραπάνω συνάρτηση ορίζει όντως μια απόλυτη τιμή στο $\mathbb{Q}$ (άσκηση). Είναι σημαντικό να παρατηρήσουμε ότι αντί της τριγωνικής ανισότητας ισχύει η πιο ισχυρή ανιστότητα

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

Μία μετρική που ικανοποιεί την παραπάνω ανισότητα θα λέγεται *ultrametric*.

Παρατήρηση XIII.7.8. Οι απόλυτες τιμές $\|\cdot\|_\infty, \|\cdot\|_p$ είναι μη ισοδύναμες, όπως και η $\|\cdot\|_p$ δεν είναι ισοδύναμη με την $\|\cdot\|_q$ για $p \neq q$. Πράγματι η ακολουθία p^n έχει όριο

$$\lim_{n\to\infty} p^n = \begin{cases} +\infty & \text{στην } \|\cdot\|_\infty \\ 1 & \text{στην } \|\cdot\|_q,\ p \neq q \\ 0 & \text{στην } \|\cdot\|_p. \end{cases}$$

Παρατήρηση XIII.7.9. Βασικό ρόλο στην ανάπτυξη της *αριθμητικής αλγεβρικής γεωμετρίας* έπαιξαν οι αναλογίες ανάμεσα στα *αλγεβρικά σώματα αριθμών* και στα *αλγεβρικά σώματα συναρτήσεων μιάς μεταβλητής*. Τα πρώτα ορίζονται ως αλγεβρικές, πεπερασμένες επεκτάσεις του $\mathbb{Q}$, ενώ τα δεύτερα ως αλγεβρικές, πεπερασμένες επεκτάσεις του σώματος $k(x)$. Το ανάλογο σώμα του $\mathbb{Q}$ στα σώματα συναρτήσεων είναι το σώμα $k(x)$ των ρητών συναρτήσεων. Αν $k = \mathbb{C}$, τότε το σώμα $\mathbb{C}(x)$ αποτελεί το σώμα των μερόμορφων συναρτήσεων της απλούστερης συμπαγούς επιφάνειας Riemann, της προβολικής ευθείας $\mathbb{P}^1(\mathbb{C})$. Τα σώματα συναρτήσεων επιπλέον, στην περίπτωση που το k είναι το σώμα $\mathbb{C}$ των μιγαδικών αριθμών, είναι σε ένα προς ένα αντιστοιχία με τα σώματα μερομόρφων συναρτήσεων από συμπαγείς επιφάνειες Riemann [21]. Η θεώρηση αυτή μας έδωσε αρκετά γεωμετρικά και αναλυτικά εργαλεία για τη μελέτη τόσο των σωμάτων συναρτήσεων όσο και των αλγεβρικών σωμάτων αριθμών.

Η αναλογία αυτή είναι αρκετά βαθιά και σχεδόν κάθε θεώρημα που αφορά σώματα συναρτήσεων μπορεί να μεταφερθεί στην περίπτωση των σωμάτων αριθμών και αντιστρόφως. Στην κατεύθυνση αυτή αξίζει να αναφέρουμε ότι η υπόθεση του Riemann σχετικά με τις ρίζες της ζ-συνάρτησης του Riemann έχει αποδειχθεί [16] για σώματα συναρτήσεων, όταν $K = \mathbb{F}_{p^n}$, ενώ μια απόδειξη για σώματα αριθμών δεν είναι ακόμα διαθέσιμη. Είναι χαρακτηριστικό ότι αρκετές από τις προσπάθειες για την απόδειξη της εικασίας του Riemann για σώματα αριθμών κάνουν χρήση της αναλογίας αυτής. [6]

Ας θεωρήσουμε ένα πεπερασμένο σημείο στην $\mathbb{P}^1(\mathbb{C})$ το $a \in \mathbb{C}$. Κάθε *ρητή συνάρτηση* $f \in \mathbb{C}(x)$ μπορεί να γραφτεί ως

$$f(x) = (x - a)^{\nu_a(f)} p(x),$$

όπου $\nu_a(f) \in \mathbb{Z}$, $p(x) \neq 0$, και $p(x)$ είναι ρητή συνάρτηση καλά ορισμένη στο a, δηλαδή το a δεν αποτελεί πόλο της p. Αν το $\nu_a(f) \geq 0$, τότε το $\nu_a(f)$ ονομάζεται *τάξη της ρίζας της* f *στο* a, ενώ αν το $\nu_a(f) < 0$, τότε το $\nu_a(f)$ ονομάζεται *τάξη του πόλου της* f *στο* a. Έστω $0 < c < 1$. Τότε έχουμε ότι

$$\|\cdot\|_{a,c}(f) = c^{\nu_a(f)} : \mathbb{C}(x) \to \mathbb{R}^+$$

είναι μία μετρική στο $\mathbb{C}(x)$.

Άσκηση: Αποδείξτε τον παραπάνω ισχυρισμό. Τι θα συμβεί αν θεωρήσουμε το σώμα $k(x)$ των ρητών συναρτήσεων υπεράνω ενός τυχαίου σώματος;

Άσκηση: Δείξτε ότι για $0 < c_1, c_2 < 1$ οι μετρικές $\|\cdot\|_{c_1,a}, \|\cdot\|_{c_2,a}$ είναι ισοδύναμες, ενώ για $a \neq b$ οι μετρικές $\|\cdot\|_{c,a}, \|\cdot\|_{c',b}$ δεν είναι ισοδύναμες.

Άσκηση: Έστω μια ρητή συνάρτηση f/g, όπου $f(x), g(x) \in k(x)$. Δείξτε ότι για $0 < c < 1$ η συνάρτηση

$$\|\cdot\|_{\infty,c} : k(x) \to \mathbb{R}^+,$$

που ορίζεται ως

$$\|f/g\|_{\infty,c} = c^{\deg(f)-\deg(g)}$$

είναι μία μετρική. Δείξτε ότι διαφορετικά c οδηγούν σε ισοδύναμες μετρικές. Δείξτε ότι καμία μετρική $\|\cdot\|_{\infty,c}$ δεν είναι ισοδύναμη με την $\|\cdot\|_{a,c'}$.

Άσκηση: Δείξτε ότι το σύνολο των κλάσεων ισοδυναμίας μετρικών στο $k(x)$ είναι σε ένα προς ένα αντιστοιχία με τα σημεία του $\mathbb{P}^1(k)$.

