Σώμα του Hilbert, Μιγαδικός Πολλαπλασιασμός και το Jugendtraum του Kronecker

Αλέξανδρος Γ. Γαλανάκης
(alexandros.galanakis@gmail.com)

Επιβλέπων καθηγητής:
Ιωάννης Α. Αντωνιάδης

Πτυχιακή εργασία

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών,
Πανεπιστήμιο Κρήτης,
Ηράκλειο,
Οκτώβριος 2015

Ευχαριστίες

Πριν από κάθε μαθηματική έννοια, απόδειξη και θεωρία που θα αναπτυχθεί σε αυτή την πτυχιακή εργασία είναι αναγκαίο να ευχαριστήσω κάποιους ανθρώπους, οι οποίοι κατά τη διάρκεια της συγγραφής της παρούσας πτυχιακής εργασίας, καθώς και εξ αρχής των σπουδών μου, στάθηκαν αρωγοί στην προσπάθεια αυτή.

Έτσι, οφείλω να ευχαριστήσω την οικογένεια μου, τους γονείς μου Γιώργο και Μαριάνθη και την αδελφή μου Αγγελική, της οποίας η στήριξη και η συμπαράσταση είναι αρκετά σημαντική. Η υποστήριξη που έχω από τους γονείς μου δεν ήταν μόνο ψυχολογική, αλλά ήταν κυρίως πνευματική. Στα πρόσωπά τους δε βλέπω μονάχα του ανθρώπους που ακούν υπομονετικά οτιδήποτε επιθυμώ να μοιραστώ, αλλά και τους εκπαιδευτικούς στους οποίους αποδίδω το πάθος γι' αυτό που έχω επιλέξει να κάνω. Ιδιαιτέρως, στη μητέρα μου οφείλω τα πρώτα βήματα στο γοητευτικό κόσμο των μαθηματικών, ήδη από την παιδική μου ηλικία.

Έχοντας φοιτήσει για τέσσερα χρόνια ως προπτυχιακός φοιτητής στο Πανεπιστήμιο Κρήτης, έχω γνωρίσει αρκετούς επιστήμονες και δασκάλους, στους οποίους αξίζει μνεία, καθότι αυτοί διαμορφώνουν την μαθηματική, και γενικότερα την επιστημονική, προσωπικότητα των πνευματικών τους απογόνων. Έτσι, είναι αρκετά δύσκολο να προσδιορίσω πλήρως όλους όσους, έστω και με μία συμβουλή, με βοήθησαν έως εδώ. Για το λόγο αυτό, δε θα αναφερθώ συγκεκριμένα σε πρόσωπα.

Μπορώ, όμως, να διακρίνω έναν άνθρωπο, του οποίου η συμβολή στη μέχρι τώρα ακαδημαϊκή ζωή υπήρξε, και συνεχίζει να είναι, κομβική. Πρόκειται για τον επιβλέποντα καθηγητή της παρούσας πτυχιακής εργασίας κ. Ιωάννη Αντωνιάδη, ο οποίος επανειλημμένα στάθηκε στο πλευρό μου, είτε ως επιστήμονας και έμπειρος ερευνητής, είτε ως άνθρωπος. Πέραν της μαθηματικής γνώσεως που απέκτησα και η οποία αποδίδεται στην εξαιρετική διδασκαλία του ανθρώπου αυτού, με την αρωγή του είχα την τύχη να φοιτήσω εκτός Ελλάδος και να γνωρίσω εξέχουσες προσωπικότητες της παγκόσμιας μαθηματικής διανόησης.

Τέλος, θα ήθελα να ευχαριστήσω τον κ. Νίκο Τζανάκη και τον κ. Αριστείδη Κοντογεώργη ως μέλη της κριτικής επιτροπής της πτυχιακής αυτής εργασίας. Εκτιμώ και σέβομαι τον κ. Τζανάκη, καθότι εξαιρετικός δάσκαλος, αφοσιωμένος και καταξιωμένος ερευνητής. Από την άλλη, στον κ. Κοντογεώργη αναγνωρίζω τον υποδειγματικό ακαδημαϊκό, μιας και είναι νέος με διάθεση για δουλειά και πλούσιο ερευνητικό έργο.

Αισθάνομαι τυχερός που στο μονοπάτι αυτό της γνώσης βρέθηκαν άτομα που βοήθησαν ουσιαστικά ώστε να συνεχίσω να το διάβα μου. Έτσι ως φοιτητής, αλλά κυρίως ως άνθρωπος, οφείλω να ευχαριστήσω τους ευεργέτες των προσπαθειών μου.

Αλέξανδρος Γαλανάκης,
ΤΜΕΜ, Πανεπιστήμιο Κρήτης.

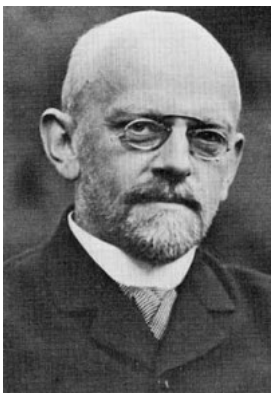
Εισαγωγή

Σκοπός της παρούσας πτυχιακής εργασίας είναι η επίλυση του Jugendtraum του Kronecker. Η λέξη "Jugendtraum" είναι η γερμανική μετάφραση του "νεανικού ονείρου". Πράγματι, ο Kronecker σε γράμμα του προς τον Dedekind, χαρακτηρίζει ως νεανικό του όνειρο την εύρεση συναρτήσεων, των οποίων συγκεκριμένες τιμές θα μπορούσαν να παράγουν αβελιανές επεκτάσεις τυχόντων αλγεβρικών σωμάτων αριθμών. Όταν το σώμα που επιλέγουμε είναι το $\mathbb{Q}$, η απάντηση στο πρόβλημα αυτό είναι το θεώρημα των Kronecker και Weber. Αυτό μας πληροφορεί ότι κάθε αβελιανή επέκταση του $\mathbb{Q}$ περιέχεται σε ένα κυκλοτομικό σώμα. Με άλλα λόγια, κάθε αβελιανή επέκταση του $\mathbb{Q}$ περιέχεται σε σώμα που προκύπτει από επισύναψη στο $\mathbb{Q}$ συγκεκριμένης τιμής της εκθετικής συνάρτησης. Το Jugendtraum είναι η γενίκευση του θεωρήματος των Kronecker και Weber στην περίπτωση κατά την οποία το αλγεβρικό σώμα που επιλέγεται δεν ειναι το $\mathbb{Q}$, αλλά ένα τυχαίο τετραγωνικό μιγαδικό σώμα αριθμών. Η προσπάθεια για τη λύση του εν λόγω προβλήματος οδήγησε στην ανάπτυξη κλάδων των μαθηματικών όπως η θεωρία του μιγαδικού πολλαπλασιασμού και η θεωρία κλάσεων σωμάτων.

*Leopold Kronecker (*1823-1891*)*

Από τα παραπάνω γίνεται φανερό ότι η μελέτη του Jugendtraum απαιτεί τη γνώση και το χειρισμό εκλεπτυσμένων μαθηματικών εννοιών και γενικότερα θεωριών. Για το λόγο αυτό, η επιλογή των κεφαλαίων και η παρουσίαση της θεωρίας, δεν αποσκοπεί μονάχα στην επίτευξη του στόχου, ήτοι στην επίλυση του Jugendtraum στην περίπτωση των τετραγωνικών σωμάτων αριθμών, αλλά και στη γνωριμία με αρκετά γοητευτικά μαθηματικά. Ποιητικά μιλώντας, δεν εστιάζουμε μονάχα στην Ιθάκη, αλλά ενδιαφερόμαστε και για το ταξίδι.

Προς τούτο ξεκινάμε τη μελέτη μας με κάποια στοιχεία αλγεβρικής θεωρίας αριθμών. Το πρώτο κεφάλαιο έχει ως στόχο την εμβάθυνση στη γνώση των αλγεβρικών σωμάτων αριθμών. Το κεφάλαιο αυτό είναι γραμμένο, με βάση το βιβλίο "Θεωρία Αριθμών" του κ. Λάκκη, ήτοι το [2] της βιβλιογραφίας, γι' αυτό και παραπέμπουμε σε αυτό. Πρόκειται για τα στοιχεία αυτά της θεωρίας που πρέπει να γνωρίζει κανείς, ώστε να έχει ολοκληρωμένη γνώση περί των αλγεβρικών αριθμητικών σωμάτων.



*David Hilbert (*1862-1943*)*

Όπως προαναφέρθηκε, ο στόχος αυτής της πτυχιακής εργασίας αφορά σε τετραγωνικά αριθμητικά σώματα. Έτσι, το δεύτερο κεφάλαιο αφιερώνεται στη μελέτη αυτών. Τα τετραγωνικά σώματα αριθμών αποτελούν αλγεβρικά αριθμητικά σώματα βαθμού 2. Επομένως, έχοντας ήδη τα εφόδια που χρειάζονται από το πρώτο κεφάλαιο και με προσθήκη νέων στοιχείων θεωρίας, όπως για παράδειγμα της έννοιας των τάξεων τετραγωνικών σωμάτων αριθμών, έχουμε εμβαθύνει αρκετά σε αυτά.

Εφόσον απαραίτητη για τη μελέτη μας είναι η θεωρία κλάσεων σωμάτων, το τρίτο κεφάλαιο αναφέρεται σε αυτή. Παρά ταύτα, επειδή πρόκειται για μία θεωρία, της οποίας τα αποτελέσματα ποικίλουν και είναι αδύνατο να παρουσιαστούν στα πλαίσια μίας πτυχιακής εργασίας, επικεντρωνόμαστε σε στοιχεία της θεωρίας διακλαδώσεως του Hilbert και στον ορισμό του σώματος του Hilbert ενός αλγεβρικού σώματος αριθμών. Το τελευταίο διαδραματίζει ουσιαστικό ρόλο στην επίτευξη του στόχου μας.

Στο τέταρτο κεφάλαιο εισάγονται οι έννοιες των ελλειπτικών και modular συναρτήσεων, οι οποίες εκ των προτέρων δε φαίνεται να σχετίζονται με όσα μελετήθηκαν στα προηγούμενα κεφάλαια. Παρ' όλα αυτά, η θεωρία του κεφαλαίου αυτού είναι ιδιαιτέρως σημαντική και για το λόγο ότι στη μελέτη μας υπεισέρχεται και ο γοητευτικός κλάδος της μιγαδικής αναλύσεως. Το κεφάλαιο αυτό είναι γραμμένο στα πρότυπα του βιβλίου "Modular Functions and Dirichlet Series in Number Theory" του Tom Apostol, ήτοι το [3] της βιβλιογραφίας.

Η συσχέτιση των εννοιών που παρουσιάστηκαν στο τέταρτο κεφάλαιο με αυτές των προηγούμενων κεφαλαίων φανερώνεται στο πέμπτο κεφάλαιο. Σε αυτό αναφέρουμε βασικά στοιχεία των ελλειπτικών καμπυλών και εισάγουμε την έννοια του μιγαδικού πολλαπλασιασμού. Ακόμα, αποδεικνύουμε ότι η $\mathcal{J}$-αναλλοίωτος μίας ελλειπτικής καμπύλης με μιγαδικό πολλαπλασιασμό είναι ακέραιος αλγεβρικός αριθμός.

Ύστερα από όλα αυτά, είμαστε έτοιμοι να παρουσιάσουμε το βασικό μας πρόβλημα, ήτοι το Jugendtraum για τετραγωνικά μιγαδικά σώματα αριθμών. Αν και μικρότερο σε μέγεθος, το έκτο και τελευταίο κεφάλαιο της εν λόγω εργασίας παρουσιάζει πλήρως το Jugendtraum και την απόδειξη αυτού. Η προσέγγιση που ακολουθείται στο έκτο κεφάλαιο, βασίζεται στο βιβλίο "Advanced Topics in the Arithmetic of Elliptic Curves" του Joseph Silverman, ήτοι το [12] της βιβλιογραφίας.

Κλείνουμε την εισαγωγή με το σχόλιο ότι υπάρχει αρκετό γόνιμο έδαφος ερευνητικά στον κλάδο της αλγεβρικής θεωρίας αριθμών. Μάλιστα, όπως γίνεται αντιληπτό και από αυτήν την πτυχιακή εργασία, τα μαθηματικά μέσα που χρησιμοποιούνται δεν είναι μόνο αλγεβρικά ή αριθμοθεωρητικά.

Περιεχόμενα

Κεφάλαιο 1

Στοιχεία Αλγεβρικής Θεωρίας Αριθμών

1.1 Αλγεβρικοί και ακέραιοι αλγεβρικοί αριθμοί

Έστω πολυώνυμο $f(X)$ με ρητούς αριθμούς ως συντελεστές. Από το θεμελιώδες θεώρημα της άλγεβρας τα σημεία μηδενισμού του πολυωνύμου αυτού περιέχονται στο $\mathbb{C}$. Θωρούμε το σύνολο $\tilde{\mathbb{Q}}$ που περιέχει όλα τα σημεία μηδενισμού μη τετριμμένων πολυωνύμων με ρητούς συντελεστές. Τα στοιχεία του συνόλου αυτού ονομάζονται αλγεβρικοί αριθμοί.

Ορισμος 1.1.1. Ο $\alpha \in \mathbb{C}$ θα καλείται αλγεβρικός, εάν υπάρχει μη τετριμμένο μονικό πολυώνυμο $f(X) \in \mathbb{Q}[X]$ με σημείο μηδενισμού το α, ήτοι $f(\alpha) = 0$.

Εύκολα προκύπτει ότι

$$\mathbb{Q} \subseteq \tilde{\mathbb{Q}} \subsetneq \mathbb{C},$$

αφού κάθε ρητός αριθμός α είναι σημείο μηδενισμού του πολυωνύμου $X - \alpha \in \mathbb{Q}[X]$, αλλά κάθε μιγαδικός αριθμός δεν είναι αλγεβρικός. Για παράδειγμα, οι αριθμοί π και e δεν είναι αλγεβρικοί.

Θεωρούμε ένα στοιχείο $\alpha \in \tilde{\mathbb{Q}}$. Τότε υπάρχει ένα μονικό πολυώνυμο στο $\mathbb{Q}[X]$ με το α ως σημείο μηδενισμού και τον ελάχιστο βαθμό. Βάσει αυτής της επιλογής το πολυώνυμο αυτό είναι ανάγωγο στο $\mathbb{Q}[X]$. Το πολυώνυμο αυτό το καλούμε *ανάγωγο πολυώνυμο του* α *ή ελάχιστο πολυώνυμο του* α και το συμβολίζουμε με $Irr(\alpha, \mathbb{Q})$. Ακόμα αν υποθέσουμε ότι το β είναι ένα διάφορο του α σημείο μηδενισμού του $Irr(\alpha, \mathbb{Q})$, τότε το $Irr(\alpha, \mathbb{Q})$ είναι και ελάχιστο πολυώνυμο του β, δηλαδή $Irr(\beta, \mathbb{Q}) = Irr(\alpha, \mathbb{Q})$. Πράγματι, εφόσον το β είναι σημείο μηδενισμού του $Irr(\beta, \mathbb{Q})$, τότε θα ισχύει ότι

$$Irr(\beta, \mathbb{Q}) \mid Irr(\alpha, \mathbb{Q}).$$

Κι αφού εξ ορισμού του ελαχίστου πολυωνύμου αυτό είναι ανάγωγο, τότε ισχύει κατ' ανάγκη η ισότητα.

Προταση 1.1.2. *Αν* $\alpha \in \tilde{\mathbb{Q}}$ *τότε το* $Irr(\alpha, \mathbb{Q})$ *έχει απλά σημεία μηδενισμού.*

Απόδειξη. Έστω ότι το $p(X) := Irr(\alpha, \mathbb{Q})$ έχει το β ως σημείο μηδενισμού πολλαπλότητας > 1. Τότε $Irr(\beta, \mathbb{Q}) = Irr(\alpha, \mathbb{Q}) = p(X)$ και η παράγωγος $p'(X) \in \mathbb{Q}[X]$ έχει το β ως σημείο μηδενισμού και βαθμό μικρότερο από αυτόν του $p(X)$. Αυτό, όμως, αντίκειται στον ορισμό του $Irr(\beta, \mathbb{Q})$. □

Αν, επομένως, ισχύει ότι $\alpha, \beta \in \tilde{\mathbb{Q}}$ τα ελάχιστα πολυώνυμα αυτών θα έχουν τη μορφή:

$$p_\alpha(X) = Irr(\alpha, \mathbb{Q}) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_m)$$

$$p_\beta(X) = Irr(\beta, \mathbb{Q}) = (X - \beta_1)(X - \beta_2) \cdots (X - \beta_n),$$

όπου χ.β.τ.γ. θεωρούμε ότι $\alpha_1 = \alpha$ και $\beta_1 = \beta$ και $\alpha_i, \beta_j \in \tilde{\mathbb{Q}}$, για κάθε $1 \leq i \leq m$ και $1 \leq j \leq n$. Αν ορίσουμε τα πολυώνυμα

$$\prod_{i,j=1}^{m,n} (X - (\alpha_i - \beta_j)) \ , \ \prod_{i,j=1}^{m,n} (X - (\alpha_i \beta_j)) \text{ και } X^m p_\alpha \left(\frac{1}{X} \right),$$

τότε αυτά έχουν ως σημεία μηδενισμού τους αριθμούς $\alpha - \beta, \alpha\beta$ και α^{-1}, αντίστοιχα. Μάλιστα, από τους τύπους Vieta έπεται ότι έχουν ρητούς συντελεστές, επομένως, $\alpha - \beta, \alpha\beta, \alpha^{-1} \in \tilde{\mathbb{Q}}$. Κι εφόσον $\tilde{\mathbb{Q}} \subseteq \mathbb{C}$, ισχύει η παρακάτω πρόταση:

ΠΡΟΤΑΣΗ 1.1.3. *Το σύνολο $\tilde{\mathbb{Q}}$ είναι υπόσωμα του $\mathbb{C}$. Ιδιαιτέρως, είναι η αλγεβρική θήκη του $\mathbb{Q}$.*

Είμαστε, τώρα, έτοιμοι να εισάγουμε την έννοια του ακέραιου αλγεβρικού αριθμού. Για το λόγο αυτό, αναφέρουμε το παρακάτω λήμμα:

ΛΗΜΜΑ 1.1.4 (Gauss)**.** *Αν ένα μονικό πολυώνυμο $f(X) \in \mathbb{Z}[X]$ αναλύεται γνήσια στο $\mathbb{Q}[X]$ σε γινόμενο δύο άλλων μονικών πολυωνύμων, έστω $g(X)$ και $h(X)$, τότε κατ' ανάγκη θα έχουμε ότι $g(X), h(X) \in \mathbb{Z}[X]$.*

ΘΕΩΡΗΜΑ 1.1.5. *Έστω $\alpha \in \tilde{\mathbb{Q}}$. Τα παρακάτω είναι ισοδύναμα:*

(1) $Irr(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$

(2) Υπάρχει μονικό πολυώνυμο $f(X) \in \mathbb{Z}[X]$ με σημείο μηδενισμού το α.

Απόδειξη. (1) $\Rightarrow$ (2) Προφανές.
(2) $\Rightarrow$ (1) Έστω μονικό πολυώνυμο $f(X) \in \mathbb{Z}[X]$ με την ιδιότητα ότι $f(\alpha) = 0$. Θέτουμε $g(X) := Irr(\alpha, \mathbb{Q}) \in \mathbb{Q}[X]$. Τότε υπάρχει πολυώνυμο $h(X) \in \mathbb{Q}[X]$, τέτοιο ώστε:

$$f(X) = g(X)h(X).$$

Το h είναι επίσης μονικό. Επομένως το συμπέρασμα προκύπτει άμεσα από το λήμμα του Gauss. □

ΟΡΙΣΜΟΣ 1.1.6. Ο αριθμός $\alpha \in \tilde{\mathbb{Q}}$ λέγεται ακέραιος αλγεβρικός αριθμός, όταν πληρεί μία από τις δύο, και συνεπώς και τις δύο, συνθήκες του θεωρήματος 1.1.5.

Ισχύει κάτι πιο γενικό από το θεώρημα 1.1.5, το οποίο μας δίνει ένα επιπλέον κριτήριο για το πότε ένας αριθμός είναι ακέραιος αλγεβρικός.

ΠΡΟΤΑΣΗ 1.1.7. *Αν ο αριθμός α είναι σημείο μηδενισμού ενός μονικού πολυωνύμου $f(X)$ με ακέραιους αλγεβρικούς συντελεστές, τότε είναι και ο ίδιος ακέραιος αλγεβρικός.*

Απόδειξη. Έστω ότι το πολυώνυμο f γράφεται υπό τη μορφή

$$f(X) = f_0 + f_1 X + \cdots + f_{n-1} X^{n-1} + X^n,$$

όπου τα f_i είναι ακέραιοι αλγεβρικοί αριθμοί, και έστω $\rho_1, \rho_2, \ldots, \rho_n$ τα σημεία μηδενισμού αυτού. Θεωρούμε τα σημεία μηδενισμού $\rho^{(1)}, \rho^{(2)}, \ldots, \rho^{(m_0)}$ του $Irr(\rho_1, \mathbb{Q})$, τα σημεία μηδενισμού $\rho^{(m_0+1)}, \rho^{(m_0+2)}, \ldots, \rho^{(m_0+m_1)}$ του $Irr(\rho_2, \mathbb{Q})$ και συνεχίζοντας κατ' αυτό τον τρόπο, τα σημεία μηδενισμού $\rho^{(m_0+m_1+\ldots+m_{n-2}+1)}, \rho^{(m_0+m_1+\ldots+m_{n-2}+2)}, \ldots,$
$\rho^{(m_0+m_1+\ldots+m_{n-2}+m_{n-1})}$ του $Irr(\rho_n, \mathbb{Q})$. Θέτουμε, ακόμα,

$$r = m_0 + m_1 + \cdots + m_{n-1}.$$

Κατασκευάζουμε το πολυώνυμο

$$g(X) = \prod_{\sigma \in S_r} \left(\rho^{(\sigma(1))} + \rho^{(\sigma(2))} X + \cdots + \rho^{(\sigma(n))} X^{n-1} + X^n \right),$$

όπου S_r είναι η ομάδα των μεταθέσεων των r στοιχείων του συνόλου $\{1, 2, \ldots, r\}$. Προφανώς, ο α είναι σημείο μηδενισμού του μονικού πολυωνύμου $g(X)$. Εύκολα επίσης προκύπτει από τους τύπους Vieta ότι οι συντελεστές του $g(X)$ είναι ακέραιοι αριθμοί. Συνεπώς, ο α είναι εξ ορισμού ακέραιος αλγεβρικός. □

Το σύνολο όλων των ακέραιων αλγεβρικών αριθμών το συμβολίζουμε ως $\tilde{\mathbb{Z}}$. Προφανώς ισχύει ότι $\tilde{\mathbb{Z}} \subseteq \tilde{\mathbb{Q}}$. Μάλιστα, εάν θεωρήσουμε δύο στοιχεία $\alpha, \beta \in \tilde{\mathbb{Z}}$, τότε $\alpha - \beta, \alpha\beta \in \tilde{\mathbb{Z}}$, οπότε ισχύει το παρακάτω αποτέλεσμα:

ΠΡΟΤΑΣΗ 1.1.8. *Το σύνολο $\tilde{\mathbb{Z}}$ με πράξεις την πρόσθεση και τον πολλαπλασιασμό αποτελεί ακέραια περιοχή με σώμα κλασμάτων το $\tilde{\mathbb{Q}}$. Ιδιαίτερα, ισχύει ότι*

$$\tilde{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$$

1.2 Αλγεβρικά σώματα αριθμών

ΟΡΙΣΜΟΣ 1.2.1. Αλγεβρικό σώμα αριθμών ονομάζεται κάθε πεπερασμένη επέκταση του $\mathbb{Q}$, η οποία περιέχεται στο $\mathbb{C}$.

Κάθε στοιχείο ενός αλγεβρικού σώματος αριθμών είναι αλγεβρικός αριθμός. Πράγματι, εάν υποθέσουμε ότι το K είναι ένα αλγεβρικό σώμα αριθμών βαθμού $[K : \mathbb{Q}] = n$ και θ ένα στοιχείο αυτού, τότε οι αριθμοί $1, \theta, \ldots, \theta^{n-1}$ είναι γραμμικώς εξαρτημένοι, άρα υπάρχουν $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, όχι όλα μηδέν, ώστε

$$a_0 \cdot 1 + a_1\theta + \cdots + a_n\theta^n = 0,$$

ήτοι ο αριθμός θ είναι σημείο μηδενισμού του μη μηδενικού πολυωνύμου $f(X) = a_0 + a_1X + \cdots + a_nX^n$, άρα και αλγεβρικός.

Για να κατανοήσουμε την έννοια του αλγεβρικού σώματος αριθμών θα κάνουμε αναφορά σε μερικά στοιχεία θεωρίας σωμάτων. Για το τυχαίο θ, το οποίο ανήκει σε μία επέκταση του $\mathbb{Q}$, ορίζουμε την ακέραια περιοχή

$$\mathbb{Q}[\theta] = \{f(\theta) \mid f(X) \in \mathbb{Q}[X]\}$$

και το σώμα κλασμάτων αυτής

$$\mathbb{Q}(\theta) = \{\frac{f(\theta)}{g(\theta)} \mid f(X), g(X) \in \mathbb{Q}[X] \text{ με } g(\theta) \neq 0\}.$$

Προφανώς ισχύει ότι $\mathbb{Q}[\theta] \subseteq \mathbb{Q}(\theta)$. Στην περίπτωση που ο θ είναι αλγεβρικός αριθμός ισχύει ότι $\mathbb{Q}(\theta) = \mathbb{Q}[\theta]$.

Υποθέτουμε ότι $p(X) = Irr(\theta, \mathbb{Q})$ και $deg(p(X)) = n$. Εάν το a είναι στοιχείο του σώματος $\mathbb{Q}(\theta)$, τότε υπάρχει πολυώνυμο $g(X) \in \mathbb{Q}[X]$ με την ιδιότητα $a = g(\theta)$. Έστω, λοιπόν,

$$g(X) = q(X)p(X) + r(X) \text{ , όπου } r \equiv 0 \text{ ή } deg(r(X)) < n.$$

Τότε $a = g(\theta) = r(\theta)$. Κι εφόσον το $r(\theta)$ είναι ένας $\mathbb{Q}$-γραμμικός συνδυασμός των $1, \theta, \ldots, \theta^{n-1}$ και αυτά είναι $\mathbb{Q}$-γραμμικώς ανεξάρτητα, τότε παράγουν το $\mathbb{Q}(\theta)$ ως $\mathbb{Q}$-διανυσματικό χώρο. Συνεπώς λαμβάνουμε ότι $[\mathbb{Q}(\theta) : \mathbb{Q}] = deg(p(X))$. Από τα παραπάνω προκύπτει και ότι μία πεπερασμένη επέκταση του $\mathbb{Q}$ είναι και πεπερασμένα παραγόμενη.

Θεωρημα 1.2.2. *Ένα σώμα K είναι αλγεβρικό σώμα αριθμών εάν, και μόνο εάν ισχύει ότι $K = \mathbb{Q}(\theta)$ για κάποιο αλγεβρικό αριθμό θ.*

Απόδειξη. ($\Leftarrow$) Άμεσο εξ ορισμού του αλγεβρικού σώματος αριθμών.
($\Rightarrow$) Έστω K ένα αλγεβρικό σώμα αριθμών. Τότε αυτό είναι μία πεπερασμένη επέκταση του $\mathbb{Q}$. Έστω, λοιπόν, $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, όπου το α είναι το ελάχιστο πλήθος στοιχείων για το οποίο ισχύει αυτό. Υποθέτουμε ότι $n > 1$ και ότι

$$p_{\alpha_1}(X) = Irr(\alpha_1, \mathbb{Q}) = (X - {\alpha_1}^{(1)})(X - {\alpha_1}^{(2)}) \cdots (X - {\alpha_1}^{(r)}) \text{ με } {\alpha_1}^{(1)} = \alpha_1$$

$$p_{\alpha_2}(X) = Irr(\alpha_2, \mathbb{Q}) = (X - {\alpha_2}^{(1)})(X - {\alpha_2}^{(2)}) \cdots (X - {\alpha_2}^{(s)}) \text{ με } {\alpha_2}^{(1)} = \alpha_2.$$

Τα πολυώνυμα αυτά έχουν απλά σημεία μηδενισμού, επομένως για κάθε $i = 1, 2$ και $j_1 \neq j_2$ ισχύει ότι ${\alpha_i}^{(j_1)} \neq {\alpha_i}^{(j_2)}$. Αυτο σημαίνει ότι υπάρχει το πολύ ένας ρητός αριθμός b για τον οποίο έχουμε

$${\alpha_1}^{(i)} + b{\alpha_2}^{(j)} = {\alpha_1}^{(1)} + b{\alpha_2}^{(1)} \text{ , } \forall i \times j \in \{1, 2, \ldots, r\} \times \{1, 2, \ldots, s\}.$$

Το πλήθος, όμως, των εξισώσεων αυτών είναι πεπερασμένο, οπότε κατά συνέπεια υπάρχει ρητός αριθμός c για τον οποίο ισχύει

$${\alpha_1}^{(i)} + c{\alpha_2}^{(j)} \neq {\alpha_1}^{(1)} + c{\alpha_2}^{(1)} = \alpha_1 + c\alpha_2 \text{ , } \forall i \times j \in \{2, \ldots, r\} \times \{1, 2, \ldots, s\}.$$

Έστω $\beta = \alpha_1 + c\alpha_2$. Θα δείξουμε ότι $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha_1, \alpha_2)$. Ο εγκλεισμός $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha_1, \alpha_2)$ είναι προφανής. Επιδιώκουμε να δείξουμε τον αντίστροφο εγκλεισμό. Ορίζουμε το πολυώνυμο

$$f(X) = p_{\alpha_1}(\beta - cX) \in \mathbb{Q}(\beta)[X],$$

που έχει ως σημείο μηδενισμού το α_2. Συνεπώς τα πολυώνυμα $p_{\alpha_2}(X)$ και $f(X)$ έχουν ως κοινό σημείο μηδενισμού το α_2, το οποίο λόγω της σχέσης

$${\alpha_1}^{(i)} + c{\alpha_2}^{(j)} \neq \alpha_1 + c\alpha_2 \Rightarrow \alpha_1 + c\alpha_2 - c{\alpha_2}^{(i)} \neq {\alpha_1}^{(j)} \text{ , } \forall j = 1, 2, \ldots, r$$

είναι μοναδικό. Με άλλα λόγια ισχύει ότι $(p_{\alpha_2}(X), f(X)) = X - \alpha_2$, άρα:

$$Irr(\alpha_2, \mathbb{Q}(\beta)) \mid p_{\alpha_2} \text{ και } Irr(\alpha_2, \mathbb{Q}(\beta)) \mid f(X) \Rightarrow Irr(\alpha_2, \mathbb{Q}(\beta)) \mid X - \alpha_2$$

$$\Rightarrow Irr(\alpha_2, \mathbb{Q}(\beta)) = X - \alpha_2 \in \mathbb{Q}(\beta)[X] \Rightarrow \alpha_2 \in \mathbb{Q}(\beta),$$

οπότε $\alpha_1 \in \mathbb{Q}(\beta) \Rightarrow \mathbb{Q}(\alpha_1, \alpha_2) \subseteq \mathbb{Q}(\beta)$. Έτσι αποδείξαμε την ισότητα των δύο συνόλων. Αυτό, όμως, μας δίνει ότι

$$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n) = \mathbb{Q}(\beta, \alpha_3, \ldots, \alpha_n),$$

που είναι αντίφαση στην επιλογή του n άρα και στην υπόθεση $n > 1$. □

Εάν θεωρήσουμε κάποιο στοιχείο $a \in K$, το ανάγωγο πολυώνυμο αυτού

$$f(X) := Irr(\alpha, \mathbb{Q}) = f_0 + f_1 X + \cdots + f_{n-1}X^{n-1} + X^n$$

και το ελάχιστο κοινό πολλαπλάσιο e_f των παρονομαστών των συντελεστών του f, τότε ο αριθμός $e_f\alpha$ είναι σημείο μηδενισμού του πολυωνύμου $(e_f)^n \cdot f\left(\frac{X}{e_f}\right)$, το οποίο είναι μονικό με ακέραιους συντελεστές. Αυτό σημαίνει ότι ο αριθμός $\gamma = e_f\alpha$ είναι ακέραιος αλγεβρικός. Άρα αποδείξαμε το εξής:

Προταση 1.2.3. *Κάθε αλγεβρικός αριθμός ενός αλγεβρικού σώματος αριθμών K μπορεί να γραφεί ως πηλίκο ενός ακέραιου αλγεβρικού αριθμού δια ενός φυσικού αριθμού.*

Από αυτό το σημείο θα συμβολίζουμε ως R_K το σύνολο που περιέχει όλους τους ακέραιους αλγεβρικούς αριθμούς του σώματος K. Κατ' αντιστοιχία με την περίπτωση όπου $K = \mathbb{Q}$, που ο δακτύλιος των ακέραιων αλγεβρικών αριθμών είναι ο $\mathbb{Z}$, ισχύει ότι

Προταση 1.2.4. *Το σύνολο R_K, με πράξεις την πρόσθεση και τον πολλαπλασιασμό αποτελεί ακέραια περιοχή με σώμα κλασμάτων το K.*

1.3 Συζυγείς αριθμοί, norm και ίχνος και κύριο πολυώνυμο.

Θεωρούμε ένα αλγεβρικό αριθμητικό σώμα $K = \mathbb{Q}(\theta)$ βαθμού $[K : \mathbb{Q}] = n$ και έστω $p(X) = Irr(\theta, \mathbb{Q})$. Τότε το $p(X)$ έχει n διακεκριμένα σημεία μηδενισμού, έστω τα $\theta^{(1)} = \theta, \theta^{(2)}, \ldots, \theta^{(n)}$. Συνεπώς ισχύει ότι $[\mathbb{Q}(\theta^{(i)}) : \mathbb{Q}] = n$ για κάθε $i = 1, 2, \ldots, n$. Άρα κάθε στοιχείο $a \in \mathbb{Q}(\theta^{(i)})$ έχει τη μορφή:

$$a = \sum_{k=0}^{n-1} a_k {\theta^{(i)}}^k.$$

Εάν ορίσουμε τις απεικονίσεις:

$$\begin{aligned} \sigma_i \quad : \quad & \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta^{(i)}) \\ & \sum_{k=0}^{n-1} a_k \theta^k \longmapsto \sum_{k=0}^{n-1} a_k {\theta^{(i)}}^k \ , \forall i = 1, 2, \ldots, n \end{aligned}$$

τότε προφανώς, για κάθε $a, b \in \mathbb{Q}(\theta)$ ισχύουν οι σχέσεις

$$\sigma_i(a + b) = \sigma_i(a) + \sigma_i(b) \ , \sigma_i(ab) = \sigma_i(a) + \sigma_i(b) \ , \sigma_i(\theta) = \theta^{(i)}.$$

Μάλιστα, κάθε ρητός αριθμός παραμένει αναλλοίωτος από τη δράση της σ_i. Αυτό σημαίνει ότι οι σ_i είναι $\mathbb{Q}$-ομομορφισμοί[1], διακεκριμένοι ανά δύο. Προφανώς, καθένας από τους σ_i είναι μονομορφισμός. Θεωρώντας έναν τυχαίο $\mathbb{Q}$-μονομορφισμό σ, παρατηρούμε ότι $0 = \sigma(p(\theta)) = p(\sigma(a))$, ήτοι στέλνει το σημείο μηδενισμού θ του $p(X)$ σε κάποια άλλο σημείο μηδενισμού. Είναι, με άλλα λόγια, κάποιος από τους σ_i. Άρα οι μοναδικοί $\mathbb{Q}$-μονομορφισμοί του σώματος $K = \mathbb{Q}(\theta)$ είναι οι σ_i και προσδιορίζονται πλήρως από την εικόνα τους στο θ .

Ορισμος 1.3.1. Έστω αλγεβρικό σώμα αριθμών $K = \mathbb{Q}(\theta)$. Τα σώματα $\sigma_i(K) = \mathbb{Q}(\theta^{(i)})$, για κάθε $i = 1, 2, \ldots, n$, θα καλούνται *συζυγή σώματα του* K. Αν ο a είναι τυχόν στοιχείο του K, τότε οι αριθμοί $a^{(i)} = \sigma_i(a)$, για κάθε $i = 1, 2, \ldots, n$, θα λέγονται *συζυγείς αριθμοί του* a.

Παρατηρηση 1.3.2. Τονίσαμε ότι το $Irr(\theta, \mathbb{Q})$ έχει διακεκριμένα σημεία μηδενισμού, ήτοι οι συζυγείς αριθμοί του θ διαφέρουν ανά δύο. Κάτι τέτοιο δεν ισχύει εν γένει, αφού για παράδειγμα, όλοι οι συζυγείς ενός ρητού αριθμού ταυτίζονται με αυτόν.

Έστω, ότι το $p(X)$ έχει r_1 πραγματικά σημεία μηδενισμού και $2r_2$ μιγαδικά ήτοι $[K : \mathbb{Q}] = r_1 + 2r_2$. Τότε λαμβάνουμε r_1 πραγματικούς ομομορφισμούς, τους οποίους θα καλούμε *πραγματικές εμφυτεύσεις του* K, και $2r_2$ μιγαδικούς ομομορφισμούς, που θα τους ονομάζουμε *μιγαδικές εμφυτεύσεις του K*. Μάλιστα, το ζεύγος (r_1, r_2) το ονομάζουμε *υπογραφή του αλγεβρικού σώματος αριθμών* K.

Ορισμος 1.3.3. Έστω $a \in \mathbb{Q}(\theta)$. Τότε ως *ίχνος* και ως *norm του* a ορίζουμε τους αριθμούς

$$Tr_K(a) = a^{(1)} + a^{(2)} + \cdots + a^{(n)}$$

και

$$N_K(a) = a^{(1)} a^{(2)} \cdots a^{(n)}$$

αντίστοιχα, όπου ως $a^{(i)}$ συμβολίζουμε τους συζυγείς αριθμούς του a.

[1]Με τον όρο "$\mathbb{Q}$-ομομορφισμός" εννοούμε έναν ομομορφισμό δακτυλίων που περιέχουν το $\mathbb{Q}$ και αφήνει τα στοιχεία αυτού αναλλοίωτα.

Σύμφωνα με τον ορισμό αυτό, για τους αριθμούς $a, b \in \mathbb{Q}(\theta)$ και $\alpha, \beta \in \mathbb{Q}$ ισχύουν οι ισότητες

$$Tr_K(\alpha a + \beta b) = \alpha Tr_K(a) + \beta Tr_K(b)\ , Tr_K(\alpha) = n\alpha$$
$$N_K(ab) = N_K(a)N_K(b)\ , N_K(\alpha) = \alpha^n.$$

ΟΡΙΣΜΟΣ 1.3.4. Έστω $a \in K = \mathbb{Q}(\theta)$.Θεωρούμε τον ενδομορφισμό του K

$$\begin{array}{rcl} \varphi_a & : & K \to K \\ & & x \longmapsto ax. \end{array}$$

Ως *κύριο ή χαρακτηριστικό* πολυώνυμο του a ορίζουμε το χαρακτηριστικό πολυώνυμο του φ_a και το συμβολίζουμε ως $\chi_a(X)$.