Παρατήρηση XIII.7.10. Ισχύει ότι για $x \in \mathbb{Q}$

$$\|x\|_\infty \cdot \prod_p \|x\|_p = 1.$$

Ο τύπος αυτός αντιστοιχεί στο γνωστό θεώρημα για *συμπαγείς επιφάνειες Riemann*: *μία μερόμορφη συνάρτηση σε συμπαγή επιφάνεια Riemann έχει, μετρημένης της πολλαπλότητας, τόσες ρίζες όσες και πόλους.*

Παρατήρηση XIII.7.11. Το λεγόμενο *θεώρημα του Ostrowski* εξασφαλίζει ότι οι $\|\cdot\|_\infty$, $\|\cdot\|_p$ είναι όλες οι δυνατές μή ισοδύναμες απόλυτες τιμές που μπορούμε να έχουμε στο σώμα των ρητών αριθμών.

Τα σώματα $\mathbb{Q}$ και $k(x)$ με τις παραπάνω μετρικές δεν είναι πλήρη. Μπορούμε να σχηματισούμε τις πληρώσεις τους. Η πλήρωση του $\mathbb{Q}$ ως προς τη συνηθισμένη μετρική οδηγεί στο σώμα των πραγματικών αριθμών $\mathbb{R}$, το οποίο δεν είναι αλγεβρικά κλειστό. Η αλγεβρική κλειστότητα του $\mathbb{C}$ είναι το σώμα των μιγαδικών αριθμών, το οποίο είναι αλγεβρικά κλειστό και πλήρες.

Αν θεωρήσουμε την πλήρωση του $\mathbb{Q}$ ως προς μία από τις μετρικές $\|\cdot\|_p$ σχηματίζουμε το *σώμα των* p*-αδικών αριθμών* $\mathbb{Q}_p$, το οποίο είναι πλήρες αλλά όχι αλγεβρικά κλειστό. Η αλγεβρική κλειστότητά του είναι αλγεβρικά κλειστό αλλά όχι πλήρες, σε αντίθεση με πριν. Αν σχηματίσουμε την πλήρωση της αλγεβρικής κλειστότητας του $\mathbb{Q}_p$ καταλήγουμε στο σώμα $\mathbb{C}_p$, το οποίο είναι και αλγεβρικά κλειστό και πλήρες.

Έστω $a \in k$. Αν θεωρήσουμε την πλήρωση του $k(x)$ ως προς το $\|\cdot\|_a$ σχηματίζουμε τον χώρο των *τυπικών δυναμοσειρών* $k\langle x\rangle$, που περιέχει τυπικά αθροίσματα της μορφής $\sum_{i=0}^{\infty} a_i(x-a)^i$.

XIII.8 Κλειστές Μπάλες

Θεωρούμε έναν δακτύλιο R, εφοδιασμένο με μία απόλυτη τιμή $\|\cdot\|$, και έστω το σύνολο των διατεταγμένων n-άδων $R^n = \{(a_1, \ldots, a_n),\ a_i \in R\}$, εφοδιασμένο με την απόλυτη τιμή

$$\|(a_1, \ldots, a_i)\| = \max_i \|a_i\|_R.$$

Ορίζουμε την *κλειστή μπάλα* με κέντρο a και ακτίνα $\epsilon \in \mathbb{R}^+$

$$B_{R^n}(a, \epsilon) = \{x \in R^n : \|x - a\| \leq \epsilon\}.$$

Παρατήρηση XIII.8.1. Μία από τις πολλές ιδιαιτερότητες των ultrametric μετρικών είναι ότι η κλειστή μπάλα $B_{R^n}(a, \epsilon)$ είναι τοπολογικά ανοιχτή. Πράγματι, έστω $y \in R^n$ που να ανήκει στο σύνορο της $B_{R^n}(a, \epsilon)$, δηλαδή $\|y - a\| = \epsilon$. Θα δείξουμε ότι υπάρχει ανοιχτή μπάλα κέντρου y που να ανήκει εξολοκλήρου στην $B_{R^n}(a, \epsilon)$.

Θεωρούμε το σύνολο των σημείων $b \in R^n$, ώστε $\|y - b\|_R < \epsilon/2$. Παρατηρούμε ότι

$$\|b - a\| = \|(y - b) + (a - y)\| \leq \max\{\|y - b\|, \|a - y\|\} = \max\{\epsilon/2, \epsilon\} = \epsilon,$$

δηλαδή το ζητούμενο!

Ένα από τα πολλά προβλήματα που έχουν οι χώροι R^n είναι ότι απέχουν πολύ από το να είναι συνεκτικοί.

Ορισμός XIII.8.2. Ένας τοπολογικός χώρος θα λέγεται *πλήρως μη-συνεκτικός (totally disconnected)* αν και μόνο αν οι συνεκτικές συνιστώσες του είναι τα σημεία.

Οι χώροι R^n εφοδιασμένοι με την τοπολογία των ultrametric απόλυτων τιμών είναι πλήρως μη-συνεκτικοί χώροι.

XIII.8.1 Δακτύλιοι Εκτίμησης

Ορισμός XIII.8.3. Θα λέμε ότι μία ακεραία περιοχή R είναι *δακτύλιος εκτίμησης* του σώματος $K = Quot(R)$, αν και μόνο αν για κάθε $x \in K$ ισχύει $x \in R$ ή $x^{-1} \in R$.

Άσκηση Αποδείξτε ότι κάθε δακτύλιος εκτίμησης είναι *τοπικός*, δηλαδή έχει μοναδικό μέγιστο ιδεώδες.

Παρατηρούμε ότι σε ένα πλήρες ultametric σώμα η κλειστή μπάλα

$$R := B_K(0,1) = \{x \in K : \|x\|_K \leq 1\}$$

αποτελεί δακτύλιο εκτίμησης, και ότι το μέγιστο ιδεώδες είναι το

$$p_R := \{x \in K : \|x\|_K < 1\}.$$

XIII.8.2 Άπειρες επεκτάσεις Galois

Έστω K σώμα και N/K μια επέκταση του Galois, δηλαδή N/K αλγεβρική, κανονική και διαχωρίσιμη. Η ομάδα Galois της N/K

$$G := \mathrm{Gal}(N/K) = \{\sigma \in \mathrm{Aut}(N) : \sigma|_K = \mathrm{Id}_K\}.$$

Έστω $\{N : K\}$ ο σύνδεσμος των ενδιαμέσων σωμάτων L, $K \subset L \subset N$ και $\{G : 1\}$ ο σύνδεσμος των υποομάδων της G, $H \leq G$.