Υπενθυμίζουμε ότι ως χαρακτηριστικό πολυώνυμο του ενδομορφισμού φ_a ορίζουμε το χαρακτηριστικό πολυώνυμο του πίνακα του φ_a όταν αυτός ειδωθεί ως γραμμική απεικόνιση μεταξύ διανυσματικών χώρων. Με άλλα λόγια, από τις σχέσεις

$$\varphi_a(1) = a = a_{11} + a_{12}\theta + \cdots + a_{1n}\theta^{n-1},$$
$$\varphi_a(\theta) = a\theta = a_{21} + a_{22}\theta + \cdots + a_{2n}\theta^{n-1},$$
$$\vdots$$
$$\varphi_a(\theta^{n-1}) = a\theta^{n-1} = a_{n1} + a_{n2}\theta + \cdots + a_{nn}\theta^{n-1},$$

λαμβάνουμε την ισότητα πινάκων

$$(A - aI_n)\Theta = \mathbf{0},$$

όπου

$$A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}\ , \Theta := \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{n-1} \end{pmatrix}$$

και ως I_n και $\mathbf{0}$ συμβολίζουμε το μοναδιαίο και το μηδενικό πίνακα αντίστοιχα. Επομένως το σύστημα $(A - aI_n)X = \mathbf{0}$ έχει μη τετριμμένη λύση, οπότε κατ' ανάγκη ισχύει ότι

$$\det(A - aI_n) = 0.$$

Άρα το a είναι σημείο μηδενισμού του πολυωνύμου

$$\chi_a(X) = (-1)^n \det(A - XI_n),$$

το οποίο είναι και το χαρακτηριστικό πολυώνυμο του a. Μάλιστα, μπορούμε να αποδείξουμε (βλ. [10], σελ. 259, Θεώρ. 2.1.) ότι το χαρακτηριστικό πολυώνυμο του a είναι μία δύναμη του $Irr(a, \mathbb{Q})$. Από το γεγονός αυτό εξάγουμε δύο συμπεράσματα. Κατά πρώτον, το χαρακτηριστικό πολυώνυμο του a έχει τη μορφή

$$\chi_a(X) = \left((X - a^{(1)})(X - a^{(2)}) \cdots (X - a^{(n)})\right)^k,$$

όπου $k \in \mathbb{N}$ και $a^{(1)} = a, a^{(2)}, \ldots, a^{(n)}$ είναι οι συζυγείς αριθμοί του a και κατά δεύτερον, αν $Irr(a, \mathbb{Q}) = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} + X^m$, τότε

$$Tr_K(a) = -\frac{n}{m}a_{m-1} \text{ και } N_K(a) = (-1)^n {a_0}^s.$$

Εν γένει, λοιπόν, το ίχνος και η norm ενός αλγεβρικού αριθμού είναι ρητοί αριθμοί. Αν, επιπροσθέτως, ο αριθμός a είναι ακέραιος αλγεβρικός, τότε $Tr_K(a), N_K(a) \in \mathbb{Z} \subseteq \tilde{\mathbb{Z}}$. Από όσα αναφέρθηκαν για το χαρακτηριστικό πολυώνυμο του a προκύπτει ένα κριτήριο ισότητας δύο αλγεβρικών σωμάτων αριθμών.

ΠΡΟΤΑΣΗ 1.3.5. *Για κάποιο $a \in \mathbb{Q}(\theta)$ ισχύει ότι $\mathbb{Q}(\theta) = \mathbb{Q}(a)$ εάν, και μόνο εάν οι συζυγείς αριθμοί του a είναι διακεκριμένοι μεταξύ τους.*

1.4 Διακρίνουσα και βάση ακεραιότητας

Πριν περάσουμε στα αποτελέσματα αυτής της παραγράφου υπενθυμίζουμε ένα αποτέλεσμα περί γραμμικής ανεξαρτησίας. Ένα αλγεβρικό σώμα αριθμών είναι μία επέκταση του $\mathbb{Q}$ άρα και ένας $\mathbb{Q}$-διανυσματικός χώρος. Έστω αλγεβρικό σώμα αριθμών $K = \mathbb{Q}(\theta)$ και n στοιχεία αυτού

$$a_i = \sum_{j=1}^{n} a_{ij}\theta^{j-1}, \text{ με } a_{ij} \in \mathbb{Q} \text{ και } i = 1, 2, \ldots, n.$$

Τότε το σύνολο $\{a_i \mid i = 1, 2, \ldots, n\}$ είναι $\mathbb{Q}$-γραμμικά ανεξάρτητο τότε, και μόνο τότε, όταν

$$\det\left((a_{ij})_{i,j\in\{1,2,\ldots,n\}}\right) \neq 0.$$

Ορισμος 1.4.1. Θεωρούμε τους n αριθμούς $a_1, a_2, \ldots, a_n \in K$. Τους n συζυγείς του a_i, τους συμβολίζουμε με ${a_i}^{(j)}$, όπου $j = 1, 2, \ldots, n$. Τότε ως *διακρίνουσα των αριθμών* $a_1, a_2, \ldots, a_n$, ορίζουμε το τετράγωνο της ορίζουσας:

$$\det\left(({a_i}^{(j)})_{i,j\in\{1,2,\ldots,n\}}\right),$$

και τη συμβολίζουμε ως $d(a_1, a_2, \ldots, a_n)$, ήτοι

$$d(a_1, a_2, \ldots, a_n) = \left(\det\left(({a_i}^{j})_{i,j\in\{1,2,\ldots,n\}}\right)\right)^2 = \left(\det\begin{pmatrix} {a_1}^{(1)} & {a_1}^{(2)} & \cdots & {a_1}^{(n)} \\ {a_2}^{(1)} & {a_2}^{(2)} & \cdots & {a_2}^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ {a_n}^{(1)} & {a_n}^{(2)} & \cdots & {a_n}^{(n)} \end{pmatrix}\right)^2.$$

Μάλιστα, αν $A = ({a_i}^{(j)})_{i,j\in\{1,2,\ldots,n\}}$, τότε από τη σχέση $\det(A) = \det(A^t)$, προκύπτει άμεσα ότι

$$d(a_1, a_2, \ldots, a_n) = \det\begin{pmatrix} Tr_K({a_1}^2) & Tr_K(a_1a_2) & \cdots & Tr_K(a_1a_n) \\ Tr_K(a_2a_1) & Tr_K({a_2}^2) & \cdots & Tr_K(a_2a_n) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_K(a_na_1) & Tr_K(a_na_2) & \cdots & Tr_K({a_n}^2) \end{pmatrix}.$$

Αυτό μας πληροφορεί ότι εν γένει ισχύει $d(a_1, a_2, \ldots, a_n) \in \mathbb{Q}$. Αν, επιπρόσθετα, οι $a_1, a_2, \ldots, a_n$ είναι ακέραιοι αλγεβρικοί, τότε $d(a_1, a_2, \ldots, a_n) \in \mathbb{Z}$.

Στον ορισμό της διακρίνουσας μίας n-άδας αλγεβρικών αριθμών, βασίζεται και ο ορισμός της διακρίνουσας αλγεβρικού αριθμού.

Ορισμος 1.4.2. Ονομάζουμε *διακρίνουσα ενός* $a \in K$, και τη συμβολίζουμε με $d(a)$, την διακρίνουσα των αριθμών $1, a, \ldots, a^{n-1}$, ήτοι

$$d(a) = d(1, a, \ldots, a^{n-1})$$

Εξ ορισμού προκύπτει ότι

$$d(a) = \prod_{i>j}\left(a^{(i)} - a^{(j)}\right)^2,$$

οπότε αμέσως βλέπουμε ότι $d(\theta) \neq 0$, διότι γνωρίζουμε πως οι συζυγείς του θ είναι διακεκριμένοι ανά δύο. Άρα μία αναδιατύπωση της προτάσεως 1.3.5 είναι η παρακάτω.

Προταση 1.4.3. *Ισχύει ότι* $K = \mathbb{Q}(a)$*, όπου* $a \in K$ *εάν, και μόνο εάν,* $d(a) \neq 0$*.*

Επομένως στην περίπτωση κατά την οποία $K \neq \mathbb{Q}(a)$, ήτοι $\mathbb{Q}(a) \subset K$ και $deg(Irr(a,\mathbb{Q})) < [K : \mathbb{Q}]$, λαμβάνουμε ότι $d(a) = 0$. Αν ισχύει η ισότητα των βαθμών, τότε οι συζυγείς $a^{(1)} = a, a^{(2)}, \ldots, a^{(n)}$ του a, είναι διακεκριμένοι ανά δύο. Συμβολίζοντας ως $p(X)$ το $Irr(a,\mathbb{Q})$, παρατηρούμε ότι

$$p(X) = (X - a^{(1)})(X - a^{(2)}) \cdots (X - a^{(n)}) \Rightarrow$$

$$p'(X) = \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} (X - a^{(j)}) \Rightarrow p'(a^{(i)}) = \prod_{\substack{j=1 \\ j \neq i}}^{n} (a^{(i)} - (a^{(j)}).$$

Άρα δείξαμε την κατωτέρω πρόταση.

ΠΡΟΤΑΣΗ 1.4.4. *Για τη διακρίνουσα ενός στοιχείου $a \in K$ ισχύει ότι:*

$$d(a) = \begin{cases} (-1)^{n(n-1)/2} N_K(p'(a)) & , \alpha\nu\ deg(p(X)) = [K : \mathbb{Q}] \\ 0 & , \alpha\nu\ deg(p(X)) < [K : \mathbb{Q}] \end{cases},$$

όπου $p(X) := Irr(a,\mathbb{Q})$.

ΠΡΟΤΑΣΗ 1.4.5. *Οι αριθμοί $a_1, a_2, \ldots, a_n$ είναι γραμμικά ανεξάρτητοι εάν, και μόνο εάν, ισχύει ότι*

$$d(a_1, a_2, \ldots, a_n) \neq 0.$$

Απόδειξη. Πράγματι, εάν υποθέσουμε μία σχέση γραμμικής εξάρτησης:

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n = 0 \text{ , όπου } \lambda_i \in \mathbb{Q} \text{ , } \forall i = 1, 2, \ldots, n$$

και εφαρμόσουμε διαδοχικά όλους τους $\mathbb{Q}$-ομομορφισμούς σ_i, όπως αυτοί ορίστηκαν στο 1.3, τότε λαμβάνουμε το σύστημα των εξισώσεων

$$\begin{cases} \lambda_1\sigma_1(a_1) + \lambda_2\sigma_1(a_2) + \cdots + \lambda_n\sigma_1(a_n) = 0 \\ \lambda_1\sigma_2(a_1) + \lambda_2\sigma_2(a_2) + \cdots + \lambda_n\sigma_2(a_n) = 0 \\ \vdots \\ \lambda_1\sigma_n(a_1) + \lambda_2\sigma_n(a_2) + \cdots + \lambda_n\sigma_n(a_n) = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} \lambda_1 {a_1}^{(1)} + \lambda_2 {a_2}^{(1)} + \cdots + \lambda_n {a_n}^{(1)} = 0 \\ \lambda_1 {a_1}^{(2)} + \lambda_2 {a_2}^{(2)} + \cdots + \lambda_n {a_n}^{(2)} = 0 \\ \vdots \\ \lambda_1 {a_1}^{(n)} + \lambda_2 {a_2}^{(n)} + \cdots + \lambda_n {a_n}^{(n)} = 0 \end{cases}.$$

Επομένως η ύπαρξη μοναδικής λύσης, της τετριμμένης, ισοδυναμεί με τη συνθήκη

$$d(a_1, a_2, \ldots, a_n) \neq 0.$$

□

Η παρακάτω πρόταση, της οποίας την απόδειξη θα παραλείψουμε, συνδυάζει τη διακρίνουσα οποιασδήποτε n-άδας στοιχείων του $K = \mathbb{Q}(\theta)$ με την διακρίνουσα του στοιχείου θ.

ΠΡΟΤΑΣΗ 1.4.6. *Για τους αριθμούς*

$$a_i = \sum_{j=1}^{n} a_{ij}\theta^{j-1} \text{ , } i = 1, 2, \ldots, n$$

ισχύει ότι

$$d(a_1, a_2, \ldots, a_n) = \left(\det\left((a_{ij})_{i,j\in\{1,2,\ldots,n\}}\right)\right)^2 \cdot d(\theta).$$

ΠΡΟΤΑΣΗ 1.4.7. *Αν $\omega_1, \omega_2, \ldots, \omega_n$ είναι μία βάση της επέκτασης $K/\mathbb{Q}$, τότε για τους αριθμούς*

$$a_i = \sum_{j=1}^{n} a_{ij}\omega_j \text{ , } i = 1, 2, \ldots, n$$

ισχύει ότι:

$$d(a_1, a_2, \ldots, a_n) = \left(\det\left((a_{ij})_{i,j\in\{1,2,\ldots,n\}}\right)\right)^2 \cdot d(\omega_1, \omega_2, \ldots, \omega_n).$$

ΟΡΙΣΜΟΣ 1.4.8. Οι ακέραιοι αλγεβρικοί αριθμοί $\omega_1, \omega_2, \ldots, \omega_n \in K$ καλούνται *βάση ακεραιότητας του K* εάν είναι γραμμικά ανεξάρτητοι και κάθε στοιχείο $a \in K$ γράφεται υπό τη μορφή

$$a = \sum_{i=1}^{n} a_i\omega_i \text{ , όπου } a_i \in \mathbb{Z}.$$

Η έκφραση αυτή, λόγω του ότι τα ω_i αποτελούν βάση του $\mathbb{Q}$-διανυσματικού χώρου K, είναι μονοσήμαντη.

ΠΑΡΑΤΗΡΗΣΗ 1.4.9. Η έννοια της βάσης ακεραιότητας ενός αλγεβρικού σώματος αριθμών εμπεριέχει την έννοια της βάσης $\mathbb{Q}$-διανυσματικού χώρου. Έτσι, όταν γνωρίζουμε ότι μία n-άδα στοιχείων του K είναι βάση ακεραιότητας αυτού, τότε είναι και βάση του αν το σώμα K ειδωθεί ως $\mathbb{Q}$-διανυσματικός χώρος. Το αντίστροφο δεν ισχύει. Ιδιαίτερα, εάν $K = \mathbb{Q}(\theta)$ και το θ δεν είναι ακέραιος αλγεβρικός αριθμός, τότε οι αριθμοί $1, \theta, \ldots, \theta^{n-1}$ αποτελούν βάση, αλλά όχι βάση ακεραιότητας μιας και δεν είναι όλοι ακέραιοι αλγεβρικοί.

Θα αποδείξουμε τώρα την ύπαρξη βάσης ακεραιότητας για κάθε αλγεβρικό σώμα αριθμών. Προτού όμως το δείξουμε αυτό, διατυπώνουμε ένα κριτήριο, με το οποίο αποφασίζουμε πότε μία δοθείσα n-άδα αριθμών αποτελεί βάση ακεραιότητας.

ΛΗΜΜΑ 1.4.10. *Έστω R_K ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του σώματος K, βαθμού n. Αν οι $\omega_1, \omega_2, \ldots, \omega_n \in R_K$ είναι γραμμικά ανεξάρτητοι και ο αριθμός $\mid d(\omega_1, \omega_2, \ldots, \omega_n) \mid$ είναι ο ελάχιστος δυνατός, τότε οι αριθμοί αυτοί αποτελούν βάση ακεραιότητας.*

Απόδειξη. Προφανώς κάθε αλγεβρικός αριθμός a της μορφής

$$a = \sum_{i=1}^{n} a_i\omega_i \text{ , όπου } a_i \in \mathbb{Z}$$

είναι ακέραιος αλγεβρικός. Η ιδέα της απόδειξης είναι ότι αν ένας τουλάχιστον από τους συντελεστές a_i δεν είναι ακέραιος, τότε ο a δεν είναι ακέραιος αλγεβρικός. Ας υποθέσουμε χ.β.τ.γ. ότι ο a_1 δεν είναι ακέραιος. Τότε θα γράφεται υπό τη μορφή

$$a_1 = [a_1] + a_1', 0 < a_1' < 1,$$

όπου ως $[a_1]$ συμβολίζουμε το ακέραιο μέρος του a_1. Θεωρούμε τον αριθμό

$$b := a - [a_1]\omega_1 = a_1'\omega_1 + \cdots + a_n\omega_n.$$

Τότε θα ισχύει ότι

$$d(b, \omega_2, \ldots, \omega_n) = \left(\det\begin{pmatrix} a_1' & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}\right)^2 d(\omega_1, \ldots, \omega_n) = {a_1'}^2 \cdot d(\omega_1, \ldots, \omega_n).$$

Άρα

$$0 < |d(b, \omega_2, \ldots, \omega_n)| < |d(\omega_1, \omega_2, \ldots, \omega_n)|.$$

Συνεπώς οι αριθμοί $b, \omega_2, \ldots, \omega_n$ είναι γραμμικά ανεξάρτητοι και ο b δεν είναι ακέραιος αλγεβρικός αριθμός καθώς έχουμε υποθέσει ότι η $\mid d(\omega_1, \omega_2, \ldots, \omega_n) \mid$ είναι ελάχιστη. Επομένως ούτε και ο $a = b + [a_1]\omega_1$ είναι ακέραιος αλγεβρικός. Άρα κάθε αριθμός $a \in R_K$ έχει τη μορφή $a = \sum_{i=1}^{n} a_i\omega_i$, όπου $a_i \in \mathbb{Z}$, και για να είναι ακέραιος αλγεβρικός θα πρέπει κατ' ανάγκη όλα τα a_i να είναι ακέραιοι. Άρα οι $\omega_1, \omega_2, \ldots, \omega_n$ είναι βάση ακεραιότητας. □

Θεωρημα 1.4.11 (Ύπαρξη βάσης ακεραιότητας)**.** *Κάθε αλγεβρικό σώμα αριθμών K έχει μία τουλάχιστον βάση ακεραιότητας.*

Απόδειξη. Ορίζουμε το σύνολο Ω, το οποίο περιέχει όλες τις n-άδες γραμμικά ανεξάρτητων στοιχείων του R_K, όπου $n = [K : \mathbb{Q}]$. Το Ω είναι προφανώς μη κενό, αφού εάν $K = \mathbb{Q}(\theta)$, τότε $\{1, \theta, \ldots, \theta^{n-1}\} \in \Omega$. Αν θεωρήσουμε τις απόλυτες τιμές των διακρινουσών των στοιχείων του Ω, τότε αυτές είναι φυσικοί αριθμοί, άρα μπορούμε να βρούμε στοιχείο του Ω με την ελάχιστη απόλυτη διακρίνουσα, σύμφωνα με το λήμμα 1.4.10. Το στοιχείο αυτό θα είναι και η ζητούμενη βάση ακεραιότητας, □

Προταση 1.4.12. *Όλες οι βάσεις ακεραιότητας ενός αλγεβρικού σώματος αριθμών K έχουν ίσες διακρίνουσες.*

Απόδειξη. Εάν υποθέσουμε ότι τα σύνολα $\{\omega_1, \omega_2, \ldots, \omega_n\}$ και $\{\omega'_1, \omega'_2, \ldots, \omega'_n\}$ αποτελούν δύο βάσεις ακεραιότητας, τότε βάσει του 2.1.4 οι διακρίνουσες τους έχουν ίδιο πρόσημο και μάλιστα υπάρχουν πίνακες A και B με στοιχεία ακέραιους αριθμούς τέτοιοι, ώστε

$$d(\omega_1, \ldots, \omega_n) = \big(\det(A)\big)^2 d(\omega'_1, \ldots, \omega'_n)$$

$$d(\omega'_1, \ldots, \omega'_n) = \big(\det(B)\big)^2 d(\omega_1, \ldots, \omega_n).$$

Από τις σχέσεις αυτές έπεται ότι

$$d(\omega'_1, \ldots, \omega'_n) \mid d(\omega_1, \ldots, \omega_n)$$

$$d(\omega_1, \ldots, \omega_n) \mid d(\omega'_1, \ldots, \omega'_n).$$

Άρα ισχύει η ισότητα των διακρινουσών. □

Ορισμος 1.4.13. Την κοινή διακρίνουσα των βάσεων ακεραιότητας ενός αλγεβρικού σώματος αριθμών K, την ονομάζουμε *διακρίνουσα του σώματος K* και τη συμβολίζουμε ως d_K.

Προταση 1.4.14. *Αν υποθέσουμε ότι η $\{\omega_1, \omega_2, \ldots., \omega_n\}$ είναι μία βάση ακεραιότητας και ο*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

είναι ένας πίνακας με στοιχεία ακέραιους αριθμούς, τότε για να είναι οι αριθμοί

$$\omega'_i = \sum_{j=1}^{n} a_{ij}\omega_j \text{ , } \forall i = 1, 2, \ldots, n$$

βάση ακεραιότητας θα πρέπει $\det(A) = \pm 1$.

Προταση 1.4.15. *Η διακρίνουσα μίας n-άδας γραμμικά ανεξάρτητων στοιχείων του R_K ενός αλγεβρικού σώματος αριθμών K, είναι ίση με το γινόμενο του d_K επί το τετράγωνο ενός φυσικού. Συνεπώς, η διακρίνουσα του K διαιρεί οποιαδήποτε διακρίνουσα προκύπτει από n γραμμικά ανεξάρτητα στοιχεία του R_K.*

Πορισμα 1.4.16. *Εάν η διακρίνουσα μίας n-άδας ακεραίων αλγεβρικών αριθμών του σώματος K είναι αριθμός ελεύθερος τετραγώνου, τότε η n-άδα αυτή αποτελεί βάση ακεραιότητας για το σώμα K.*

1.5 Μονάδες και ανάλυση σε γινόμενο πρώτων αριθμών

Ορισμος 1.5.1. Ένας ακέραιος αλγεβρικός αριθμός ε ενός αλγεβρικού σώματος αριθμών K θα καλείται *μονάδα*, αν ο αντίστροφος αυτού είναι επίσης ακέραιος αλγεβρικός. Με άλλα λόγια, ο ε καλείται μονάδα όταν $\varepsilon \in \mathcal{U}_K := {R_K}^{\times}$.

Πως όμως, διαπιστώνουμε αν ένας αριθμός είναι μονάδα ή όχι; Στο ερώτημα αυτό απαντούν τα παρακάτω αποτελέσματα.

Προταση 1.5.2. *Αν ο αλγεβρικός αριθμός $\varepsilon \in K$ είναι σημείο μηδενισμού ενός μονικού πολυωνύμου $f(X) \in \mathbb{Z}[X]$ με $f(0) = \pm 1$, τότε αυτός είναι μονάδα. Αντιστρόφως, αν ο αριθμός ε είναι μονάδα του αλγεβρικού σώματος αριθμών K, τότε το ελάχιστο πολυώνυμο αυτού έχει ακέραιους συντελεστές και ως σταθερό όρο το ± 1.*

Απόδειξη. ($\Rightarrow$) Έστω ότι το ε είναι σημείο μηδενισμού του πολυωνύμου

$$f(X) = \pm 1 + f_1 X + \cdots + f_{n-1} X^{n-1} + X^n \text{ , όπου } f_i \in \mathbb{Z} \text{ , } \forall = 1, 2, \ldots, n.$$

Τότε εξ ορισμού ο ε είναι ακέραιος αλγεβρικός. Ο ε^{-1} είναι σημείο μηδενισμού του $X^n f(\frac{1}{X})$, συνεπώς και ο ε^{-1} είναι επίσης ακέραιος αλγεβρικός. Άρα ο ε είναι μονάδα.
($\Leftarrow$) Θεωρούμε, τώρα, ότι ο ε είναι μονάδα. Τότε

$$Irr(\varepsilon, \mathbb{Q}) = a_0 + a_2 X + \cdots + a_{n-1} X^{n-1} + X^n \in \mathbb{Z}[X].$$

Τότε, ο ε^{-1} είναι σημείο μηδενισμού του πολυωνύμου

$$1 + a_{n-1} X + \cdots + a_0 X^n$$

και άρα και του

$$g(X) = \frac{1}{a_0} + \frac{a_{n-1}}{a_0} X + \cdots + X^n \text{ , } a_i \in \mathbb{Z},$$

το οποίο είναι ανάγωγο, αφού και το $Irr(\varepsilon, \mathbb{Q})$ είναι ανάγωγο. Άρα

$$g(X) = Irr(\varepsilon^{-1}, \mathbb{Q}).$$

Κι εφόσον $\varepsilon^{-1} \in R_K$, τότε $Irr(\varepsilon^{-1}, \mathbb{Q}) \in \mathbb{Z}[X]$, οπότε και $\frac{1}{a_0} \in \mathbb{Z}$, δηλαδή $a_0 = \pm 1$. □

Γενικότερα, ισχύει ότι:

Προταση 1.5.3. *Αν ο αριθμός ε είναι σημείο μηδενισμού ενός μονικού πολυωνύμου με ακέραιους αλγεβρικούς συντελεστές και μονάδα στο σταθερό όρο, τότε είναι μονάδα.*

Πορισμα 1.5.4. *Ο αλγεβρικός αριθμός $\varepsilon \in K$ είναι μονάδα, αν είναι ακέραιος αλγεβρικός αριθμός και επιπρόσθετα ισχύει ότι*

$$N_K(\varepsilon) = \pm 1.$$

Παρατηρηση 1.5.5. Το αντίστροφο του παραπάνω θεωρήματος δεν είναι εν γένει αληθές. Επι παραδείγματι, ο αριθμός $\frac{3+4i}{5} \in \mathbb{Q}(i)$ έχει norm ίση με 1, αλλά δεν είναι μονάδα καθώς $Irr(\frac{3+4i}{5}, \mathbb{Q}) = X^2 - \frac{6}{5}X + 1 \notin \mathbb{Z}[X]$.

Μία εύκολη παρατήρηση για την ομάδα των μονάδων ενός αλγεβρικού σώματος αριθμών K, είναι ότι η ομάδα των ριζών της μονάδας που ανήκουν στο K είναι υποομάδα αυτής. Ιδιαίτερα, ισχύει το παρακάτω θεώρημα, το οποίο θα διατυπώσουμε εδώ στη γενική του μορφή, και θα το αποδείξουμε στο επόμενο κεφάλαιο στην ειδική περίπτωση των τετραγωνικών σωμάτων αριθμών.

Θεωρημα 1.5.6 (Dirichlet)**.** *Έστω K ένα αλγεβρικό σώμα αριθμών διακρίνουσας d_K. Υποθέτουμε ότι (r_1, r_2) είναι η υπογραφή του K και $r := r_1 + r_2 - 1$. Τότε υπάρχουν μονάδες $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r \in K$, τις οποίες καλούμε θεμελιώδεις, και μία ρίζα της μονάδας ζ μέγιστης τάξης m, με $m \mid 2d_K$, έτσι ώστε, κάθε άλλη μονάδα ε του K γραφεται υπό τη μορφή*

$$\varepsilon = \zeta^s {\varepsilon_1}^{s_1} {\varepsilon_2}^{s_2} \cdots {e_r}^{s_r} \text{ , } 0 \leq s \leq m \text{ , } s_i \in \mathbb{Z}.$$

Από το θεώρημα Dirichlet προκύπτει ότι η ομάδα των μονάδων του αλγεβρικού σώματος αριθμών K είναι μία πεπερασμένα παραγόμενη αβελιανή ομάδα βαθμίδας (rank) n και, μάλιστα, ισχύει ότι

$$\mathcal{U}_K \cong \langle \zeta \rangle \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle,$$

δηλαδή, η ομάδα των μονάδων είναι το ευθύ γινόμενο μίας κυκλικής ομάδας πεπερασμένης τάξης με πεπερασμένες στο πλήθος κυκλικές ομάδες άπειρης τάξης.

Τέλος, γνωρίζουμε από το θεμελιώδες θεώρημα της αριθμητικής ότι κάθε ακέραιος αριθμός γράφεται ως προσημασμένο γινόμενο πρώτων αριθμών, ήτοι ως γινόμενο μίας μονάδας του $\mathbb{Z}$ και πρώτων του $\mathbb{Z}$. Εγείρεται συνεπώς το ερώτημα, αν κάτι τέτοιο είναι αληθές και για το δακτύλιο R_K.

Ορισμος 1.5.7. Ένα μη μηδενικό στοιχείο a του δακτυλίου R των ακέραιων αλγεβρικών αριθμών του σώματος K θα καλείται *πρώτο* ή *ανάγωγο στοιχείο της R*, εάν δεν είναι μονάδα του R και δεν αναλύεται σε γινόμενο της μορφής $a = \alpha\beta$, όπου τα α και β δεν είναι μονάδες.[2].

Θεωρημα 1.5.8. *Στο δακτύλιο R_K, είναι πάντα δυνατή η ανάλυση σε γινόμενο πρώτων στοιχείων*

Απόδειξη. Θεωρούμε ένα μη μηδενικό στοιχείο $\alpha \in R_K$. Θα δείξουμε το ζητούμενο εφαρμόζοντας επαγωγή στην απόλυτη τιμή της norm του α. Εάν $|N_K(\alpha)| = 1$, τότε γνωρίζουμε ότι $\alpha \in \mathcal{U}_K$ οπότε το συμπέρασμα του θεωρήματος είναι αληθές. Υποθέτουμε τώρα, ότι το συμπέρασμα ισχύει για όλα τα στοιχεία του R_K, τα οποία έχουν norm $\leq |N_K(\alpha)|$. Ο α πλέον δεν είναι μονάδα. Ακόμα, δεν είναι ούτε πρώτος, αφού σε αντίθετη περίπτωση το θεώρημα θα ίσχυε τετριμμένα. Επομένως, υπάρχουν $\beta, \gamma \in R_K \setminus \mathcal{U}_K$, με την ιδιότητα $\alpha = \beta\gamma$. Άρα

$$N_K(\alpha) = N_K(\beta)N_K(\gamma) \text{ και } |N_K(\alpha)| > 1, |N_K(\alpha)| > 1,$$

απ' όπου προκύπτουν οι ανισότητες

$$1 < |N_K(\beta)| < |N_K(\alpha)| \text{ και } 1 < |N_K(\gamma)| < |N_K(\alpha)|.$$

Για τους β και γ το θεώρημα είναι αληθές λόγω της επαγωγική υπόθεσης, άρα γράφονται ως γινόμενο πρώτων αριθμών. Κι εφόσον γράφονται οι β και γ ως γινόμενο πρώτων παραγόντων, το αυτό ισχύει και για το γινόμενό τους. □

Παρατηρηση 1.5.9. Η μονοσήμαντη παραγοντοποίηση εν γένει δεν ισχύει. Επί παραδείγματι, ας υποθέσουμε το αλγεβρικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{-6})$. Ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του K είναι ο $R_K = \mathbb{Z}[\sqrt{-6}]$. Τότε έχουμε το εξής:

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

Θα δείξουμε ότι καθένας από τους αριθμούς $2, 3, -\sqrt{-6}$ και $\sqrt{-6}$ είναι πρώτος στο δακτύλιο R_K. Ας υποθέσουμε ότι το 2 δεν είναι πρώτος αριθμός στο δακτύλιο R_K, ήτοι έχει ανάλυση της μορφής

$$2 = (\alpha + \beta\sqrt{-6})(\gamma + \delta\sqrt{-6}),$$

[2]Εν γένει, οι έννοιες "πρώτο" και "ανάγωγο" στοιχείο δακτυλίου διαφέρουν, παρά ταύτα όταν κάνουμε λόγο για δακτυλίους ακεραίων αλγεβρικών αριθμών οι έννοιες ταυτίζονται καθώς, όπως θα δούμε στη συνέχεια, είναι περιοχές Noether.

όπου κανένας από τους αριθμούς $\alpha+\beta\sqrt{-6}$ και $\gamma+\delta\sqrt{-6}$ δεν είναι μονάδα του R_K. Τότε παίρνοντας norm έχουμε

$$(\alpha^2+6\beta^2)(\gamma^2+6\delta^2)=4.$$

Κι εφόσον θέλουμε κανένας από τους $\alpha+\beta\sqrt{-6}$ και $\gamma+\delta\sqrt{-6}$ να μην είναι μονάδα θα πρέπει να ισχύει ότι

$$\alpha^2+6\beta^2\neq 1\neq\gamma^2+6\delta^2.$$

Όμως οι norm ακέραιων αλγεβρικών αριθμών είναι ακέραιοι αριθμοί. Επομένως ισχύει ότι

$$\alpha^2+6\beta^2=\gamma^2+6\delta^2=2.$$

Ας ασχοληθούμε με την εξίσωση

$$\alpha^2+6\beta^2=2.$$

Εάν ο β είναι μη μηδενικό, τότε $6\beta^2\geq 6>2$. Αυτό σημαίνει ότι $\alpha^2<0$, το οποίο είναι άτοπο. Άρα $\beta=0$. Σε αυτή την περίπτωση έχουμε $\alpha^2=2\Rightarrow\alpha\notin\mathbb{Z}$, όποτε ξανά καταλήγουμε σε άτοπο. Έχουμε, λοιπόν, αντίφαση στην υπόθεση ότι ο 2 δεν είναι πρώτος αριθμός. Ομοίως αποδεικνύουμε και ότι το 3 και το $\sqrt{-6}$ είναι πρώτοι αριθμοί. Αυτό σημαίνει ότι για το 6 στο δακτύλιο $R_K=\mathbb{Z}[\sqrt{-6}]$ βρήκαμε δύο παραγοντοποιήσεις σε πρώτους αριθμούς.

1.6 Ιδεώδη

Η μέχρι τώρα μελέτη μας για τα αλγεβρικά σώματα αριθμών έχει αναδείξει μία μεγάλη διαφορά που έχουν αυτά συγκριτικά με το $\mathbb{Q}$. Αυτή είναι, όπως αναφέρεται και στην παρατήρηση 1.5.9, ότι για τους δακτυλίους των ακεραίων αλγεβρικών αριθμών δεν ισχύει εν γένει η μονοσήμαντη ανάλυση σε γινόμενο πρώτων στοιχείων. Η απάντηση στο πρόβλημα αυτό είναι η εισαγωγή της έννοιας των ιδεωδών του σώματος K, από τον Kummer στα μέσα του 19ου αιώνα. Τα ιδεώδη ενός σώματος έχουν μεν τις ιδιότητες των συνήθων ιδεωδών που γνωρίζουμε από τη θεωρία δακτυλίων, παρ' όλα αυτά δεν πρέπει να ταυτίζουμε τις δύο έννοιες.

Ορισμος 1.6.1. Ένα μη κενό υποσύνολο A του αλγεβρικού σώματος αριθμών K θα καλείται *ιδεώδες* αυτού, αν ικανοποιούνται οι παρακάτω συνθήκες:

(i) $A\neq\{0\}$[3].

(ii) Αν $a_1,a_2\in A$, τότε $a_1-a_2\in A$, ήτοι το A με την πράξη της πρόσθεσης αποτελεί ομάδα.

(iii) Αν $a\in A$ και $r\in R_K$, τότε $ra\in A$.

(iv) Υπάρχει $\delta\neq 0$ στο K, ώστε $\delta A\subseteq R_K$.

Όταν $A\subseteq R_K$, το A ονομάζεται *ακέραιο ιδεώδες*, αλλιώς αν $R_K\subseteq A\subseteq K$ τότε το A καλείται *κλασματικό ιδεώδες*.

Παρατηρηση 1.6.2. Μπορούμε να βελτιώσουμε τη συνθήκη (iv) του ορισμού. Χ.β.τ.γ. μπορούμε να υποθέσουμε ότι $\delta\in R_K$, διότι αν $\delta=\delta_1/m$, όπου $\delta_1\in R_K$ και $m\in\mathbb{N}$, τότε

$$\delta_1 A=\delta mA\subseteq\delta A\subseteq R_K.$$

Μάλιστα, παρατηρούμε ότι εάν έχουμε ένα κλασματικό ιδεώδες A του K, τότε υπάρχει ένας $\delta\in R_K$, τέτοιος ώστε $\delta A=:B\subseteq R_K\Rightarrow A=\delta^{-1}B$, ισότητα που αιτιολογεί τον όρο κλασματικό ιδεώδες.

Παρατηρηση 1.6.3. Τα ακέραια ιδεώδη του σώματος K αποτελούν ιδεώδη του δακτυλίου R_K με τη συνήθη έννοια. Έτσι, εάν το A είναι ακέραιο ιδεώδες του K τότε θα γράφουμε $A\trianglelefteq R_K$.

[3]Το μηδενικό ιδεώδες, στα πλαίσια της αλγεβρικής θεωρίας αριθμών δεν το λαμβάνουμε υπόψιν.

Πρέπει σε αυτό το σημείο να τονίσουμε ότι εάν επιλέξουμε ένα στοιχείο $a \in K$, τότε αυτό παράγει ένα κύριο ιδεώδες, το $\langle a \rangle = aR_K$, το οποίο είναι ιδεώδες του K. Μονάχα στην περίπτωση που ισχύει $a \in R_K$ το ιδεώδες $\langle a \rangle$ είναι ακέραιο.

Προφανώς εάν εξασφαλίσουμε ότι ένα ιδεώδες A του K περιέχει μία μονάδα του K, τότε θα περιέχει ολόκληρο τον R_K. Θα μπορούσε επομένως να είναι αυτός ο ορισμός του κλασματικού ιδεώδους. Αν από την άλλη $A \trianglelefteq R_K$ και το A περιέχει μία μονάδα του K, τότε κατ' ανάγκη $A = R_K$.

Στην πορεία πρόκειται να χρησιμοποιήσουμε την έννοια του αθροίσματος και του γινομένου ιδεωδών του K. Αυτά ορίζονται ως εξής:

$$A + B = \{\alpha + \beta | \alpha \in A \, , \beta \in B\}$$

$$AB = \{\sum_{\pi\varepsilon\pi.} \alpha\beta | \alpha \in A \, , \beta \in B\},$$

όπου A και B ιδεώδη του K. Ο λόγος είναι ότι τα ιδεώδη αυτά ενδεχομένως να είναι και ακέραια οπότε βάσει της παρατήρησης 1.6.3, οι ορισμοί πρέπει να συμφωνούν με αυτούς της θεωρίας των δακτυλίων. Για τον ίδιο ακριβώς λόγο, ορίζουμε την έννοια του διαιρείν δύο ιδεωδών του K, ως εξής:

$$\text{το } A \text{ διαιρεί το } B \;\Leftrightarrow A|B \Leftrightarrow B \equiv 0 \pmod{A} \Leftrightarrow B \subseteq A.$$

Θα λέμε ακόμα ότι το ιδεώδες A διαιρεί τον αριθμό $\alpha \in K$, όταν $A|\langle\alpha\rangle$. Επί τη βάσει αυτού ισχύει ότι

$$\langle\alpha\rangle|\langle\beta\rangle \Leftrightarrow \exists r \in R_K : \alpha = r\beta$$

και

$$\langle\alpha\rangle = \langle\beta\rangle \Leftrightarrow \exists \varepsilon \in \mathcal{U}_K : \alpha = \varepsilon\beta.$$

Προκύπτει επίσης ότι, εάν $A, B \trianglelefteq R_K$, τότε $\varepsilon.\kappa.\pi.(A, B) = A \cap B$ και $\mu.\kappa.\delta.(A, B) = A + B$. Υποθέτοντας επιπροσθέτως ότι $A + B = R_K$, τα A και B καλούνται *πρώτα μεταξύ τους*. Μάλιστα, το να είναι τα A και B πρώτα μεταξύ τους, είναι ισοδύναμο συμπέρασμα με αυτό της ύπαρξης στοιχείων $\alpha \in A$ και $\beta \in B$, με την ιδιότητα $\alpha + \beta = 1_{R_K}$.

Για τα ακέραια ιδεώδη A και B ισχύει ο συνολοθεωρητικός εγκλεισμός

$$AB \subseteq A \cap B,$$

με την ισότητα να ισχύει όταν τα ιδεώδη είναι πρώτα μεταξύ τους. Ο εν λόγω εγκλεισμός γενικεύεται για οποιαδήποτε n-άδα, ανά δύο πρώτων μεταξύ τους, ιδεωδεών του K, ήτοι

$$A_1A_1 \cdots A_n \subseteq A_1 \cap A_2 \cap \cdots \cap A_n.$$

Πρόταση 1.6.4. *Κάθε ιδεώδες A του αλγεβρικού σώματος αριθμών K περιέχει μη μηδενικούς φυσικούς αριθμούς.*

Απόδειξη. Έστω $\delta \in R_K$ τέτοιος ώστε $\delta A \subseteq R_K$. Αν υποθέσουμε ένα στοιχείο $0 \neq a \in A$, τότε ισχύει ότι $\delta a \in \subseteq R_K$ και κατά συνέπεια $0 \neq N_K(\delta a) \in \mathbb{Z}$. Όμως

$$N_K(\delta a) = (\delta a)^{(1)}(\delta a)^{(2)} \cdots (\delta a)^{(n)},$$

όπου $(\delta a)^{(i)}$, με $i = 1, 2, \ldots, n$ είναι οι συζυγείς αριθμοί του $(\delta a)^{(1)} = \delta a$. Αλλά οι συζυγείς ακέραιου αλγεβρικού αριθμού είναι επίσης ακέραιοι αλγεβρικοί, άρα

$$b = (\delta a)^{(2)}(\delta a)^{(3)} \cdots (\delta a)^{(n)} \in R_K.$$

Άρα από τη σχέση

$$N_K(\delta a) = \delta ab \in \mathbb{Z},$$

έπεται ότι $b \in K$, αφού $\delta a \in K$. Συνεπώς εφόσον $N_K(\delta a) = \delta ab$, λαμβάνουμε ότι $N_K(\delta a) \in A$ άρα και ότι $|N_K(\delta a)| \in A$. □

Παρατηρηση 1.6.5. Η παραπάνω πρόταση, όπως φανερώνει η απόδειξή της, μας δίνει ένα ενδιαφέρον αποτέλεσμα. Αν έχουμε ένα στοιχείο $a \in A$, όπου A ιδεώδες του K, τότε $N_K(a) \in A$.

1.7 Norm ακέραιου ιδεώδους

Αν υποθέσουμε ένα ιδεώδες $A \trianglelefteq R_K$, τότε μέσω της σχέσης ισοδυναμίας

$$a \sim b :\Leftrightarrow a - b \in A,$$

ορίζεται ο πηλικοδακτύλιος R_K/A, ο οποίος καλείται *δακτύλιος κλάσεων υπολοίπων* $(\mathrm{mod}\ A)$.

ΠΡΟΤΑΣΗ 1.7.1. *Αν $A \trianglelefteq R_K$, τότε ο R_K/A έχει πεπερασμένου πλήθους στοιχεία.*

Απόδειξη. Έστω $m \in \mathbb{N}$ ο ελάχιστος μη μηδενικός φυσικός αριθμός που ανήκει στο A, την ύπαρξη του οποίου εξασφαλίζει η πρόταση 1.6.4. Αν υποθέσουμε ότι το σύνολο $\{\omega_1, \omega_2, \ldots, \omega_n\}$ είναι μία βάση ακεραιότητας του K, τότε κάθε στοιχείο $a \in K$ γράφεται υπό τη μορφή μορφή

$$a = a_1\omega_1 + a_2\omega_1 + \cdots + a_n\omega_n.$$

Θεωρούμε τους φυσικούς αριθμούς $a_1', a_2', \ldots, a_n'$ με την ιδιότητα

$$0 \leq a_i' < m \text{ και } a_i' \equiv a_i \pmod{m}.$$

Τότε, αν

$$a' = a_1'\omega_1 + a_2'\omega_1 + \cdots + a_n'\omega_n$$

ισχύει

$$a - a' = (a_1 - a_1')\omega_1 + (a_2 - a_2')\omega_2 + \cdots + (a_n - a_n')\omega_n = mb,$$

όπου b είναι κάποιος ακέραιος αλγεβρικός του K. Άρα

$$a - a' = mb \in A.$$

Η τυχούσα, λοιπόν, κλάση ισοδυναμίας $(\mathrm{mod}\ A)$ έχει αντιπρόσωπο κάποιο a', του οποίου όμως η επιλογή, συνίσταται στην επιλογή των a_i'. Λόγω, όμως, της ανισότητας $0 \leq a_i' < m$, για το a' έχουμε m^n επιλογές, άρα

$$\#\left(R_K/A\right) < +\infty.$$

□

ΟΡΙΣΜΟΣ 1.7.2. Έστω $A \trianglelefteq R_K$. Ορίζουμε ως *norm του ακέραιου ιδεώδους* A, και τη συμβολίζουμε με $N_K(A)$, τον πληθάριθμο του πηλικοδακτυλίου R_K/A, ήτοι

$$N_K(A) := \#\left(R_K/A\right).$$

Χωρίς απόδειξη αναφέρουμε το παρακάτω αποτέλεσμα το οποίο είναι γενίκευση της παρατήρησης 1.6.5.

ΠΡΟΤΑΣΗ 1.7.3. *Για κάθε ακέραιο ιδεώδες A του R_K ισχύει ότι:*

$$N_K(A) \in A.$$

1.8 Βάσεις ιδεώδους

ΟΡΙΣΜΟΣ 1.8.1. Οι αριθμοί $a_1, a_2, \ldots, a_n \in A$, όπου το A είναι ιδεώδες του αλγεβρικού σώματος αριθμών K, βαθμού $[K : \mathbb{Q}] = n$, θα αποτελούν βάση του ιδεώδους A, αν είναι γραμμικά ανεξάρτητοι και επιπλέον ισχύει ότι

$$A = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z},$$

ήτοι κάθε αριθμός του A γράφεται υπό τη μορφή

$$a = \sum_{i=1}^{n} b_i a_i \ , \ b_i \in \mathbb{Z}.$$

Προφανώς η παράσταση αυτή είναι μονοσήμαντη.

Θεωρημα 1.8.2 (Ύπαρξη βάσης ιδεώδους)**.** *Κάθε ιδεώδες A του αλγεβρικού σώματος αριθμών έχει τουλάχιστον μία βάση.*

Απόδειξη. Κατ' αρχάς θεωρούμε ότι το ιδεώδες A είναι ακέραιο. Αν η $\{\omega_1, \omega_2, \ldots, \omega_n\}$ είναι μία βάση ακεραιότητας του K και $0 \neq a \in K$, τότε οι αριθμοί $a\omega_i$, όπου $i = 1, 2, \ldots, n$ είναι γραμμικά ανεξάρτητοι. Θεωρούμε το γραμμικά ανεξάρτητο σύνολο $\{a_1, a_2, \ldots, a_n\}$ με την ελάχιστη διακρίνουσα. Θα δείξουμε ότι η n-άδα αυτή είναι, πράγματι, βάση του ιδεώδους A. Κάθε αριθμός της μορφής

$$\sum_{i=1}^{n} b_i a_i \ , \ b_i \in \mathbb{Z},$$

είναι στοιχείο του A. Αρκεί, λοιπόν, να δείξουμε ότι κάθε αριθμός του A είναι αυτής της μορφής. Έστω ότι υπάρχει $a \in A$ της μορφής

$$\sum_{i=1}^{n} b_i a_i \ , \ b_i \in \mathbb{Q},$$

όπου τουλάχιστον ένας από τους b_i δεν είναι ακέραιος αριθμός. Επιθυμούμε να αποδείξουμε ότι αν υπάρχει ένας συντελεστής ο οποίος δεν είναι ακέραιος, τότε $a \notin A$. Έστω ότι $b_1 \in \mathbb{Q} \setminus \mathbb{Z}$. Αν θέσουμε $b_1' = b_1 - [b_1]$, όπου με $[b_1]$ συμβολίζουμε την απόλυτη τιμή του b_1, και

$$\beta = a - [b_1]a_1 = b_1' a_1 + b_2 a_2 + \cdots + b_n a_n,$$

τότε θα έχουμε:

$$\begin{aligned} |d(\beta, a_2, \ldots, a_n)| &= \left(\det \begin{pmatrix} b_1' & b_2 & \cdots & b_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \right)^2 |d(a_1, a_2, \ldots, a_n)| \\ &= (b_1')^2 |d(a_1, a_2, \ldots, a_n)| < |d(a_1, a_2, \ldots, a_n)|. \end{aligned}$$

Επειδή η διακρίνουσα $d(\beta, a_2, \ldots, a_n)$ είναι μη μηδενική, οι αριθμοί $\beta, a_2, \ldots, a_n$ είναι γραμμικά ανεξάρτητοι. Και λόγω της σχέσης

$$|d(\beta, a_2, \ldots, a_n)| < |d(a_1, a_2, \ldots, a_n)|,$$

έπεται ότι $\beta \notin A \Rightarrow a = \beta + [b_1]a_1 \notin A$. Απομένει η περίπτωση κατά την οποία το A δεν είναι ακέραιο. Τότε υπάρχει $\delta \in R_K$ τέτοιο ώστε το δA να είναι ακέραιο και τότε, αν τα $\delta a_1, \delta a_2, \ldots, \delta a_n$ από τελούν βάση του δA, τότε τα $a_1, a_2, \ldots, a_n$ είναι βάση του A. □

Παρατηρηση 1.8.3. Το θεώρημα αυτό μας λέει ότι κάθε ιδεώδες του R_K είναι πεπερασμένα παραγόμενο, γεγονός το οποίο μας πληροφορεί ότι ο R_K είναι *δακτύλιος της Noether*, ή αλλιώς *περιοχή Noether*.

Ποία είναι η σχέση της διακρίνουσας μίας βάσης ακεραιότητας του αλγεβρικού σώματος αριθμών K, με τη διακρίνουσα μίας βάσης οποιουδήποτε ιδεώδους του; Αν υποθέσουμε ότι τα $\omega_1, \omega_2, \ldots, \omega_n$ είναι βάση ακεραιότητας του K και τα $a_1, a_2, \ldots, a_n$ βάση του ιδεώδους A του K, τότε

$$d(a_1, a_2, \ldots, a_n) = N_K(A)^2 d(\omega_1, \omega_2, \ldots, \omega_n).$$

Μάλιστα, αν τα a_i είναι της μορφής

$$a_i = \sum_{j=1}^{n} a_{ij}\omega_j \ , \ a_{ij} \in \mathbb{Z} \ , \ i = 1, 2, \ldots, n,$$

τότε

$$N_K(A) = |\det\left((a_{ij})_{1\leq i,j\leq n}\right)|.$$

Αυτό μας οδηγεί στο συμπέρασμα ότι για τον αριθμό $a \in R_K$ ισχύει ότι

$$|N_K(a)| = N_K(\langle a\rangle).$$

Επιπροσθέτως, αν $a \in \mathbb{Z}$, τότε

$$N_K(\langle a\rangle) = |a|^n.$$

Για να έχουν νόημα οι ανωτέρω υπολογισμοί πρέπει το ιδεώδες $\langle a\rangle$ να είναι ακέραιο, το οποίο σημαίνει ότι ο αριθμός a είναι κατ' ανάγκη στοιχείο του δακτυλίου R_K.

1.9 Πρώτα ιδεώδη

Υπενθυμίζουμε σε αυτό το σημείο την παρατήρηση 1.5.9. Αυτή μας υποδεικνύει ότι μπορούμε να ορίσουμε πρώτα και μεγιστικά ιδεώδη του R_K, με τον ίδιο τρόπο που τα ορίζουμε για οποιοδήποτε μεταθετικό δακτύλιο με μοναδιαίο στοιχείο. Έτσι, δοθέντος ιδεώδους $P \lhd$ [4]R_K, τότε αυτό είναι *πρώτο* εάν, και μόνο εάν

$$P|\alpha\beta \Rightarrow P|\alpha \text{ ή } P|\beta,$$

όπου $\alpha, \beta \in R_K$. Γνωρίζουμε ότι $P \lhd R_K$ είναι πρώτο τότε, και μόνο τότε, όταν ο πηλικοδακτύλιος R_K/P είναι ακέραια περιοχή. Επιλέγουμε τώρα, ένα άλλο ιδεώδες $M \trianglelefteq R_K$. Τότε αυτό, θα το καλούμε *μεγιστικό* εάν, και μόνο εάν, ισχύει ότι

$$\forall A \trianglelefteq R_K : M \subseteq A \subseteq R_K \Rightarrow A = M \text{ ή } A = R_K.$$

Κατ' αντιστοιχία με τα πρώτα ιδεώδη, το να είναι μεγιστικό το M είναι ισοδύναμο με το να είναι ο πηλικοδακτύλιος R_K/M σώμα. Μάλιστα, σημειώνουμε ότι εφόσον ο R_K/P αποτελείται από πεπερασμένου πλήθους στοιχεία, οι έννοιες πρώτο και μεγιστικό ιδεώδες ταυτίζονται. Εύκολα προκύπτει ότι τα μόνα ακέραια ιδεώδη του R_K, τα οποία διαιρούν ένα πρώτο ιδεώδες P, είναι τα $\langle 1\rangle = R_K$ και το P. Επομένως ισχύει ότι κάθε $A \trianglelefteq R_K$ έχει ένα πρώτο διαιρέτη P. Όλα αυτά είναι γενικά αποτελέσματα της θεωρίας δακτυλίων, τα οποία προσαρμόζουμε στην περίπτωση του δακτύλιου των ακέραιων αλγεβρικών του K.

Θεωρημα 1.9.1. *Κάθε πρώτο ιδεώδες P του R_K περιέχει ακριβώς ένα πρώτο αριθμό $p \in \mathbb{P}$ για τον οποίο μάλιστα ισχύει ότι*

$$N_K(P) = p^f \text{ , όπου } f \in \mathbb{N} \setminus \{0\}.$$

Απόδειξη. Ο R_K/P είναι σώμα. Κι εφόσον $\#(R_K/P) < +\infty$, είναι πεπερασμένο σώμα. Ας υποθέσουμε ότι $char(R_K/P) = p \in \mathbb{P}$. Για το λόγο αυτό, το σώμα $\mathbf{F}_p$ περιέχεται ισόμορφα στο R_K/P. Μπορούμε επομένως να ορίσουμε την επέκταση σωμάτων $(R_K/P)/\mathbf{F}_p$ και να επιλέξουμε μία βάση αυτής, έστω την $\omega_1, \omega_2, \ldots, \omega_n$. Έτσι, το τυχόν στοιχείο $a \in R_K/P$ έχει τη μορφή:

$$a = \sum_{i=1}^{f} a_i\omega_i \text{ , } a_i \in \mathbf{F}_p.$$

Από τον τύπο αυτό συμπεραίνουμε ότι για το a έχουμε p^f επιλογές, ήτοι

$$N_K(P) = p^f.$$

[4]Με το σύμβολο αυτό, εννοούμε ότι $P \trianglelefteq R_K$ και $P \neq R_K$.

Επειδή δε ισχύει ότι $N_K(P) \in P$, βάσει της πρότασης 1.7.3 λαμβάνουμε ότι $p^f \in P \Rightarrow p \in P$, μιας και το P είναι πρώτο. Θα δείξουμε τη μοναδικότητα του πρώτου αριθμού p. Αν υποθέσουμε ότι ο $m \in \mathbb{N}$ είναι ο ελάχιστος ο φυσικός που ανήκει στο P, τότε

$$p = ml + r \, , 0 \leq r < m.$$

Ομως, θα πρέπει να ισχύει ότι $r = 0$, διότι διαφορετικά θα είχαμε $r \in P$ και $r < m$, το οποίο είναι άτοπο. Ακόμα ισχύει ότι $m \neq 1$, καθώς διαφορετικά το $P = R_K$ δε θα ήταν πρώτο ιδεώδες. Άρα από τη σχέση $p = ml$ προκύπτει ότι $p = m$. Αυτό σημαίνει ότι ο p είναι ο ελάχιστος φυσικός που ανήκει στο ιδεώδες P. Έστω τώρα $q \in \mathbb{P}$, ο οποίος ανήκει στο P. Αν υποθέσουμε ότι

$$q = pl' + r' \, , 0 \leq r' < p,$$

τότε λόγω ιδιότητας του p θα πρέπει $r' = 0$, συνεπώς $q = pl'$. Κατ' ανάγκη λοιπόν ισχύει ότι $l' = 1 \Leftrightarrow q = p$. Άρα ο p είναι ο μοναδικός πρώτος που ανήκει στο P. □

Εάν θεωρήσουμε έναν πρώτο αριθμό p, τότε το ιδεώδες $\langle p \rangle$ έχει ένα πρώτο διαιρέτη, έστω το P. Για το ιδεώδες αυτό και τον πρώτο αριθμό p ισχύει ότι $p \in P$. Για κάθε πρώτο αριθμό p, λοιπόν, αντιστοιχεί ένα πρώτο ιδεώδες P που το περιέχει. Ακόμα, παρατηρούμε ότι για τα $p, q \in \mathbb{P}$ με $p \neq q$, τα ιδεώδη P και Q, για τα οποία $p \in P$ και $q \in Q$, είναι κατ' ανάγκη διαφορετικά, λόγω του θεωρήματος 1.9.1. Επομένως έχουμε αποδείξει το κατωτέρω αποτέλεσμα.

ΠΡΟΤΑΣΗ 1.9.2. *Υπάρχουν άπειρα πρώτα ιδεώδη του αλγεβρικού σώματος αριθμών K.*

ΟΡΙΣΜΟΣ 1.9.3. Έστω P, ένα πρώτο ιδεώδες του αλγεβρικού σώματος αριθμών K. Ορίζουμε ως *βαθμό* του πρώτου ιδεώδους P, το βαθμό f της επέκτασης σωμάτων $(R_K/P)/\mathbf{F}_p$. Με άλλα λόγια,

$$f := [R_K/P : \mathbf{F}_p]$$

και, μάλιστα, ισχύει ότι

$$N_K(P) = p^f,$$

όπου p είναι ο μοναδικός πρώτος αριθμός που ανήκει στο P.

1.10 Ανάλυση ιδεωδών σε γινόμενο πρώτων ιδεωδών

Μετά από όλα αυτά, είμαστε έτοιμοι να εισάγουμε το βασικό αποτέλεσμα που μας επιτρέπει να κάνουμε αριθμητική με ιδεώδη και να υπερπηδήσουμε το εμπόδιο της μονοσήμαντης παραγοντοποίησης στα στοιχεία του δακτυλίου των ακέραιων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών. Πριν όμως περάσουμε στο βασικό θεώρημα, αναφέρουμε κάποια προκαταρκτικά αποτελέσματα.

ΛΗΜΜΑ 1.10.1. *Αν $A \lhd R_K$, τότε υπάρχουν πρώτα ιδεώδη $P_1, P_2, \ldots, P_r$ με την ιδιότητα*

$$P_1 P_2 \cdots P_r \subseteq A.$$

Απόδειξη. (βλ. [2], σελ.211, Λημ. 13.2) □

ΛΗΜΜΑ 1.10.2. *Για κάθε $A \trianglelefteq R_K$, το σύνολο*

$$A^{-1} = \{x \in K | xA \subseteq R_K\},$$

αποτελεί ιδεώδες του K και μάλιστα, αν $A \neq R_K$, τότε $R_K \subseteq A^{-1}$.

Απόδειξη. (βλ. [2], σελ.212, Λημ. 13.3) □

Λημμα 1.10.3. *Αν $A \trianglelefteq R_K$ και ο αριθμός $s \in K$ έχει την ιδιότητα $sA \subseteq A$, τότε θα είναι ακέραιος αλγεβρικός αριθμός.*

Απόδειξη. (βλ. [2], σελ.213, Λημ. 13.4) □

Λημμα 1.10.4. *Για κάθε πρώτο ιδεώδες P του αλγεβρικού σώματος αριθμών K ισχύει ότι*

$$PP^{-1} = R_K.$$

Γενικότερα, αν $A \trianglelefteq R_K$, τότε

$$AA^{-1} = R_K.$$

Απόδειξη. (βλ. [2], σελ.214, Λημ. 13.5) □

Το βασικό μας αποτέλεσμα είναι το εξής:

Θεωρημα 1.10.5. *Τα ιδεώδη ενός αλγεβρικού σώματος αριθμών K αποτελούν αβελιανή ομάδα με πράξη τον πολλαπλασιασμό ιδεωδών.*

Απόδειξη. Προφανώς, η πράξη του πολλαπλασιασμού ιδεωδών είναι προσεταιριστική και μεταθετική. Το ιδεώδες $\langle 1 \rangle = R_K$ αποτελεί προφανώς το μοναδιαίο στοιχείο του πολλαπλασιασμού. Απομένει, λοιπόν, για ένα ιδεώδες A του K να προσδιορίσουμε το αντίστροφό του. Γνωρίζουμε ότι υπάρχει $\delta \in R_K$, με την ιδιότητα ότι το $B := \delta A$ είναι ακέραιο ιδεώδες. Τότε $A = \delta^{-1}B$. Θεωρώντας το ιδεώδες $A' = \delta B^{-1}$ λαμβάνουμε ότι

$$AA' = \delta^{-1}B\delta B^{-1} = \delta\delta^{-1}BB^{-1} = R_K.$$

Αυτό ολοκληρώνει την απόδειξή μας. □

Αν θεωρήσουμε τυχόν $A \trianglelefteq R_K$, τότε το αντίστροφο του ταυτίζεται με το ιδεώδες A^{-1}, που ορίστηκε στο λήμμα 1.10.3. Επεκτείνοντας επομένως τον ορισμό μας σε κάθε κλασματικό ιδεώδες A του K, το αντίστροφο του A είναι το ιδεώδες

$$A^{-1} = \{x \in K | xA \subseteq R_K\}.$$

Φυσιολογικά, λοιπόν, ορίζουμε την έννοια του διαιρείν για τα ιδεώδη ενός αλγεβρικού σώματος αριθμών K. Έτσι,

$$A|B \Leftrightarrow \exists \Gamma \trianglelefteq R_K : B = \Gamma A.$$

Στην περίπτωση όπου τα ιδεώδη είναι κύρια, έστω ότι $A = \langle \alpha \rangle$ και $B = \langle \beta \rangle$ ισχύει η ισοδυναμία:

$$\langle \alpha \rangle \mid \langle \beta \rangle \Rightarrow \exists r \in R_K : \beta = r\alpha.$$

Θα δείξουμε τώρα ότι, ενώ για τα στοιχεία του R_K η μονοσήμαντη παραγοντοποίηση εν γένει δεν ισχύει, για τα ιδεώδη του K έχουμε την επιθυμητή αυτή ιδιότητα. Αρχικά, δείχνουμε το ζητούμενο για τα ακέραια ιδεώδη του K.

Θεωρημα 1.10.6. *Κάθε γνήσιο ιδεώδες $A \trianglelefteq R_K$ αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών του K, μέχρις αναδιάταξης*[5] *αυτών.*

[5] Ο όρος "μέχρις αναδιάταξης" χρησιμοποιείται ως ελεύθερη μετάφραση της αγγλικής ορολογίας "up to rearrangement".

Απόδειξη. Κατ' αρχάς αποδεικνύουμε ότι η ανάλυση σε πρώτα ιδεώδη είναι εφικτή. Για το σκοπό αυτό θεωρούμε το σύνολο Ω όλων των ακεραίων ιδεωδών του K, διάφορων του R_K, για τα οποία το συμπέρασμα του θεωρήματος είναι ψευδές. Θα δείξουμε ότι $\Omega = \varnothing$. Υποθέτουμε το αντίθετο. Τότε υπάρχει μεγιστικό στοιχείο αυτού, έστω το A. Αν, λοιπόν, ο P είναι ένας πρώτος διαιρέτης του A, τότε

$$A \subsetneq AP^{-1} \subseteq R_K \Rightarrow AP^{-1} \notin \Omega \Rightarrow \exists P_2, P_2, \ldots, P_r : AP^{-1} = P_2P_3 \cdots P_r \Rightarrow A = P_1P_2 \cdots P_r,$$

όπου $P_1 := P$. Άρα $A \notin \Omega$, το οποίο είναι άτοπο. Άρα $\Omega = \varnothing$. Απομένει η απόδειξη του μονοσημάντου της ανάλυσης. Θα χρησιμοποιήσουμε τη μέθοδο της μαθηματικής επαγωγής. Θεωρούμε την ισότητα

$$P_1P_2 \cdots P_r = Q_1Q_2 \cdots Q_s,$$

όπου τα P_j και τα Q_j είναι πρώτα ιδεώδη του K. Αν $r = 1$, τότε

$$P_1 = Q_1Q_2 \cdots Q_s.$$

Χ.β.τ.γ. υποθέτουμε ότι $P_1|Q_1$. Όμως ως πρώτα ιδεώδη τα P_1 και Q_1 είναι και μεγιστικά, άρα $P_1 = Q_1$. Επομένως έχουμε ότι $Q_2 \cdots Q_s = R_K \Rightarrow R_K \subseteq Q_2 \cap Q_3 \cap \cdots \cap Q_s$. Αυτό όμως συνεπάγεται ότι $R_K \subseteq Q_i$,για κάθε $i = 2, 3, \ldots, r$, το οποίο είναι άτοπο εάν $s > 1$. Υποθέτουμε ότι η πρόταση ισχύει για $r - 1$ παράγοντες, ήτοι αν

$$P_2P_3 \cdots P_r = Q_2Q_3 \cdots Q_s,$$

τότε $r-1 = s-1 \Rightarrow r = s$ και τα Q_j αποτελούν αναδιάταξη των P_i. Επομένως, αφού από το πρώτο βήμα της επαγωγής ισχύει $P_1 = Q_1$, το αποτέλεσμα είναι άμεσο. □

Πορισμα 1.10.7. *Κάθε κλασματικό ιδεώδες A του αλγεβρικού σώματος αριθμών K, έχει μία μονοσήμαντη ανάλυση της μορφής*

$$A = \prod_P P^{a_P},$$

όπου το P διατρέχει όλα τα πρώτα ιδεώδη του K, και $a_P \in \mathbb{Z}$, σχεδόν όλοι ίσοι με το 0.

Απόδειξη. Έστω A ένα κλασματικό ιδεώδες του K. Υπάρχει ένας ακέραιος αλγεβρικός του K, έστω δ, για τον οποίο το ιδεώδες $B := \delta A$ είναι ακέραιο. Τότε ισχύει ότι $B = \langle\delta\rangle A$. Όμως $\delta \in R_K \Rightarrow \langle\delta\rangle \trianglelefteq R_K$. Οπότε

$$B = \prod_P P^{a_P}\ , \langle\delta\rangle = \prod_P P^{b_P},$$

όπου οι a_P και b_P είναι φυσικοί αριθμοί σχεδόν όλοι ίσοι με 0 και η ανάλυση αυτή των B και $\langle\delta\rangle$ είναι μονοσήμαντη. Επομένως, το A γράφεται μονοσήμαντα υπό τη μορφή

$$A = \prod_P P^{a_P - b_P},$$

όπου οι διαφορές $a_P - b_P$ είναι ακέραιοι αριθμοί, σχεδόν όλοι 0. □

Προταση 1.10.8. *Δοθέντων δύο ακέραιων ιδεωδών*

$$A = \prod_P P^{a_P} \text{ και } B = \prod_P P^{b_P}$$

ο μέγιστος κοινός διαιρέτης και το ελάχιστο κοινό πολλαπλάσιο αυτών, για τα οποία έχει ήδη γίνει λόγος, είναι τα ιδεώδη

$$A + B = \prod_P P^{\min\{a_P, b_P\}} \text{ και } A \cap B = \prod_P P^{\max\{a_P, b_P\}},$$

αντίστοιχα.

Απόδειξη. (βλ. [2], σελ.220, Θεώρ. 13.14) □

Επί τη βάσει της ανωτέρω πρότασης είναι άμεσο το παρακάτω αποτέλεσμα.

ΠΡΟΤΑΣΗ 1.10.9. *Για τα* $A, B \trianglelefteq R_K$ *ισχύει ότι*

$$AB = (A + B)(A \cap B).$$

Απόδειξη. (βλ. [2], σελ.221, Πόρ. 13.14) □

Επικεντρώνουμε την προσοχή μας στη σχέση που έχει η norm του γινομένου δύο ακέραιων ιδεωδών με το γινόμενο των norm αυτών. Αποδεικνύεται ότι αν $A, B \trianglelefteq R_K$, τότε μπορούμε να βρούμε ιδεώδες $\Gamma \trianglelefteq R_K$, το οποίο να είναι πρώτο ως προς το B και επιπλέον, το γινόμενο $A\Gamma$ να καθίσταται κύριο ιδεώδες. Βάσει αυτού εξάγουμε το συμπέρασμα το παρακάτω συμπέρασμα

ΠΡΟΤΑΣΗ 1.10.10. *Κάθε ακέραιο ιδεώδες παράγεται από δύο στοιχεία του* R_K*, το ένα εκ των οποίων επιλέγουμε αυθαίρετα.*

Απόδειξη. (βλ. [2], σελ.222, Θεώρ. 13.17) □

Χρησιμοποιώντας τα συμπεράσματα αυτά αποδεικνύεται (βλ. [2], σελ.222, Θεώρ. 13.18) το παρακάτω θεώρημα.

ΘΕΩΡΗΜΑ 1.10.11. *Αν* $A, B \trianglelefteq R_K$*, τότε ισχύει ότι*

$$N_K(AB) = N_K(A)N_K(B)$$

ΠΟΡΙΣΜΑ 1.10.12. *Έστω* $P \trianglelefteq R_K$ *ένα πρώτο ιδεώδες. Τότε*

$$N_K(P^n) = \big(N_K(P)\big)^n$$

Απόδειξη. Άμεση από το προηγούμενο θεώρημα. □

ΟΡΙΣΜΟΣ 1.10.13. Αν A είναι ένα κλασματικό ιδεώδες του αλγεβρικού σώματος αριθμών K και

$$A = \prod_P P^{a_P},$$

όπου $a_P \in \mathbb{Z}$, σχεδόν όλοι ίσοι με 0, είναι η ανάλυσή του σε γινόμενο πρώτων ιδεωδών, τότε η norm του A ορίζεται από τη σχέση

$$N_K(A) = \prod_P N_K(P)^{a_P}.$$

Είναι προφανές ότι $N_K(A) \in \mathbb{Q}$ για κάθε κλασματικό ιδεώδες A. Τέλος, από τον τρόπο που ορίστηκε η norm ενός κλασματικού ιδεώδους έπεται και η σχέση

$$N_K(AB) = N_K(A)N_K(B).$$

Ισχύει επομένως το εξής θεώρημα:

ΘΕΩΡΗΜΑ 1.10.14. *Η norm έχει την πολλαπλασιαστική ιδιότητα, ήτοι δοθέντων τυχόντων ιδεωδών* A *και* B *του αλγεβρικού σώματος αριθμών* K *ισχύει ότι*

$$N_K(AB) = N_K(A)N_K(B).$$

ΠΑΡΑΤΗΡΗΣΗ 1.10.15. Η διαφορά του θεωρήματος 1.10.14 από το θεώρημα 1.10.11 είναι ότι γενικεύει την πολλαπλασιαστική ιδιότητα της norm σε όλα τα ιδεώδη, ακέραια ή κλασματικά, του K. Το 1.10.11 αναφέρεται μόνο σε ακέραια ιδεώδη.

1.11 Αριθμός κλάσεων ιδεωδών

Θεωρούμε ένα αλγεβρικό σώμα αριθμών K και το δακτύλιο των ακέραιων αλγεβρικών αυτού, R_K. Ως I_K συμβολίζουμε το σύνολο όλων των ιδεωδών του K και ως P_K το σύνολο όλων των κύριων ιδεωδών $\langle\alpha\rangle$, με $\alpha \neq 0$, του K. Με την πράξη του πολλαπλασιασμού ιδεωδών τα σύνολα I_K και P_K δομούν αμφότερα ομάδες, για τις οποίες μάλιστα ισχύει λόγω της μεταθετικότητας της πράξης ότι $P_K \trianglelefteq I_K$, ήτοι η P_K αποτελεί κανονική υποομάδα της I_K. Μπορούμε επομένως να ορίσουμε την πηλικοομάδα I_K/P_K. Αυτή καλείται *ομάδα κλάσεων ιδεωδών του* K και στα πλαίσια αυτής της εργασίας θα τη συμβολίζουμε ως $Cl(K)$. Ο πληθάριθμος της ομάδας $Cl(K)$ ονομάζεται *αριθμός κλάσεων ιδεωδών* και συμβολίζεται ως h_K, δηλαδή

$$h_K := \#\big(Cl(K)\big).$$

Δύο ιδεώδη A και B ανήκουν στην ίδια κλάση της $Cl(K)$ εξ ορισμού εάν

$$\exists \gamma, \delta \in R_K \ : \ \gamma A = \delta B.$$

Όταν ισχύει αυτό για τα A και B θα γράφουμε $A \sim B$. Αν θεωρήσουμε ότι το ιδεώδες A είναι κλασματικό, τότε υπάρχει $\delta \in R_K$ τέτοιο ώστε το ιδεώδες $\Gamma = \delta A$ να είναι ακέραιο. Εξ ορισμού λοιπόν του Γ λαμβάνουμε ότι $A \sim \Gamma$. Το συμπέρασμα είναι ότι κάθε κλάση της $Cl(K)$ περιέχει τουλάχιστον ένα ακέραιο ιδεώδες.

Στόχος μας είναι να δείξουμε ότι η ομάδα που κατασκευάσαμε είναι πεπερασμένη. Για το λόγο αυτό θα χρειαστούμε κάποια αποτελέσματα, των οποίων την απόδειξη θα παραλείψουμε.

Λημμα 1.11.1. *Για κάθε $0 \neq s \in \mathbb{N}$ υπάρχουν πεπερασμένου πλήθους ακέραια ιδεώδη του αλγεβρικού σώματος αριθμών K με norm το s.*

Απόδειξη. (βλ. [2], σελ.231, Λήμ.14.2) □

Λημμα 1.11.2. *Για κάθε αλγεβρικό σώμα αριθμών K υπάρχει ένας φυσικός αριθμός $m > 0$ τέτοιος, ώστε για κάθε $A \trianglelefteq R_K$ να υπάρχει $0 \neq a \in A$ με την ιδιότητα*

$$|N_K(a)| \leq m \cdot N_K(A)$$

Απόδειξη. (βλ. [2], σελ.231, Λήμ.14.3) □

Θεωρημα 1.11.3. *Ο αριθμός h_K είναι πεπερασμένος.*

Απόδειξη. Θεωρούμε τον αριθμό m του λήμματος 1.11.2. Σύμφωνα με το λήμμα 1.11.1 υπάρχουν πεπερασμένου πλήθους ακέραια ιδεώδη $A_1, A_2, \ldots, A_r$ με την ιδιότητα

$$|N_K(A_i)| \leq m.$$

Θα δείξουμε ότι για κάθε ιδεώδες A του K υπάρχει κάποιο A_i, όπου $i \in \{1, 2, \ldots, r\}$ τέτοιο, ώστε $A \sim A_i$. Αρχικά, έστω $\delta \in R_K$ για το οποίο ισχύει ότι $B := \delta A \trianglelefteq R_K$. Τότε $B \sim A$. Επομένως αρκεί να δείξουμε το ζητούμενο για ακέραια ιδεώδη. Χ.β.τ.γ. υποθέτουμε ότι $A \trianglelefteq R_K$. Για το ιδεώδες A^{-1} μπορούμε να βρούμε κάποιο στοιχείο $\delta_0 \in R_K$ για το οποίο ισχύει ότι $\Gamma := \delta_0 A^{-1} \trianglelefteq R_K$. Εφαρμόζοντας το λήμμα 1.11.2 λαμβάνουμε ότι

$$N_K(\langle\beta\rangle) = |N_K(\beta)| \leq m \cdot N_K(\delta_0 A^{-1}),$$

για κάποιο μη μηδενικό $\beta \in \delta_0 A^{-1}$. Όμως ισχύει ότι $\beta {\delta_0}^{-1} A \trianglelefteq R_K$. Συνεπώς έχουμε

$$N_K(\beta {\delta_0}^{-1} A) N_K(\langle\delta_0\rangle) = N_K(\beta A) = N_K(A) N_K(\langle\beta\rangle) \leq N_K(A) N_K({\delta_0}^{-1} A) m = m \cdot N_K(\langle\delta_0\rangle)$$

$$\Rightarrow N_K(\beta{\delta_0}^{-1}A) \leq m.$$

Από την τελευταία ανισότητα συμπεραίνουμε ότι υπάρχει κάποιος δείκτης $i \in \{1, 2, \ldots, r\}$ για τον οποίο να ισχύει ότι

$$\beta{\delta_0}^{-1}A = A_i \Rightarrow \beta A = \delta_0 A_i \Rightarrow A \sim A_i.$$

□

ΘΕΩΡΗΜΑ 1.11.4. *Αν h_K είναι ο αριθμός κλάσεων ιδεωδών του σώματος K, τότε για κάθε ιδεώδες A του K, το A^{h_K} είναι ακέραιο ιδεώδες.*

Απόδειξη. Ο αριθμός h_K αποτελεί την τάξη τος ομάδας $Cl(K)$. Αυτό σημαίνει ότι για κάθε στοιχείο $I \in Cl(K)$ ισχύει ότι:

$$[I]_{Cl(K)}{}^{h_K} = 1_{Cl(K)}.$$

Όμως τα στοιχεία της $Cl(K)$ έχουν τη μορφή AH, όπου το A είναι ιδεώδες του K και H είναι η ομάδα όλων των κύριων ιδεωδών του K. Η ανωτέρω σχέση, λοιπόν, είναι ισοδύναμη με τη σχέση

$$(AH)^{h_K} = H \Leftrightarrow A^{h_K}H = H \Leftrightarrow A^{h_K} \in H,$$

το οποίο είναι και το ζητούμενο. □

1.12 Διακλάδωση και νόμος ανάλυσης

Θεωρούμε ένα αλγεβρικό σώμα αριθμών K και το δακτύλιο των ακέραιων αλγεβρικών αυτού, τον R_K. Εάν θεωρήσουμε ένα πρώτο αριθμό p, τότε επί τη βάσει του 1.10.6 το ιδεώδες $\langle p \rangle = pR_K$ γράφεται υπό τη μορφή

$$pR_K = {P_1}^{e_1}{P_2}^{e_2} \cdots {P_r}^{e_r},$$

όπου τα P_i, για $i = 1, 2, \ldots, r$, είναι τα μόνα πρώτα ιδεώδη του K που περιέχουν τον πρώτο αριθμό p. Επίσης οι εκθέτες e_i είναι οι μέγιστοι εκθέτες, ήτοι

$${P_i}^{e_i} \mid \langle p \rangle \text{ και } {P_i}^{e_i+1} \nmid \langle p \rangle.$$

ΟΡΙΣΜΟΣ 1.12.1. Ο αριθμός r των πρώτων ιδεωδών του K, τα οποία περιέχουν τον πρώτο αριθμό p καλείται *αριθμός αναλύσεως του p στο K*.

ΟΡΙΣΜΟΣ 1.12.2. Για κάθε $i = 1, 2, \ldots, r$, ο αριθμός e_i που ορίζεται από τη σχέση

$$pR_K = {P_1}^{e_1}{P_2}^{e_2} \cdots {P_r}^{e_r}$$

καλείται *δείκτης διακλαδώσεως του P_i στο K*. Αν $e_i = 1$ τότε το P_i καλείται *μη διακλαδιζόμενο στο K*. Αν από την άλλη $e_i > 1$ λέμε ότι το P_i είναι *διακλαδιζόμενο στο K*. Εάν, τώρα, ισχύει ότι $e_1 = e_2 = \cdots = e_r = 1$, τότε λέμε ότι ο πρώτος αριθμός p δε διακλαδίζεται στο K.Έτσι, εάν ένα από τα e_i είναι > 1 λέμε ότι ο p διακλαδίζεται στο K.

ΟΡΙΣΜΟΣ 1.12.3. Θεωρούμε τους βαθμούς αδρανείας $f_1, f_2, \ldots, f_r$ των ιδεωδών $P_1, P_2, \ldots, P_r$ που διαιρούν τον πρώτο αριθμό p, αντιστοίχως. Αν $f_i = 1$ τότε λέμε το ιδεώδες P_i καλείται *αδρανές στο K*. Αν δε ισχύει ότι $f_1 = f_2 = \cdots = f_r = 1$, τότε ο πρώτος αριθμός p καλείται *αδρανής* στο K.

Οι παραπάνω ορισμοί δόθηκαν με την προϋπόθεση ότι γνωρίζουμε την ανάλυση του ιδεώδους $\langle p \rangle$ για τον τυχαίο πρώτο αριθμό p. Η διαδικασία που ακολουθούμε για την εύρεση της αναλύσεως ενός πρώτου αριθμού ονομάζεται *νόμος ανάλυσης για το K*. Ο προσδιορισμός του νόμου αναλύσεως είναι ένα ιδιαίτερα σημαντικό και θέμα της αλγεβρικής θεωρίας αριθμών.

Στα πλαίσια της παρούσας μελέτης θα επιμείνουμε σε αβελιανές επεκτάσεις του σώματος των ρητών αριθμών, ήτοι σε επεκτάσεις σωμάτων Galois, των οποίων η ομάδα Galois είναι αβελιανή.

Θεωρημα 1.12.4. *Θεωρούμε ένα αλγεβρικό σώμα αριθμών K και ένα πρώτο αριθμό p. Εάν η ανάλυση του αριθμού p είναι της μορφής*

$$pR_K = {P_1}^{e_1}{P_2}^{e_2}\cdots {P_r}^{e_r},$$

τότε ισχύει ότι

$$\sum_{i=1}^{r} e_i f_i = n,$$

όπου f_i είναι ο βαθμός αδρανείας του ιδεώδους P_i και $n = [K:\mathbb{Q}]$.