Είναι σε όλους γνωστό ότι αν N/K είναι πεπερασμένη, ισχύει το

Θεώρημα XIII.8.4 (Θεμελιώδες θεώρημα της Θεωρίας του Galois)**.**

1. $[N : K] = \#\mathrm{Gal}(N/K)$
2. *Οι απεικονίσεις*
$$\{N : K\} \underset{\Psi}{\overset{\Phi}{\leftrightarrows}} \{G : 1\}$$
με
$$\Phi(L) = \{\sigma \in \mathrm{Gal}(N/K) : \sigma|_L = \mathrm{Id}_L\} = \mathrm{Gal}(N/L)$$
$$\Psi(H) = \{x \in N : Hx = x\} = N^H,$$
όπου $K \subset L \subset N$ *και* $H \leq \mathrm{Gal}(N/K)$*, είναι ένας αντι-ισομορφισμός συνδέσμων.*
3. *Αν* $L \in \{N : K\}$ *και* $\Phi(L) = \mathrm{Gal}(N/L)$*, τότε η* L/K *είναι Galois, αν και μόνο αν* $\mathrm{Gal}(N/L) \lhd \mathrm{Gal}(N/K) = G$ *και σε αυτή την περίπτωση ισχύει*
$$\mathrm{Gal}(L/K) \cong \frac{\mathrm{Gal}(N/K)}{\mathrm{Gal}(N/L)}.$$

Υποθέτουμε τώρα ότι η N/K δεν είναι πεπερασμένη. Οι Φ και Ψ ορίζονται όπως παραπάνω και αποτελούν και πάλι αντι-μορφισμό συνδέσμων.

Ισχύει, ότι $\Psi \circ \Phi = \mathrm{Id}_{N:K}$, κάτι το οποίο σημαίνει ότι η Φ είναι 1-1 και η Ψ είναι επί. Όμως στις άπειρες επεκτάσεις δεν είναι εν γένει αντι-ισομορφισμοί. Είναι δυνατόν διαφορετικές υποομάδες της $\mathrm{Gal}(N/K)$ να έχουν το ίδιο σώμα σταθερών στοιχείων.

Αντιπαράδειγμα:

Έστω $K = \mathbb{F}_p$, p πρώτος αριθμός και έστω $\ell \neq 2$, επίσης πρώτος αριθμός. Θεωρούμε τον πύργο σωμάτων

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots$$

όπου K_i η μοναδική επέκταση του K βαθμού $[K_i : K] = \ell^i$ και $N = \cup_{i=1}^{\infty} K_i$. Το N είναι η αλγεβρική θήκη του σώματος K. Είναι φανερό ότι

$$K_i = \{x \in N : x^{p^{\ell^i}} - x = 0\}.$$

Έστω $G = \mathrm{Gal}(N/K)$ και Frob_p ο K αυτομορφισμός του Frobenious

$$\begin{aligned}\mathrm{Frob}_p : N &\longrightarrow N\\ x &\longmapsto x^p \text{ για κάθε } x \in N.\end{aligned}$$

Θεωρούμε την ομάδα

$$H = \langle \mathrm{Frob}_p \rangle = \{\mathrm{Frob}_p^n : n \in \mathbb{Z}\} < G.$$

Αποδεικνύεται ότι οι H και G έχουν το ίδιο σώμα σταθερών στοιχείων, δηλαδή $\psi(G) = \psi(H)$, δηλαδή η ψ δεν είναι 1-1.

Το κενό αυτό κάλυψε ο Krull έναν αιώνα αργότερα (το 1928) από το θεώρημα του Galois ορίζοντας μια τοπολογία στην ομάδα $\mathrm{Gal}(N/K)$.

Ορισμός XIII.8.5. (Τοπολογία του Krull) Έστω K ένα σώμα και $\overline{K}$ η διαχωρίσιμη θήκη του K, $G = \mathrm{Gal}(\overline{K}/K)$, των K-αυτομορφισμών του σώματος K και $\sigma \in G$. Μία βάση ανοιχτών περιοχών του σ ορίζεται το σύνολο

$$\mathcal{B}_\sigma = \left\{ \sigma\mathrm{Gal}(\overline{K}/L) : \begin{array}{l}\text{όπου } L \text{ διατρέχει τα ενδιάμεσα σώματα } K \subset L \subset \overline{K}\\ \text{για τα οποία η } L/K \text{ είναι πεπερασμένη και Galois.}\end{array} \right\}$$

Παρατήρηση XIII.8.6. Αν N/K είναι πεπερασμένη επέκταση Galois, τότε η τοπολογία του Krull είναι η Διακεκριμένη (discrete) τοπολογία, δηλαδή όλα τα υποσύνολα της $\mathrm{Gal}(N/K)$ είναι ανοιχτά.

Η ομάδα Galois $\mathrm{Gal}(\overline{K}/K)$ είναι μια τοπολογική ομάδα η οποία είναι Hausdorff, συμπαγής και *πλήρως μη συνεκτική*.

Οι ανοιχτές υποομάδες της $\mathrm{Gal}(\overline{K}/K)$ είναι ακριβώς οι υποομάδες $\mathrm{Gal}(\overline{K}/L)$, όπου L/K πεπερασμένη υποεπέκταση της $\overline{K}/K$. Οι κλειστές υποομάδες είναι τομές ανοιχτών υποομάδων.

Θεώρημα XIII.8.7 (του Krull)**.** *Έστω K ένα σώμα και $\overline{K}$ η διαχωρίσιμη θήκη αυτού. Έστω $G := \mathrm{Gal}(\overline{K}/K)$ και $\{\overline{K} : K\}$ ο σύνδεσμος των ενδιάμεσων σωμάτων $K \subset L \subset \overline{K}$ και $\{G : 1\}$ ο σύνδεσμος των κλειστών υποομάδων της G. Για κάθε $L \in \{N : K\}$ ορίζουμε*

$$\Phi(L) = \{\sigma \in G : \sigma|_L = \mathrm{Id}_L\} = \mathrm{Gal}(\overline{K}/K).$$

Η Φ είναι ένας αντι-ισομορφισμός των συνδέσμων $\{N : K\}$ και $\{G : 1\}$. Επιπρόσθετα, $L \in \{N : K\}$ είναι επέκταση Galois υπεράνω του K αν και μόνο αν $\Phi(L) \lhd G$ και σε αυτή την περίπτωση

$$\mathrm{Gal}(L/K) \cong \frac{G}{\Phi(L)}.$$

Απόδειξη. [17, σελ. 10]

□

XIII.8.3 Προβολικό (αντίστροφο) όριο

Η έννοια του προβολικού ορίου γενικεύει την έννοια της τομής μιας οικογένειας συνόλων. Αν $(X_i)_{i\in I}$ είναι μια οικογένεια υποσυνόλων ενός τοπολογικού X η οποία για οποιαδήποτε στοιχεία X_i, X_j της οικογένειας περιέχεται σ' αυτήν και η τομή τους, τότε το προβολικό όριο της οικογένειας ορίζεται ως

$$\varprojlim_{i\in I} = \bigcap_{i\in I} X_i.$$

Ορίζουμε $i < j$ τότε και μόνο τότε, αν $X_j \subset X_i$. Τότε το σύνολο δεικτών I γίνεται *κατευθυνόμενο (directed)*. Αυτό σημαίνει ότι το I έχει μια σχέση μερικής διάταξης $\leq$ για την οποία ισχύει επιπλέον:

- Αν i, j οποιαδήποτε στοιχεία του I, υπάρχει $k \in I$ τέτοια ώστε $i \leq k$ και $j \leq k$. Ο δείκτης k αντιστοιχεί στο $X_k = X_i \cap X_j$. Αν $i \leq j$ θα συμβολίζουμε τη σχέση του περιέχεσθαι $X_j \hookrightarrow X_i$ με τη συνάρτηση ϕ_{ij}.

Κατ' αυτό τον τρόπο λαμβάνουμε ένα σύστημα $\{X_i, \phi_{ij}\}$ συνόλων και απεικονίσεων.

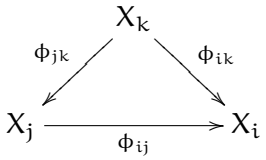
Ορισμός XIII.8.8. Αν I είναι ένα μερικά διατεταγμένο σύνολο δεικτών το οποίο είναι κατευθυνόμενο. Ένα *προβολικό σύστημα* υπέρ το I είναι μια οικογένεια

$$\{(X_i, \phi_{ij}) : i, j \in I, i \leq j\}$$

τοπολογικών χώρων X_i και συνεχών συναρτήσεων $\phi_{ij} : X_j \to X_i$ τέτοια ώστε

(i) Αν $i = j$ η $\phi_{ii} = \mathrm{Id}_{X_i}$.

(ii) Αν $i \leq j \leq k$, τότε $\phi_{ik} = \phi_{ij} \circ \phi_{jk}$ και το ακόλουθο διάγραμμα



είναι αντιμεταθετικό.

Ορισμός XIII.8.9. Το *προβολικό όριο* ενός προβολικού συστήματος $\{(X_i, \phi_{ij}) : i, j \in I, i \leq j\}$ ορίζεται ως το υποσύνολο του ευθέως γινομένου $\prod_{i\in I} X_i$:

$$\varprojlim_{i\in I} X_i = \left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i : \phi_{ij}(x_j) = x_i \text{ για } i \leq j \right\}.$$

Παρατήρηση XIII.8.10. Αν οι τοπολογικοί χώροι X_i είναι Hausdorff, ως γνωστό και το ευθύ γινόμενο $\prod_{i\in I} X_i$ είναι Hausdorff. Στην περίπτωση αυτή το προβολικό όριο $\varprojlim_{i\in I} X_i$ είναι κλειστός υπόχωρος του $\prod_{i\in I} X_i$.

Τώρα, αν (G_i, ϕ_{ij}) είναι ένα προβολικό σύστημα *τοπολογικών ομάδων* (ομάδων οι οποίες είναι και τοπολογικοί χώροι στους οποίους η συνάρτηση πολλαπλασιασμού

$$\begin{aligned} G \times G &\longrightarrow G \\ (x, y) &\longrightarrow xy \end{aligned}$$

και η συνάρτηση αντίστροφο στοιχείο

$$\begin{aligned} G &\longrightarrow G \\ x &\longmapsto x^{-1} \end{aligned}$$

είναι συνεχείς), τότε και το προβολικό όριο $G := \varprojlim_{i\in I} G_i$ είναι επίσης τοπολογική ομάδα.

Ορισμός XIII.8.11. Μια *προπεπερασμένη ομάδα (profinite group)* είναι μια τοπολογική ομάδα η οποία είναι υλοποιήσιμη ως το προβολικό όριο πεπερασμένων τοπολογικών ομάδων.

Θεώρημα XIII.8.12. *Αν G προπεπερασμένη ομάδα και το N διατρέχει όλες τις ανοιχτές, κανονικές υποομάδες της G, τότε η*

$$G \cong \varprojlim_{N} G/N$$

αλγεβρικά και τοπολογικά, [17].

Στη συνέχεια θα αναφερθούμε σε μερικά παραδείγματα προπεπερασμένων ομάδων ιδιαίτερα σημαντικών για τη Θεωρία Αριθμών.

Παράδειγμα XIII.8.13. Έστω K σώμα και $\overline{K}$ μια διαχωρίσιμη θήκη του K. Η απόλυτη ομάδα Galois $\mathrm{Gal}(\overline{K}/K)$, η οποία είναι τοπολογική ομάδα ως προς την *τοπολογία του Krull*, είναι μια προπεπερασμένη ομάδα.

Όταν το L διατρέχει όλες τις πεπερασμένες κανονικές υποεπεκτάσεις της $\overline{K}/K$, τότε οι ομάδες $\mathrm{Gal}(\overline{K}/L)$ διατρέχουν τις ανοιχτές, κανονικές υποομάδες της ομάδας $\mathrm{Gal}(\overline{K}/K)$, σύμφωνα με τον ορισμό της τοπολογίας του Krull.

Επομένως,

$$G_K = \lim_{\substack{\leftarrow \\ L}} \mathrm{Gal}(\overline{K}/L),$$

όπου $K \leq L \leq \overline{K}$ και L/K πεπερασμένη Galois επέκταση.

Αφού $\mathrm{Gal}(\overline{K}/L) \lhd \mathrm{Gal}(\overline{K}/K)$, έπεται ότι η επέκταση L/K είναι πεπερασμένη Galois επέκταση και

$$\mathrm{Gal}(L/K) \cong \frac{\mathrm{Gal}(\overline{K}/K)}{\mathrm{Gal}(\overline{K}/L)}.$$

Σημείωση XIII.8.14. Ιδιαίτερα σημαντική είναι η περίπτωση $K = \mathbb{Q}$ και $\overline{K} = \overline{\mathbb{Q}}$, η αλγεβρική θήκη του $\mathbb{Q}$.

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \cong \lim_{\substack{\leftarrow \\ K}} \mathrm{Gal}(K/\mathbb{Q}),$$

όπου $\mathbb{Q} \leq K \leq \overline{Q}$ και $K/\mathbb{Q}$ πεπερασμένη Galois επέκταση.