Απόδειξη. Παίρνοντας norm στη σχέση που μας δίνεται για το ιδεώδες έχουμε ότι

$$N_K(\langle p\rangle) = N_K\big({P_1}^{e_1}{P_2}^{e_2}\cdots {P_r}^{e_r}\big) = N_K\big({P_1}^{e_1}\big)N_K\big({P_2}^{e_2}\big)\cdots N_K\big({P_r}^{e_r}\big) \Rightarrow$$

$$p^n = p^{f_1e_1}p^{f_2e_2}\cdots p^{f_re_r} = p^{\sum_{i=1}^{r} e_if_i} \Rightarrow n = \sum_{i=1}^{r} e_if_i.$$

□

Πορισμα 1.12.5. *Αν $P \trianglelefteq R_K$ είναι ένα πρώτο ιδεώδες του αλγεβρικού σώματος αριθμών K, τότε ο βαθμός αδρανείας του και ο δείκτης διακλαδώσεως του δεν μπορούν να υπερβαίνουν το βαθμό της επέκτασης $K/\mathbb{Q}$.*

Πορισμα 1.12.6. *Το πλήθος των διακεκριμένων πρώτων ιδεωδών του K που περιέχουν ένα συγκεκριμένο πρώτο αριθμό p δεν μπορεί να υπερβαίνει το βαθμό της επέκτασης $K/\mathbb{Q}$.*

Το θεώρημα που ακολουθεί καθορίζει το νόμο ανάλυσης σε ένα αλγεβρικό σώμα αριθμών μόνο κατά την περίπτωση όπου αυτό έχει μία συγκεκριμένη βάση ακεραιότητας.

Θεωρημα 1.12.7 (Dedekind)**.** *Έστω αλγεβρικό σώμα αριθμών K, βαθμού n. Υποθέτουμε ότι υπάρχει κάποιος ακέραιος αλγεβρικός αριθμός $\theta \in R_K$ με την ιδιότητα το σύνολο $\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ να αποτελεί βάση ακεραιότητας του K. Θεωρούμε τον πρώτο αριθμό $p \in K$ και το ανάγωγο πολυώνυμο του θ, έστω το $p(X) := Irr(\theta,\mathbb{Q})$. Εάν η μονοσήμαντη ανάλυση του $p(X)$ στο δακτύλιο $\mathbb{Z}_p[X]$ είναι της μορφής*

$$p(X) \equiv p_1(X)^{e_1}p_2(X)^{e_2}\cdots p_r(X)^{e_r} \pmod{p},$$

τότε τα ιδεώδη

$$\langle p, p_i(\theta)\rangle = pR_K + p_i(\theta)R_K\ ,\ i = 1,2,\ldots,r$$

είναι πρώτα και ισχύει ότι

$$\langle p\rangle = {P_1}^{e_1}{P_2}^{e_2}\cdots {P_r}^{e_r}.$$

Απόδειξη. Εφόσον το σύνολο $\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ είναι βάση ακεραιότητας του K, τότε ο δακτύλιος των ακέραιων αλγεβρικών αυτού θα γράφεται υπό τη μορφή

$$R_K = \mathbb{Z} + \theta\mathbb{Z} + \cdots + \theta^{n-1}\mathbb{Z} = \mathbb{Z}[\theta].$$

Θεωρούμε για κάθε $i = 1,2,\ldots,r$ ένα σημείο μηδενισμού θ_i του πολυωνύμου $p_i(\theta) \pmod{p}$ στο σώμα $\mathbb{Z}_p(\theta_i) \cong \mathbb{Z}_p(X)/\langle p_i(X) \pmod{p}\rangle$. Θεωρούμε την απεικόνιση

$$\begin{array}{rcl} \psi_i & : & \mathbb{Z}[\theta] \longrightarrow \mathbb{Z}_p[\theta_i] \\ & & g(\theta) \longmapsto g(\theta_i) \pmod{p}. \end{array}$$

Αυτή είναι προφανώς ένα επιμορφισμός δακτυλίων. Επομένως, εάν θέσουμε $P_i := Kerf(\psi_i)$, τότε το P_i είναι ακέραιο ιδεώδες του K και επί τη βάσει του πρώτου θεωρήματος των ισομορφισμών θα έχουμε ότι

$$\mathbb{Z}[\theta]/P_i \cong \mathbb{Z}_p[\theta_i].$$

Όπως το $\mathbb{Z}_p[\theta_i]$ είναι σώμα, από το οποίο συνεπάγεται ότι το P_i είναι μεγιστικό ιδεώδες του K και κατά συνέπεια πρώτο. Αποδεικνύουμε, τώρα, την ισότητα $P_i = \langle p, p_i(\theta)\rangle$. Προφανώς ισχύει ότι

$$\langle p, p_i(\theta)\rangle \subseteq P_i.$$

Θα δείξουμε τον αντίστροφο εγκλεισμό. Προς τούτο θεωρούμε ένα τυχαίο στοιχείο $g(\theta) \in P_i$. Τότε θα ισχύει ότι $g(\theta_i) \equiv 0 \pmod p$, άρα θα υπάρχει πολυώνυμο $h(X) \in \mathbb{Z}[X]$ τέτοιο, ώστε να ισχύει ότι

$$g(X) \equiv p_i(X)h(X) \pmod p \Rightarrow g(X) - p_i(X)h(X) \equiv 0 \pmod p.$$

Αυτό σημαίνει ότι όλοι οι συντελεστές του πολυωνύμου $g(X) - p_i(X)h(X)$ είναι διαιρετοί δια p. Έχουμε ότι

$$g(\theta) = g(\theta) - p_i(\theta)h(\theta) + p_i(\theta)h(\theta).$$

Κι εφόσον $g(\theta) - p_i(\theta)h(\theta) \in \langle p\rangle \subseteq \langle p, p_i(\theta)\rangle$ και $p_i(\theta)h(\theta) \in \langle p_i(\theta)\rangle \subseteq \langle p, p_i(\theta)\rangle$, τότε έχουμε ότι $P_i \subseteq \langle p, p_i(\theta)\rangle$, γεγονός που ολοκληρώνει την απόδειξή της ισότητας $P_i = \langle p, p_i(\theta)\rangle$. Τέλος, πρέπει να δείξουμε ότι η ανάλυση του $\langle p\rangle$ είναι πράγματι η ${P_1}^{e_1}{P_2}^{e_2}\cdots{P_r}^{e_r}$. Έχουμε ότι

$$ {P_1}^{e_1}{P_2}^{e_2}\cdots{P_r}^{e_r} \subseteq \langle p, p_1(\theta)\rangle^{e_1}\langle p, p_2(\theta)\rangle^{e_2}\cdots\langle p, p_r(\theta)\rangle^{e_r} = $$

$$ (\langle p\rangle + \langle p_1(\theta)\rangle)^{e_1}(\langle p\rangle + \langle p_2(\theta)\rangle)^{e_2}\cdots(\langle p\rangle + \langle p_r(\theta)\rangle)^{e_r} \subseteq $$

$$ \langle p\rangle + \langle p_1(X)^{e_1}p_2(X)^{e_2}\cdots p_r(X)^{e_r}\rangle = \langle p, p(\theta)\rangle = \langle p\rangle. $$

Άρα ισχύει ότι $\langle p\rangle \mid {P_1}^{e_1}{P_2}^{e_2}\cdots{P_r}^{e_r}$. Αυτό σημαίνει ότι

$$\langle p\rangle = {P_1}^{m_1}{P_2}^{m_2}\cdots{P_r}^{m_r}\ , 0 < m_i \leq e_i.$$

Παίρνοντας norm στη σχέση αυτή λαμβάνουμε ότι

$$p^n = N_K(P_1)^{e_1}N_K(P_2)^{e_2}\cdots N_K(P_r)^{e_r}.$$

Αληθεύει όμως ότι

$$N_K(P_i) = \#(\mathbb{Z}(\theta)/P_i) = \#(\mathbb{Z}_p(\theta_i)) = p^{f_i},$$

όπου f_i είναι ο βαθμός του πολυωνύμου $p_i(X) \pmod p$. Συνεπώς έχουμε

$$p^n = N_K(P_1)^{e_1}N_K(P_2)^{e_2}\cdots N_K(P_r)^{e_r} = p^{\sum_{i=1}^r m_i f_i} \Rightarrow$$

$$n = \sum_{i=1}^{r} m_i f_i.$$

Όμως γνωρίζουμε ότι

$$n = \sum_{i=1}^{n} e_i f_i$$

και

$$m_i \leq e_i\ , \forall\ i = 1, 2, \ldots, r.$$

Αυτό σημαίνει ότι κατ' ανάγκη ισχύει ότι $m_i = e_i$, για κάθε $i = 1, 2, \ldots, r$. Με τη διαπίστωση αυτή ολοκληρώνεται η απόδειξή μας. □

Τό ερώτημα που τίθεται ύστερα από τη διατύπωση του ανωτέρω αποτελέσματος είναι τι συμβαίνει στην περίπτωση όπου το αλγεβρικό σώμα K δεν έχει βάση ακεραιότητας της μορφής $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$. Η απάντηση είναι ότι δε γνωρίζουμε ποια είναι η βάση ακεραιότητας σε αυτή την περίπτωση.

Παρ' όλο που το θεώρημα Dedekind δεν έχει καθολική ισχύ, ήτοι υπάρχουν αλγεβρικά σώματα αριθμών για τα οποία δεν ισχύει, υπάρχει ένα θεώρημα το οποίο αποτελεί ένα κριτήριο που αποφασίζει πότε ένας πρώτος αριθμός διακλαδίζεται σε ένα αλγεβρικό σώμα αριθμών.

ΘΕΩΡΗΜΑ 1.12.8 (Θεώρημα διακλαδώσεως πρώτων αριθμών)**.** *Θεωρούμε ένα αλγεβρικό σώμα αριθμών K, διακρίνουσας d_K. Τότε ο πρώτος αριθμός p διακλαδίζεται στο K εάν, και μόνο εάν ισχύει ότι $p \mid d_K$.*

Το θεώρημα διακλαδώσεως πρώτων αριθμών ουσιαστικά συσχετίζει τη διακρίνουσα του αλγεβρικού σώματος με την έννοια της διακλάδωσης. Ένα σημαντικό αποτέλεσμα προς αυτή την κατεύθυνση είναι το παρακάτω, του οποίου την απόδειξη παραλείπουμε λόγω του ότι απαιτεί γνώση εννοιών που δεν έχουμε πραγματευτεί.

ΘΕΩΡΗΜΑ 1.12.9 (Θεώρημα διακρίνουσας του Minkowski)**.** *Έστω αλγεβρικό σώμα αριθμών K, βαθμού > 1. Η απόλυτη τιμή της διακρίνουσας του σώματος K είναι μεγαλύτερη της μονάδος, ήτοι*

$$|d_K| > 1.$$

Το θεώρημα διακρίνουσας του Minkowski μας δίνει ένα αρκετά ασθενές κάτω φράγμα για την απόλυτη τιμή της διακρίνουσας. Η αλήθεια είναι ότι μπορούμε να έχουμε ακριβές κάτω φράγμα όταν γνωρίζουμε το βαθμό της επέκτασης $K/\mathbb{Q}$. Παρά ταύτα, και σε αυτή του τη μορφη, το θεώρημα διακρίνουσας του Minkowski είναι ιδιαίτερα σημαντικό. Πράγματι, εφόσον γνωρίζουμε ότι $|d_K| > 1$, σύμφωνα με το θεμελιώδες θεώρημα της αριθμητικής υπάρχει κάποιος πρώτος αριθμός p με την ιδιότητα $p \mid d_K$. Η παρατήρηση αυτή σε συνδυασμό με το θεώρημα διακλαδώσεως των πρώτων αριθμών, μας οδηγεί στο παρακάτω πόρισμα:

ΠΟΡΙΣΜΑ 1.12.10. *Υπάρχει τουλάχιστον ένας διακλαδιζόμενος πρώτος αριθμός σε κάθε αλγεβρικό σώμα αριθμών $K \neq \mathbb{Q}$. Επιπροσθέτως, δοθέντος αλγεβρικού σώματος αριθμών, υπάρχουν πεπερασμένοι πρώτοι αριθμοί οι οποίοι διακλαδίζονται σε αυτό.*

Κεφάλαιο 2

Τετραγωνικά Αριθμητικά Σώματα

Στο παρόν κεφάλαιο θα μελετήσουμε σε βάθος την έννοια των τετραγωνικών σωμάτων αριθμών, τα οποία αποτελούν μια ειδική περίπτωση αλγεβρικών σωμάτων αριθμών. Πέρα από την αναγωγή αποτελεσμάτων του πρώτου κεφαλαίου στην ειδική αυτή περίπτωση, θα επεκτείνουμε τη μελέτη μας και σε νέα συμπεράσματα.

2.1 Εισαγωγικά στοιχεία

Αρχικά πρέπει να δώσουμε τον ορισμό του τετραγωνικού σώματος αριθμών. Ήδη στην εισαγωγή του κεφαλαίου αναφέρουμε ότι τα τετραγωνικά σώματα αριθμών είναι μία ειδική περίπτωση των αλγεβρικών σωμάτων αριθμών. Επομένως πρόκειται για σώματα, τα οποία είναι πεπερασμένες επεκτάσεις του $\mathbb{Q}$.

Ορισμος 2.1.1. Ένα σώμα ονομάζεται *τετραγωνικό σώμα αριθμών* όταν είναι επέκταση του σώματος των ρητών αριθμών βαθμού 2, ήτοι όταν

$$[K : \mathbb{Q}] = 2.$$

Ήδη από το θεώρημα 1.2.2 γνωρίζουμε ότι υπάρχει κάποιος αλγεβρικός αριθμός θ για τον οποίο ισχύει ότι:

$$K = \mathbb{Q}(\theta).$$

Εξ ορισμού του τετραγωνικού σώματος αριθμών λαμβάνουμε ότι

$$\deg\big(Irr(\theta, \mathbb{Q})\big) = [K : Q] = 2 \Rightarrow Irr(\theta, \mathbb{Q}) = X^2 + aX + b \in \mathbb{Q}[X].$$

Εφαρμόζοντας το μετασχηματισμό $X \longmapsto X - a/2$ και θέτοντας $b' := a^2/4 - b$ λαμβάνουμε ότι το ανάγωγο πολυώνυμο είναι της μορφής

$$p(X) := Irr(\theta, \mathbb{Q}) = X^2 - b'.$$

Προφανώς, εφόσον το $p(X)$ είναι ανάγωγο, το b' δεν είναι ίσο με τετράγωνο ρητού αριθμού και άρα ούτε και με το 0. Μπορούμε συνεπώς να γράψουμε το b' υπό τη μορφή

$$b' = m \cdot r^2,$$

όπου ο $m \in \mathbb{Z} \setminus \{0, 1\}$ είναι ελεύθερος τετραγώνου και $r \in \mathbb{Q}^\times$. Άρα τα σημεία μηδενισμού του $p(X)$ είναι τα $\pm r\sqrt{m}$. Κατά συνέπεια έχουμε ότι

$$K = \mathbb{Q}(\theta) = \mathbb{Q}(r\sqrt{m}) = \mathbb{Q}(\sqrt{m}).$$

Τα παραπάνω μας πληροφορούν ότι το τυχόν τετραγωνικό σώμα K έχει τη μορφή $\mathbb{Q}(\sqrt{m})$, όπου ο $m \in \mathbb{Z} \setminus \{0, 1\}$ είναι ελεύθερος τετραγώνου. Τα στοιχεία του σώματος αυτού είναι τα στοιχεία του συνόλου

$$\{\alpha + \beta\sqrt{m} \mid \alpha, \beta \in \mathbb{Q}\}.$$

Από αυτό, λοιπόν, το σημείο όταν κάνουμε λόγο για τετραγωνικό σώμα αριθμών θα εννοούμε το σώμα $\mathbb{Q}(\sqrt{m})$, με το m να έχει τις προαναφερθείσες ιδιότητες.

Πριν ολοκληρώσουμε αυτή την παράγραφο πρέπει να κάνουμε ένα ακόμα διαχωρισμό. Εάν ο m είναι θετικός ακέραιος τότε το σώμα $\mathbb{Q}(\sqrt{m})$ περιέχεται στο σώμα των πραγματικών αριθμών. Σε αυτή την περίπτωση το $\mathbb{Q}(\sqrt{m})$ καλείται *τετραγωνικό πραγματικό σώμα αριθμών*. Από την άλλη, αν $m < 0$ το σώμα ονομάζεται *τετραγωνικό μιγαδικό σώμα αριθμών*. Στα επόμενα κεφάλαια, η μελέτη μας θα επικεντρωθεί στα τετραγωνικά μιγαδικά σώματα αριθμών.

Επιθυμούμε τώρα να προσδιορίσουμε το δακτύλιο R_K όταν $K = \mathbb{Q}(\sqrt{m})$. Αρχικά, παρατηρούμε ότι ως επέκταση σωμάτων βαθμού 2 η $K/\mathbb{Q}$ είναι κανονική. Επιπλέον, αφού $char(\mathbb{Q}) = 0$ η $K/\mathbb{Q}$ είναι και διαχωρίσιμη. Άρα η $K/\mathbb{Q}$ είναι επέκταση Galois. Κάθε στοιχείο της ομάδας Galois της επέκτασης $K/\mathbb{Q}$ απεικονίζει σημεία μηδενισμού του αναγώγου πολυωνύμου του $\sqrt{m}$ σε σημεία μηδενισμού αυτού. Αυτό σημαίνει ότι

$$Gal(K/\mathbb{Q}) = \{Id, \sigma\},$$

όπου

$$Id : \alpha + \beta\sqrt{m} \longmapsto \alpha + \beta\sqrt{m}$$
$$\sigma : \alpha + \beta\sqrt{m} \longmapsto \alpha - \beta\sqrt{m}.$$

Έστω τυχόν $a \in K$. Το ανάγωγο πολυώνυμο του a είναι το

$$Irr(a, \mathbb{Q}) = X^2 - sX + p \in \mathbb{Q}[X],$$

όπου s είναι το άθροισμα των σημείων μηδενισμού του αναγώγου πολυωνύμου και p το γινόμενο αυτών.Όμως $s = a + \sigma(a)$ και $p = a \cdot \sigma(a)$. Όμως εξ ορισμού ισχύει ότι

$$Tr_K(a) = a + \sigma(a)$$

$$N_K(a) = a \cdot \sigma(a).$$

Επομένως το ανάγωγο πολυώνυμο γράφεται υπό τη μορφή

$$Irr(a, \mathbb{Q}) = X^2 - Tr_K(a) \cdot X + N_K(a) \in \mathbb{Q}[X].$$

Συνδυάζοντας τη μορφή αυτή του αναγώγου πολυωνύμου με τον ορισμό των ακέραιων αλγεβρικών αριθμών λαμβάνουμε την παρακάτω πρόταση.

ΠΡΟΤΑΣΗ 2.1.2. *Έστω τετραγωνικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{m})$. Ο αριθμός $a \in K$ είναι ακέραιος αλγεβρικός αριθμός εάν, και μόνο εάν,*

$$Tr_K(a) \in \mathbb{Z} \text{ και } N_K(a) \in \mathbb{Z}.$$

Θεωρούμε τον αριθμό

$$a = \frac{\alpha + \beta\sqrt{m}}{2}.$$

Θέλουμε να ελέγξουμε πότε αυτός είναι ακέραιος αλγεβρικός και πότε δεν είναι. Επί τη βάσει της τελευταίας πρότασης θα πρέπει να ισχύει ότι

$$Tr_K(a) \in \mathbb{Z} \text{ και } N_K(a) \in \mathbb{Z}.$$

Τότε

$$Tr_K(a) = a + \sigma(a) = \frac{\alpha+\beta\sqrt{m}}{2} + \sigma\left(\frac{\alpha+\beta\sqrt{m}}{2}\right) = \frac{\alpha+\beta\sqrt{m}}{2} + \frac{\alpha-\beta\sqrt{m}}{2} = \alpha \in \mathbb{Z}$$

και

$$N_K(a) = a \cdot \sigma(a) = \frac{\alpha+\beta\sqrt{m}}{2} \cdot \sigma\left(\frac{\alpha+\beta\sqrt{m}}{2}\right) = \frac{\alpha+\beta\sqrt{m}}{2} \cdot \frac{\alpha-\beta\sqrt{m}}{2} = \frac{\alpha^2-m\beta^2}{4} \in \mathbb{Z}.$$

Επομένως

$$\alpha, \frac{\alpha^2-m\beta^2}{4} \in \mathbb{Z} \Rightarrow \alpha^2 - 4\cdot\frac{\alpha^2-m\beta^2}{4} \in \mathbb{Z} \Rightarrow m\beta^2 \in \mathbb{Z}.$$

Εφόσον ο m είναι ελεύθερος τετραγώνων η σχέση $m\beta^2 \in \mathbb{Z}$ ισοδυναμεί με τη σχέση $\beta \in \mathbb{Z}$. Επανερχόμαστε στη συνθήκη

$$\frac{\alpha^2-m\beta^2}{4} \in \mathbb{Z} \Leftrightarrow \alpha^2 \equiv m\beta^2 \pmod 4.$$

Εδώ πρέπει να διακρίνουμε τις περιπτώσεις όπου $m \equiv 1 \pmod 4$ ή $m \equiv 2,3 \pmod 4$. Η περίπτωση $m \equiv 0 \pmod 4$ δεν υφίσταται καθώς έχουμε υποθέσει ότι ο m είναι ελεύθερος τετραγώνων.

- Έστω ότι $m \equiv 1 \pmod 4$. Τότε

$$\alpha^2 \equiv m\beta^2 \pmod 4 \Rightarrow \alpha^2 \equiv \beta^2 \pmod 4 \Rightarrow \alpha \equiv \beta \pmod 2$$

- Αν, από την άλλη, για το m ισχύει ότι $m \equiv 2,3 \pmod 4$, τότε

$$\alpha^2 \equiv 2\beta^2 \pmod 4 \text{ ή } \alpha^2 \equiv 3\beta^2 \pmod 4.$$

Εύκολα προκύπτει ότι οι δύο ισοδυναμίες έχουν λύση μόνο στην περίπτωση κατά την οποία

$$\alpha \equiv \beta \equiv 0 \pmod 2.$$

Έτσι, έχουμε έναν ακόμα χαρακτηρισμό των ακέραιων αλγεβρικών αριθμών, ο οποίος συνοψίζεται στην παρακάω πρόταση.

Πρόταση 2.1.3. *Ο αριθμός $a = \frac{\alpha+\beta\sqrt{m}}{2} \in \mathbb{Q}(\sqrt{m}) =: K$ είναι ακέραιος αλγεβρικός του K, εάν και μόνο εάν, πληρεί τις παρακάτω δύο ιδιότητες:*

(i) $\alpha, \beta \in \mathbb{Z}$,

(ii) $\alpha \equiv \beta \pmod 2$ *για* $m \equiv 1 \pmod 4$ *ή* $\alpha \equiv \beta \equiv 0 \pmod 2$ *για* $m \equiv 2,3 \pmod 4$.

Το ευθύ της ανωτέρω πρότασης το αποδείξαμε ήδη, ενώ το αντίστροφο έπεται άμεσα από το ότι $Tr_K(a), N_K(a) \in \mathbb{Z}$. Με την τελευταία πρόταση έχουμε προσδιορίσει πλήρως τα στοιχεία του R_K όταν $K = \mathbb{Q}(\sqrt{m})$. Το ερώτημα, λοιπόν, είναι αν θα μπορούσαμε με βάση το χαρακτηρισμό των στοιχείων του R_K να βρούμε μια βάση ακεραιότητας αυτού. Πράγματι, κάτι τέτοιο είναι εφικτό.

Θεωρημα 2.1.4. *Έστω τετραγωνικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{m})$. Μία βάση ακεραιότητας του R_K είναι είναι η $\{1, \omega\}$, όπου*

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} & , \alpha\nu\ m \equiv 1 \pmod 4 \\ \sqrt{m} & , \alpha\nu\ m \equiv 2,3 \pmod 4 \end{cases}.$$

Απόδειξη. Αρχικά δείχνουμε ότι σε κάθε περίπτωση οι αριθμοί 1 και ω είναι γραμμικά ανεξάρτητοι. Πράγματι, αν $m \equiv 1 \pmod 4$ και υποθέσουμε τη σχέση γραμμικής εξάρτησης

$$\lambda_1 \cdot 1 + \lambda_2 \cdot \omega = 0,$$

όπου τα λ_1 και λ_2 είναι ρητοί αριθμοί, τότε

$$\lambda_1 \cdot 1 + \lambda_2 \cdot \omega = 0 \Rightarrow \lambda_1 + \lambda_2 \cdot \frac{1+\sqrt{m}}{2} = 0 \Rightarrow \left(\lambda_1 + \frac{\lambda_2}{2}\right) + \frac{\lambda_2}{2} \cdot \sqrt{m} = 0 \Rightarrow$$

$$\begin{cases} \lambda_1 + \frac{\lambda_2}{2} = 0 \\ \frac{\lambda_2}{2} = 0 \end{cases} \Rightarrow \lambda_1 = \lambda_2 = 0.$$

Ομοίως πράττουμε κατά την περίπτωση όπου $m \equiv 2, 3 \pmod 4$. Θέλουμε τώρα να διαπιστώσουμε ότι πράγματι οι αριθμοί 1 και ω παράγουν τον R_K. Επικεντρωνόμαστε ξανά στην περίπτωση όπου $m \equiv 1 \pmod 4$. Τότε ο τυχόν αριθμός

$$a = \frac{\alpha + \beta\sqrt{m}}{2}$$

μπορεί να γραφεί ως

$$a = \frac{\alpha - \beta}{2} + \beta\omega.$$

Αφού $\alpha \equiv \beta \pmod 2$ ο αριθμός $\frac{\alpha-\beta}{2}$ είναι ακέραιος. Επομένως η ανωτέρω έκφραση του a είναι επιτρεπτή. Ομοίως στην περίπτωση όπου $m \equiv 2, 3 \pmod 4$ ο a γράφεται υπό τη μορφή

$$a = \frac{\alpha}{2} + \frac{\beta}{2}\sqrt{m}.$$

Πρέπει να παρατηρήσουμε ότι όταν $m \equiv 2, 3 \pmod 4$ έχουμε δείξει ότι $\alpha \equiv \beta \equiv 0 \pmod 2$. Άρα οι αριθμοί $\frac{\alpha}{2}$ και $\frac{\beta}{2}$ είναι ακέραιοι. Και η απόδειξη ολοκληρώθηκε □

Πορισμα 2.1.5. *Η διακρίνουσα d_K ενός τετραγωνικού σώματος αριθμών $K := \mathbb{Q}(\sqrt{m})$ είναι ίση με:*

$$d_K = \begin{cases} m & , \alpha\nu\ m \equiv 1 \pmod 4 \\ 4m & , \alpha\nu\ m \equiv 2, 3 \pmod 4 \end{cases}.$$

Το θεώρημα 2.1.4 μας πληροφορεί ότι, εάν $m \equiv 1 \mod 4$, τότε

$$R_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right],$$

και

$$R_K = \mathbb{Z}[\sqrt{m}],$$

αν $m \equiv 2, 3 \pmod 4$. Εφόσον η διακρίνουσα d_K του τετραγωνικού μιγαδικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ είναι είτε m, είτε $4m$, σύμφωνα με το παραπάνω πόρισμα, τότε ισχύει ότι

$$K = \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{d_K}).$$

Αν $m \equiv 1 \pmod 4$, τότε

$$d_K = m \Rightarrow \frac{d_K + \sqrt{d_K}}{2} = \frac{m + \sqrt{m}}{2} = \frac{m-1}{2} + \frac{1+\sqrt{m}}{2} \Rightarrow$$

$$\mathbb{Z}\left[\frac{d_K+\sqrt{d_K}}{2}\right]=\mathbb{Z}\left[\frac{m-1}{2}+\frac{1+\sqrt{m}}{2}\right]=\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]=R_K.$$

Αν, από την άλλη έχουμε $m\equiv 2,3 \pmod 4$, τότε

$$d_K=4m\Rightarrow\frac{d_K+\sqrt{d_K}}{2}=\frac{4m+\sqrt{4m}}{2}=2m+\sqrt{m}\Rightarrow$$

$$\mathbb{Z}\left[\frac{d_K+\sqrt{d_K}}{2}\right]=\mathbb{Z}\left[2m+\sqrt{m}\right]=\mathbb{Z}[\sqrt{m}]=R_K.$$

Οι ανωτέρω υπολογισμοί αποδεικνύουν την εξής πρόταση:

ΠΡΟΤΑΣΗ 2.1.6. *Έστω ένα τετραγωνικό σώμα αριθμών K με διακρίνουσα d_K. Τότε ισχύει ότι $K=\mathbb{Q}(\sqrt{d_K})$ και*

$$R_K=\mathbb{Z}\left[\frac{d_K+\sqrt{d_K}}{2}\right].$$

2.2 Μονάδες

Θεωρούμε τετραγωνικό αριθμητικό σώμα $K=\mathbb{Q}(\sqrt{m})$ και το δακτύλιο R_K των ακέραιων αλγεβρικών αυτού. Ενδιαφερόμαστε να μελετήσουμε την ομάδα των μονάδων του δακτυλίου R_K. Υπενθυμίζουμε ότι ο αριθμός $\varepsilon=\alpha+\beta\sqrt{m}\in R_K$ είναι μονάδα του δακτυλίου R_K τότε και μόνο τότε, όταν ισχύει ότι $N_K(\varepsilon)=\pm 1$. Εάν $m\equiv 2,3 \pmod 4$, τότε έχουμε ότι

$$N_K(\varepsilon)=\pm 1\Rightarrow\alpha^2-m\beta^2=\pm 1,$$

ενώ εάν $m\equiv 1 \pmod 4$, έχουμε ότι

$$\alpha^2+\alpha\beta+\frac{1-m}{4}\beta^2=\pm 1.$$

Για να διευκολύνουμε τη μελέτη μας θα διακρίνουμε περιπτώσεις.

Έστω ότι $m<0$. Εάν $m\equiv 2,3 \pmod 4$, τότε έχουμε ότι $\alpha^2-m\beta^2>0$. Άρα εναπομένει να εξετάσουμε μόνο την περίπτωση

$$\alpha^2+|m|\beta^2=1.$$

Αν $|m|>1$, τότε η μόνη λύση είναι η $(\alpha,\beta)=(\pm 1,0)\Rightarrow\varepsilon=\pm 1$. Αν $m=-1$, έχουμε $\alpha^2+\beta^2=1$, από την οποία λαμβάνουμε άμεσα τις λύσεις $(\alpha,\beta)=(\pm 1,0)$ ή $(0,\pm 1)\Rightarrow\varepsilon\in\{\pm 1,\pm i\}$. Υποθέτουμε, τώρα, ότι $m\equiv 1 \pmod 4$. Εφόσον ισχύει ότι

$$\alpha^2+\alpha\beta+\frac{1-m}{4}\beta^2=\left(\alpha+\frac{\beta}{2}\right)^2+\frac{|m|\beta^2}{4}\geq 0,$$

είναι αρκετό να επιλύσουμε την

$$\alpha^2+\alpha\beta+\frac{1-m}{4}\beta^2=\left(\alpha+\frac{\beta}{2}\right)^2+\frac{|m|\beta^2}{4}=1.$$

Εάν $|m|>4$, τότε $(\alpha,\beta)=(\pm 1,0)\Rightarrow\varepsilon=\pm 1$. Αν από την άλλη έχουμε $|m|\leq 4$, από τη συνθήκη $m\equiv 1 \pmod 4$ αρκεί να εξετάσουμε την περίπτωση $m=-3$. Σε αυτή την περίπτωση έχουμε ότι

$$\left(\alpha+\frac{\beta}{2}\right)^2+\frac{3\beta^2}{4}=1.$$

Προφανώς, για $|\beta| \geq 2$ η ανωτέρω εξίσωση είναι αδύνατη. Για $b = 1$, λαμβάνουμε την

$$\alpha^2 + \alpha + 1 = 1 \Rightarrow \alpha = 0 \text{ ή } -1,$$

ήτοι $(\alpha, \beta) = (1, 0)$ ή $(0, 1) \Rightarrow \varepsilon \in \{1, i\}$. Για $\beta = 0$ λαμβάνουμε ότι $\alpha = \pm 1$, ενώ για $b = -1$ ότι $\alpha = 0$. Άρα οι μονάδες σε αυτή την περίπτωση είναι οι

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

Έτσι, καταλήγουμε στο εξής θεώρημα:

Θεωρημα 2.2.1. *Θεωρούμε το τετραγωνικό μιγαδικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{m})$. Η ομάδα $\mathcal{U}_K$ των μονάδων του δακτυλίου R_K των ακέραιων αλγεβρικών αριθμών του K είναι η εξής:*

$$\mathcal{U}_K := \begin{cases} \{\pm 1\} & , \alpha\nu\ m \neq -1, -3 \\ \{\pm 1, \pm i\} & , \alpha\nu\ m = -1 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} & , \alpha\nu\ m = -3 \end{cases}.$$

Εναπομένει η περίπτωση, κατά την οποία $m > 0$. Η περίπτωση αυτή απαιτεί πιο σύνθετη αντιμετώπιση. Αρχικά, πρέπει να παρατηρήσουμε ότι στην περίπτωση $m < 0$, το πλήθος των μονάδων είναι πεπερασμένο. Εδώ, θα αποδείξουμε ότι κάθε τετραγωνικό πραγματικό σώμα έχει άπειρες στο πλήθος μονάδες.

Λημμα 2.2.2. *Για κάθε πραγματικό αριθμό a και για κάθε φυσικό αριθμό n, υπάρχει ένα ζεύγος $(r, s) \in \mathbb{Z} \times \mathbb{Z}$, με την ιδιότητα*

$$|ar - s| \leq \frac{1}{n} \text{ και } 1 \leq r \leq n.$$

Απόδειξη. (βλ. [2], σελ. 245, Λήμ.14.5) □

Λημμα 2.2.3. *Για κάθε φυσικό αριθμό n, υπάρχει ένας ακέραιος αριθμός αλγεβρικός αριθμός a του τετραγωνικού πραγματικού αριθμητικού σώματος $K = \mathbb{Q}(\sqrt{m})$ τέτοιος, ώστε να ισχύει*

$$|a| \leq \frac{1}{n} \text{ και } N_K(a) < 1 + \sqrt{d_K},$$

όπου ως d_K συμβολίζουμε τη διακρίνουσα του σώματος K.

Απόδειξη. (βλ. [2], σελ.246, Λήμ. 16.6) □

Λημμα 2.2.4. *Αν ο μ είναι ένας θετικός πραγματικός αριθμός και το K είναι ένα πραγματικό τετραγωνικό σώμα αριθμών, τότε υπάρχουν πεπερασμένου πλήθους ακέραιοι αλγεβρικοί αριθμοί a του K τέτοιοι, ώστε*

$$|a^{(i)}| \leq \mu$$

για όλους τους συζυγείς αριθμούς $a^{(i)}$ του a.

Απόδειξη. (βλ. [2], σελ.247, Λήμ. 16.7) □

Τα παραπάνω λήμματα είναι αναγκαία για την απόδειξη του παρακάτω θεωρήματος, το οποίο προσδιορίζει τη μορφή του συνόλου $\mathcal{U}_K$ των μονάδων του K.

Θεωρημα 2.2.5. *Έστω τετραγωνικό πραγματικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{m})$ και έστω $\mathcal{U}_K$ η ομάδα των μονάδων του K. Υπάρχει μία μονάδα ε_0 τέτοια, ώστε το $\mathcal{U}_K$ να γράφεται υπό τη μορφή*

$$\mathcal{U}_K = \{\pm {\varepsilon_0}^k \mid k \in \mathbb{Z}\}.$$

Απόδειξη. Σύμφωνα με το λήμμα 2.2.3 υπάρχει ένας αριθμός $0 \neq a_1 \in R_K$ τέτοιος ώστε να ισχύει ότι

$$|a_1| < \frac{1}{1} = 1 \text{ και } |N_K(a_1)| < 1 + \sqrt{d_K},$$

όπου ως d_K συμβολίζουμε τη διακρίνουσα του σώματος K. Επιλέγουμε ένα φυσικό αριθμό n_2 με την ιδιότητα

$$n_2 > \frac{1}{|a_1|}.$$

Τότε, υπάρχει ένας αριθμός $0 \neq a_2 \in R_K$, σύμφωνα ξανά με το λήμμα 2.2.3, με την ιδιότητα

$$|a_2| < \frac{1}{n_2} < |a_1| \text{ και } |N_K(a_2)| < 1 + \sqrt{d_K}.$$

Επαναλαμβάνοντας τη διαδικασία αυτή, μπορούμε να βρούμε άπειρο πλήθος ακεραίων αλγεβρικών αριθμών με την ιδιότητα

$$|N_K(a_1)| < 1 + \sqrt{d_K}.$$

Όμως γνωρίζουμε ότι $N_K(a) \in \mathbb{Z}$, όταν $a \in R_K$. Συνεπώς, υπάρχει ένας φυσικός αριθμός $s \in [1, 1 + \sqrt{d_K}]$ τέτοιος, ώστε η εξίσωση

$$|N_K(a)| = s$$

να ικανοποιείται για άπειρο πλήθος $a \in R_K$. Θεωρούμε, τώρα, το κύριο ιδεώδες $\langle s \rangle = sR_K$. Επί τη βάσει της προτάσεως 1.7.1 ισχύει ότι

$$\#(R_K/\langle s \rangle) < +\infty.$$

Αυτό σημαίνει ότι υπάρχουν άπειροι ακέραιοι αλγεβρικοί αριθμοί $a \neq 0$ του που ανήκουν στην ίδια κλάση $(\text{mod } s)$ και για τους οποίους ισχύει ότι

$$|N_K(a)| = s.$$

Συνεπώς, μπορούμε να βρούμε άπειρα ζεύγη $(a, b) \in R_K \times R_K$, με $(a, b) \neq (0, 0)$ και $a \neq \pm b$, ώστε να ισχύει ότι

$$|N_K(a)| = |N_K(b)| = s \text{ και } a \equiv b \pmod{\langle s \rangle}.$$

Από αυτό έπεται ότι

$$a \equiv b \pmod{\langle s \rangle} \Rightarrow a\bar{b} \equiv b\bar{b} \equiv N_K(b) \pmod{\langle s \rangle},$$

όπου ως $\bar{b}$ συμβολίζουμε το συζυγή του b στο K. Άρα υπάρχει $\varepsilon \in R_K$ τέτοιος, ώστε

$$a\bar{b} = \varepsilon s = \varepsilon |N_K(b)| \Rightarrow \frac{a\bar{b}}{|N_K(b)|} = \pm\varepsilon \Rightarrow \frac{a}{b} = \pm\varepsilon.$$

Κι εφόσον $|N_K(a) = |N_K(b)|$, λαμβάνουμε ότι

$$N_K(\varepsilon) = \pm 1. \Rightarrow \varepsilon \in \mathcal{U}_K.$$

Μάλιστα,

$$a \neq \pm b \Rightarrow \varepsilon \neq \pm 1.$$

Για κάθε μονάδα $\varepsilon \neq \pm 1$ του K ισχύει ότι $\varepsilon^{-1}, -\varepsilon, -\varepsilon^{-1} \in \mathcal{U}_K$. Επιλέγουμε μία εκ των μονάδων $\varepsilon, \varepsilon^{-1}, -\varepsilon$ και $-\varepsilon^{-1}$ ώστε να είναι μεγαλύτερη του 1. Αυτό σημαίνει υπάρχει μονάδα του K μεγαλύτερη του 1. Έστω, τώρα, ένας πραγματικός αριθμός $\mu > 1$. Αν η ε είναι θετική μονάδα του K για

την οποία ισχύει ότι $1 < \varepsilon < \mu$ και έστω $\bar{\varepsilon}$ η συζυγής αυτής. Τότε από τη σχέση $N_K(\varepsilon) = \varepsilon\bar{\varepsilon} = \pm 1$, προκύπτει ότι

$$\frac{1}{\mu} < \bar{\varepsilon} < 1 \ \text{ ή } \ -1 < \bar{\varepsilon} < -\frac{1}{\mu}.$$

Επομένως, έχουμε ότι

$$|\bar{\varepsilon}| < \mu.$$

Επί τη βάσει του λήμματος 2.2.4 το σύνολο των μονάδων ε, για τις οποίες ισχύει ότι $1 < \varepsilon < \mu$ είναι πεπερασμένο και κατά συνέεια υπάρχει ελάχιστο στοιχείο. Το ελάχιστο αυτό στοιχείο, ήτοι την ελάχιστη μονάδα που είναι μεγαλύτερη του 1, το συμβολίζουμε ως ε_0. Εάν ε είναι μία μονάδα του K, τότε μπορούμε να προσδιορίσουμε ένα ακέραιο αριθμό k τέτοιο, ώστε

$${\varepsilon_0}^k \leq \varepsilon {\varepsilon_0}^{k+1}.$$

Από τη σχέση αυτή έπεται άμεσα ότι

$$1 \leq \frac{\varepsilon}{{\varepsilon_0}^k} < \varepsilon_0.$$

Κι εφόσον η ε_0 είναι εξ ορισμού της η ελάχιστη μονάδα, η οποία είναι μεγαλύτερη του 1, τότε έχουμε ότι

$$\frac{\varepsilon}{{\varepsilon_0}^k} = 1 \Rightarrow \varepsilon = \varepsilon^k.$$

Ομοίως, οι αρνητικές μονάδες του K είναι της μορφής $-{\varepsilon_0}^k$, όπου $k \in \mathbb{Z}$. Εν τέλει, η τυχουσα μονάδα του K μπορεί να γραφτεί υπό τη μορφή

$$(-1)^r {\varepsilon_0}^k,$$

όπου $r = 0, 1$ και $k \in \mathbb{Z}$, το οποίο είναι και το ζητούμενο. □

Παρατηρηση 2.2.6. Το ανωτέρω θεώρημα μας πληροφορεί ότι η ομάδα των μονάδων μπορεί να ειδωθεί ως ευθύ γινόμενο κυκλικών ομάδων, βάσει του ισομορφισμού

$$\mathcal{U}_K \cong \langle -1 \rangle \times \langle \varepsilon_0 \rangle.$$

Ουσιαστικά, αυτό είναι το θεώρημα Dirichlet, ήτοι το 1.5.6, στην περίπτωση των τετραγωνικών πραγματικών σωμάτων αριθμών.