Παράδειγμα XIII.8.15. Έστω p ένας πρώτος αριθμός. Για κάθε φυσικό αριθμό n ορίζουμε $G_n := \mathbb{Z}/p^n\mathbb{Z}$. Αν $n \geq m$, τότε $p^m \mid p^n$ και συνεπώς μπορούμε να ορίσουμε τις απεικονίσεις

$$\begin{aligned} \phi_{m,n} : \quad \mathbb{Z}/p^n\mathbb{Z} &\longrightarrow \mathbb{Z}/p^m\mathbb{Z} \\ a \mod p^n &\longmapsto a \mod p^m \end{aligned}$$

Η οικογένεια $\{(G_n, \phi_{m,n}) : m \leq n\}$ αποτελεί ένα προβολικό όριο που ορίζεται

$$\lim_{\substack{\leftarrow \\ n\in\mathbb{N}}} \frac{\mathbb{Z}}{p^n\mathbb{Z}} = \mathbb{Z}_p$$

όπου $\mathbb{Z}_p$ είναι ο δακτύλιος των p-αδικών ακεραίων.

Παράδειγμα XIII.8.16. Οι δακτύλιοι $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$ αποτελούν ένα προβολικό σύστημα ως προς τις προβολές

$$\phi_{n,m} : \frac{\mathbb{Z}}{m\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}},$$

με $n \mid m$, όπου η διάταξη στο $\mathbb{N}$ δίνεται μέσω της διαιρετότητας, δηλαδή $n \leq m \Leftrightarrow n \mid m$. Το αντίστροφο όριο είναι ο λεγόμενος *δακτύλιος του Prüfer*.

Και αυτός είναι σημαντικός για τη θεωρία αριθμών. Αν $n = \prod_{p\in\mathbb{P}} p^{\nu_p}$, όπου $\nu_p \geq 0$ και για σχεδόν όλους τους πρώτους $\nu_p = 0$. Απο το κινέζικο θεώρημα, έπεται ότι ισχύει ο ισομορφισμός

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \prod_{p\in\mathbb{P}} \frac{\mathbb{Z}}{p^{\nu_n}\mathbb{Z}}.$$

Επίσης γνωρίζουμε ότι το προβολικό όριο σέβεται το ευθύ γινόμενο. Επομένως,

$$\lim_{\substack{\leftarrow \\ n\in\mathbb{N}}} \mathbb{Z}/n\mathbb{Z} \cong \lim_{\substack{\leftarrow \\ \nu_p}} \left(\prod_{p\in\mathbb{P}} \frac{\mathbb{Z}}{p^{\nu_p}\mathbb{Z}} \right) \cong \prod_{p\in\mathbb{P}} \left(\lim_{\substack{\leftarrow \\ \nu_p\in\mathbb{N}}} \frac{\mathbb{Z}}{p^{\nu_p}\mathbb{Z}} \right) \cong \prod_{p\in\mathbb{P}} \mathbb{Z}_p,$$

το ευθύ γινόμενο όλων των δακτυλίων των p-αδικών ακεραίων, για κάθε πρώτο p.

Παρατήρηση XIII.8.17. Η οικογένεια $(R_i, \phi_{ij}), i, j \in I\ i \leq j$ είναι ένα προβολικό σύστημα δακτυλίων R_i με μοναδιαίο 1_i και ϕ_{ij} ομομορφισμούς δακτυλίων

$$\phi_{ij} : R_j \longrightarrow R_i,$$

τέτοιοι ώστε $\phi_{ij}(1_j) = 1_i$. Τότε το προβολικό όριο

$$R := \varprojlim_{i \in I} R_i,$$

είναι επίσης δακτύλιος με μοναδιαίο. Ιδιαίτερα ισχύει

$$E(R) = \varprojlim_{i \in I} E(R_i).$$

Παράδειγμα XIII.8.18. Αν $G_n = E(\mathbb{Z}/n\mathbb{Z})$, τότε

$$E(\widehat{\mathbb{Z}}) = \varprojlim_{n \in \mathbb{Z}} E(\mathbb{Z}/n\mathbb{Z})$$

καθώς και

$$E(\mathbb{Z}_p) = \varprojlim_{n \in \mathbb{N}} E(\mathbb{Z}/p^n\mathbb{Z}).$$

Επειδή η ομάδα $E(\mathbb{Z}/p^n\mathbb{Z})$ είναι αβελιανή τάξης $\phi(p^n) = p^{n-1}(p-1)$, έπεται ότι

$$E(\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

Επομένως

$$\begin{aligned}
\mathbb{Z}_p^* &= \varprojlim_{n \in \mathbb{N}} \left(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}\right) \\
&\cong \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/(p-1)\mathbb{Z} \times \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^{n-1}\mathbb{Z} \\
&\cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.
\end{aligned}$$

Παράδειγμα XIII.8.19. Έστω $\mathbb{F}_q$ το πεπερασμένο σώμα με q στοιχεία. Γνωρίζουμε ότι για κάθε $n \in \mathbb{N}$ η επέκταση $\mathbb{F}_{q^n}/\mathbb{F}_q$ είναι κυκλική επέκταση Galois βαθμού n και ότι η κυκλική ομάδα Galois παράγεται από τον αυτομορφισμό του Frobenius

$$\begin{aligned}
\mathrm{Frob}_q : \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n} \\
x &\longmapsto x^q
\end{aligned}$$

Επομένως

$$\begin{aligned}
\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) &\cong \mathbb{Z}/n\mathbb{Z} \\
\mathrm{Frob}_q &\longmapsto 1 \mod n\mathbb{Z}
\end{aligned}$$

Συνεπώς

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \varprojlim_{n \in \mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z} \cong \widehat{\mathbb{Z}}.$$

Ο ισομορφισμός

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$$

στέλνει τον αυτομορφισμό του Frobenius $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ στο $1 \in \widehat{\mathbb{Z}}$ και την υποομάδα

$$\langle \mathrm{Frob}_q \rangle = \{\mathrm{Frob}_q^n : n \in \mathbb{Z}\} \cong \mathbb{Z} \leq \widehat{\mathbb{Z}}$$

στην πυκνή αλλά όχι κλειστή υποομάδα $\mathbb{Z}$ της $\widehat{\mathbb{Z}}$. Μπορεί κανείς να διαπιστώσει ότι υπάρχει $\psi \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ τέτοιο ώστε $\psi \notin \langle \mathrm{Frob}_q \rangle$ και ότι το θεμελιώδες θεώρημα της θεωρίας του Galois δεν ισχύει για άπειρες επεκτάσεις, κάτι που το κάλυψε η τοπολογία του Krull, εκατό χρόνια αργότερα (1928) από το θεώρημα του Galois.

Παράδειγμα XIII.8.20. Θεωρούμε την επέκταση $\mathbb{Q}^{ab}/\mathbb{Q}$, όπου $\mathbb{Q}^{ab}$ η *maximal αβελιανή επέκταση του* $\mathbb{Q}$. Γνωρίζουμε από το θεώρημα των Kronecker-Weber ότι

$$\mathbb{Q}^{ab} = \mathbb{Q}(\{\zeta_n | n \in \mathbb{N}\}).$$

Το σώμα $\mathbb{Q}(\{\zeta_n | n \in \mathbb{N}\})$ είναι το σώμα ανάλυσης όλων των διαχωρίσιμων πολυωνύμων

$$\{x^n - 1 : n \in \mathbb{N}\}$$

υπεράνω του $\mathbb{Q}$.

Συνεπώς η $\overline{\mathbb{Q}}/\mathbb{Q}$ είναι Galois. Για κάθε $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$, αν γνωρίζουμε την τιμή $\sigma(\zeta_n)$ για κάθε n, τότε ο σ καθορίζεται πλήρως από την $\mathbb{Q}^{ab}$. Για σταθερό $n \in \mathbb{N}$, γνωρίζουμε ότι

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong E(\mathbb{Z}/n\mathbb{Z}).$$

Επομένως

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}} E(\mathbb{Z}/n\mathbb{Z}) \cong E(\widehat{\mathbb{Z}}).$$

XIII.9 Ασκήσεις

1. Δείξτε ότι σε μία ακέραια περιόχη
   (α′) Το x είναι μονάδα αν και μόνο αν $x \mid 1$.
   (β′) Θα λέμε ότι τα x, y είναι συνεταιρικά και θα το συμβολίζουμε με $x \cong y$ αν υπάρχει μονάδα u, ώστε $x = uy$. Δείξτε ότι κάθε δύο μονάδες είναι συνεταιρικές και κάθε στοιχείο συνεταιρικό με μονάδα είναι και αυτό μονάδα.
   (γ′) Δείξτε ότι $x \cong y$ αν και μόνο αν $x \mid y$ και $y \mid x$.
   (δ′) Θα λέμε ότι το x είναι ανάγωγο αν $x = ab$, τότε a ή b είναι μονάδα. Δείξτε ότι κάθε συνεταιρικό ανάγωγου είναι ανάγωγο.
2. Έστω R μια ακέραια περιοχή και x, y μη μηδενικά στοιχεία του R. Δείξτε ότι
   (α′) $x \mid y$ αν και μόνο αν $\langle x \rangle \supset \langle y \rangle$.
   (β′) $x \cong y$ αν και μόνο αν $\langle x \rangle = \langle y \rangle$.
   (γ′) x είναι μονάδα αν και μόνο αν $\langle x \rangle = R$.
   (δ′) Το x είναι ανάγωγο αν και μόνο αν το x είναι μέγιστο ανάμεσα στα γνήσια κύρια ιδεώδη του R.
3. Θα λέμε ότι μία ακέραια περιοχή R είναι ένας ευκλείδιος δακτύλιος αν υπάρχει συνάρτηση $\phi : R\backslash\{0\} \to \mathbb{N}$ ώστε
   - Αν $a, b \in R\backslash\{0\}$ και $a \mid b$, τότε $\phi(a) \leq \phi(b)$.
   - Αν $a, b \in R\backslash\{0\}$, τότε υπάρχουν $q, r \in R$ με $a = bq + r$ όπου $r = 0$ ή $\phi(r) < \phi(b)$.

   Δείξτε ότι σε κάθε ευκλείδειο δακτύλιο κάθε ιδεώδες είναι κύριο. Αναφέρετε τρία διαφορετικά παραδείγματα ευκλείδειων δακτυλίων.
4. Αποδείξτε ότι σε κάθε περιοχή κυρίων ιδεωδών έχουμε μοναδική παραγοντοποίηση σε ανάγωγα, δηλαδή κάθε μη μηδενικό στοιχείο γράφεται ως

$$x = up_1 \cdots p_r,$$

   όπου το u είναι μονάδα για κάθε άλλη παραγοντοποίηση του $x = wp'_1 \cdots p'_s$ σε ανάγωγα ισχύει $r = s$ και κάθε p_i σχετίζεται με ένα $p'_{\sigma(i)}$ για κατάλληλη μετάθεση σ.
5. Θέτουμε $\omega = e^{2\pi i/3} = -\frac{1}{2} + i\sqrt{3}2$. Ορίζουμε την $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ με $N(a + b\omega) = a^2 - ab + b^2$. Δείξτε ότι αν $a + b\omega$ γράφεται στη μορφή $u + vi$ με $u, v \in \mathbb{R}$, τότε $N(a + b\omega) = u^2 + v^2$. Δείξτε ότι για όλα τα $z_1, z_2 \in \mathbb{Z}[\omega]$, $N(z_1 z_2) = N(z_1)N(z_2)$. Δείξτε αν $z_1 \mid z_2$, τότε $N(z_1) \mid N(z_2)$. Δείξτε ότι $z \in \mathbb{Z}[\omega]$ είναι μονάδα αν και μόνο αν $N(z) = 1$ και να βρεθούν όλες οι μονάδες του $\mathbb{Z}[\omega]$. Δείξτε ότι το $1 - \omega$ είναι ανάγωγο στο $\mathbb{Z}[\omega]$ και ότι $3 = u(1 - \omega)^2$ για κάποια μονάδα u. Δείξτε ότι το $\mathbb{Z}[\omega]$ είναι περιοχή μονοσήμαντης ανάλυσης.

Βιβλιογραφία

[1] Adamson, I. T. *Elementary Rings and Modules*. University Mathematical Texts. Barnes & Noble Books [A division of Harper & Row, Publishers, Inc.], New York; Oliver and Boyd, Edinburgh-London, 1972, pp. vi+136.

[2] Alaca, Ş. & Williams, K. S. *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, 2004, pp. xviii+428. ISBN: 0-521; 0-521-54011-9.

[3] Bosch, S. *Algebra*. Springer-Lehrbuch. Springer Berlin, 2013. ISBN: 9783662056493. URL: https://books.google.gr/books?id=4BiyBgAAQBAJ.

[4] Chatland, H. & Davenport, H. *Euclid's algorithm in real quadratic fields*. *Canad. J. Math.* 2 (1950), pp. 289–296. ISSN: 0008-414X. URL: https://doi.org/10.4153/cjm-1950-026-7.