Ορισμος 2.2.7. Η μονάδα ε_0 του τετραγωνικού πραγματικού σώματος K, όπως αυτή προσδιορίστηκε στο θεώρημα 2.2.5, καλείται *θεμελιώδης μονάδα του* K.

Επομένως, το ερώτημα που εγείρεται φυσιολογικά είναι πως μπορούμε να υπολογίσουμε τη θεμελιώδη μονάδα δοθέντος τετραγωνικού πραγματικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{d_K})$. Πλήρη απάντηση σε αυτό το ερώτημα δε θα δώσουμε στα πλαίσια της εργασίας αυτής χάριν συντομίας. Αξίζει, όμως, να αναφέρουμε ότι ο υπολογισμός της θεμελιώδους μονάδας σχετίζεται με την επίλυση της εξίσωσης του Pell, ήτοι της διοφαντικής εξίσωσης

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

2.3 Υπολογισμός του αριθμού κλάσεων ιδεωδών

Σε αυτή την παράγραφο θα υπολογίσουμε τον αριθμό κλάσεων ιδεωδών μόνο κατά την περίπτωση των μιγαδικών τετραγωνικών αριθμητικών σωμάτων. Ο λόγος είναι ότι ενδιαφερόμαστε ιδιαιτέρως γι' αυτά. Η εύρεση του αριθμού κλάσεων ιδεωδών των πραγματικών τετραγωνικών αλγεβρικών σωμάτων αριθμών είναι ιδιαιτέρως απαιτητική. Θα έπρεπε, επομένως να γίνει αρκετή προεργασία για την αντιμετώπιση του προβλήματος αυτού, το οποίο είναι δύσκολο στα πλαίσια αυτής της εργασίας.

Σε ότι αφορά στον αριθμό κλάσεων ιδεωδών των μιγαδικών τετραγωνικών αριθμητικών σωμάτων, πρόκειται να τον προσδιορίσουμε κάνοντας χρήση της θεωρίας των τετραγωνικών μορφών. *Τετραγωνική διωνυμική μορφή*, ή αλούστερα *τετραγωνική μορφή* καλείται μία έκφραση της μορφής

$$q(x,y) = ax^2 + bxy + cy^2 \text{ , όπου } x, y \in \mathbb{Z},$$

και $a, b, c \in \mathbb{Z}$. Ιδιαιτέρως, ονομάζεται *πρωταρχική*, όταν $(a, b, c) = 1$. Είναι προφανές ότι κάθε τετραγωνική μορφή είναι ακέραιο πολλαπλάσιο κάποιας πρωταρχικής τετραγωνικής μορφής. Εάν θεωρήσουμε ένα ακέραιο αριθμό m, τότε λέμε ότι αυτός *παρίσταται από την τετραγωνική μορφή* q, όταν υπάρχει ζεύγος ακεραίων (x_0, y_0) τέτοιοι ώστε να ισχύει

$$m = q(x_0, y_0).$$

Αν επιπροσθέτως, συμβεί να ισχύει ότι $(x_0, y_0) = 1$, τότε λέμε ότι *ο* m *παρίσταται γνήσια από την* q. Έστω τετραγωνική μορφή $q'(x, y)$. Τότε η $q(x, y)$ και $q'(x, y)$ ονομάζονται *ισοδύναμες* όταν υπάρχουν ακέραιοι αριθμοί k, l, m, n με την ιδιότητα

$$kn - lm = \pm 1,$$

για τους οποίους ισχύει ότι

$$q(x, y) = q'(kx + ly, mx + ny).$$

Επομένως ισχύει ότι

$$\begin{pmatrix} k & l \\ m & n \end{pmatrix} \in GL_2(\mathbb{Z}).$$

Ιδιαίτερα εάν η ισοδυναμία είναι *γνήσια* τότε, και μόνο τότε όταν $kn - lm = 1$, ήτοι

$$\begin{pmatrix} k & l \\ m & n \end{pmatrix} \in SL_2(\mathbb{Z})$$

και *μη γνήσια* εάν $kn - lm = -1$. Η ισοδυναμία, και προφανώς και η γνήσια ισοδυναμία τετραγωνικών μορφών, αποτελεί σχέση ισοδυναμίας. Αρκετά σημαντική είναι η παρατήρηση ότι στοιχεία της ίδιας κλάσεως ισοδυναμίας παριστούν τους ίδιους αριθμούς.

Εν ολίγοις, και προς τούτο δόθηκαν και οι ανωτέρω ορισμοί, η ιδέα είναι να μετασχηματίζουμε τετραγωνικές μορφές σε άλλες που ανήκουν στην ίδια κλάση και με αυτές να εργαζόμαστε.

ΠΡΟΤΑΣΗ 2.3.1. *Ο ακέραιος αριθμός* m *παρίσταται γνήσια από μια τετραγωνική μορφή* $q(x, y)$ *εάν, και μόνο εάν η* $q(x, y)$ *είναι γνησίως ισοδύναμη με μία τετραγωνική μορφή* $mx^2 + b'xy + c'y^2$.

Απόδειξη. ($\Rightarrow$) Υποθέτουμε ότι για σχετικά πρώτους ακέραιους αριθμούς α και β ισχύει ότι

$$q(\alpha, \beta) = m,$$

όπου $q(x, y) = ax^2 + bxy + cy^2$. Αφού $(\alpha, \beta) = 1$, μπορούμε να βρούμε ακέραιους αριθμούς r και s για τους οποίους να ισχύει

$$s\alpha - r\beta = 1.$$

Υπολογίζοντας το $q(\alpha x + ry, \beta x + sy)$, λαμβάνουμε ότι

$$q(\alpha x + ry, \beta x + sy) = q(\alpha, \beta)x^2 + \big(q(\alpha, s) + q(r, \beta)\big)xy + q(r, s)y^2 = mx^2 + b'xy + c'y^2,$$

το οποίο έχει τη ζητούμενη μορφή.
($\Leftarrow$) Εάν υποθέσουμε την τετραγωνική μορφή $mx^2+b'xy+cy^2$ τότε για $(x, y) = (1, 0)$, ο m πράγματι παρίσται από αυτή. □

Ως *διακρίνουσα* D της τετραγωνικής μορφής $q(x,y) = ax^2 + bxy + cy^2$ ορίζουμε τον ακέραιο αριθμό $b^2 - 4ac$. Εάν θεωρήσουμε μία ισοδύναμη τετραγωνική μορφή της q, έστω την q', τότε θα υπάρχουν εξ ορισμού της ισοδυναμίας ακέραιοι αριθμοί k, l, m και n τέτοιοι, ώστε

$$q(x,y) = q'(kx + ly, mx + ny) \text{ , με } kn - lm = \pm 1.$$

Εύκολα υπολογίζουμε με αντικατάσταση στον τύπο της $q(x,y)$ ότι

$$D = (kn - lm)^2 \cdot D' = D',$$

όπου D' είναι η διακρίνουσα της τετραγωνικής μορφής q'. Αυτό σημαίνει ότι ισοδύναμες τετραγωνικές μορφές έχουν την ίδια διακρίνουσα.

Σημαντικό ρόλο στη μελέτη μας παίζει και το πρόσημο της διακρίνουσας. Παρατηρούμε ότι ισχύει η ταυτότητα

$$4a \cdot q(x,y) = (2ax + by)^2 - Dy^2.$$

Βάσει αυτής, εάν $D > 0$ τότε η q παριστά θετικούς και αρνητικούς ακέραιους. Αν, από την άλλη, $D < 0$ τότε η q παριστά μονάχα θετικούς ή μονάχα αρνητικούς ακεραίους, γεγονός που εξαρτάται από το πρόσημο του a. Ακόμα, από την ισοδυναμία

$$D \equiv b^2 \pmod 4,$$

λαμβάνουμε ότι

$$D \text{ άρτιος αριθμός } \Leftrightarrow b \text{ άρτιος αριθμός}$$

και

$$D \text{ περιττός αριθμός } \Leftrightarrow b \text{ περιττός αριθμός .}$$

Το επόμενο αποτέλεσμα αποτελεί ικανή και αναγκαία συνθήκη για να παρίσταται ένας αριθμός από μία τετραγωνική μορφή

Πρόταση 2.3.2. *Έστω ακέραιος αριθμός D, τέτοιος ώστε $D \equiv 0, 1 \pmod 4$ και περιττός ακέραιος m σχετικά πρώτος με το D. Τότε ο m παρίσταται γνήσια από μια τετραγωνική μορφή διακρίνουσας D εάν, και μόνο εάν*

$$\left(\frac{D}{m}\right) = 1,$$

όπου ως $\left(\frac{D}{m}\right)$ συμβολίζουμε το σύμβολο Jacobi.

Απόδειξη. ($\Rightarrow$) Εάν υποθέσουμε ότι ο m παρίσταται από κάποια τετραγωνική μορφή, σύμφωνα με την πρόταση 2.3.1 μπορούμε να υποθέσουμε χ.β.τ.γ. ότι αυτή είναι η

$$q(x,y) = mx^2 + bxy + cy^2 \Rightarrow D = b^2 - 4mc \Rightarrow D \equiv b^2 \pmod m.$$

Κι εφόσον $(m, D) = 1$, έπεται ότι

$$\left(\frac{D}{m}\right) = 1.$$

($\Leftarrow$) Έστω ότι

$$\left(\frac{D}{m}\right) = 1.$$

Τότε υπάρχει ακέραιος αριθμός b, με την ιδιότητα $D \equiv b^2 \pmod m$. Εφόσον ο m είναι περιττός, μπορούμε να υποθέσουμε ότι είτε και οι δύο είναι άρτιοι αριθμοί, είτε και οι δύο περιττοί. Συνεπώς

$$D \equiv 0, 1 \pmod 4 \Rightarrow D \equiv b^2 \pmod{4m} \Rightarrow \exists\, c \in \mathbb{Z} : D = b^2 - 4mc.$$

Αυτό σημαίνει ότι η τετραγωνική μορφή $mx^2 + bxy + cy^2$ παριστά τον αριθμό m και έχει διακρίνουσα D. □

Πορισμα 2.3.3. *Έστω ακέραιος n και περιττός πρώτος p, ο οποίος δε διαιρεί τον n. Τότε*

$$\left(\frac{-n}{p}\right) = 1$$

εάν, και μόνο εάν το p παρίσταται από μία τετραγωνική μορφή διακρίνουσας $-4n$.

Μέχρι τώρα κάναμε λόγο για τετραγωνικές μορφές χωρίς κάποιο ιδιαίτερο περιορισμό για τους συντελεστές αυτών, πέραν της περίπτωσης των πρωταρχικών τετραγωνικών μορφών. Από αυτό το σημείο θα εστιάσουμε την προσοχή μας στην περίπτωση των θετικά ορισμένων τετραγωνικών μορφών. Εάν θεωρήσουμε την τετραγωνική μορφή $q(x, y) = ax^2 + bxy + cy^2$, τότε αυτή καλείται *θετικά ορισμένη* όταν $D > 0$ και $a > 0$. Παρατηρούμε ότι εάν μία τετραγωνική μορφή είναι θετικά ορισμένη, τότε και κάθε γνήσια ισοδύναμή της είναι θετικά ορισμένη.

Ορισμος 2.3.4. Η πρωταρχική, θετικά ορισμένη τετραγωνική μορφή $ax^2 + bxy + cy^2$ καλείται *ανάγωγη* εάν

$$|b| \leq a \leq c,$$

και αν $|b| = a$ ή $a = c$, τότε $b \geq 0$.

Θεωρημα 2.3.5. *Κάθε πρωταρχική, θετικά ορισμένη τετραγωνική μορφή είναι γνησίως ισοδύναμη με μία και μόνο ανάγωγη τετραγωνική μορφή.*

Απόδειξη. Θεωρούμε τη θετικά ορισμένη τετραγωνική μορφή $Q(x, y) = Ax^2 + Bxy + Cy^2$, όπου $A, B, C \in \mathbb{Z}$. Μπορούμε, αντί να δουλέψουμε με αυτή την Q, να υποθέσουμε εκείνη την τετραγωνική μορφή, η οποία είναι γνήσια ισοδύναμη με την Q και η απόλυτη τιμή του συντελεστή του xy να είναι η ελάχιστη δυνατή, και για αυτήν να αποδείξουμε το ζητούμενο. Έστω, λοιπόν, $q(x, y) = ax^2 + bxy + cy^2$, όπου $a, b, c \in \mathbb{Z}$, τέτοια ώστε $q \sim Q$ και $|b|$ ελάχιστο. Αρχικά, θα δείξουμε ότι υπάρχει μία τετραγωνική μορφή, γνήσια ισοδύναμη με την q, με την ιδιότητα $|b| \leq a \leq c$. Θεωρούμε την μορφή:

$$q'(x, y) = q(x + my, y) = ax^2 + (2am + b)xy + c'y^2,$$

για κάποιο ακέραιο c'. Τότε, αν $a < |b|$, μπορούμε να επιλέξουμε $m \in \mathbb{Z}$ τέτοιο ώστε $|2am + b| < |b|$, το οποίο είναι άτοπο, από την επιλογή της q. Εάν, τώρα, $a > c$ εφαρμόζουμε το μετασχηματισμό:

$$x \mapsto -y \text{ και } y \mapsto x,$$

επομένως προκύπτει τετραγωνική μορφή με τη ζητούμενη ιδιότητα, δηλαδή την $|b| \leq a \leq c$. Η q είναι η ανάγωγη μορφή η οποία ψάχνουμε, εκτός εάν $b < 0$ και $a = -b$ ή $a = c$. Σε αυτή την περίπτωση μας αρκεί να δείξουμε ότι οι τετραγωνικές μορφές $ax^2 + bxy + cy^2$ και $ax^2 - bxy + cy^2$ είναι γνήσια ισοδύναμες. Πράγματι:

- αν $a = -b$, εφαρμόζουμε το μετασχηματισμό $(x, y) \mapsto (x + y, y)$, ο οποίος στέλνει την τετραγωνική μορφή $ax^2 - axy + cy^2$ στην $ax^2 + axy + cy^2$, ενώ
- αν $a = c$, εφαρμόζουμε το μετασχηματισμό $(x, y) \mapsto (-y, x)$, που στέλνει τη μορφή $ax^2 + bxy + ay^2$ στην $ax^2 - bxy + ay^2$.

Τέλος, αποδεικνύουμε τη μοναδικότητα. Ας υποθέσουμε ότι η $q(x, y) = ax^2 + bxy + cy^2$ είναι ανάγωγη μορφή για την οποία ισχύει η ανισότητα $|b| < a < c$. Παρατηρούμε ότι:

- αν $0 < |x| \leq |y|$, τότε $bxy + cy^2 \geq 0 \Rightarrow q(x, y) \geq a$,
- αν $0 < |y| \leq |x|$, τότε $ax^2 + bxy \geq 0 \Rightarrow q(x, y) \geq a$ και
- αν $x = 0$ ή $y = 0$, τότε ισχύει επίσης ότι $q(x, y) \geq a$.

Για $x = \pm 1$ και $y = 0$ έχουμε $q(\pm 1, 0) = a$. Αν επιπροσθέτως ισχύει ότι $c > a$, τότε για $|x| > 1$ έπεται ότι $q(x, 0) = ax^2 > a$ και είτε $x \geq y \geq 1$, οπότε

$$ax^2 + bxy + cy^2 \geq cy^2 > a,$$

είτε $|y| \geq |x| \geq 1$, οπότε

$$ax^2 + bxy + cy^2 \geq ax^2 > a.$$

Επομένως, αν $c > a$, ο a είναι ο ελάχιστος αριθμός που μπορεί να παρασταθεί από την q. Ομοίως μπορούμε να δείξουμε ότι ο c παρίσταται από την q τότε, και μόνο τότε, όταν $(x, y) = (0, \pm 1)$. Άρα ο c είναι, μετά τον a, ο αμέσως επόμενος πιο μικρός αριθμός που παρίσταται από την q. Έστω, τώρα, $q'(x, y) = a'x^2 + b'xy + c'y^2$ μία γνήσια ισοδύναμη της q, ανάγωγη τετραγωνική μορφή. Η γνήσια ισοδυναμία συνεπάγεται ότι οι q και q' παριστούν τους ίδιους ακριβώς αριθμούς. Κι αφού και οι δύο μορφές είναι ανάγωγες, τότε $a = a'$. Αφού η q' είναι ανάγωγη τότε $a \leq c'$. Εάν, όμως, ίσχυε η ισότητα τότε $a = q(\pm 1, 0) = q(0, \pm 1)$, που είναι άτοπο διότι τότε και η q θα παριστά το a για τέσσερις διαφορετικές τιμές του ζεύγους (x, y) . Ισχύει λοιπόν, ότι $a < c'$, οπότε και $c = c'$. Τέλος, από την ισότητα των διακρινουσών, προκύπτει και ότι $b' = \pm b$. Έστω τώρα ότι

$$q'(x, y) = q(\alpha x + \beta y, \gamma x + \delta y), \text{ όπου } \alpha\delta - \beta\gamma = 1.$$

Από τη σχέση αυτή έπονται οι

$$a = q(\pm 1, 0) = q(\alpha, \gamma)$$
$$c = q(0, \pm 1) = q(\beta, \delta).$$

Είδαμε, όμως, ότι τα $(\pm 1, 0)$ είναι τα μοναδικά ζεύγη με την ιδιότητα η q να παριστά τον a. Αυτό σημαίνει ότι $(\alpha, \gamma) = (\pm 1, 0)$. Ομοίως έπεται και ότι $(\beta, \gamma) = (0, \pm 1)$. Τελικά, από τη σχέση $\alpha\delta - \beta\gamma = 1$, λαμβάνουμε ότι είτε

$$\alpha = \delta = 1 \text{ και } \beta\gamma = 0,$$

τι οποίο αποδεικνύει το ζητούμενο, είτε ότι

$$\alpha = \delta = -1 \text{ και } \beta\gamma = 0,$$

από το οποίο επίσης συνεπάγεται ότι $q = q'$. Άρα αποδείξαμε τη μοναδικότητα της ανάγωγης τετραγωνικής μορφής και ολοκληρώσαμε την απόδειξη του θεωρήματος. □

Πορισμα 2.3.6. *Εάν $q(x, y) = ax^2 + bxy + cy^2$ είναι μία ανάγωγη τετραγωνική μορφή διακρίνουσας $D < 0$, τότε ισχύει ότι*

$$a \leq \sqrt{\frac{-D}{3}}.$$

Απόδειξη. Άμεση από την ανισότητα $|b| \leq a \leq c$. □

Πορισμα 2.3.7. *Υπάρχουν πεπερασμένου πλήθους κλάσεις γνήσιας ισοδυναμίας τετραγωνικών μορφών διακρίνουσας D.*

Προς το παρόν, δεν έχουμε αναφερθεί στον υπολογισμό του αριθμού κλάσεων ιδεωδών των τετραγωνικών αριθμητικών σωμάτων, αν και αυτός είναι ο στόχος της παραγράφου. Η σύνδεση που επιθυμούμε με όλα τα παραπάνω επιτυγχάνεται μέσω του παρακάτω θεωρήματος:

Θεωρημα 2.3.8. *Υφίσταται αμφιμονοσήμαντη αντιστοιχία μεταξύ της ομάδας κλάσεων ιδεωδών $Cl(K)$ ενός μιγαδικού τετραγωνικού σώματος K και του συνόλου των ανάγωγων τετραγωνικών μορφών διακρίνουσας ίσης με τη διακρίνουσα του σώματος K.*

Απόδειξη. (βλ. [16], σελ.94, Πρ.) □

Παραδειγμα 2.3.9. Θα υπολογίσουμε τον αριθμό κλάσεων ιδεωδών, βάσει του ανωτέρω θεωρήματος, του σώματος $K = \mathbb{Q}(\sqrt{-14})$. Θεωρούμε την τετραγωνική μορφή

$$ax^2 + bxy + cy^2,$$

όπου $a, b, c \in \mathbb{Z}$. Υποθέτουμε ότι αυτή είναι θετικά ορισμένη, ανάγωγη τετραγωνική μορφή διακρίνουσας d_K, όπου ως d_K συμβολίζουμε τη διακρίνουσα του K. Έχουμε

$$-14 \equiv 2 \pmod 4 \Rightarrow d_K = 4 \cdot (-14) = -56.$$

Από το πόρισμα 2.3.6 έχουμε ότι

$$a < \sqrt{\frac{-d_K}{3}} = \sqrt{\frac{56}{3}} \Rightarrow a \leq 4.$$

Ακόμα, έχουμε ότι

$$b^2 - 4ac = -56 \Rightarrow b^2 = 4(ac - 14) \Rightarrow b \equiv 0 \pmod 2.$$

Τέλος, υποθέσαμε ότι η τετραγωνική μορφή είναι θετικά ορισμένη και ανάγωγη, άρα $a > 0$. Επομένως, διακρίνουμε περιπτώσεις:

- Εάν $a = 1$, από την ανισότητα $|b| \leq a$ και την ισοτιμία $b \equiv 0 \pmod 2$ λαμβάνουμε $b = 0$. Τότε

  $$0^2 - 4c = -56 \Rightarrow c = 14.$$

  Άρα $(a, b, c) = (1, 2, 14)$.

- Εάν $a = 2$, τότε κατ' ανάγκη $b \in \{0, \pm 2\}$. Όμως, έχουμε

  $$b^2 - 4 \cdot 2c = -56 \Rightarrow 2c = \left(\frac{b}{2}\right)^2 + 14.$$

  Αν $b = 2$, εύκολα προκύπτει ότι $c \notin \mathbb{Z}$. Από την άλλη, εάν $b = 0$, τότε έχουμε $c = 7$. Άρα $(a, b, c) = (2, 0, 7)$.

- Αν $a = 3$, έχουμε ξανά ότι $b \in \{0, \pm 2\}$ και

  $$3c = \left(\frac{b}{2}\right)^2 + 14.$$

  Από αυτά συμπεραίνουμε ότι $b = \pm 2$ και $c = 5$. Άρα $(a, b, c) = (3, \pm 2, 5)$.

- Για $a = 4$, δεν προκύπτει άλλη τετραγωνική μορφή.

Συνολικά από τις παραπάνω περιπτώσεις βρήκαμε τέσσερις διαφορετικές θετικά ορισμένες ανάγωγες τετραγωνικές μορφές διακρίνουσας -56. Κατά συνέπεια έχουμε ότι

$$h_{\mathbb{Q}(\sqrt{-14})} = 4.$$

2.4 Νόμος ανάλυσης για τετραγωνικά αριθμητικά σώματα

Στο πρώτο κεφάλαιο έγινε λόγος για την έννοια του νόμου ανάλυσης σε σχετικά αλγεβρικά σώματα αριθμών. Σε αυτή την παράγραφο στόχος είναι να εφαρμόσουμε τη γνώση αυτή στην περίπτωση κατά την οποία έχουμε τετραγωνικά αριθμητικά σώματα. Θεωρούμε το σώμα $K = \mathbb{Q}(\sqrt{m})$, όπου ο m είναι ένας ακέραιος αριθμός στερούμενος τετραγώνων. Η επέκταση $K/\mathbb{Q}$ αποτελεί επέκταση Galois βαθμού 2, όπως έχουμε ήδη αναφέρει. Εάν υποθέσουμε ένα πρώτο ιδεώδες του $R_{\mathbb{Q}} = \mathbb{Z}$, για παράδειγμα το $\langle p \rangle$, όπου p είναι ένας πρώτος αριθμός, τότε σύμφωνα με το πόρισμα 3.2.2 ισχύει ότι

$$\langle p \rangle R_K := pR_K = (Q_1 Q_2 \cdots Q_R)^e$$

και

$$efr = [K : \mathbb{Q}] = 2,$$

όπου f είναι ο βαθμός των Q_i. Η σχέση $efr = 2$ έχει ως άμεση συνέπεια της τις συνθήκες

$$0 \neq e \leq 2\ ,\ 0 \neq f \leq 2\ ,\ 0 \neq r \leq 2.$$

Κι εφόσον $e, f, r \in \mathbb{N}$, τότε ισχύει ότι $e, f, r \in \{1, 2\}$. Επομένως αρκεί να διακρίνουμε τρεις περιπτώσεις:

- Αν $r = 2$ και $e = f = 1$, τότε το ιδεώδες pR_K αναλύεται σε γινόμενο δύο διακεκριμένων πρώτων ιδεωδών του R_K, βαθμού 1. Με άλλα λόγια, ο πρώτος αριθμός p αναλύεται πλήρως στο K.
- Αν $f = 2$ και $e = r = 1$, τότε το ιδεώδες pR_K είναι πρώτο βαθμού 2. Στην περίπτωση αυτή ο p αδρανεί στο K.
- Αν $e = 2$ και $f = r = 1$, τότε το ιδεώδες pR_K είναι τετράγωνο ενός πρώτου ιδεώδους βαθμού 1. Σε αυτή την περίπτωση ο πρώτος αριθμός p διακλαδίζεται στο K.

Αυτή η προσέγγιση καθορίζει ουσιαστικά ποίες είναι οι τρεις δυνατότητες για την ανάλυση ενός πρώτου ιδεώδους $\langle p \rangle$ σε ένα τετραγωνικό αριθμητικό σώμα. Τα δύο παρακάτω θεωρήματα προσδιορίζουν πλήρως το νόμο ανάλυσης που αναζητάμε για κάθε επιλογή πρώτου αριθμού.

Ας υποθέσουμε ότι πράγματι έχουμε ένα ικανοποιητικό υπολογιστικά νόμο ανάλυσης. Μπορούμε να προσδιορίσουμε πλήρως τα πρώτα ιδεώδη του R_K που συμμετέχουν στην ανάλυση του pR_K; Η απάντηση είναι ότι πράγματι μπορούμε. Ας υποθέσουμε ότι οι αριθμοί 1 και ω αποτελούν βάση ακεραιότητας του K. Υποθέτουμε ακόμα ότι $f(X) = Irr(\omega, \mathbb{Q})$, όπου $\deg(f(X)) = 2$. Ας υποθέσουμε ότι αυτό έχει παραγοντοποίηση $\pmod p$, της μορφής

$$\overline{f}(X) = \overline{f_1}(X)\overline{f_2}(X)$$

και ω_1 και ω_2 είναι σημεία μηδενισμού των πολυωνύμων $\overline{f_1}$ και $\overline{f_2}$, αντιστοίχως. Θεωρούμε την απεικόνιση

$$\begin{aligned} \varphi_i \ &: \ \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}_p[\omega_i] \\ &\quad\ g(\omega) \longmapsto \overline{g(\omega_i)}, \end{aligned}$$

όπου $i = 1, 2$. Εύκολα προκύπτει ότι είναι επιμορφισμός δακτυλίων. Άρα από το πρώτο θεώρημα των ισομορφισμών ισχύει ότι

$$\mathbb{Z}[\omega]/P_i \cong \mathbb{Z}_p[\omega_i],$$

όπου $P_i := Ker f(\varphi_i)$. Όμως εξ ορισμού του ω_i προκύπτει ότι το $\mathbb{Z}_p[\omega_i]$ είναι σώμα. Κατά συνέπεια το ιδεώδες P_i είναι πρώτο. Προφανώς ισχύει ότι

$$\langle p, f_i(\omega) \rangle \subseteq P_i.$$

Θεωρούμε τώρα ένα στοιχείο $g(\omega) \in P_i$. Για το εν λόγω στοιχείο θα ισχύει ότι

$$\overline{g}(X) = \overline{f_i}(X) \cdot \overline{h}(X).$$

Αυτό σημαίνει ότι καθένας από τους συντελεστές του πολυωνύμου $g - f_i \cdot h$ είναι διαιρετός με το p. Επομένως υπάρχει $k(\omega) \in \mathbb{Z}[\omega]$ τέτοιο ώστε

$$g(\omega) - f_i(\omega) \cdot h(\omega) = p \cdot k(\omega) \Rightarrow g(\omega) = f_i(\omega) \cdot h(\omega) + p \cdot k(\omega) \Rightarrow g(\omega) \in \langle p, f_i(\omega) \rangle.$$

Συνεπώς, δείξαμε και τη σχέση εγκλεισμού

$$P_i \subseteq \langle p, f_i(\omega) \rangle.$$

Άρα προκύπτει η ισότητα. Συνεπώς έχουμε αποδείξει την εξής πρόταση:

ΠΡΟΤΑΣΗ 2.4.1. *Έστω $K = \mathbb{Q}(\sqrt{m})$ ένα τετραγωνικό αριθμητικό σώμα και $\{1, \omega\}$ βάση ακεραιότητας αυτού, όπου $\omega \in R_K$. Αν υπάρχουν υπάρχουν πολυώνυμα $f_1, f_2 \in \mathbb{Z}[X]$, τέτοια ώστε*

$$Irr(\omega, \mathbb{Q}) = f_1 \cdot f_2,$$

τότε τα ιδεώδη του R_K,

$$P_i = \langle p, f_i(\omega) \rangle = pR_K + f_i(\omega)R_K \text{ , } i = 1, 2$$

είναι πρώτα, και μάλιστα ισχύει ότι

$$pR_K = P_1P_2.$$

Πριν όμως περάσουμε στα θεωρήματα, υπενθυμίζουμε την έννοια του συμβόλου του Kronecker. Αν $\alpha \in \mathbb{Z}$ και $p \in \mathbb{P}$, το σύμβολο του Kronecker ορίζεται ως εξής:

$$\left(\frac{\alpha}{p}\right) := \begin{cases} 1 & \text{, αν } p \nmid \alpha \text{ και } \exists r \in \mathbb{Z} : r^2 \equiv \alpha \pmod{p} \\ -1 & \text{, αν } p \nmid \alpha \text{ και } \nexists r \in \mathbb{Z} : r^2 \equiv \alpha \pmod{p} \\ 0 & \text{, αν } p | \alpha \end{cases}.$$

ΘΕΩΡΗΜΑ 2.4.2 (Νόμος ανάλυσης του $p \neq 2$)**.** *Δοθέντος τετραγωνικού αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ και πρώτου αριθμού $p \neq 2$, έχουμε τις τρεις περιπτώσεις:*

(i) Αν $\left(\frac{m}{p}\right) = 1$, τότε $pR_K = P_1P_2$, όπου τα P_1 και P_2 είναι διακεκριμένα πρώτα ιδεώδη του R_K βαθμού 1.

(ii) Αν $\left(\frac{m}{p}\right) = -1$, τότε το ιδεώδες pR_K είναι πρώτο στο K

(iii) Αν $\left(\frac{m}{p}\right) = 0$, τότε $pR_K = P^2$, όπου το P είναι πρώτο ιδεώδες του R_K βαθμού 1.

Απόδειξη. Αρχικά, εργαζόμαστε στην περίπτωση $m \equiv 2, 3 \pmod 4$. Τότε

$$Irr(\sqrt{m}, \mathbb{Q}) = X^2 - m =: f(X) \Rightarrow f(X) \equiv X^2 - m \pmod p \Leftrightarrow \overline{f}(X) = X^2 - \overline{m},$$

όπου ως $\overline{m}$ συμβολίζουμε την κλάση $m \pmod p$. Αν υποθέσουμε ότι

$$\left(\frac{m}{p}\right) = 1,$$

τότε υπάρχει ακέραιος αριθμός x_0, με την ιδιότητα

$${x_0}^2 \equiv m \pmod p \Rightarrow \overline{f}(x_0) = \overline{0} \Rightarrow \overline{f}(X) = (X - \overline{x_0})(X + \overline{x_0}).$$

Επομένως, το πρώτο ιδεώδες pR_K αναλύεται σε γινόμενο δύο ιδεωδών P_1 και P_2. Επί τη βάσει της προτάσεως 2.4.1 αυτά είναι τα $P_1 = \langle p, \sqrt{m} + x_0 \rangle$ και $P_2 = \langle p, \sqrt{m} - x_0 \rangle$. Εάν τώρα ισχύει ότι

$$\left(\frac{m}{p}\right) = -1,$$

τότε το $\overline{f}$ δεν επιδέχεται παραγοντοποίηση. Πράγματι, εάν ίσχυε το αντίθετο, θα έπρεπε να υπάρχουν $a, b \in \mathbb{Z}_p$ με την ιδιότητα $\overline{f}(a) = \overline{f}(b) = \overline{0}$. Όμως από τους τύπους Vieta θα είχαμε

$$\begin{cases} \overline{a} + \overline{b} = \overline{0} \\ \overline{a}\overline{b} = -\overline{m} \end{cases} \Rightarrow \overline{a}^2 = \overline{m},$$

το οποίο αντίκειται στην υπόθεση ότι το σύμβολο του Kronecker είναι ίσο με -1. Άρα το ιδεώδες pR_K είναι πρώτο. Τέλος, όταν

$$\left(\frac{m}{p}\right) = 0$$

το πολυώνυμο f λαμβάνει τη μορφή $f(X) = X^2$, οπότε άμεσα προκύπτει ότι

$$pR_K = P^2,$$

όπου $P = \langle p, \sqrt{m} \rangle$.

Εναπομένει η περίπτωση $m \equiv 1 \pmod 4$. Κατά την περίπτωση αυτή η βάση ακεραιότητας είναι η

$$\{1, \omega\} = \{1, \frac{1 + \sqrt{m}}{2}\},$$

και το ελάχιστο πολυώνυμο είναι το

$$f(X) := Irr(\omega, \mathbb{Q}) = X^2 - X - \frac{m-1}{4} \Rightarrow \overline{f}(X) = X^2 - X - \overline{\frac{m-1}{4}}.$$

Αν

$$\left(\frac{m}{p}\right) = 1,$$

τότε βλέπουμε ότι

$$\overline{f}(X) = \left(X - \overline{\frac{1 + x_0}{2}}\right)\left(X - \overline{\frac{1 - x_0}{2}}\right),$$

όπου το x_0 είναι λύση της ισοδυναμίας

$$x^2 \equiv m \pmod p.$$

Επομένως σε αυτή την περίπτωση έχουμε ότι

$$pR_K = P_1 P_2,$$

όπου βάσει της προτάσεως 2.4.1 λαμβάνουμε ότι

$$P_1 = \langle p, \frac{\sqrt{m} - x_0}{2} \rangle \text{ και } P_2 = \langle p, \frac{\sqrt{m} + x_0}{2} \rangle.$$

Αν

$$\left(\frac{m}{p}\right) = -1,$$

τότε το $\overline{f}$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}_p[X]$, καθώς αν ίσχυε το αντίθετο από τους τύπους Vieta για τα σημεία μηδενισμού a, b του f, θα λαμβάναμε ότι

$$\begin{cases} \overline{a+b} = \overline{1} \\ \overline{ab} = \overline{-\frac{m-1}{4}} \end{cases} .$$

Οπότε αν θέσουμε $\overline{a} = \overline{\frac{1+x_0}{2}}$ για τυχόν x_0, από την πρώτη σχέση του συστήματος προκύπτει ότι $\overline{b} = \overline{\frac{1-x_0}{2}}$. Τότε από τη δεύτερη σχέση του συστήματος προκύπτει άμεσα ότι

$$x_0{}^2 \equiv m \pmod{p},$$

το οποίο είναι άτοπο. Επομένως το pR_K είναι πρώτο ιδεώδες του R_K. Τέλος, αν

$$\left(\frac{m}{p}\right) = 0,$$

έχουμε

$$\overline{f}(X) = (X - \overline{a})^2,$$

όπου το a είναι λύση της ισοδυναμίας

$$2x \equiv 1 \pmod{p}.$$

Επομένως

$$pR_K = P^2,$$

όπου

$$P = \langle p, \frac{1+\sqrt{m}}{2} - a \rangle.$$

□

Θεωρημα 2.4.3 (Νόμος ανάλυσης του 2)**.** *Δοθέντος τετραγωνικού αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ έχουμε τις τρεις περιπτώσεις:*

(i) Αν $m \equiv 1 \pmod 8$, τότε $2R_K = P_1P_2$, όπου τα P_1 και P_2 είναι διακεκριμένα πρώτα ιδεώδη του R_K.

(ii) Αν $m \equiv 5 \pmod 8$, τότε το ιδεώδες $2R_K$ είναι πρώτο.

(iii) Αν $m \equiv 2, 3 \pmod 8$, τότε $2R_K = P^2$, όπου το P είναι πρώτο ιδεώδες του R_K.

Απόδειξη. Για $m \equiv 2, 3 \pmod 4$ εργαζόμαστε με βάση ακεραιότητα την $\{1, \sqrt{m}\}$. Έστω $f(X) := Irr(\sqrt{m}, \mathbb{Q}) = X^2 - m$. Αν $m \equiv 2 \pmod 4$, τότε $\overline{f} = X^2 - \overline{m} = X^2 \in \mathbb{Z}_2[X]$, επομένως

$$2R_K = P^2 \text{ , όπου } P = \langle 2, \sqrt{m} \rangle.$$

Αν $m \equiv 3 \pmod 4$, τότε έχουμε

$$\overline{f} = X^2 - \overline{m} = X^2 + \overline{1} = (X + \overline{1})^2,$$

οπότε ξανά έχουμε ότι

$$2R_K = P^2,$$

όμως τώρα

$$P = \langle 2, \sqrt{m} + 1 \rangle.$$

Εναπομένει η περίπτωση $m \equiv 1 \pmod 4$. Τότε η βάση ακεραιότητας μας είναι η $\{1, \frac{1+\sqrt{m}}{2}\}$ και το ελάχιστο πολυώνυμο είναι το

$$f(X) := Irr(\omega, \mathbb{Q}) = X^2 - X - \frac{m-1}{4} \Rightarrow \overline{f}(X) = X^2 - X - \frac{\overline{m-1}}{4}.$$

Αν $m \equiv 1 \pmod 8$, τότε

$$\overline{f}(X) = X^2 - X - \frac{\overline{m-1}}{4} = X^2 - X = X(X - \overline{1}).$$

Επομένως σύμφωνα με την πρόταση 2.4.1 λαμβάνουμε ότι

$$2R_K = P_1 P_2,$$

όπου

$$P_1 = \langle 2, \frac{1+\sqrt{m}}{2} \rangle \text{ και } P_1 = \langle 2, \frac{1-\sqrt{m}}{2} \rangle.$$

Αν, τέλος, $m \equiv 5 \pmod 8$, τότε

$$\overline{f}(X) = X^2 - X - \frac{\overline{m-1}}{4} = X^2 - X - \overline{1} = X^2 + X + \overline{1},$$

το οποίο είναι ανάγωγο στο δακτύλιο $\mathbb{Z}_2[X]$ και συνεπώς το ιδεώδες $2R_K$ είναι πρώτο. □

2.5 Τάξεις τετραγωνικών αριθμητικών σωμάτων

Στη συνέχεια αναφέρουμε, χωρίς ιδιαίτερη εμβάθυνση σε αυτήν, την έννοια της τάξεως ενός τετραγωνικού αλγεβρικού σώματος αριθμών, η οποία θα χρησιμεύσει ιδιαιτέρως στη θεμελίωση του μιγαδικού πολλαπλασιασμού στο επόμενο κεφάλαιο.