[5] Clark, D. A. *A quadratic field which is Euclidean but not norm-Euclidean*. *Manuscripta Math.* 83.3-4 (1994), pp. 327–330. ISSN: 0025-2611. URL: https://doi.org/10.1007/BF02567617.

[6] Connes, A. *Trace formula in noncommutative geometry and the zeros of the Riemann zeta function*. *Selecta Math. (N.S.)* 5.1 (1999), pp. 29–106. ISSN: 1022-1824.

[7] Conrad, K. *Finitely Generated Modules over a PID*. URL: http://math.stanford.edu/~conrad/210APage/handouts/PIDGreg.pdf.

[8] Harper, H. $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*. PhD thesis. Mc Gill Montreal Canada, 2000.

[9] Harper, M. $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*. *Canad. J. Math.* 56.1 (2004), pp. 55–70. ISSN: 0008-414X. URL: https://doi.org/10.4153/CJM-2004-003-9.

[10] Hartley, B. & Hawkes, T. O. *Rings, modules and linear algebra*. Chapman & Hall, London-New York, 1980, pp. xi+210. ISBN: 0-412-09810-5.

[11] Jacobson, N. *Basic algebra. II*. Second. New York: W. H. Freeman and Company, 1989, pp. xviii+686. ISBN: 0-7167-1933-9.

[12] Motzkin, T. *The Euclidean algorithm*. *Bull. Amer. Math. Soc.* 55 (1949), pp. 1142–1146. ISSN: 0002-9904. URL: https://doi.org/10.1090/S0002-9904-1949-09344-8.

[13] Narkiewicz, W. *Euclidean Algorithm in small abelian fields*. *Funct. Approx. Comment. Math.* 37.part 2 (2007), pp. 337–340. ISSN: 0208-6573. URL: https://doi.org/10.7169/facm/1229619657.

[14] Pollack, P. *A Conversational Introduction to Algebraic Number Theory, Arithmetic beyond* $\mathbb{Z}$. Vol. 84. Student Mathematical Library. American Mathematical Society, Providence, RI, 2017, pp. ix + 316. ISBN: 978-1-4704-3653-7.

[15] Samuel, P. *About Euclidean rings*. *J. Algebra* 19 (1971), pp. 282–301. ISSN: 0021-8693. URL: https://doi.org/10.1016/0021-8693(71)90110-4.

[16] Stichtenoth, H. *Algebraic function fields and codes*. Berlin: Springer-Verlag, 1993, pp. x+260. ISBN: 3-540-56489-6.

[17] Zervou, A. *Profinite Groups and Cohomology*. MA thesis. Πανεπιστήμιο Κρήτης, 2017.

[18] Αντωνιάδης, Ι. Α. *Σημειώσεις Τοπικών Σωμάτων*. Πανεπιστήμιο Κρήτης, 1992.

[19] Βάρσος, Δ. et al. *Μια εισαγωγή στην Άλγεβρα*. Εκδ. Σοφία, 2012.

[20] Λάκκης, Κ. *Άλγεβρα*. Εκδ. Ζήτη, 1991.

[21] Σωτήρης, Κ. *Uniformization Αλγεβρικών Καμπυλών*. MA thesis. Πανεπιστήμιο Αιγαίου, Μαθηματικό Τμήμα, 2005.

Κατάλογος Συμβόλων

$(\mathbb{Z}/n\mathbb{Z})^*$ Αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}/n\mathbb{Z}$, σελ. 113

$[x_1 : y_1 : z_1]$ Ομογενείς συντεταγμένες σημείου, σελ. 255

$\overline{\mathbb{F}}_\ell$ Η αλγεβρική θήκη του πεπερασμένου σώματος $\mathbb{F}_\ell$, σελ. 277

$\overline{E}_{ns}$ Το σύνολο των μή-ιδιαζόντων σημείων ελλειπτικής καμπύλης, σελ. 267

$\chi_\pi(\alpha)$ Διτετραγωνικός χαρακτήρας, σελ. 144

$\chi_{\alpha,L/K}(x)$ Χαρακτηριστικό πολυώνυμο ακέραιου αλγεβρικού α, σελ. 47

δ_{ij} Σύμβολο του Kronecker, σελ. 205

$\Gamma_1(N)$ Congruenge ομάδα, σελ. 278

$\left(\frac{\alpha}{\pi}\right)_3$ Κυβικό σύμβολο αντιστροφής, σελ. 146

$\left(\frac{D_K}{p}\right)$ Σύμβολο Kronecker, σελ. 139

$\left(\frac{L/K}{P}\right)$ Σύμβολο του Artin, σελ. 150

$\left[\frac{L/K}{P}\right]$ Σύμβολο του Frobenius, σελ. 149

$\mathbb{A}^2_K$ Αφινικό επίπεδο, σελ. 251

$\mathbb{A}^2_K(L)$ L-ρητά σημεία του επιπέδου, σελ. 251

$\mathbb{P}^2_K(L)$ L-ρητά σημεία του προβολικού επιπέδου, σελ. 255

$\mathbb{P}^2_K$ Προβολικό επίπεδο υπεράνω του σώματος K, σελ. 255

$\mathcal{D}_{L/K}$ Σχετική διακρίνουσα επέκτασης, σελ. 196

$\mathrm{Aut}(E[\ell^n])$ Αυτομορφισμοί της ομάδας των ℓ^n-σημείων στρέψης, σελ. 272

$\mathrm{Diff}_{K/\mathbb{Q}}$ Διαφορίζουσα του σώματος K, σελ. 208

$\mathrm{Diff}_{L/K}$ Σχετική διαφορίζουσα της επέκτασης L/K, σελ. 210

Frob_p Frobenius ομομορφισμός, σελ. 268

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ Απόλυτη ομάδα Galois, σελ. 268

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ Ομάδα Galois της επέκτασης που παράγεται από τα ℓ^n-σημεία στρέψης, σελ. 272