Ορισμος 2.5.1. Μία *τάξη* ενός τετραγωνικού αριθμητικού σώματος K είναι ένα σύνολο $O \subseteq R_K$ με τις ιδιότητες

(i) Το O είναι υποδακτύλιος του K που περιέχει το 1.

(ii) Το O είναι ένα πεπερασμένα παραγόμενο $\mathbb{Z}$-module.

(iii) Το O περιέχει μια $\mathbb{Q}$-βάση του K.

Ο παραπάνω ορισμός, επί τη βάσει της παρατηρήσεως ότι ο δακτύλιος των ακέραιων αλγεβρικών αριθμών R_K δεν έχει στοιχεία πεπερασμένης τάξης, ισοδυναμεί με το ότι η τάξη O είναι ένα ελεύθερο $\mathbb{Z}$-module, βαθμού[1] 2. Ακόμα, από την απαίτηση (iii) του ορισμού συνεπάγεται ότι το K είναι το σώμα κλασμάτων της τάξης O.

Προφανώς ο δακτύλιος R_K είναι σε κάθε περίπτωση μία τάξη του K. Μάλιστα, από τα (i) και (ii) ο R_K είναι η μέγιστη τάξη του K, ήτοι κάθε άλλη τάξη O περιέχεται στον R_K. Έχουμε ήδη δει ότι ο R_K γράφεται υπό τη μορφή

$$R_K = \mathbb{Z} + \omega\mathbb{Z},$$

όπου το σύνολο $\{1, \omega\}$ απότελεί βάση ακεραιότητας του R_K. Επί παραδείγματι, θα μπορούσαμε να κάνουμε την επιλογή

$$\omega_K = \frac{d_K + \sqrt{d_K}}{2}.$$

Έχοντας περιγράψει τη μέγιστη τάξη, μπορούμε περιγράψουμε και κάθε άλλη.

[1]Εδώ ο όρος βαθμός αποτελεί μετάφραση του αγγλικού όρου rank.

ΠΡΟΤΑΣΗ 2.5.2. *Έστω O μία τάξη του τετραγωνικού αριθμητικού σώματος K, διακρίνουσας d_K. Τότε ο δείκτης της O στην R_K είναι πεπερασμένος και μάλιστα, εάν $f := [R_K : O]$, τότε*

$$O = \mathbb{Z} + f \cdot R_K = \langle 1, f \cdot \omega_K \rangle,$$

όπου

$$\omega_K = \frac{d_K + \sqrt{d_K}}{2}.$$

Απόδειξη. Εφόσον οι τάξεις O και R_K είναι $\mathbb{Z}$-modules βαθμού 2, τότε από τη σχέση

$$[R_K : \mathbb{Z}] = [R_K : O] \cdot [O : \mathbb{Z}],$$

έπεται το πεπερασμένο του βαθμού $[R_K : O]$. Έστω $f := [R_K : O]$. Εφόσον το f είναι η τάξη της ομάδας R_K/O, τότε για κάθε $r \in R_K$ θα ισχύει ότι $f \cdot r \in O$. Επομένως, θα έχουμε $f \cdot R_K \subseteq O$. Εξ ορισμού του O ισχύει ότι $\mathbb{Z} \subseteq O$. Άρα έχουμε $\mathbb{Z} + f \cdot R_K \subseteq O$. Έχουμε δείξει, λοιπόν, ότι ισχύει η σχέση εγκλεισμού

$$\mathbb{Z} + f \cdot R_K \subseteq O \subseteq R_K.$$

Όμως $\mathbb{Z} + f \cdot R_K = \mathbb{Z} + (f \cdot \omega_K)\mathbb{Z}$, ήτοι το σύνολο $\mathbb{Z} + f \cdot R_K$ είναι επίσης ένα ελεύθυρο $\mathbb{Z}$-module βαθμού 2. Άρα θα έχουμε ότι

$$[R_K : \mathbb{Z} + f \cdot R_K] = [R_K : O] \cdot [O : \mathbb{Z} + f \cdot R_K].$$

Για να δείξουμε, επομένως, την ισότητα $O = \mathbb{Z} + f \cdot R_K$ αρκεί να αποδείξουμε ότι $[R_K : \mathbb{Z} + f \cdot R_K] = f$. Επομένως εάν θεωρήσουμε τα $\mathbb{Z} + f \cdot R_K = \mathbb{Z} + (f \cdot \omega_K)\mathbb{Z}$ και R_K ως $\mathbb{Z}$-modules, τότε για τις βάσεις αυτών θα ισχύει ότι

$$\begin{pmatrix} 1 \\ f \cdot \omega_K \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & f \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \omega_K \end{pmatrix}.$$

Άρα έχουμε ότι

$$[R_K : \mathbb{Z} + f \cdot R_K] = \det \begin{pmatrix} 1 & 0 \\ 0 & f \end{pmatrix} = f,$$

το οποίο είναι και το ζητούμενο. □

ΟΡΙΣΜΟΣ 2.5.3. Δοθείσης τάξης O σε ένα τετραγωνικό αριθμητικό σώμα ο αριθμός $f = [R_K : O]$ ονομάζεται *οδηγός της τάξης* O.

ΟΡΙΣΜΟΣ 2.5.4. *Διακρίνουσα* μίας τάξης O ενός τετραγωνικού αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ καλείται ο ακέραιος αριθμός d_O, όπου

$$d_O = f^2 \cdot d_K = \begin{cases} f^2 m & , \text{αν } m \equiv 1 \pmod 4 \\ 4f^2 m & , \text{αν } m \equiv 2, 3 \pmod 4 \end{cases},$$

όπου f είναι ο οδηγός της τάξης O και d_K η διακρίνουσα του σώματος K.

ΠΑΡΑΤΗΡΗΣΗ 2.5.5. Κάθε γνήσια τάξη O του τετραγωνικού αριθμητικού σώματος K, ήτοι κάθε τάξη για την οποία ισχύει ότι $O \neq R_K$, δεν είναι περιοχή Dedekind, καθώς δεν είναι εν γένει ακέραια κλειστή.

Κεφάλαιο 3

Θεωρία διακλαδώσεως και σώμα του Hilbert

Στα προηγούμενα κεφάλαια μελετήσαμε τα αλγεβρικά σώματα αριθμών, τα οποία αποτελούν πεπερασμένες επεκτάσεις του σώματος $\mathbb{Q}$. Σε αυτό το κεφάλαιο, πρόκειται να επεκτείνουμε τη μελέτη μας σε επεκτάσεις, οι οποίες δε θα έχουν το σώμα των ρητών αριθμών ως βάση. Ο κύριος στόχος του κεφαλαίου αυτού είναι ο ορισμός και η μελέτη του σώματος του Hilbert ενός αλγεβρικού σώματος αριθμών.

3.1 Σχετικές επεκτάσεις αλγεβρικών σωμάτων αριθμών

Η παράγραφος αυτή βασίζεται στο [1], γι αυτό και παραπέμπουμε τον ενδιαφερόμενο αναγνώστη σε αυτό για τις αποδείξεις των αποτελεσμάτων.

Πριν κάνουμε λόγο για θεωρία διακλαδώσεως και σώμα του Hilbert πρέπει να περιγράψουμε την έννοια της σχετικής επέκτασης αλγεβρικών σωμάτων αριθμών. Έτσι, δίνουμε τον παρακάτω ορισμό:

ΟΡΙΣΜΟΣ 3.1.1. *Σχετική επέκταση αλγεβρικών σωμάτων αριθμών* (ή απλά *σχετική επέκταση*) καλούμε μία επέκταση σωμάτων της μορφής L/K, όπου καθένα από τα σώματα L και K είναι αλγεβρικό σώμα αριθμών.

Σύμφωνα με τον ορισμό που προηγήθηκε το σώμα K μπορεί να είναι οποιαδήποτε πεπερασμένη επέκταση του $\mathbb{Q}$. Εάν ισχύει ότι $K = \mathbb{Q}$, τότε κάνουμε λόγο για *απόλυτη επέκταση αλγεβρικών σωμάτων αριθμών*. Υπ' αυτή την έννοια, τα όσα μελετήθηκαν στα δύο πρώτα κεφάλαια της παρούσας πτυχιακής εργασίας αναφέρονται σε απόλυτες επεκτάσεις αλγεβρικών αριθμητικών σωμάτων.

Θεωρούμε τώρα τους δακτυλίους των ακέραιων αλγεβρικών αριθμών R_K και R_L των σωμάτων K και L, αντιστοίχως. Ο R_L είναι για προφανείς λόγους ένα R_K-module. Όμως, η διαφορά είναι ότι ενώ στην απόλυτη περίπτωση, ήτοι στην περίπτωση όπου $K = \mathbb{Q}$, ο R_L είναι ένα ελεύθερο R_K-module ($\mathbb{Z}$-module), κάτι τέτοιο δεν ισχύει εν γένει όταν $K \neq \mathbb{Q}$.

Η έννοια της norm και του ίχνους ενός στοιχείου μίας σχετικής επέκτασης αλγεβρικών σωμάτων αριθμών ορίζονται ανάλογα προς την απόλυτη περίπτωση. Μάλιστα, για λόγους ακριβείας της ορολογίας, όταν αναφερόμαστε στη norm ή στο ίχνος ενός στοιχείου a του σώματος L ως προς το σώμα K, θα λέμε ότι κάνουμε λόγο για τη *σχετική norm του* a ή το *σχετικό ίχνος του* a αντιστοίχως, και θα συμβολίζουμε ως $N_{L/K}(a)$ ή $Tr_{L/K}(a)$ αντιστοίχως.

Το αυτό ισχύει και για την έννοια της διακρίνουσας n-άδας αριθμών μίας σχετικής επέκτασης, ήτοι ο ορισμός αυτής είναι εντελώς ανάλογος προς την απόλυτη περίπτωση. Είναι φανερό ότι εάν υποθέσουμε ότι $[L : K] = n$ και επιλέξουμε μία n-άδα $a_1, a_2, \ldots, a_n$ στοιχείων του L, τότε η σχετική διακρίνουσα $d_{L/K} = d_{L/K}(a_1, a_2, \ldots, a_n)$ είναι στοιχείο του σώματος K. Επιπροσθέτως, αν καθένας από τους αριθμούς a_i, όπου $i = 1, 2, \ldots, n$, είναι ακέραιος αλγεβρικός του L, τότε $d_{L/K} \in R_K$.

Θεωρούμε, τώρα, ένα πρώτο ιδεώδες P του K. Τότε αυτό έχει μία επέκταση PR_L στο δακτύλιο R_L. Ο R_L είναι περιοχή Dedekind, άρα το ιδεώδες PR_L αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών.

$$PR_L = {Q_1}^{e_1}{Q_2}^{e_2}\cdots{Q_r}^{e_r},$$

όπου τα Q_i είναι πρώτα ιδεώδη του R_L και τα e_i φυσικοί αριθμοί, για κάθε $i = 1, 2, \ldots, r$. Τα ιδεώδη Q_i είναι τα μοναδικά πρώτα ιδεώδη του R_L για τα οποία ισχύει ότι

$$Q_i \cap R_K = P\,, \forall\, i = 1, 2, \ldots, r.$$

ΟΡΙΣΜΟΣ 3.1.2. Ο φυσικός αριθμός $e_i := e(Q_i/P)$ θα ονομάζεται *σχετικός δείκτης διακλαδώσεως* του Q_i υπεράνω του P. Μάλιστα, θα λέμε ότι το Q_i διακλαδίζεται υπεράνω του P όταν ισχύει $e_i > 1$. Ακόμα, θα λέμε ότι το P διακλαδίζεται στο σώμα L όταν υπάρχει κάποιο πρώτο ιδεώδες Q_i για το οποίο ισχύει $e_i > 1$.

Αν το Q είναι ένα πρώτο ιδεώδες του R_L, το οποίο εμφανίζεται στην ανάλυση του PR_L[1], τότε το R_L/Q αποτελεί σώμα. Μάλιστα, το R_K/P αποτελεί υπόσωμα αυτού. Το βαθμό της επέκτασης αυτής, ήτοι το

$$f = f(Q/P) = [R_L/Q : R_K/P],$$

τον καλούμε *σχετικό βαθμό αδρανείας του Q υπεράνω του P*. Άμεση συνέπεια της θεωρίας των πεπερασμένων σωμάτων είναι ότι

$$N_{L/K}(Q) = N_{K/\mathbb{Q}}(P)^{f(Q/P)}.$$

Έστω, τώρα, σώμα M για το οποίο ισχύει ότι $K \leq M \leq L$. Ως R_K, R_M και R_L συμβολίζουμε τους δακτυλίους των ακέραιων αλγεβρικών αριθμών των σωμάτων K, M και L, αντιστοίχως. Ακόμα, θεωρούμε τα πρώτα ιδεώδη P, Q και U των R_K, R_M και R_L, για τα οποία ισχύει ότι το Q βρίσκεται υπεράνω του P και το U υπεράνω του Q. Τότε ισχύουν οι σχέσεις

$$e(U/P) = e(U/Q)e(Q/P)$$

$$f(U/P) = f(U/Q)f(Q/P).$$

Κατ' αντιστοιχία προς την απόλυτη περίπτωση ισχύει το παρακάτω θεώρημα:

ΘΕΩΡΗΜΑ 3.1.3. *Υποθέτουμε ότι η L/K είναι μία επέκταση αλγεβρικών σωμάτων αριθμών, βαθμού $[L : K] = n$. Θεωρούμε ένα πρώτο ιδεώδες P του K και την μονοσήμαντη ανάλυση του ιδεώδους PR_L του R_L*

$$PR_L = {Q_1}^{e_1}{Q_2}^{e_2}\cdots{Q_r}^{e_r}.$$

Τότε ισχύει ότι

$$n = \sum_{i=1}^{r} e_i(Q_i/P)f_i(Q_i/P).$$

Όταν δε, η επέκταση L/K είναι Galois, τότε ισχύει ότι

$$e_1 = e_2 = \cdots = e_r$$

$$f_1 = f_2 = \cdots = f_r.$$

Μας ενδιαφέρει να ξέρουμε ποια ιδεώδη του K διακλαδίζονται στο σώμα $L = K(\theta)$. Προς αυτή την κατεύθυνση βοηθάει το κατωτέρω αποτέλεσμα:

ΘΕΩΡΗΜΑ 3.1.4. *Υποθέτουμε ότι η επέκταση L/K είναι μία (πεπερασμένη) επέκταση αλγεβρικών σωμάτων αριθμών και έστω ότι $L = K(\theta)$, όπου $\theta \in R_L$. Αν το πρώτο ιδεώδες P του R_K δε διαιρεί τη διακρίνουσα $d_{L/K}(\theta)$, τότε το P δε διακλαδίζεται στο σώμα L.*

[1]Όταν το Q εμφανίζεται στην ανάλυση του PR_L θα λέμε ότι το Q βρίσκεται υπεράνω του P.

ΠΑΡΑΤΗΡΗΣΗ 3.1.5. Άμεση συνέπεια του παραπάνω θεωρήματος είναι ότι υπάρχουν πεπερασμένου πλήθους πρώτα ιδεώδη του R_K τα οποία διακλαδίζονται στο L.

Επιδιώκοντας τον πλήρη προσδιορισμό των πρώτων ιδεωδών του K που διακλαδίζονται στο L, ανακύπτει η δυσκολία του ορισμού της διακρίνουσας μίας σχετικής επέκτασης. Μέχρι τώρα, έχουμε κάνει λόγο μόνο για σχετική διακρίνουσα n-άδας αριθμών. Ιδιαίτερα, δεν υπάρχει κάποιος, αντίστοιχος προς την απόλυτη περίπτωση, ορισμός για τη διακρίνουσα καθότι δεν υπάρχει εν γένει βάση ακεραιότητας του L υπεράνω του K. Με άλλα λόγια, το θεώρημα ύπαρξης βάσης ακεραιότητας παύει να έχει ισχύ στην περίπτωση των σχετικών επεκτάσεων. Παρά ταύτα, δίνουμε τον εξής ορισμό:

ΟΡΙΣΜΟΣ 3.1.6. Ονομάζουμε *σχετική διακρίνουσα της* L/K το ιδεώδες

$$\mathcal{R}_{L/K} := \langle d_{L/K}(\omega_1, \omega_2, \ldots, \omega_n) \mid \omega_1, \omega_2, \cdots, \omega_n \in R_L \rangle R_K,$$

του R_L, ήτοι το ιδεώδες που παράγεται από τις διακρίνουσες όλων των n-άδων στοιχείων του R_L.

Στην ειδική περίπτωση όπου $K = \mathbb{Q}$ ισχύει ότι

$$\mathcal{R}_{L/\mathbb{Q}} = \mathbb{Z} \cdot d_{L/\mathbb{Q}}.$$

Έτσι, κατ' αντιστοιχία με την απόλυτη περίπτωση, μπορούμε να προσδιορίσουμε πλήρως τα ιδεώδη που διακλαδίζονται μέσω του παρακάτω αποτελέσματος:

ΘΕΩΡΗΜΑ 3.1.7 (Θεώρημα της διακρίνουσας)**.** *Θεωρούμε τη σχετική επέκταση αλγεβρικών σωμάτων αριθμών L/K και P ένα πρώτο ιδεώδες του R_K. Τότε το P διακλαδίζεται στο L εάν, και μόνο εάν $P \mid \mathcal{R}_{L/K}$.*

3.2 Στοιχεία θεωρίας διακλαδώσεως του Hilbert

Όπως και η προηγούμενη παράγραφος, έτσι και αυτή βασίζεται στο [1]. Εκεί παραπέμπουμε για τις αποδείξεις των αποτελεσμάτων, αλλά και για επιπρόσθετα στοιχεία θεωρίας.

Θεωρούμε ένα αλγεβρικό σώμα αριθμών K και μία πεπερασμένη επέκταση αυτού, έστω L. Συμβολίζουμε ως R_K και R_L τους δακτύλιους των ακέραιων αλγεβρικών αριθμών των σωμάτων K και L, αντιστοίχως. Υποθέτουμε ότι η επέκταση L/K είναι επέκταση Galois. Έτσι, θέτουμε

$$G := Gal(L/K).$$

ΘΕΩΡΗΜΑ 3.2.1. *Έστω L αλγεβρικό σώμα αριθμών τέτοιο, ώστε η επέκταση L/K να είναι Galois και ένα πρώτο ιδεώδες P του . Θεωρούμε το ιδεώδες*

$$PR_L = \left(Q_1 Q_2 \cdots Q_r\right)^e.$$

Τότε η G δρα μεταβατικά στο σύνολο των Q_i, ήτοι

$$PR_L = \prod_{\sigma \in G_\#} \sigma(Q)\,,\ Q \in \{Q_1, Q_2, \ldots, Q_r\}\,,$$

όπου ως $G_\#$ συμβολίζουμε το σύνολο των στοιχείων της G που δίνουν διαφορετικές μεταξύ τους εικόνες.

ΠΟΡΙΣΜΑ 3.2.2. *Βάσει του θεωρήματος 3.1.3 ισχύει ότι*

$$efr = n =: [L : K].$$

Επομένως ο προσδιορισμός του νόμου ανάλυσης στην ειδική περίπτωση όπου η επέκταση μας είναι Galois, ανάγεται στη μελέτη της ομάδας G και των υποομάδων αυτής.

Ορισμος 3.2.3. Θωρούμε το πρώτο ιδεώδες P του K και ένα πρώτο ιδεώδες Q του L, το οποίο βρίσκεται υπεράνω του P. Τότε ορίζουμε τα υποσύνολα της G

$$G_Z := G_Z(Q/P) := \{\sigma \in G \mid \sigma(Q) = Q\}$$

$$G_T := G_T(Q/P) := \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{Q}, \forall \alpha \in R_L\}.$$

Τα σύνολα αυτά με πράξη τη σύνθεση απεικονίσεων αποτελούν ομάδες. Άρα είναι υποομάδες της G. Η μεν G_Z καλείται *ομάδα αναλύσεως του* Q, ενώ η δε G_T ονομάζεται *ομάδα αδρανείας του* Q. Επί τη βάσει του θεμελιώδους θεωρήματος της θεωρίας Galois, οι ομάδες G_Z και G_T αντιστοιχούν σε κάποια υποσώματα του L, έστω τα

$$L_Z := L_Z(Q/P) \text{ και } L_T := L_T(Q/P),$$

αντιστοίχως. Το L_Z ονομάζεται *σώμα αναλύσεως του* Q και το L_T καλείται *σώμα αδρανείας του* Q.

Παρατηρηση 3.2.4. Ισχύει ότι

$$G_T \leq G_Z \leq G$$

και λόγω της θεωρίας Galois έχουμε

$$K \leq K_Z \leq K_T \leq L.$$

Μάλιστα, για τις ομάδες αναλύσεως και αδρανείας έχουμε κάτι ισχυρότερο, ότι

$$G_T \trianglelefteq G_Z.$$

Έστω δυο στοιχεία $\sigma \in G_Z$ και $\tau \in G_T$. Τότε όταν το α διατρέχει τα στοιχεία του R_L το αυτό ισχύει και για το $\sigma^{-1}(\alpha)$, όταν $\sigma \in G$. Επομένως έχουμε ότι

$$\tau(\alpha) \equiv \alpha \pmod{Q}, \forall \alpha \in R_L \Rightarrow \tau\big(\sigma^{-1}(\alpha)\big) \equiv \sigma^{-1}(\alpha) \pmod{Q}, \forall \alpha \in R_L \Rightarrow$$

$$\sigma\tau\sigma^{-1}(\alpha) \equiv \alpha \pmod{Q}, \forall \alpha \in R_L \Rightarrow \sigma\tau\sigma^{-1} \in G_T \Rightarrow \sigma^{-1}G_T\sigma \subseteq G_T.$$

Εφαρμόζοντας την τελευταία σχέση για σ^{-1} έχουμε ότι

$$\sigma G_T \sigma^{-1} \subseteq G_T \Rightarrow G_T \subseteq \sigma^{-1}G_T\sigma.$$

Τελικά για κάθε $\sigma \in G_Z$ ισχύει ότι

$$G_T = \sigma^{-1}G_T\sigma,$$

γεγονός το οποίο αποδεικνύει ότι $G_T \trianglelefteq G_Z$.

Εάν $Q \trianglelefteq R_L$ είναι ένα πρώτο ιδεώδες, η εικόνα του μέσω ενός στοιχείου της ομάδας G, έστω το σ είναι επίσης πρώτο ιδεώδες του R_L. Πράγματι, εάν θεωρήσουμε δύο στοιχεία $\alpha, \beta \in R_L$, τέτοια ώστε $\alpha\beta \in \sigma(Q)$, τότε έχουμε

$$\alpha\beta \in \sigma(Q) \Rightarrow \exists q \in Q : \sigma(q) = \alpha\beta \Rightarrow \sigma^{-1}(\alpha)\sigma^{-1}(\beta) = \sigma^{-1}(\alpha\beta) = q \in Q \Rightarrow$$

$$\sigma^{-1}(\alpha) \in Q \text{ ή } \sigma^{-1}(\beta) \in Q \Rightarrow \alpha \in \sigma(Q) \text{ ή } \beta \in \sigma(Q).$$

Το ερώτημα είναι ποία είναι η σχέση των ομάδων αδρανείας και αναλύσεως του Q και του $\sigma(Q)$. Υποθέτουμε ένα στοιχείο $\tau \in G_Z(\sigma(Q)/P)$. Τότε εξ ορισμού της ομάδας αναλύσεως ισχύει ότι

$$\tau\big(\sigma(Q)\big) = \sigma(Q) \Rightarrow \big(\sigma^{-1}\tau\sigma\big)(Q) = Q \Rightarrow \tau \in \sigma G_Z(Q/P)\sigma^{-1}.$$

Επομένως ισχύει ότι

$$G_Z(\sigma(Q)/P) \subseteq \sigma G_Z(Q/P)\sigma^{-1}.$$

Από την άλλη τώρα, εάν επιλέξουμε ένα στοιχείο $\rho \in G_Z(Q/P)$, τότε έχουμε

$$\rho(Q) = Q \Rightarrow \sigma\rho\sigma^{-1}\big(\sigma(Q)\big) = \sigma(Q) \Rightarrow \sigma\rho\sigma^{-1} \in G_Z(\sigma(Q)/P) \Rightarrow \sigma G_Z(Q/P)\sigma^{-1} \subseteq G_Z(\sigma(Q)/P).$$

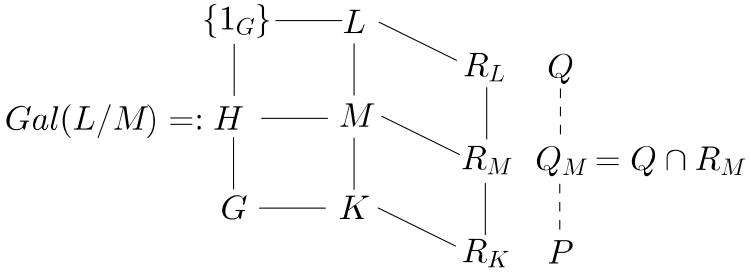
Οπότε τελικά προκύπτει η ισότητα

$$G_Z(\sigma(Q)/P) = \sigma G_Z(Q/P)\sigma^{-1}.$$

Η ισότητα αυτή μας λέει ότι οι ομάδες αναλύσεως των ιδεωδών Q και $\sigma(Q)$ είναι συζυγείς υποομάδες της G. Το αυτό ισχύει και για τις ομάδες αδρανείας, ήτοι

$$G_T(\sigma(Q)/P) = \sigma G_T(Q/P)\sigma^{-1}.$$

Ας υποθέσουμε τώρα ότι το M είναι ένα ενδιάμεσο της επέκτασης L/K, ήτοι ένα σώμα M για το οποίο ισχύει ότι $K \leq M \leq L$. Τότε έχουμε σχηματικά την εξής κατάσταση:



Για τις ομάδες αναλύσεως και αδρανείας του ιδεώδους $Q_M \in R_M$ έχουμε ότι

$$\begin{aligned} G_Z(Q/Q_M) &= \{\sigma \in H \mid \sigma(Q) = Q\} \\ &= \{\sigma \in G \mid \sigma(Q) = Q \text{ και } \sigma|_M = 1_G\} \\ &= H \cap G_Z(Q/P). \end{aligned}$$

Αναλόγως, ισχύει ότι

$$G_T(Q/Q_M) = H \cap G_T(Q/P).$$

Ας υποθέσουμε τώρα ότι το ενδιάμεσο σώμα στο οποίο αναφερόμαστε είναι το K_Z. Εφόσον έχουμε υποθέσει ότι η επέκταση L/K είναι επέκταση Galois, το αυτό θα ισχύει και για την επέκταση L/K_Z. Αρχικά, θα υπολογίσουμε το δείκτη $[G : G_Z]$. Υποθέτουμε ότι $[G : G_Z] = g$. Τότε μπορούμε να γράψουμε την ομάδα G υπό τη μορφή

$$G = \dot{\bigcup_{i\in\{1,2,\ldots,r\}}} \sigma_i(G_Z),$$

όπου τα σ_i δημιουργούν ένα πλήρες σύστημα αριστερών αντιπροσώπων της G_Z εντός της G. Προφανώς ισχύει ότι

$$\sigma_i(Q) \neq \sigma_j(Q)\ , \forall i \neq j.$$

Πράγματι, αν ίσχυε το αντίθετο θα είχαμε

$$\sigma_j{}^{-1}\sigma_i(Q) = Q \Rightarrow \sigma_j{}^{-1}\sigma_i \in G_Z \Rightarrow \sigma_i \in \sigma_j G_Z \Rightarrow \sigma_i G_Z \subseteq \sigma_j G_Z \Rightarrow \sigma_i G_Z = \sigma_j G_Z \Rightarrow i = j,$$

το οποίο είναι άτοπο. Από την άλλη, εάν υποθέσουμε ότι $\sigma \in G$, τότε υπάρχει $i \in \{1, 2, \ldots, g\}$, τέτοιο ώστε

$$\sigma = \sigma_i \tau \, , \tau \in G_Z.$$

Άρα

$$\sigma(Q) = \sigma_i\big(\tau(Q)\big) = \sigma_i(Q).$$

Αυτό μας λέει ότι $g = r$. Άρα έχουμε αποδείξει την εξής πρόταση:

ΠΡΟΤΑΣΗ 3.2.5. *Έστω αλγεβικά σώματα αριθμών K και L με την ιδιότητα ότι το L να είναι επέκταση Galois του K. Υποθέτουμε ακόμα ότι το ιδεώδες PR_L, όπου R_L είναι ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του L και P ένα πρώτο ιδεώδες του K, γράφεται υπο τη μορφή*

$$PR_L = \big(\sigma_1(Q)\sigma_2(Q)\cdots\sigma_r(Q)\big)^e.$$

Τότε ισχύει ότι

$$[G : G_Z(Q/P)] = r \;\; \textit{και} \;\; [K_Z : K] = r.$$

Επομένως έχουμε και ότι

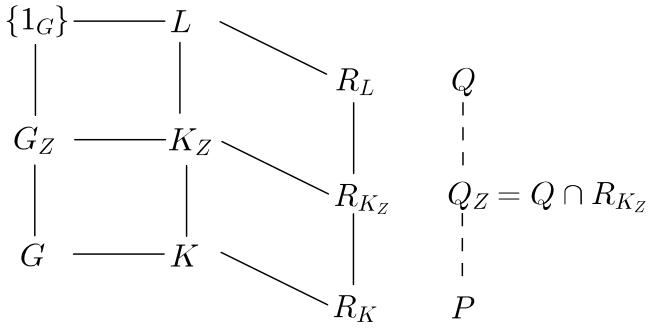
$$[G_Z : \{1_G\}] = ef,$$

άρα και

$$[L : K_Z] = ef,$$

όπου το f είναι ο βαθμός αδρανείας του ιδεώδους Q στην επέκταση L/K.

Παρατηρούμε τώρα ότι η ομάδα ανάλυσης της επέκτασης Galois L/K_Z είναι, βάσει των όσων έχουμε αναφέρει, η $G_Z \cap G_Z = G_Z$, ήτοι η ομάδα ανάλυσης της επέκτασης L/K



Αυτό σημαίνει ότι θα έχουμε και

$$G_Z(Q/Q_Z) = G_Z(Q/P).$$

Επομένως το ιδεώδες $Q_Z R_L$ έχει ως μοναδικό του παράγοντα το πρώτο ιδεώδες Q, το οποίο μας πληροφορεί ότι

$$Q_Z R_L = Q^{e'} \, , e' := e(Q/Q_Z) \leq e(Q/P) =: e.$$

Ομοίως για τους βαθμούς αδρανείας των ιδεωδών έπεται ότι

$$f' := f(Q/Q_Z) \leq f(Q/P) =: f.$$

Επί τη βάσει της προτάσεως 3.2.5 για την G_Z ειδωμένη ως ομάδας ανάλυσης της επέκτασης L/K ισχύει ότι $[G_Z : \{1_G\}] = ef$. Εάν δούμε όμως την G_Z ως ομάδα ανάλυσης της L/K_Z, τότε ισχύει ότι $[G_Z : \{1_G\}] = e'f'$. Κι εφόσον έχουμε δείξει τις σχέσεις $e' \leq e$ και $f' \leq f$ λαμβάνουμε ότι $e = e'$ και $f = f'$. Εφόσον το ιδεώδες Q είναι πρώτο θα είναι και μεγιστικό. Επομένως ο πηλικοδακτύλιος R_L/Q είναι σώμα. Μάλιστα, έχουμε δει ότι ο R_K/Q έχει πεπερασμένου πλήθους στοιχεία. Αυτό σημαίνει ότι πρόκειται για πεπερασμένο σώμα, το οποίο μάλιστα είναι επέκταση σωμάτων του $\mathbf{F}_p$.

Το αυτό ισχύει και για τον πηλικοδακτύλιο R_K/P. Είναι επέκταση σωμάτων του $\mathbf{F}_p$. Ο βαθμός της επέκτασης αυτής

$$f = [R_L/Q : R_K/P],$$

είναι ο (σχετικός) βαθμός αδρανείας. Από τη θεωρία των πεπερασμένων σωμάτων είναι γνωστό ότι η επέκταση $(R_K/Q)/(R_L/P)$ είναι επέκταση Galois. Επιπροσθέτως, είναι κυκλική τάξης f. Επιθυμούμε σε αυτό το σημείο να συσχετίσουμε την ομάδα

$$\bar{G} := Gal\big((R_L/Q)/(R_K/P)\big)$$

με τις ομάδες G_Z και G_T που έχουμε ορίσει παραπάνω. Προς τούτο θεωρούμε το φυσικό επιμορφισμό του R_L

$$\begin{array}{rcl} \pi & : & R_L \longrightarrow R_L/Q \\ & & r \longmapsto r + Q \end{array}$$

και ένα στοιχείο $\sigma \in G_Z$. Για τυχόν $r \in R_L$ και $\tau \in G$ έχουμε ότι

$$\tau(r) \in R_L \Rightarrow \tau(R_L) \subseteq R_L.$$

Ακόμα έχουμε και ότι

$$\tau^{-1}(r) \in R_L \Rightarrow \tau^{-1}(R_L) \subseteq R_L \Rightarrow R_L \subseteq \tau(R_L).$$

Τελικά ισχύει ότι $\tau(R_L) = R_L$, ήτοι ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του σώματος L παραμένει αναλλοίωτος από τη δράση οποιουδήποτε στοιχείου της ομάδας $G = Gal(L/K)$. Επί τη βάσει αυτής της παρατηρήσεως, αν για το $\sigma \in G_Z$ ορίσουμε την απεικόνιση

$$\begin{array}{rcl} \bar{\sigma} & : & R_L/Q \longrightarrow R_L/Q \\ & & r + Q \longmapsto \sigma(r) + Q, \end{array}$$

αυτή αποτελεί και R_K/P-αυτομορφισμό του σώματος R_L/Q, δηλαδή

$$\bar{\sigma} \in \bar{G}.$$

Εάν, λοιπόν, ορίσουμε την απεικόνιση

$$\begin{array}{rcl} \phi & : & G_Z \longrightarrow \bar{G} \\ & & \sigma \longmapsto \bar{\sigma}, \end{array}$$

τότε ο ϕ είναι ένας ομομορφισμός ομάδων. Ακόμα παρατηρούμε ότι

$$\begin{array}{rcl} Ker(\phi) & = & \{\sigma \in G_Z \mid \bar{\sigma} = \phi(\sigma) = Id_{\bar{G}}\} \\ & = & \{\sigma \in G_Z \mid \bar{\sigma}(\alpha + Q) = \alpha + Q\,, \forall \alpha \in R_L\} \\ & = & \{\sigma \in G_Z \mid \sigma(\alpha) + Q = \alpha + Q\,, \forall \alpha \in R_L\} \\ & = & \{\sigma \in G_Z \mid \sigma(\alpha) \equiv \alpha \pmod{Q}\,, \forall \alpha \in R_L\} \\ & = & G_T. \end{array}$$

Η ϕ είναι επιμορφισμός, αποτέλεσμα του οποίου την απόδειξη εγκαταλείπουμε για λόγους συντομίας. Έτσι, εφαρμόζοντας το πρώτο θεώρημα των ισομορφισμών αποδεικνύουμε το παρακάτω αποτέλεσμα:

Θεωρημα 3.2.6. *Θεωρούμε τη σχετική επέκταση Galois L/K αλγεβρικών σωμάτων αριθμών, ένα πρώτο ιδεώδες P του K και το πρώτο ιδεώδες Q του L που βρίσκεται υπεράνω του P. Τότε, αν θέσουμε*

$$G_Z := G_Z(Q/P) \ \textit{και}\ G_T := G_T(Q/P),$$

ισχύει ότι

$$G_Z/G_T \cong \bar{G}.$$

Επομένως η ομάδα G_Z/G_T είναι κυκλική τάξης f. Και βάσει του θεμελιώδους θεωρήματος της θεωρίας Galois για την επέκταση K_T/K_Z, ισχύει ότι

$$[K_T : K_Z] = f \Rightarrow [L : K_T] = e = [G_T : \{1_G\}].$$

Τα ανωτέρω αποτελέσματα συνοψίζονται στο παρακάτω θεώρημα

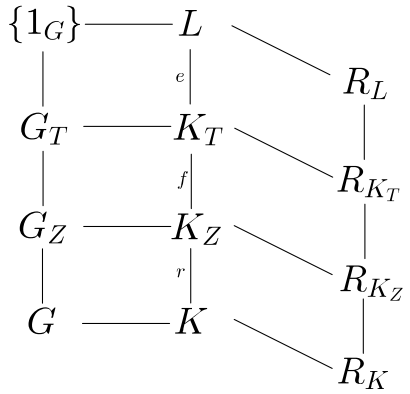
Θεωρημα 3.2.7. *Θεωρούμε αλγεβρικά σώματα αριθμών K και L τέτοια, ώστε το L να αποτελεί επέκταση Galois του K. Έστω, ακόμα, P ένα πρώτο ιδεώδες του K και Q ένα πρώτο ιδεώδες του L, το οποίο βρίσκεται υπεράνω του P. Εάν συμβολίσουμε ως $G_Z(Q/P)$ και $G_T(Q/P)$ τις ομάδες αναλύσεως και αδρανείας αντίστοιχα της επέκτασης L/K και θέσουμε*

$$\bar{G} := Gal\big((R_L/Q)/(R_K/P)\big),$$

τότε η

$$1_G \to G_T(Q/P) \to G_Z(Q/P) \to \bar{G} \to 1_G$$

αποτελεί βραχεία ακριβή ακολουθία[2].



Πορισμα 3.2.8. *Τα παρακάτω είναι ισοδύναμα:*

(i) Το πρώτο ιδεώδες P δε διακλαδίζεται στο σώμα L.

(ii) Για κάθε ιδεώδες πρώτο Q του L, το οποίο βρίσκεται υπεράνω του Q, ισχύει ότι

$$G_T(Q/P) = \{1_G\}.$$

(iii) Ο ομομορφισμός $\phi : G_Z \longrightarrow \bar{G}$ είναι ισομορφισμός ομάδων.

Πορισμα 3.2.9. *Έστω ότι $G_Z \trianglelefteq G$. τότε το πρώτο ιδεώδες P αναλύεται σε γινόμενο r πρώτων ιδεωδών στο K_Z. Αν ακόμα ισχύει ότι $G_T \trianglelefteq G$ τότε καθένα από τα προαναφερθέντα πρώτα ιδεώδη αδρανεί στο K_T και στη συνέχεια κάθε πρώτο ιδεώδες γίνεται e-οστή δύναμη ενός πρώτου ιδεώδους του L.*

Απόδειξη. Έστω ότι ισχύει $G_Z \trianglelefteq G$. Αυτό σημαίνει ότι η επέκταση K_Z/K είναι επέκταση Galois βαθμού r. Για το ιδεώδες Q_Z ισχύει ότι

$$f(Q_Z/P) = e(Q_Z/P) = 1 \Rightarrow PR_{K_Z} = Q_{Z,1}Q_{Z,2}\cdots Q_{Z,r},$$

[2]Κάθε *Βραχεία ακριβής ακολουθίας* δίνεται από δύο απεικονίσεις $\alpha : A \to B$ και $\beta : B \to C$ και συμβολίζεται ως

$$1 \to A \to B \to C \to 1.$$

Η απεικόνιση α είναι μονομορφισμός, ενώ η β είναι επιμορφισμός. Μάλιστα, ο πυρήνας της β είναι η εικόνα της α. Έτσι, αποδεικνύεται και ότι $C \cong B/A$.

όπου τα $Q_{Z,i}$ με $i = 1, 2, \ldots, r$ είναι ιδεώδη του K_Z που βρίσκονται υπεράνω του P και έχουν τον ίδιο βαθμό αδρανείας και αναλύσεως. Επειδή δε το πλήθος των πρώτων ιδεωδών στο K_Z που βρίσκονται υπεράνω του P είναι r, το ίδιο πλήθος πρώτων ιδεωδών θα συναντάται και στην παραγοντοποίηση στο K_T.
Εάν τώρα ισχύει και ότι $G_T \trianglelefteq G$, τότε η επέκταση K_T/K είναι Galois. Άρα για κάθε πρώτο ιδεώδες $Q_T \in R_{K_T}$ το οποίο βρίσκεται υπεράνω του Q_Z θα ισχύει ότι

$$e(Q_T/Q_Z) = e(Q_T/P) = 1.$$

Επομένως έχουμε:

$$Q_Z R_{K_T} = Q_T,$$

με $f(Q_T/Q_Z) = [K_T : K_Z]$. Κατά συνέπεια έχουμε ότι

$$P R_{K_T} = Q_{T,1} Q_{T,2} \cdots Q_{T,r},$$

οπότε $e = e(Q/Q_T)$, αφού για κάθε $Q \trianglelefteq R_L$ που διαιρεί το P, ήτοι βρίσκεται υπεράνω αυτού, ισχύει ότι $efr = n$. □

ΠΑΡΑΤΗΡΗΣΗ 3.2.10. Οι υποθέσεις του τελευταίου πορίσματος ικανοποιούνται εάν η επέκταση L/K είναι επί παραδείγματι αβελιανή.

3.3 Το σύμβολο του Artin για αβελιανές σχετικές επεκτάσεις

Θεωρούμε μία σχετική επέκταση L/K αλγεβρικών σωμάτων αριθμών, η οποία να είναι επέκταση σωμάτων Galois, και ένα πρώτο ιδεώδες P του K, το οποίο δε διακλαδίζεται στο L. Έστω, ακόμα, ιδεώδες Q του L, το οποίο βρίσκεται υπεράνω του P. Λόγω της σύμβασης ότι το P δε διακλαδίζεται ισχύει ότι

$$e(Q/P) = 1 \Rightarrow \#\big(G_T(Q/P)\big) = 1$$

Σύμφωνα με το θεώρημα 3.2.6, αυτό σημαίνει ότι

$$\bar{G} \cong G_Z(Q/P).$$

Υπενθυμίζουμε ότι η ομάδα $\bar{G}$ είναι ομάδα Galois μίας επέκτασης πεπερασμένων σωμάτων και, μάλιστα, έχουμε δει ότι είναι τάξης f. Ιδιαίτερα, είναι μία κυκλική ομάδα τάξης $f = [R_L/Q : R_K/P]$. Επομένως και η ομάδα αναλύσεως $G_Z(Q/P)$ είναι μία κυκλική ομάδα τάξης f.

Σύμφωνα με τη θεωρία των πεπερασμένων σωμάτων η ομάδα $\bar{G}$ παράγεται από τον αυτόμορφισμό του Frobenius. Περνώντας στην ισόμορφη ομάδα της $\bar{G}$, ήτοι στην $G_Z(Q/P)$, τότε παράγεται από τον αυτομορφισμό

$$\begin{aligned} \chi \;:\; & R_L/Q \longrightarrow R_L/Q \\ & x + Q \longmapsto (x+Q)^{N_K(P)} = x^{N_K(P)} + Q \end{aligned}$$

Αυτό σημαίνει ότι ο αυτομορφισμός χ εξαρτάται από την επιλογή του ιδεώδους Q που βρίσκεται υπεράνω του P. Για να αναδείξουμε αυτή την εξάρτηση από αυτό το σημείο θέτουμε

$$\left[\frac{L/K}{Q}\right] := \chi.$$

Αυτό είναι το σύμβολο του Frobenius.

ΠΡΟΤΑΣΗ 3.3.1. *Έστω πρώτο ιδεώδες P του K, το οποίο δε διακλαδίζεται στο L, και ένα πρώτο ιδεώδες Q του L που βρίσκεται υπεράνω του K. Τότε, για τυχόντα αυτομορφισμό $\sigma \in G$ ισχύει ότι*

$$\left[\frac{L/K}{\sigma(Q)}\right] = \sigma\left[\frac{L/K}{Q}\right]\sigma^{-1}$$

Απόδειξη. Κάθε στοιχείο του R_L μπορεί να γραφεί υπό τη μορφή $\sigma^{-1}(x)$, όπου $x \in R_L$. Αυτό σημαίνει ότι

$$\left[\frac{L/K}{Q}\right]\left(\sigma^{-1}(x)\right) \equiv \left(\sigma^{-1}(x)\right)^{N_K(P)} \pmod{Q}.$$

Εφαρμόζοντας τον αυτομορφισμό σ στην ανωτέρω ισοτιμία λαμβάνουμε ότι

$$\sigma\left[\frac{L/K}{Q}\right]\sigma^{-1}(x) \equiv x^{N_K(P)} \pmod{\sigma(Q)}.$$

Το επιθυμητό αποτέλεσμα προκύπτει από τη μοναδικότητα του συμβόλου Frobenius. □

Μέχρι τώρα, πέραν της υποθέσεως ότι η σχετική επέκταση είναι Galois, δεν έχουμε υποθέσει τίποτα παραπάνω. Από αυτό σημείο θεωρούμε ότι η επέκταση L/K είναι επιπροσθέτως αβελιανή, ήτοι η ομάδα Galois αυτής είναι αβελιανή. Τότε η πρόταση 3.3.1 έχει ως συνέπεια το εξής:

ΠΟΡΙΣΜΑ 3.3.2. *Θεωρούμε μία αβελιανή σχετική επέκταση L/K , ένα μη διακλαδιζόμενο πρώτο ιδεώδες P του K και ένα πρώτο ιδεώδες Q του L που βρίσκεται υπεράνω του K. Τότε ισχύει ότι*

$$\left[\frac{L/K}{Q}\right] = \left[\frac{L/K}{\sigma(Q)}\right], \forall\, \sigma \in G := Gal(L/K).$$

Το ανωτέρω αποτέλεσμα μας υποδεικνύει ότι ο αυτομορφισμός Frobenius στην περίπτωση των αβελιανών επεκτάσεων εξαρτάται μονάχα από το πρώτο ιδεώδες P και όχι από την επιλογή του πρώτου ιδεώδους Q που βρίσκεται υπεράνω αυτού. Προς τούτο, αντί του συμβόλου

$$\left[\frac{L/K}{Q}\right],$$

θα χρησιμοποιούμε το σύμβολο

$$\left[\frac{L/K}{P}\right].$$

Υπ' αυτή την έννοια ο αυτομορφισμός του Frobenius μπορεί να ειδωθεί ως αντιστοιχία μεταξύ των μη διακλαδιζόμενων πρώτων ιδεωδών του K και των στοιχείων της ομάδας G. Εάν θεωρήσουμε ένα τυχόν ιδεώδες A του K, στου οποίου την ανάλυση συμμετέχουν μόνο μη διακλαδιζόμενα πρώτα ιδεώδη, τότε αυτό γράφεται μονοσήμαντα υπό τη μορφή

$$A = \prod_P P^{a_P},$$

όπου το P διατρέχει το σύνολο όλων των πρώτων ιδεωδών του K και οι αριθμοί $a_P \in \mathbb{Z}$ είναι σχεδόν όλοι ίσοι με 0. Θέτοντας

$$\left(\frac{L/K}{A}\right) = \prod_P \left[\frac{L/K}{P}\right]^{a_P}$$

είμαστε έτοιμοι να ορίσουμε το σύμβολο του Artin.

ΟΡΙΣΜΟΣ 3.3.3. Θεωρούμε αβελιανή σχετική επέκταση L/K και I_* το ιδεώδες του L που παράγεται από όλα τα μη διακλαδιζόμενα πρώτα ιδεώδη του K. Η απεικόνιση

$$\begin{aligned}\left(\frac{L/K}{\cdot}\right) \quad : \quad & I_* \longrightarrow Gal(L/K) \\ & A \longmapsto \left(\frac{L/K}{A}\right)\end{aligned}$$

είναι ομομορφισμός ομάδων και καλείται *απεικόνιση του Artin*. Την εικόνα

$$\left(\frac{L/K}{A}\right)$$

την όνομάζουμε *σύμβολο Artin του* A.

ΠΡΟΤΑΣΗ 3.3.4. *Έστω L/K μία αβελιανή επέκταση Galois και P ένα μη διακλαδιζόμενο πρώτο ιδεώδες του . Δοθέντος πρώτου ιδεώδους Q του L που βρίσκεται υπεράνω του P έχουμε ότι*

(i) Η τάξη του στοιχείου

$$\left(\frac{L/K}{Q}\right)$$

στην ομάδα $G := Gal(L/K)$ είναι $f = f(Q/P)$.

(ii) Το ιδεώδες P αναλύεται πλήρως στο L εάν, και μόνο εάν ισχύει ότι

$$\left(\frac{L/K}{Q}\right) = 1_G.$$

Απόδειξη. (i) Εύκολο εξ ορισμού του αυτομορφισμού Frobenius.

(ii) Το ιδεώδες P του K αναλύεται πλήρως στο L όταν ισχύει ότι $e(Q/P) = f(Q/P) = 1$. Ήδη γνωρίζουμε ότι $e(Q/P) = 1$. Το συμπέρασμα προκύπτει από το (i).

□

3.4 Θεωρία κλάσεων σωμάτων

Αναφερόμενοι στη θεωρία κλάσεων σωμάτων ουσιαστικά κάνουμε λόγο για μία πλήρη θεωρία που μελετά τις πεπερασμένες αβελιανές επεκτάσεις αλγεβρικών σωμάτων αριθμών.

Θεωρούμε μία σχετική επέκταση L/K αλγεβρικών σωμάτων αριθμών[3]. Εάν ως R_K συμβολίσουμε το δακτύλιο των ακέραιων αλγεβρικών αριθμών του σώματος K, τότε τα πρώτα ιδεώδη του R_K τα καλούμε *πεπερασμένους πρώτους του* K. Εκτός αυτών υπάρχουν και οι *άπειροι πρώτοι του* K, οι οποίοι ορίζονται μέσω εμφυτεύσεων του K. Ένας *πραγματικός άπειρος πρώτος* είναι μία εμφύτευση του σώματος K στο $\mathbb{R}$. Από την άλλη, ένας *μιγαδικός άπειρος πρώτος του* K είναι ένα ζεύγος συζυγών εμφυτεύσεων του K στο $\mathbb{C}$. Θα λέμε ότι ένας άπειρος πρώτος του K διακλαδίζεται εάν είναι πραγματικός άπειρος πρώτος αλλά έχει μια μιγαδική επέκταση στο L. Η σχετική επέκταση L/K θα ονομάζεται *μη διακλαδιζόμενη* εάν κάθε πρώτος του K (πεπερασμένος ή άπειρος) δε διακλαδίζεται στο L.

[3]Στην πορεία θα εγκαταλείψουμε την έννοια της σχετικής επέκτασης αλγεβρικών σωμάτων αριθμών και θα κάνουμε λόγο για (πεπερασμένες) αβελιανές επεκτάσεις ενός αλγεβρικού σώματος αριθμων.

ΟΡΙΣΜΟΣ 3.4.1. Ονομάζουμε *modulus στο* K ένα τυπικό γινόμενο της μορφής

$$\mathfrak{m} := \prod_P P^{n_P},$$

όπου το γινόμενο λαμβάνεται στο σύνολο όλων των πρώτων του K, πεπερασμένων ή άπειρων, και οι εκθέτες $n_P \in \mathbb{Z}$ ικανοποιούν τις εξής ιδιότητες:

(i) $n_P \geq 0$, και σχεδόν όλοι είναι ίσοι με 0[4].

(ii) $n_P = 0$, όταν ο P είναι ένας μιγαδικός άπειρος πρώτος.

(iii) $n_P \leq 1$, όταν ο P είναι πραγματικός άπειρος πρώτος.

Επί τη βάσει του ανωτέρω ορισμού κάθε modulus $\mathfrak{m}$ μπορεί να γραφεί υπό τη μορφή

$$\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty,$$

όπου το $\mathfrak{m}_0$ αποτελεί ένα ακέραιο ιδεώδες του δακτυλίου R_K των ακέραιων αλγεβρικών αριθμών του K και το $\mathfrak{m}_\infty$ είναι γινόμενο διακεκριμένων πραγματικών άπειρων πρώτων του K.

Είναι δυνατόν όλοι οι εκθέτες n_P να είναι ίσοι με το 0 και τότε $\mathfrak{m} = 1$.

Στην περίπτωση που το K είναι *πλήρως μιγαδικό*, ήτοι αλγεβρικό σώμα αριθμών του οποίου όλοι οι άπειροι πρώτοι είναι μιγαδικοί, το modulus $\mathfrak{m}$ λαμβάνει τη μορφή $\mathfrak{m} = \mathfrak{m}_0$, είναι δηλαδή ένα ακέραιο ιδεώδες του R_K. Το να είναι ένα αλγεβρικό σώμα αριθμών $K = \mathbb{Q}(\theta)$, πλήρως μιγαδικό ισοδυναμεί με το συμπέρασμα ότι όλα τα σημεία μηδενισμού του πολυωνύμου $Irr(\theta, \mathbb{Q})$ είναι μιγαδικοί αριθμοί. Έτσι, εάν θεωρήσουμε ένα τετραγωνικό μιγαδικό σώμα $K = \mathbb{Q}(\sqrt{m})$, με $m < 0$, μιας και αυτή είναι η περίπτωση για την οποία ενδιαφερόμαστε, τότε τα σημεία μηδενισμού του πολυωνύμου $Irr(\sqrt{m}, \mathbb{Q}) = X^2 - m$ είναι τα $\pm\sqrt{m}$, τα οποία είναι μιγαδικοί αριθμοί. Επομένως, κάθε τετραγωνικό μιγαδικό σώμα αριθμών είναι πλήρως μιγαδικό αλγεβρικό σώμα αριθμών.

ΟΡΙΣΜΟΣ 3.4.2. Δοθέντος τυχόντος modulus $\mathfrak{m}$, θεωρούμε την ομάδα

$$\begin{aligned} I_K(\mathfrak{m}) \quad := \quad & \{\frac{A}{B} \mid A, B \text{ ακέραια ιδεώδη του } K \text{ τέτοια, ώστε τα ιδεώδη} \\ & \frac{A}{B} \text{ και } \mathfrak{m} \text{ να είναι πρώτα μεταξύ τους}\} \end{aligned}$$

και την υποομάδα αυτής

$$P_{K,1}(\mathfrak{m}) := \{\alpha R_K \in I_K(\mathfrak{m}) \, , \, \alpha \in K^\times \mid \alpha \equiv 1 \pmod{\mathfrak{m}}\}.$$

ΠΑΡΑΤΗΡΗΣΗ 3.4.3. Πριν συνεχίσουμε πρέπει να εξηγήσουμε την ισοτιμία

$$\alpha \equiv 1 \pmod{\mathfrak{m}}.$$

Η ισχύς της εν λόγω ισοτιμίας ισοδυναμεί με την ταυτόχρονη ικανοποίηση των συνθηκών

$$\alpha \equiv 1 \pmod{\mathfrak{m}_0}$$

και $\sigma(\alpha) > 0$, $\forall$ πραγματικό άπειρο πρώτο σ του K που διαιρεί το $\mathfrak{m}_\infty$.

Σε ότι αφορά στην ισοτιμία

$$\alpha \equiv 1 \pmod{\mathfrak{m}_0},$$

[4]Όταν λέμε ότι σχεδόν όλοι οι εκθέτες είναι ίσοι με 0, εννοούμε ότι εκτός κάποιου πεπερασμένου πλήθους εξαιρέσεων είναι όλοι ίσοι με 0.

αφού $\alpha \in K^{\times}$ και το K είναι το σώμα κλασμάτων του δακτυλίου R_K, υπάρχουν αριθμοί $a, b \in R_K$ τέτοιοι, ώστε

$$\alpha = \frac{a}{b}\text{, με } \big(\langle a\rangle, \mathfrak{m}\big) = \big(\langle b\rangle, \mathfrak{m}\big) = 1$$

Έτσι,

$$\frac{a}{b} \equiv 1 \pmod{\mathfrak{m}_0} \Leftrightarrow a \equiv b \pmod{\mathfrak{m}_0}.$$

ΠΡΟΤΑΣΗ 3.4.4. *Ισχύει ότι*

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})] < +\infty.$$

Απόδειξη. ([7], σελ.140, Πρ. 1.3.) □

ΟΡΙΣΜΟΣ 3.4.5. Μία υποομάδα $H \leq I_K(\mathfrak{m})$ θα λέγεται *ομάδα ισοδυναμίας* για το modulus $\mathfrak{m}$ εάν ισχύει ότι

$$P_{K,1}(\mathfrak{m}) \leq H \leq I_K(\mathfrak{m}).$$

Η ομάδα πηλίκων $I_K(\mathfrak{m})/H$ θα καλείται *γενικευμένη ομάδα κλάσεων ιδεωδών του σώματος K για το modulus* $\mathfrak{m}$.

ΠΑΡΑΤΗΡΗΣΗ 3.4.6. Αν θεωρήσουμε ως modulus το $\mathfrak{m} = 1$[5], τότε

$$I_K(1) = \{\frac{A}{B} \mid A, B \text{ ακέραια ιδεώδη του } K\} = I_K$$

και

$$P_{K,1}(1) = \{\alpha R_K \mid \alpha \in K^*\} = P_K.$$

Επομένως, σε αυτή την περίπτωση η γενικευμένη ομάδα κλάσεων ιδεωδών για το modulus $\mathfrak{m} = 1$ είναι η

$$I_K(1)/P_{K,1} = I_K/P_K = Cl(K),$$

ήτοι η ομάδα κλάσεων ιδεωδών που ορίσαμε στο πρώτο κεφάλαιο. Υπ' αυτή την έννοια, ο όρος "γενικευμένη ομάδα κλάσεων ιδεωδών" για την πηλικοομάδα $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ έχει νόημα.

Η βασική ιδέα της θεωρίας κλάσεων σωμάτων είναι ότι οι ομάδες Galois όλων των αβελιανών επεκτάσεων του K είναι υλοποιήσιμες ως γενικευμένες ομάδες κλάσεων ιδεωδών του K. Ο συνδετικός κρίκος μεταξύ των δύο αυτών κατηγοριών είναι η απεικόνιση του Artin.

Θεωρούμε το modulus $\mathfrak{m}$ το οποίο διαιρείται από όλους τους διακλαδιζόμενους πρώτους του K, πεπερασμένους ή άπειρους, και ένα πρώτο ιδεώδες P του K το οποίο δε διαιρεί το $\mathfrak{m}$. Συνεπώς το P είναι μη διακλαδιζόμενο πρώτο ιδεώδες. Αυτό σημαίνει ότι για το εν λόγω ιδεώδες μπορούμε να ορίσουμε το σύμβολο του Artin

$$\left(\frac{L/K}{P}\right) \in Gal(L/K).$$

Εάν θεωρήσουμε ένα ιδεώδες

$$I = \prod_{i=1}^{r} P_i^{e_i}$$

του K, όπου καθένα από τα P_i είναι πρώτα ιδεώδη του K, που δε διαιρούν το $\mathfrak{m}$, τότε μπορούμε να επεκτείνουμε το σύμβολο του Artin πολλαπλασιαστικά και να κατασκευάσουμε τον ομομορφισμό

$$\begin{aligned} \Phi_{\mathfrak{m}} \;:\; & I_K(\mathfrak{m}) \longrightarrow Gal(L/K) \\ & I \longmapsto \prod_{i=1}^{r} \left(\frac{L/K}{P_i}\right)^{e_i} =: \left(\frac{L/K}{I}\right). \end{aligned}$$

[5] Ο συμβολισμός $\mathfrak{m} = 1$ χρησιμοποιείται αντί του $\mathfrak{m} = \langle 1\rangle = R_K$.

ΟΡΙΣΜΟΣ 3.4.7. Ο ομομορφισμός $\Phi_{\mathfrak{m}}$ καλείται *απεικόνιση του Artin για την αβελιανή επέκταση* L/K *και το modulus* $\mathfrak{m}$. Μάλιστα, για να αναδείξουμε την εξάρτηση της απεικόνισης $\Phi_{\mathfrak{m}}$ από την επιλογή της αβελιανής επέκτασης και του modulus, χρησιμοποιούμε και το συμβολισμό $\Phi_{L/K,\mathfrak{m}}$ όπου είναι αναγκαίο.

Στη συνέχεια της παραγράφου ακολουθούν τρία θεμελιώδη θεωρήματα της θεωρίας κλάσεων σωμάτων. Οι αποδείξεις αυτών είναι αδύνατο να παρουσιαστούν στα πλαίσια της παρούσας εργασίας, λόγω του ότι χρειάζονται επιπρόσθετα στοιχεία θεωρίας στην οποία δεν έχουμε κάνει καμία αναφορά.

Το πρώτο θεώρημα είναι ο νόμος αντιστροφής του Artin, ο οποίος μας πληροφορεί ότι η ομάδα Galois οποιασδήποτε αβελιανής επέκτασης είναι μία γενικευμένη ομάδα κλάσεων ιδεωδών του K για κάποιο modulus $\mathfrak{m}$.

ΘΕΩΡΗΜΑ 3.4.8 (Νόμος αντιστροφής του Artin)**.** *Έστω* L/K *αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών και ένα modulus* $\mathfrak{m}$*, το οποίο είναι διαιρετό από όλους τους διακλαδιζόμενους στο* L *πρώτους του* K*. Τότε*

(i) Η απεικόνιση $\Phi_{\mathfrak{m}}$ *του Artin είναι επιμορφισμός.*

(ii) Αν οι εκθέτες των πεπερασμένων πρώτων στην ανάλυση του $\mathfrak{m}$ *είναι αρκετά μεγάλοι, τότε ο πυρήνας* $Ker(\Phi_{\mathfrak{m}})$ *της απεικόνισης* $\Phi_{\mathfrak{m}}$ *είναι ομάδα ισοδυναμίας για το δοθέν* $\mathfrak{m}$*, ήτοι*

$$P_{K,1}(\mathfrak{m}) \leq Ker(\Phi_{\mathfrak{m}}) \leq I_K(\mathfrak{m}).$$

Επομένως, σύμφωνα με το πρώτο θεώρημα των ισομορφισμών της θεωρίας ομάδων ισχύει ότι

$$I_K(\mathfrak{m})/Ker(\Phi_{\mathfrak{m}})(\mathfrak{m}) \cong Gal(L/K).$$

Φυσιολογικά εγείρεται το ερώτημα της σχέσης που του νόμου αντιστροφής του Artin με τους γνωστούς νόμους αντιστροφής της κλασικής θεωρίας αριθμών. Η απάντηση είναι ότι η ο νόμος αντιστροφής του Artin αποτελεί γενίκευση όλων των μέχρι τώρα γνωστών νόμων αντιστροφής, όπως για παράδειγμα τον τετραγωνικό νόμο αντιστροφής ή τον κυβικό νόμο αντιστροφής. Βέβαια, κάτι τέτοιο δεν είναι εμφανές εκ πρώτης όψεως.

ΠΑΡΑΔΕΙΓΜΑ 3.4.9. Εστω ότι $K = \mathbb{Q}$ και $L = \mathbb{Q}(\zeta_m)$, όπου ως ζ_m, με $m \in \mathbb{N}$, συμβολίζουμε μία πρωταρχική m-οστή ρίζα της μονάδος. Έστω ότι

$$\zeta_m := e^{2\pi i/m}.$$

Ένα modulus, στου οποίου την ανάλυση εμφανίζονται όλοι οι διακλαδιζόμενοι πρώτοι του $\mathbb{Q}$ στο $\mathbb{Q}(\zeta_m)$, είναι της μορφής

$$\mathfrak{m} = \langle m \rangle \infty.$$

Για να το ελέγξουμε αυτό χρειαζόμαστε το νόμο ανάλυσης των κυκλοτομικών σωμάτων, για τον οποίο δεν έχουμε κάνει λόγο. Επίσης από τη θεωρία των κυκλοτομικών σωμάτων γνωρίζουμε ότι

$$Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

Θέλουμε να περιγράψουμε την απεικόνιση του Artin

$$\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

Γνωρίζουμε ότι στο $\mathbb{Q}$ όλα τα ιδεώδη, ακέραια και κλασματικά, είναι κύρια. Επομένως, εάν $I \in I_{\mathbb{Q}}(\mathfrak{m})$, τότε υπάρχουν αριθμοί $a, b \in \mathbb{Z}$ τέτοιοι, ώστε

$$I = \frac{a}{b}\mathbb{Z}\text{ , όπου } (a, m) = (b, m) = 1.$$

Χ.β.τ.γ. μπορούμε να υποθέσουμε ότι $a/b > 0$. Τότε

$$\Phi_{\mathfrak{m}}(I) = \Phi_{\mathfrak{m}}\left(\frac{a}{b}\mathbb{Z}\right) = [a]_m[b]_m{}^{-1} \in (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

Ο πυρήνας της απεικόνισης του Artin είναι

$$\begin{aligned} Ker(\Phi_{\mathfrak{m}}) &= \{\frac{a}{b}\mathbb{Z} \mid a, b \in \mathbb{Z} \text{ και } \Phi_{\mathfrak{m}}\left(\frac{a}{b}\mathbb{Z}\right) = [1]_m\} \\ &= \{\frac{a}{b}\mathbb{Z} \mid a, b \in \mathbb{Z} \text{ και } [a]_m[b]_m{}^{-1} = [1]_m\} \\ &= \{\frac{a}{b}\mathbb{Z} \mid a, b \in \mathbb{Z} \text{ και } a \equiv b \pmod{m}\} \\ &= P_{\mathbb{Q},1}(\mathfrak{m}). \end{aligned}$$

Παρατηρηση 3.4.10. Το modulus $\mathfrak{m}$ για το οποίο ο πυρήνας $Ker(\Phi_{\mathfrak{m}})$ είναι μία ομάδα ισοδυναμίας δεν είναι μονοσήμαντα ορισμένο.

Προταση 3.4.11. *Αν $P_{K,1}(\mathfrak{m}) \leq Ker(\Phi_{\mathfrak{m}})$ και το $\mathfrak{n}$ είναι ένα άλλο modulus τέτοιο ώστε $\mathfrak{m} \mid \mathfrak{n}$, τότε ισχύει ότι*

$$P_{K,1}(\mathfrak{n}) \leq Ker(\Phi_{\mathfrak{n}}).$$

Απόδειξη. Έστω ένα ιδεώδες $A \in P_{K,1}(\mathfrak{n})$. Τότε υπάρχει ένας αριθμός $\alpha \in K^{\times}$ τέτοιος, ώστε

$$A = \langle\alpha\rangle \text{ και } \alpha \equiv 1 \pmod{\mathfrak{n}}.$$

Εφόσον $\alpha \equiv 1 \pmod{\mathfrak{n}}$ και $\mathfrak{m} \mid \mathfrak{n}$, ισχύει ότι

$$\alpha \equiv 1 \mod \mathfrak{m}.$$

Άρα $A \in P_{K,1}(\mathfrak{m})$. Εξ υποθέσεως, λοιπόν, ισχύει ότι $A \in Ker(\Phi_{\mathfrak{m}})$. Όμως, τα στοιχεία του πυρήνα της απεικόνισης του Artin δεν εξαρτώνται από την επίλογή του modulus. Αυτό σημαίνει ότι $A \in Ker(\Phi_{\mathfrak{n}})$. Επομένως για το τυχόν ιδεώδες $A \in P_{K,1}(\mathfrak{n})$ ισχύει ότι $A \in Ker(\Phi_{\mathfrak{n}})$. Άρα αποδείξαμε ότι $P_{K,1}(\mathfrak{n}) \leq Ker(\Phi_{\mathfrak{n}})$. □

Η παραπάνω πρόταση ουσιαστικά μας πληροφορεί ότι υπάρχουν άπειρα στο πλήθος modulus του K για τα οποία η ομάδα $Gal(L/K)$ είναι μία γενικευμένη ομάδα κλάσεων ιδεωδών. Αυτό είναι πρόβλημα καθώς θα θέλαμε να χαρακτηρίσουμε μονοσήμαντα την ομάδα Galois ως γενικευμένη ομάδα κλάσεων ιδεωδών. Τη λύση μας την παρέχει το παρακάτω αποτέλεσμα:

Θεωρημα 3.4.12 (Θεώρημα του οδηγού)**.** *Αν η L/K είναι μία αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών, τότε υπάρχει ένα modulus $\mathfrak{f} := \mathfrak{f}(L/K)$ τέτοιο, ώστε:*

(i) ένας πρώτος του K, πεπερασμένος ή άπειρος, διακλαδίζεται στο L εάν, και μόνο εάν διαιρεί το modulus $\mathfrak{f}$.

(ii) αν θεωρήσουμε κάποιο άλλο modulus $\mathfrak{m}$ που διαιρείται από όλους τους πρώτους του K που διακλαδίζονται στο σώμα L, τότε ο πυρήνας $Ker(\Phi_{\mathfrak{m}})$ είναι ομάδα ισοδυναμίας για το modulus $\mathfrak{m}$ τότε, και μόνο τότε, όταν $\mathfrak{f} \mid \mathfrak{m}$.

Το modulus $\mathfrak{f}$ που ικανοποιεί τις συνθήκες του θεωρήματος 3.4.12, ονομάζεται οδηγός της επέκτασης L/K.

Παραδειγμα 3.4.13. Επιστρέφουμε στο παράδειγμα της κυκλοτομικής επέκτασης $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Σε αυτή την περίπτωση υπολογίζεται ότι ο οδηγός $\mathfrak{f}$ είναι

$$\mathfrak{f} := \mathfrak{f}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \begin{cases} 1 & \text{, αν } m \leq 2 \\ \langle\frac{m}{2}\rangle\infty & \text{, αν } m = 2n \text{ και } n > 1 \text{ περιττός φυσικός αριθμός} \\ \langle m\rangle\infty & \text{, αλλιώς} \end{cases}.$$

Το τελευταίο θεώρημα της θεωρίας κλάσεων σωμάτων στο οποίο θα αναφερθούμε είναι το θεώρημα της ύπαρξης, σύμφωνα με το οποίο κάθε γενικευμένη ομάδα κλάσεων ιδεωδών του K ως προς κάποιο modulus $\mathfrak{m}$ αυτού είναι ομάδα Galois κάποιας πεπερασμένης αβελιανής επέκτασης L/K.

Θεωρημα 3.4.14 (Θεώρημα της ύπαρξης)**.** *Θεωρούμε ένα αλγεβρικό σώμα αριθμών K και κάποιο modulus $\mathfrak{m}$ αυτού. Ακόμα, θεωρούμε μία ομάδα ισοδυναμίας H, ήτοι μία ομάδα για την οποία ισχύει ότι*

$$P_{K,1}(\mathfrak{m}) \leq H \leq I_K(\mathfrak{m}).$$

Τότε υπάρχει μοναδική αβελιανή επέκταση L του K τέτοια, ώστε όλοι οι διακλαδιζόμενοι πρώτοι του K να διαιρούν το $\mathfrak{m}$ και επιπροσθέτως να ισχύει ότι

$$H = Ker(\Phi_{\mathfrak{m}}),$$

όπου $\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$ είναι η απεικόνιση του Artin.

Παρατηρηση 3.4.15. Το θεώρημα της ύπαρξης είναι σημαντικό, όχι μόνο γιατί μας εξασφαλίζει την ύπαρξη της αβελιανής επέκτασης, αλλά και για το λόγο ότι μας επιτρέπει να κατασκευάζουμε αβελιανές επεκτάσεις με περιορισμένη διακλάδωση. Αυτό σημαίνει ότι μπορούμε να επιλέξουμε σε ποιούς πρώτους αριθμούς επιθυμούμε διακλάδωση και το γινόμενο αυτών να είναι το ζητούμενο modulus.

Θα κλείσουμε την παράγραφο με μία εξαιρετικής γοητείας εφαρμογή των θεωρητικών αποτελεσμάτων που αναφέραμε μέχρι τώρα. Πρόκειται να αποδείξουμε το θεώρημα Kronecker-Weber με χρήση θεωρίας κλάσεων σωμάτων.

Πορισμα 3.4.16. *Θεωρούμε τις πεπερασμένες αβελιανές επεκτάσεις L/K και M/K αλγεβρικών σωμάτων αριθμών. Υπάρχει ένα modulus $\mathfrak{m}$, το οποίο διαιρείται από όλους τους διακλαδιζόμενους, είτε στο L,είτε στο M, πρώτους του K τέτοιο, ώστε*

$$P_{K,1}(\mathfrak{m}) \leq Ker(\Phi_{M/K,\mathfrak{m}}) \leq Ker(\Phi_{L/K,\mathfrak{m}})$$

εάν, και μόνο εάν $L \leq M$.

Απόδειξη. ($\Leftarrow$) Υποθέτουμε ότι $L \leq M$. Τότε έχουμε τον πύργο σωμάτων $K \leq L \leq M$. Εφόσον η επέκταση M/K είναι αβελιανή και Galois, το αυτό θα ισχύει και για την M/L. Μάλιστα, ισχύει ότι

$$Gal(L/K) \cong Gal(M/K)/Gal(M/L).$$

Θεωρούμε την απεικόνιση

$$\begin{aligned} Rest_L \quad : \quad & Gal(M/K) \longrightarrow Gal(L/K) \\ & \sigma \longmapsto \sigma|_L. \end{aligned}$$

Σύμφωνα με το νόμο αντιστροφής του Artin υπάρχει ένα modulus $\mathfrak{m}_1$ του K που περιέχει όλους τους πρώτους του K που διακλαδίζονται στο L και για το οποίο ισχύει ότι

$$P_{K,1}(\mathfrak{m}_1) \leq Ker(\Phi_{L/K,\mathfrak{m}_1}) \leq I_K(\mathfrak{m}_1).$$

Ανάλογα, υπάρχει ένα modulus $\mathfrak{m}_2$ του M, το οποίο περιέχει όλους τους πρώτους του K που διακλαδίζονται στο M και για αυτό ισχύει ότι

$$P_{K,1}(\mathfrak{m}_2) \leq Ker(\Phi_{M/K,\mathfrak{m}_2}) \leq I_K(\mathfrak{m}_2).$$

Εάν, λοιπόν, θεωρήσουμε το modulus $\mathfrak{m} = \varepsilon.\kappa.\pi.(\mathfrak{m}_1, \mathfrak{m}_2)$, τότε αυτό διαιρείται από όλους του πρώτους του K που διακλαδίζονται είτε στο L, είτε στο M. Μάλιστα, ισχύει ότι οι $Ker(\Phi_{L/K,\mathfrak{m}})$ και

$Ker(\Phi_{M/K,\mathfrak{m}})$ είναι ομάδες ισοδυναμίας για το modulus $\mathfrak{m}$. Αποδεικνύεται (βλ. [1], σελ. 179-180) ότι

$$Rest_L \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}.$$

Αυτό σημαίνει ότι

$$Ker(\Phi_{M/K,\mathfrak{m}}) \leq Ker(\Phi_{L/K,\mathfrak{m}}).$$

($\Rightarrow$) Υποθέτουμε ότι ισχύει η

$$P_{K,1}(\mathfrak{m}) \leq Ker(\Phi_{M/K,\mathfrak{m}}) \leq Ker(\Phi_{L/K,\mathfrak{m}}) \leq I_K(\mathfrak{m}).$$

Η απεικόνιση του Artin $\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$ απεικονίζει την ομάδα $Ker(\Phi_{L/K,\mathfrak{m}}) \leq I_K(\mathfrak{m})$ σε μία υποομάδα H, της ομάδας $Gal(M/K)$. Σύμφωνα με τη θεωρία Galois, στην υποομάδα H αντιστοιχεί ένα ενδιάμεσο σώμα F της επέκτασης L/K, ήτοι σώμα για το οποίο ισχύει ότι

$$K \leq F \leq L.$$

Από το αντίστροφο του πορίσματος, το οποίο έχουμε ήδη αποδείξει έπεται ότι

$$Ker(\Phi_{L/K,\mathfrak{m}}) = Ker(\Phi_{F/K,\mathfrak{m}}).$$

Άρα σύμφωνα με το θεώρημα της ύπαρξης ισχύει ότι

$$L = F \leq M.$$

□

Είμαστε πλέον σε θέση να αποδείξουμε το θεώρημα των Kronecker-Weber κάνοντας χρήση θεωρίας κλάσεων σωμάτων.

ΘΕΩΡΗΜΑ 3.4.17 (Θεώρημα Kronecker-Weber)**.** *Έστω L μία αβελιανή επέκταση του $\mathbb{Q}$. Τότε υπάρχει ένας θετικός ακέραιος m, για τον οποίο ισχύει ότι*

$$L \leq \mathbb{Q}(\zeta_m),$$

όπου $\zeta_m := e^{2\pi i/m}$.

Απόδειξη. Σύμφωνα με το νόμο αντιστροφής του Artin υπάρχει ένα modulus $\mathfrak{m}$ που είναι διαιρετό από όλους τους δικλαδιζόμενους πρώτους του $\mathbb{Q}$ στο L και για το οποίο ισχύει ότι $P_{\mathbb{Q},1}(\mathfrak{m}) \leq Ker(\Phi_{L/\mathbb{Q},\mathfrak{m}})$. Εφόσον ισχύει ότι $h_{\mathbb{Q}} = 1$, μπορούμε να υποθέσουμε ότι το εν λόγω modulus γράφεται υπό τη μορφή

$$\mathfrak{m} = \langle m \rangle \infty,$$

για κάποιο φυσικό αριθμό m. Θεωρούμε την επέκταση σωμάτων $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, όπου ως ζ_m συμβολίζεται η πρωταρχική m-οστή ρίζα της μονάδος $e^{2\pi i/m}$. Σύμφωνα με το παράδειγμα 3.4.9 το $\mathfrak{m}$ μπορεί να ειδωθεί και ως modulus του $\mathbb{Q}$, το οποίο διαιρείται από όλους τους διακλαδιζόμενους πρώτους του $\mathbb{Q}$ στο $\mathbb{Q}(\zeta_m)$. Έτσι, το $\mathfrak{m}$ αποτελεί modulus, διαιρετό από όλους τους πρώτους του $\mathbb{Q}$ που διακλαδίζονται είτε στο L, είτε στο $\mathbb{Q}(\zeta_m)$. Κι εφόσον έχουμε αποδείξει ότι ισχύει

$$Ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) = P_{\mathbb{Q},1}(\mathfrak{m}) \leq Ker(\Phi_{L/\mathbb{Q},\mathfrak{m}}),$$

το ζητούμενο έπεται άμεσα από το πόρισμα 3.4.16. □

3.5 Το σώμα κλάσεων Hilbert

Το σώμα κλάσεων του Hilbert αποτελεί ουσιαστικά μια ειδική περίπτωση της θεωρίας κλάσεων σωμάτων. Παρα ταύτα, λόγω της σημασίας του στη μελέτη μας επιλέγουμε να το παρουσιάσουμε σε ξεχωριστή παράγραφο.

Μία επέκταση L/K ονομάζεται *μη διακλαδιζόμενη* όταν κάθε πρώτος του K, πεπερασμένος ή άπειρος, δε διακλαδίζεται στο L. Αν, τώρα, η L/K είναι αβελιανή επέκταση, ικανή και αναγκαία συνθήκη για να είναι και μη διακλαδιζόμενη είναι το modulus να είναι ίσο με 1, ήτοι $\mathfrak{m} = 1$. Όπως έχουμε ήδη αποδείξει, ισχύει ότι

$$P_{K,1}(1) = P_K,$$

όπου ως P_K συμβολίζουμε την ομάδα όλων των κύριων ιδεωδών του K. Έτσι, εφαρμόζοντας το θεώρημα της ύπαρξης για το modulus $\mathfrak{m} = 1$, συμπεραίνουμε ότι υπάρχει μοναδική μη διακλαδιζόμενη αβελιανή επέκταση L του K, έτσι ώστε η απεικόνιση του Artin

$$\Phi_{L/K,1} : I_K(1)/P_{K,1}(1) \longrightarrow Gal(L/K)$$

να είναι ισομορφισμός ομάδων. Κι εφόσον

$$I_K(1)/P_{K,1}(1) = I_K/P_K = Cl(K),$$

λαμβάνουμε ότι

$$Cl(K) \cong Gal(L/K).$$

Ορισμος 3.5.1. Το (μοναδικό) σώμα L, για το οποίο ισχύει ότι

$$Cl(K) \cong Gal(L/K)$$

ονομάζεται *σώμα κλάσεων Hilbert του* K και συμβολίζεται ως $\mathscr{H}_K$.