$\mathrm{Gal}(L/K)$ Ομάδα Galois της επέκτασης L/K, σελ. 125

$\mathrm{Ind}(\alpha)$ Δείκτης του στοιχείου α, σελ. 69

$\mathrm{Spl}(L/K)$ Το σύνολο των πρώτων ιδεωδών που αναλύονται πλήρως, σελ. 158

Φ_n Το n-στό κυκλοτομικό πολυώνυμο, σελ. 113

$\mathbb{Q}(\zeta_n)$ Το n-οστό κυκλοτομικό σώμα, σελ. ii

$\mathbb{Q}^{ab}$ Maximal αβελιανή επέκταση του $\mathbb{Q}$, σελ. 312

$\mathbb{Q}_p$ Σώμα των p-αδικών αριθμών, σελ. 264

ρ_χ Αναπαράσταση του χαρακτήρα χ, σελ. 269

$\mathbb{Z}_p$ Δακτύλιος των p-αδικών αριθμών, σελ. 264

$\mathbb{Z}_p^*$ Μονάδες των p-αδικών ακέραιων, σελ. 311

ζ_p Η p-ρίζα της μονάδας, $\zeta_p = e^{\frac{2\pi i}{p}}$, σελ. 8

$C(F)$ Προβολική καμπύλη που ορίζεται από το ομογενές πολυώνυμο F, σελ. 256

$C(L)$ L-ρητά σημεία της καμπύλης C, σελ. 252

D_K Διακρίνουσα σώματος K, σελ. 19

$E(\mathbb{Q})$ Ρητά σημεία ελλειπτικής καμπύλης E, σελ. 262

$E(\mathbb{Q})_{tor}$ Ομάδα στρέψης της $E(\mathbb{Q})$, σελ. 262

$e(Q/P)$ Δείκτης διακλάδωσης του Q υπεράνω του P, σελ. 96

$E(R_K)$ Ομάδα μονάδων του δακτυλίου R_K, σελ. 20

$E[\ell^n]$ ℓ^n-σημεία στρέψης της E, σελ. 272

$E^{(p)}_{a,b,c}$ Ελλειπτική καμπύλη του Frey, για τον πρώτο p, σελ. 275

$f(Q/P)$ Βαθμός αδρανείας του Q υπεράνω του P, σελ. 96

G_T Ομάδα αδράνειας, σελ. 126

G_Z Ομάδα ανάλυσης, σελ. 126

G_{Δ_i} i-ομάδα διακλάδωσης, σελ. 126

$h(Q)$ Ύψος σημείου Q, σελ. 262

h_k Αριθμός κλάσεων του σώματος K, σελ. 85

$i(G, C; P)$ Πολλαπλότητα τομής F, G στο P, σελ. 256

$i(K)$ Δείκτης του σώματος K, σελ. 69

$K(C)$ Σώμα συναρτήσεων της C, σελ. 252

$K[C]$ Δακτύλιος συντεταγμένων της C, σελ. 252

K^{gc} Galois θήκη, σελ. 125

K_0 Σώμα αδράνειας, σελ. 136

K_n n-στό σώμα διακλάδωσης, σελ. 136

K_T Σώμα αδράνειας, σελ. 126

K_Z Σώμα ανάλυσης, σελ. 126

K_{-1} Σώμα ανάλυσης, σελ. 136

K_{Δ_i} i-στό σώμα διακλάδωσης, σελ. 126

$L(E,s)$ L-σειρά ελλειπτικής καμπύλης, σελ. 273

$m(L)$ Ελάχιστος δείκτης του σώματος K, σελ. 69

$P(L/K)$ Το σύνολο των πρώτων ιδεωδών του K που αναλύονται πλήρως στο L., σελ. ii

P_B Θεμελιώδες παραλληλεπίπεδο, σελ. 165

$S_k(\Gamma_1(N))$ Χώρος των cusp forms για την ομάδα $\Gamma_1(N)$, σελ. 278

$T_\ell(E)$ Tate module, σελ. 271

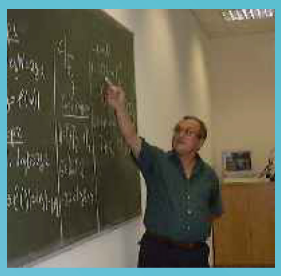
$\nu_Q(A)$ Ο εκθέτης του πρώτου ιδεώδους Q στην ανάλυση του A, σελ. 216

Κατάλογος εννοιών

Καταλογος ονομάτων

In this index you'll find only famous people's names

Αλγεβρική Θεωρία Αριθμών: Το βιβλίο αφορά τη μελέτη της αλγεβρικής θεωρίας αριθμών, η οποία αποτελεί έναν δυναμικό κλάδο των μαθηματικών, με πολλές διασυνδέσεις με σχεδόν όλα τα μαθηματικά, τη φυσική αλλά και τη σύγχρονη κρυπτογραφία. Η αλγεβρική θεωρία αριθμών ξεκίνησε από τη μελέτη των λύσεων διοφαντικών εξισώσεων, και ιδιαίτερα της εξίσωσης του Fermat. Ήταν δε, μαζί με την Αλγεβρική Γεωμετρία αλλά και τη θεωρία αναλλοίωτων, ένα από τα κίνητρα της ανάπτυξης της αντιμεταθετικής άλγεβρας, και γενικότερα της Άλγεβρας όπως τη γνωρίζουμε σήμερα. Είναι μια απαραίτητη γνώση για κάθε μαθηματικό, και ιδιαίτερα για τους μαθηματικούς που ενδιαφέρονται για τον κλάδο της Άλγεβρας.
Οι συγγραφείς έχουν διδάξει το μάθημα τόσο σε προπτυχιακό όσο και σε μεταπτυχιακό επίπεδο πολλές φορές τα τελευταία 30 έτη, σε διαφορετικά πανεπιστήμια (Κρήτης, Αιγαίου, Αθηνών). Από την πολυετή αυτή διδασκαλία είχαν προκύψει διδακτικές σημειώσεις, οι οποίες εξελίχθηκαν από την πρώτη τους έκδοση το 1984 σε ένα στοιχειοθετημένο κείμενο σε LaTeX με πολλές προσθήκες και βελτιώσεις. Το αντικείμενο του βιβλίου άλλωστε αφορά κομμάτι της έρευνας των συγγραφέων και των μαθητών τους.



Ιωάννης Αντωνιάδης: Διδάκτορας του Πανεπιστημίου της Κολωνίας, έχει διδάξει στα Πανεπιστήμια της Θεσσαλονίκης, της Κύπρου και της Κρήτης, και είναι Ομότιμος Καθηγητής στο Πανεπιστήμιο της Κρήτης. Είναι έγγαμος, πατέρας τριών παιδιών και περήφανος παππούς.

Αριστείδης Κοντογεώργης: Διδάκτορας του Πανεπιστημίου Κρήτης, έχει διδάξει στα πανεπιστήμια Κρήτης, Αιγαίου και Αθηνών. Είναι έγγαμος, πατέρας δύο παιδιών.

Το παρόν σύγγραμμα χρηματοδοτήθηκε από το Πρόγραμμα Δημοσίων Επενδύσεων του Υπουργείου Παιδείας.