Προταση 3.5.2. *Το σώμα κλάσεων του Hilbert είναι η μέγιστη μη διακλαδιζόμενη αβελιανή επέκταση του K υπό την έννοια ότι κάθε άλλη μη διακλαδιζόμενη αβελιανή επέκταση του K περιέχεται στο $\mathscr{H}_K$.*

Απόδειξη. Ήδη γνωρίζουμε ότι το $\mathscr{H}_K$ είναι μη διακλαδιζόμενη επέκταση. Θα αποδείξουμε ότι είναι και η μέγιστη. Προς τούτο, θεωρούμε μία άλλη μη διακλαδιζόμενη επέκταση M του K. Εφόσον $\mathfrak{m} = 1$, από το θεώρημα του οδηγού έπεται άμεσα ότι $\mathfrak{f} = 1$ και ότι ο $Ker(\Phi_{\mathscr{H}_K/K,1})$ είναι μία ομάδα ισοδυναμίας για το modulus $\mathfrak{m} = 1$, ήτοι ισχύει ότι

$$P_K \leq Ker(\Phi_{\mathscr{H}_K/K,1}) \leq I_K.$$

Εξ ορισμού του σώματος του Hilbert έχουμε ότι

$$P_K = Ker(\Phi_{\mathscr{H}_K/K,1}) \leq Ker(\Phi_{M/K,1}).$$

Έτσι, από το πόρισμα 3.4.16 συνεπάγεται ότι $M \leq \mathscr{H}_K$. □

Εάν κάνουμε χρήση του θεμελιώδους θεωρήματος της θεωρίας του Galois, λαμβάνουμε το παρακάτω πόρισμα, το οποίο ταξινομεί τις μη διακλαδιζόμενες αβελιανές επεκτάσεις του σώματος K.

Πορισμα 3.5.3. *Δοθέντος αλγεβρικού αριθμητικού σώματος K, υπάρχει μονοσήμαντη αντιστοιχία μεταξύ των μη διακλαδιζόμενων αβελιανών επεκτάσεων M του K και των υποομάδων H της ομάδας κλάσεων ιδεωδών $Cl(K)$. Επιπροσθέτως, εάν η επέκταση M του K αντιστοιχεί στην υποομάδα H της $Cl(K)$, τότε προκύπτει ο ισομορφισμός*

$$Cl(K)/H \cong Gal(M/K).$$

Το παραπάνω πόρισμα αποτελεί ουσιαστικά τη θεωρία κλάσεων σωμάτων για μη διακλαδιζόμενες αβελιανές επεκτάσεις. Έπισης φανερώνει ότι η εύρεση μίας συγκεκριμένης κατηγορίας επεκτάσεων ενός σώματος γίνεται μέσω της ομάδας κλάσεων ιδεωδών του σώματος.

Πορισμα 3.5.4. *Έστω $\mathscr{H}_K$ το σώμα κλάσεων Hilbert του αλγεβρικού σώματος αριθμών K και έστω P ένα πρώτο ιδεώδες του K. Τότε το ιδεώδες P αναλύεται πλήρως στο $\mathscr{H}_K$ εάν, και μόνο εάν είναι κύριο ιδεώδες.*

Πριν κλείσουμε αυτή την παράγραφο αξίζει να αναφέρουμε ένα ιδιαίτερα σημαντικό θεώρημα της θεωρίας κλάσεων σωμάτων, το οποίο σχετίζεται με το σώμα του Hilbert.

Θεωρημα 3.5.5 (Θεώρημα των κύριων ιδεωδών)**.** *Κάθε κλασματικό ιδεώδες A ενός αλγεβρικού σώματος αριθμών K, όταν επεκταθεί στο σώμα κλάσεων Hilbert $\mathscr{H}_K$ αυτού γίνεται κύριο ιδεώδες. Με άλλα λόγια, το ιδεώδες $AR_{\mathscr{H}_K}$ είναι κύριο.*

Αυτό, βέβαια, δε σημαίνει ότι ο $R_{\mathscr{H}_K}$ είναι περιοχή κύριων ιδεωδών. Υπάρχουν ιδεώδη του σώματος κλάσεων Hilbert του K, τα οποία δεν είναι κύρια. Προς τούτο, θεωρούμε το σώμα κλάσεων Hilbert του $\mathscr{H}_K$. Επομένως, στο σώμα $\mathscr{H}_{\mathscr{H}_K}$, τα ιδεώδη του $\mathscr{H}_K$ που δεν είναι κύρια, επί τη βάσει του θεωρήματος κύριων ιδεωδών, γίνονται κύρια. Επαναλαμβάνοντας τη διαδικασία, κατασκευάζουμε ένα πύργο σωμάτων

$$K \leq \mathscr{H}_K \leq \mathscr{H}_{\mathscr{H}_K} \leq \cdots .$$

Για μεγάλο χρονικό διάστημα ήταν ανοικτό ερώτημα αν αυτός ο πύργος αποτελείται από άπειρα σώματα ή αν τερματίζεται ύστερα από πεπερασμένα βήματα σε κάποιο σώμα κλάσεων Hilbert. Τελικά, στις αρχές της δεκαετίας του $60'$ οι Golod και Shafarevich έδωσαν παραδείγματα αλγεβρικών αριθμητικών σωμάτων με άπειρο πύργο σωμάτων κλάσεων. Ένα τέτοιο παράδειγμα είναι το σώμα $K = \mathbb{Q}(\sqrt{d})$, όπου $d = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23$.

Κεφάλαιο 4

Ελλειπτικές και Modular Συναρτήσεις

4.1 Διπλά περιοδικές συναρτήσεις

Ξεκινάμε τη μελέτη μας ορίζοντας την έννοια της διπλά περιοδικής συνάρτησης. Πριν όμως από αυτό, υπενθυμίζουμε την έννοια της περιοδικής συνάρτησης. Στο πλαίσιο της μελέτης μας οι συναρτήσεις θα είναι μιγαδικές. Έτσι, εάν υποθέσουμε ότι η f είναι μία μιγαδική συνάρτηση, τότε αυτή ονομάζεται *περιοδική με περίοδο* $\omega \in \mathbb{C}$ εάν για αυτήν ισχύει ότι

$$f(z) = f(z + \omega),$$

όταν τα z και $z + \omega$ ανήκουν στο πεδίο ορισμού της f. Όπως φανερώνει ο τίτλος της παραγράφου, απαιτούμε την ύπαρξη δύο περιόδων ω_1 και ω_2 για την f. Τότε θα ισχύει ότι

$$f(z + \omega_1) = f(z) = f(z + \omega_2).$$

Από αυτό έπεται άμεσα ότι για κάθε $m, n \in \mathbb{Z}$ και ο μιγαδικός αριθμός $m\omega_1 + n\omega_2$ θα αποτελεί περίοδο για την f. Είμαστε έτοιμοι να δώσουμε τον πρώτο μας ορισμό:

Ορισμος 4.1.1. Μία μιγαδική συνάρτηση f καλείται *διπλά περιοδική* εάν έχει δυο περιόδους ω_1 και ω_2, των οποίων ο λόγος ω_2/ω_1 είναι μη πραγματικός αριθμός[1].

Η απαίτηση ο λόγος ω_2/ω_1 να είναι μη πραγματικός αριθμός ουσιαστικά χρησιμοποιείται προς αποφυγή εκφυλισμένων περιπτώσεων. Επί παραδείγματι, εάν ο λόγος ω_2/ω_1 είναι πραγματικός και ρητός αριθμός τότε μπορούμε να δείξουμε ότι οι περίοδοι ω_1 και ω_2 είναι ακέραια πολλαπλάσια μιας περιόδου ω. Αν από την άλλη, ο λόγος είναι άρρητος και πραγματικός η f αποδεικνύεται ότι είναι σταθερή συνάρτηση.

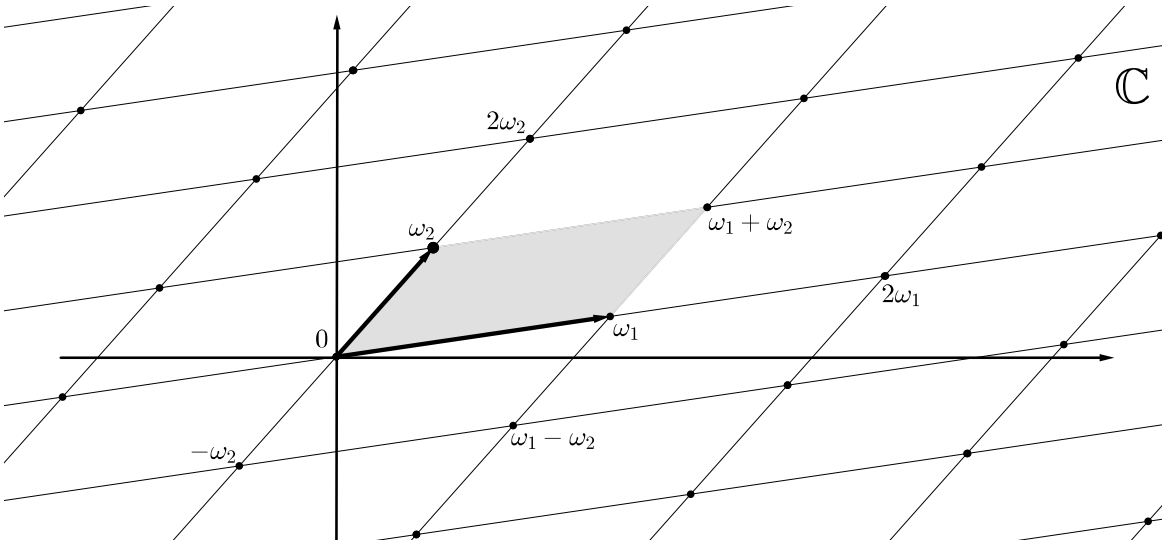
Ορισμος 4.1.2. Έστω f διπλά περιοδική συνάρτηση με περιόδους ω_1 και ω_2. Το ζεύγος (ω_1, ω_2) καλείται *θεμελιώδες ζεύγος περιόδων* εάν κάθε άλλη περίοδος της f γράφεται υπό τη μορφή $m\omega_1 + n\omega_2$, όπου οι $m, n \in \mathbb{Z}$.

Κάθε θεμελιώδες ζεύγος περιόδων (ω_1, ω_2), ορίζει το σύνολο

$$L := L(\omega_1, \omega_2) := \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}.$$

Αυτό ονομάζεται *πλέγμα* ή *κιγκλίδωμα*. Προφανώς για οποιαδήποτε επιλογή των ω_1 και ω_2 ισχύει ότι $0 \in L(\omega_1, \omega_2)$.

[1] Η απαίτηση ο αριθμός ω_2/ω_1 να είναι μη πραγματικός αριθμός, ήτοι να ανήκει στο σύνολο $\mathbb{C} \setminus \mathbb{R}$ ισοδυναμεί με τη συνθήκη να είναι το σύνολο $\{\omega_1, \omega_2\}$ $\mathbb{R}$-γραμμικά ανεξάρτητο.



Στο ανωτέρω σχήμα απεικονίζεται το σύνολο $L := L(\omega_1, \omega_2)$ εντός του μιγαδικού επιπέδου. Το χρωματισμένο χωρίο καλείται *παραλληλόγραμμο περιόδων*. Καθένα από τα ίσα προς το χρωματισμένο παραλληλόγραμμα του σχήματος είναι παραλληλόγραμμο περιόδων. Πρέπει να παρατηρήσουμε εδώ ότι στο χρωματισμένο παραλληλόγραμμο τα σημεία των πλευρών του που καταλήγουν στην κορυφή $\omega_1 + \omega_2$ δεν αποτελούν σημεία αυτού. Με άλλα λόγια, στο χρωματισμένο παραλληλόγραμμο περιόδων ανήκουν τα σημεία της μορφής

$$t_1\omega_1 + t_2\omega_2 \text{ , όπου } 0 \leq t_1, t_2 < 1.$$

Είναι προφανές ότι εάν επιλέξουμε ένα θεμελιώδες ζεύγος (ω_1, ω_2), τότε τότε το τρίγωνο με κορυφές τις 0, ω_1 και ω_2 (, άρα και το παραλληλόγραμμο περιόδων με κορυφές τις 0, ω_1, ω_2 και $\omega_1 + \omega_2$) δεν περιέχει καμία άλλη περίοδο στο εσωτερικό του ή στις πλευρές του. Ισχύει όμως και το αντίστροφο, ήτοι κάθε ζεύγος μιγαδικών αριθμών (ω_1, ω_2), το οποίο έχει την προαναφερθείσα ιδιότητα και για το οποίο ο λόγος ω_2/ω_1 είναι μη πραγματικός αριθμός αποτελεί θεμελιώδες ζεύγος περιόδων. Πράγματι, εφόσον έχουμε υποθέσει ότι $\omega_2/\omega_1 \in \mathbb{C} \setminus \mathbb{R}$, οι αριθμοί ω_1 και ω_2 είναι $\mathbb{R}$-γραμμικά ανεξάρτητοι. Συνεπώς για την τυχούσα περίοδο ω, θα ισχύει ότι

$$\exists\, t_1, t_2 \in \mathbb{R} \ : \ \omega = t_1\omega_1 + t_2\omega_2.$$

Εάν, τώρα, ως $[t]$ συμβολίσουμε το ακέραιο μέρος του αριθμού t και γράψουμε τους t_1 και t_2 υπό τη μορφή

$$t_1 = [t_1] + r_1 \ \text{ , με } 0 \leq r_1 < 1,$$
$$t_2 = [t_2] + r_2 \ \text{ , με } 0 \leq r_2 < 1,$$

τότε λαμβάνουμε ότι

$$\omega - [t_1]\omega_1 - [t_2]\omega_2 = r_1\omega_1 + r_2\omega_2.$$

Όμως ο μιγαδικός αριθμός $r_1\omega_1 + r_2\omega_2$ είναι μία περίοδος η οποία βρίσκεται στο εσωτερικό του παραλληλογράμμου περιόδων με κορυφές τις 0, ω_1, ω_2 και $\omega_1 + \omega_2$. Γενικά, εάν ο w ανήκει στο εν λόγω παραλληλόγραμμο περιόδων, το αυτό ισχύει και για το μιγαδικό $\omega_1 + \omega_2 - w$. Αυτό σημαίνει ότι ένας τουλάχιστον εκ των w και $\omega_1 + \omega_2 - w$ ανήκει στο παραλληλόγραμμο περιόδων με κορυφές τις $0, \omega_1, \omega_2$ και $\omega_1 + \omega_2$. Η παρατήρηση αυτή έχει ως συνέπεια ότι $r_1 = r_2 = 0$. Άρα $\omega = [t_1]\omega_1 + [t_2]\omega_2$, όποτε η απόδειξη ολοκληρώθηκε.

Ορισμος 4.1.3. Δύο ζεύγη περιόδων (ω_1, ω_2) και (ω_1', ω_2'), με την ιδιότητα $\omega_2/\omega_1, \omega_2'/\omega_1' \in \mathbb{C} \setminus \mathbb{R}$, χαρακτηρίζονται *ισοδύναμα* όταν τα κιγκλιδώματα που αντιστοιχούν σε αυτά ταυτίζονται, ήτοι όταν

$$L(\omega_1, \omega_2) = L(\omega_1', \omega_2').$$

Ένα κριτήριο για να ελέγχουμε πότε δύο ζεύγη περιόδων είναι ισοδύναμα είναι το παρακάτω:

ΘΕΩΡΗΜΑ 4.1.4. *Δύο ζεύγη μιγαδικών αριθμών (ω_1, ω_2) και (ω_1', ω_2') είναι ισοδύναμα εάν, και μόνο εάν, υπάρχουν ακέραιοι αριθμοί a, b, c και d με την ιδιότητα $ad - bc = \pm 1$, για τους οποίους ισχύει η κάτωθεν σχέση πινάκων:*

$$\begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}.$$

4.2 Ελλειπτικές συναρτήσεις

ΟΡΙΣΜΟΣ 4.2.1. Μία μιγαδική συνάρτηση f καλείται *ελλειπτική συνάρτηση* εάν ικανοποιεί τις παρακάτω συνθήκες;

(i) η f είναι διπλά περιοδική συνάρτηση.

(ii) η f είναι μερόμορφη συνάρτηση, ήτοι οι μοναδικές ανωμαλίες που εμφανίζονται είναι πόλοι.

ΠΡΟΤΑΣΗ 4.2.2. *Κάθε μη σταθερή ελλειπτική συνάρτηση έχει ένα θεμελιώδες ζεύγος περιόδων.*

Απόδειξη. Έστω f μια μη σταθερή ελλειπτική συνάρτηση. Τότε η f είναι μερόμορφη και κατά συνέπεια το σύνολο των σημείων στο οποίο η f είναι αναλυτική είναι ανοιχτό και συνεκτικό σύνολο. Ακόμα, η f είναι διπλά περιοδική, επομένως έχει δύο περιόδους με μη πραγματικό λόγο, ήτοι το σύνολο όλων των περιόδων αυτής είναι μη κενό. Αυτό σημαίνει ότι από αυτό μπορούμε να επιλέξουμε αυτή με τη μικρότερη απόσταση από την αρχή των αξόνων, ήτοι από το 0 του μιγαδικού επιπέδου. Πράγματι, εάν δεν μπορούσαμε να κάνουμε αυτή την επιλογή, αυτό θα σήμαινε ότι η f θα είχε οσοδήποτε μικρές περιόδους, γεγονός που θα την καθιστούσε σταθερή συνάρτηση. Επιλέγουμε λοιπόν, την εγγύτερη στην αρχή των αξόνων περίοδο και την ονομάζουμε ω. Εάν υπάρχουν περισσότερες από μία περιόδους μέτρου $|\omega|$ επιλέγουμε αυτή με το ελάχιστο όρισμα που είναι μεγαλύτερο από αυτό της ω_1. Αυτή την καλούμε ω_1. Για την εύρεση της δεύτερης περιόδου κοιτάμε ξανά στον κύκλο ακτίνας $|\omega_1|$. Εάν εκτός από τους ω_1 και $-\omega_1$ υπάρχουν και άλλες περίοδοι επιλέγουμε αυτή με το μικρότερο όρισμα, το οποίο να είναι βέβαια μεγαλύτερο από αυτό του ω_1. Αλλιώς, μεγαλώνοντας την ακτίνα βρίσκουμε τον αμέσως επόμενο κύκλο στον οποίο υπάρχει περίοδος και επαναλαμβάνουμε την προαναφερθείσα διαδικασία. Πρέπει εδώ να προσέξουμε ότι από τις περιόδους που βρίσκουμε κατά την εύρεση της δεύτερης περιόδου, πρέπει να αποκλείουμε αυτές που είναι ακέραια πολλαπλάσια του ω_1. Η ύπαρξη δεύτερης περιόδου είναι εξασφαλισμένη καθώς η συνάρτηση f είναι ελλειπτική. Μέσω αυτής της επιλογής έχουμε βρει δύο περιόδους ω_1 και ω_2 με την ιδιότητα, καμία άλλη περίοδος να μη βρίσκεται στο τρίγωνο με κορυφές τις $0, \omega_1$ και ω_2. Συνεπώς το ζεύγος (ω_1, ω_2) είναι θεμελιώδες ζεύγος περιόδων. □

Μια εύκολη παρατήρηση είναι ότι εάν έχουμε δύο ελλειπτικές συναρτήσεις f και g με περιόδους ω_1 και ω_2, τότε και οι συναρτήσεις $f \pm g$, $f \cdot g$ και f/g όταν $g \neq 0$ είναι επίσης περιοδικές με τις ίδιες περιόδους. Αυτό σημαίνει ότι το σύνολο των ελλειπτικών συναρτήσεων με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού απεικονίσεων αποτελούν σώμα. Στην πορεία θα δούμε ότι το εν λόγω σώμα προέρχεται από επισύναψη συγκεκριμένων συναρτήσεων στο $\mathbb{C}$. Ακόμα μπορούμε να ελέγξουμε ότι και η f' είναι περιοδική με τις ίδιες περιόδους.

Λόγω της (διπλής) περιοδικότητας μίας ελλειπτικής συνάρτησης είναι αρκετό να μελετήσουμε τη συμπεριφορά αυτής σε κάποιο παραλληλόγραμμο περιόδων. Από αυτό συνεπάγεται ότι εάν εξασφαλίσουμε τη μη ύπαρξη πόλων για μία ελλειπτική συνάρτηση σε ένα θεμελιώδες παραλληλόγραμμο, τότε αυτή είναι κατ' ανάγκη σταθερή συνάρτηση. Πράγματι, εάν ίσχυε το αντίθετο τότε η f θα ήταν συνεχής συνάρτηση στην (τοπολογική) κλειστότητα του παραλληλογράμμου περιόδων στο οποίο μελετάται, ήτοι φραγμένη σε ένα συμπαγές χωρίο. Επομένως από το θεώρημα του Liouville, η f θα ήταν σταθερή στο παραλληλόγραμμο περιόδων και λόγω συνέχειας και σε ολόκληρο το μιγαδικό

επίπεδο. Από αυτό συμπεραίνουμε και ότι η μη ύπαρξη σημείων μηδενισμού της f σε κάποιο παραλληλόγραμμο περιόδων επάγει ότι η f είναι σταθερή, εφαρμόζοντας ξανά το θεώρημα Liouville για τη συνάρτηση $1/f$. Από τα παραπάνω είναι φανερό ότι κάθε μη σταθερή ελλειπτική συνάρτηση έχει πόλους. Κάποιες φορές δεν επιθυμούμε να έχουμε σημεία μηδενισμού ή πόλους για την f στο σύνορο ενός παραλληλογράμμου περιόδου. Προς τούτο μετασχηματίζουμε το παραλληλόγραμμο περιόδου σε ένα νέο το οποίο να μην έχει σημεία μηδενισμού ή πόλους στο σύνορό του. Αυτό σημαίνει ότι οι κορυφές αυτού του νέου παραλληλογράμμου δεν είναι κατ' ανάγκη περίοδοι. Η ύπαρξη αυτού του μετασχηματισμού ουσιαστικά βασίζεται στο ότι σε κάθε φραγμένο χωρίο, όπως είναι ένα παραλληλόγραμμο περιόδων, κάθε μερόμορφη συνάρτηση έχει το πολύ πεπερασμένο πλήθος πόλων ή σημείων μηδενισμού. Το παραλληλόγραμμο που προκύπτει ύστερα από τον προαναφερθέντα μετασχηματισμό θα το καλούμε *κελί*.

Θα χρησιμοποιήσουμε τώρα κάποιες γνώσεις μιγαδικής αναλύσεως προκειμένου να μελετήσουμε περαιτέρω τις ελλειπτικές συναρτήσεις. Αρχικά, παρατηρούμε ότι λόγω της περιοδικότητας το ολοκλήρωμα μιας ελλειπτικής συνάρτησης f στο σύνορο ενός κελιού είναι ίσο με 0. Αυτό προκύπτει έπειτα από τη διαπίστωση ότι τα ολοκληρώματα δύο απέναντι πλευρών του κελιού ισούνται κατ' απολυτή τιμή, αλλά είναι ετερόσημα. Χρησιμοποιώντας, λοιπόν, το θεώρημα των ολοκληρωτικών υπολοίπων του Cauchy, λαμβάνουμε ότι και το άθροισμα των ολοκληρωτικών υπολοίπων στους πόλους της f σε κάθε παραλληλόγραμμο περιόδων είναι ίσο με 0. Άμεσα από αυτό συμπεραίνουμε ότι κάθε μη σταθερή ελλειπτική συνάρτηση έχει δυο τουλάχιστον πόλους, προσμετρώντας τις πολλαπλότητες[2]. Έτσι, αποδεικνύεται το παρακάτω αποτελέσμα.

Πρόταση 4.2.3. *Το πλήθος των σημείων μηδενισμού μίας ελλειπτικής συνάρτησης σε ένα παραλληλόγραμμο περιόδου είναι ίσο προς το πλήθος των πόλων αυτής, προσμετρώντας και τις πολλαπλότητες.*

Απόδειξη. (βλ. [3], σελ.6, Θεώρ. 1.8.) □

Επίσης, μπορούμε να αποδείξουμε ότι το άθροισμα των ιδιαζόντων σημείων (σημείων μηδενισμού και πόλων) μιας ελλειπτικής συνάρτησης σε ένα παραλληλόγραμμο περιόδων, το οποίο δεν εμφανίζει σημεία μηδενισμού ή πόλους στο σύνορό του, ισούται με 0. Αυτό μας οδηγεί στο παρακάτω αποτέλεσμα, του οποίου την απόδειξη παραλείπουμε.

Πρόταση 4.2.4. *Έστω ελλειπτική συνάρτηση f ορισμένη σε ένα κελί. Εάν το $\{a_i \mid 1 \leq i \leq r\,,\, r \in \mathbb{N}\}$ είναι το σύνολο όλων των ιδιαζόντων σημείων της f, τότε ισχύει ότι*

$$\sum_{i=1}^{r} m_i a_i \in L,$$

όπου ως m_i συμβολίζουμε την πολλαπλότητα ή την τάξη του a_i, ανάλογα με το αν αυτό είναι σημείο μηδενισμού ή πόλος.

Απόδειξη. (βλ. [15], σελ.259, Θεώρ. 9.1(4)) □

Μέχρι τώρα, κάναμε λόγο για μία κατηγορία συναρτήσεων χωρίς να έχουμε προσδιορίσει ποιά μορφή μπορεί να έχουν αυτές. Έτσι, από αυτό το σημείο θα ασχοληθούμε με την κατασκευή (μη σταθερών) ελλειπτικών συναρτήσεων. Προς τούτο, επιλέγουμε εξ αρχής ένα θεμελιώδες ζεύγος περιόδων (ω_1, ω_2). Σύμφωνα με όσα ήδη αναφέρθηκαν θέλουμε σε ένα παραλληλόγραμμο περιόδων η ελλειπτική συνάρτηση που επιθυμούμε να κατασκευάσουμε, έστω η f, να έχει είτε δυο τουλάχιστον απλούς πόλους, είτε τουλάχιστον ένα διπλό πόλο. Στα πλαίσια της εργασίας αυτής θα επιμείνουμε στην κατασκευή ελλειπτικών συναρτήσεων με διπλό πόλο. Μάλιστα υποθέτουμε ότι ο πόλος αυτός συναντάται στην αρχή των αξόνων, και συνεπώς σε κάθε περίοδο. Επομένως, μπορούμε να επιλέξουμε μία περιοχή γύρω από κάθε περίοδο ω, χωρίς αυτήν, στην οποία η f να είναι αναλυτική. Αυτό

[2]Κατά την περίπτωση που οι δύο πόλοι ταυτίζονται, ουσιαστικά κάνουμε λόγο για ένα διπλό πόλο.

σημαίνει ότι στην εν λόγω περιοχή η f έχει ανάπτυγμα Laurent. Κι εφόσον είμαστε στην περίπτωση του διπλού πόλου το ανάπτυγμα θα έχει τη μορφή

$$f(z) = \frac{A}{(z-\omega)^2} + \frac{B}{(z-\omega)} + \text{δυναμοσειρά κέντρου } \omega.$$

Για λόγους απλότητας επιλέγουμε $A = 1$ και $B = 0$. Κι εφόσον επιθυμούμε μία τέτοια έκφραση γύρω από κάθε περίοδο ω, θεωρούμε το άθροισμα

$$\sum_{\omega \in L(\omega_1, \omega_2)} \frac{1}{(z-\omega)^2}.$$

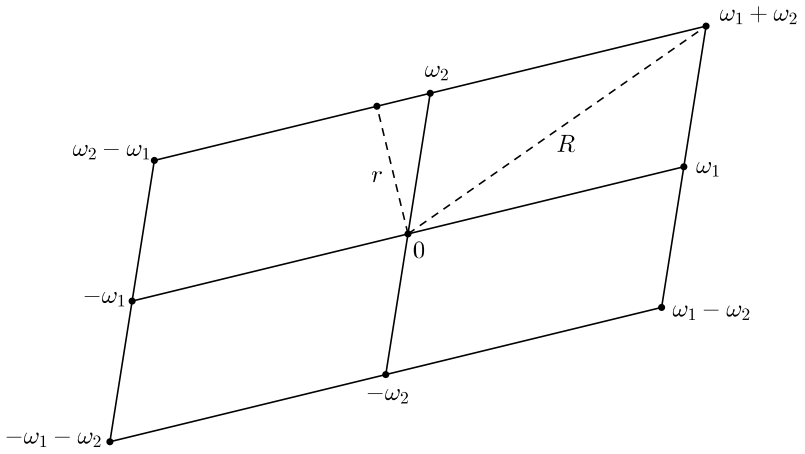
Ουσιαστικά, εάν σταθεροποιήσουμε το μιγαδικό αριθμό $z \neq \omega$, το ανωτέρω είναι ένα διπλό άθροισμα ως προς ω_1 και ω_2.

Λημμα 4.2.5. *Εάν $\alpha \in \mathbb{R}$, τότε η σειρά*

$$\sum_{0 \neq \omega \in L(\omega_1, \omega_2)} \frac{1}{\omega^\alpha}$$

συγκλίνει απόλυτα εάν, και μόνο εάν $\alpha > 2$.

Απόδειξη. Ορίζουμε ως r και R την ελάχιστη και τη μέγιστη απόσταση του 0 από το παραλληλόγραμμο κορυφών $\omega_1+\omega_2$, $\omega_1-\omega_2$, $-\omega_1-\omega_2$ και $\omega_2-\omega_1$, όπως φαίνεται στο σχήμα που ακολουθεί.



Εάν η περίοδος ω είναι μία από τις 8 που κείνται επί του παραλληλογράμμου του σχήματος, τότε γι' αυτήν ισχύει ότι

$$r \leq |\omega| \leq R.$$

Μετρούμε, τώρα, το αμέσως επόμενο παραλληλόγραμμο με κέντρο το 0 και κορυφές περιόδους. Μετρώντας τις περιόδους της περιμέτρου και διαπιστώνουμε ότι είναι 16 στο πλήθος. Τότε για καθεμία από αυτές ισχύει ότι

$$2r \leq |\omega| \leq 2R.$$

Επαναλαμβάνουμε τη διαδικασία, οπότε ύστερα από n φορές θα έχουμε την ανισότητα

$$nr \leq |\omega| \leq nR,$$

για τις επόμενες $8n$ περιόδους, Τότε θα ισχύει ότι

$$\frac{1}{R^\alpha} \leq \frac{1}{|\omega|^\alpha} \leq \frac{1}{r^\alpha} \text{ ,για τις πρώτες } 8 \text{ περιόδους}$$

$$\frac{1}{(2R)^\alpha} \leq \frac{1}{|\omega|^\alpha} \leq \frac{1}{(2r)^\alpha} \text{ ,για τις επόμενες } 16 \text{ περιόδους}$$

$$\vdots$$

Συνεπώς, θέτοντας

$$S(n) = \sum |\omega|^\alpha,$$

όπου το άθροισμα λαμβάνεται στις $8(1+2+\cdots+n)$ πρώτες περιόδους γύρω από την ω, λαμβάνουμε ότι

$$\frac{8}{R^\alpha} + \frac{2\cdot 8}{(2R)^\alpha} + \cdots + \frac{n\cdot 8}{(nR)^\alpha} \leq S(n) \leq \frac{8}{r^\alpha} + \frac{2\cdot 8}{(2r)^\alpha} + \cdots + \frac{n\cdot 8}{(nr)^\alpha} \Leftrightarrow$$

$$\frac{8}{R^\alpha}\sum_{k=1}^{n}\frac{1}{k^{\alpha-1}} \leq S(n) \leq \frac{8}{r^\alpha}\sum_{k=1}^{n}\frac{1}{k^{\alpha-1}}.$$

Από την ανισότητα αυτή είναι προφανές ότι για $\alpha > 2$ έχουμε σύγκλιση της $S(n)$. Επίσης από το αριστερό μέλος της ανισότητας είναι προφανές ότι για $\alpha \leq 2$ η ακολουθία $S(n)$ αποκλίνει. □

Λημμα 4.2.6. *Αν $\alpha > 2$ και $R > 0$ η σειρά*

$$\sum_{|\omega|>R} \frac{1}{(z-\omega)^\alpha},$$

συγκλίνει απόλυτα και ομοιόμορφα στο δίσκο $|z| \leq R$.

Απόδειξη. Προς απόδειξη του ζητουμένου θα δείξουμε ότι υπάρχει μία σταθερά M, η οποία εξαρτάται από την επιλογή του R και του α, με την ιδιότητα για κάθε $\alpha \geq 1$ να ισχύει ότι

$$\frac{1}{|z-\omega|^\alpha} \leq \frac{M}{|\omega|^\alpha},$$

για κάθε ω με $|\omega| > R$ και για κάθε z με $|z| \leq R$. Η ανισότητα αυτή είναι ισοδύναμη με την

$$\left|\frac{z-\omega}{\omega}\right|^\alpha \geq \frac{1}{M}.$$

Από τα ω που έχουν την ιδιότητα $|\omega| > R$, επιλέγουμε αυτό με το ελάχιστο μέτρο, έστω $|\omega| = R + d$, όπου $d > 0$. Τότε εάν $|z| \leq R$ και $|\omega| \geq R + d$, έχουμε

$$\left|\frac{z-\omega}{\omega}\right| = \left|1 - \frac{z}{\omega}\right| \geq 1 - \left|\frac{z}{\omega}\right| \geq 1 - \frac{R}{R+d}.$$

Άρα έχουμε ότι

$$\left|\frac{z-\omega}{\omega}\right|^\alpha \geq \left(1 - \frac{R}{R+d}\right)^\alpha = \frac{1}{M},$$

όπου

$$M = \left(1 - \frac{R}{R+d}\right)^{-\alpha}.$$

Επομένως βρήκαμε κάποιο M, το οποίο να ικανοποιεί την ανισότητα

$$\frac{1}{|z-\omega|^\alpha} \leq \frac{M}{|\omega|^\alpha}.$$

Τότε θα έχουμε

$$\sum_{|\omega|>R} \frac{1}{(z-\omega)^\alpha} \leq M \sum_{|\omega|>R} \frac{1}{|\omega|^\alpha} \leq M \sum_{0\neq\omega\in L(\omega_1,\omega_2)} \frac{1}{\omega^\alpha}.$$

Άρα, τελικά, το αποτέλεσμα προκύπτει άμεσα με εφαρμογή του λήμματος 4.2.5. □

Η κατασκευή ελλειπτικής συνάρτησης με πόλο τάξης 2 σε κάθε περίοδο θα γίνει έμμεσα. Στο τελευταίο αποτέλεσμα αυτής της παραγράφου κατασκευάζουμε ελλειπτική συνάρτηση με πόλο τάξης 3 (σε κάθε περίοδο). Στην επόμενη παράγραφο, θα επεκταθούμε περισσότερο στην κατασκευή ελλειπτικής συνάρτησης τάξης 2, ήτοι ελλειπτικής συνάρτησης με πόλο τάξης 2 (σε κάθε περίοδο).

Θεωρημα 4.2.7. *Θεωρούμε τη μιγαδική συνάρτηση που ορίζεται μέσω του τύπου*

$$f(z) = \sum_{\omega\in L(\omega_1,\omega_2)} \frac{1}{(z-\omega)^3},$$

για κάποιο θεμελιώδες ζεύγος (ω_1, ω_2). *Τότε η* f *είναι ελλειπτική συνάρτηση με περιόδους* ω_1 *και* ω_2 *και πόλο τάξης* 3 *σε κάθε περίοδο* $\omega \in L(\omega_1, \omega_2)$.

Απόδειξη. Σύμφωνα με το λήμμα 4.2.6 η συνάρτηση $f(z)$ του θεωρήματος, αθροίζοντας όμως μόνο τις περιόδους ω με την ιδιότητα $|\omega| > R$, συγκλίνει στο δίσκο $|z| \leq R$. Αυτό σημαίνει ότι η

$$\sum_{|\omega|>R} \frac{1}{(z-\omega)^3},$$

είναι αναλυτική στο δίσκο $|z| \leq R$. Οι εναπομείναντες όροι της f, οι οποίοι είναι πεπερασμένοι στο πλήθος, είναι αναλυτικές συναρτήσεις εκτός από τα σημεία των περιόδων στα οποία έχουμε πόλους. Επομένως, η f είναι μερόμορφη συνάρτηση.

Παρατηρούμε, τώρα, ότι λόγω της απόλυτης σύγκλισης της σειράς

$$\sum_{\omega\in L(\omega_1,\omega_2)} \frac{1}{(z-\omega)^3},$$

την οποία έχουμε εξασφαλίσει στο λήμμα 4.2.6, έχουμε ότι

$$\sum_{\omega\in L(\omega_1,\omega_2)} \frac{1}{(z-\omega)^3} = \sum_{-\omega_1+\omega\in L(\omega_1,\omega_2)} \frac{1}{(z+\omega_1-\omega)^3} = \sum_{\omega\in L(\omega_1,\omega_2)} \frac{1}{(z+\omega_1-\omega)^3}.$$

Πράγματι, η σειρά

$$\sum_{\omega\in L(\omega_1,\omega_2)} \frac{1}{(z+\omega_1-\omega)^3}$$

αποτελεί αναδιάταξη των όρων της αρχικής σειράς

$$\sum_{\omega\in L(\omega_1,\omega_2)} \frac{1}{(z-\omega)^3}$$

και η απόλυτη σύγκλιση αυτής εξασφαλίζει ότι το όριο παραμένει σταθερό ύστερα από αυτή την αναδιάταξη. Άρα

$$f(z) = f(z + \omega_1).$$

Ομοίως αποδεικνύουμε και ότι

$$f(z) = f(z + \omega_2).$$

Με άλλα λόγια, οι μιγαδικοί αριθμοί ω_1 και ω_2 αποτελούν περιόδους της f. Τελικά, η $f(z)$ είναι μερόμορφη συνάρτηση με περιόδους ω_1 και ω_2, ήτοι διπλά περιοδική συνάρτηση, άρα και ελλειπτική. □

4.3 Η συνάρτηση $\wp$ του Weierstrass

Η προηγούμενη παράγραφος ολοκληρώθηκε με τον προσδιορισμό ελλειπτικής συνάρτησης με πόλο τάξης 3 σε κάθε περίοδο. Επιθυμούμε τώρα να κατασκευάσουμε ελλειπτική συνάρτηση με πόλο τάξης 2 σε κάθε περίοδο. Αυτό το πετυχαίνουμε απλά ολοκληρώνοντας κάθε όρο του αθροίσματος της $f(z)$, όπως αυτή ορίστηκε στο θεώρημα 4.2.7 και πολλαπλασιάζοντας με -2. Πράγματι εάν ολοκληρώσουμε τον όρο $1/(z-\omega)^3$ ως προς z γύρω από κάθε περίοδο, λαμβάνουμε $-1/2(z-\omega)^2$. Επομένως ο πολλαπλασιασμός με -2 μας δίνει $(z-\omega)^{-2}$. Είναι βολικό, να ξεκινήσουμε την κατά όρους ολοκλήρωσή μας από την αρχή των αξόνων οπότε προς τούτο εξαιρούμε τη περίπτωση $\omega = 0$. Ο όρος που αντιστοιχεί σε αυτή την περίπτωση είναι ο $1/z^3$, του οποίου το ολοκλήρωμα μας δίνει $-1/2z^2$. Κι εφόσον πολλαπλασιάζουμε με -2 θα προσθέσουμε στο ολοκλήρωμα τον όρο z^{-2}. Η διαδικασία αυτή, ξεκινώντας από την ελλειπτική συνάρτηση $f(z)$ με περιόδους ω_1 και ω_2, μας οδηγεί στη συνάρτηση

$$\frac{1}{z^2} + \int_0^z \sum_{0 \neq \omega \in L(\omega_1, \omega_2)} \frac{-2}{(t-\omega)^3} dt.$$

Το αποτέλεσμα της κατά όρους ολοκλήρωσης είναι η συνάρτηση $\wp$ του Weierstrass.

ΟΡΙΣΜΟΣ 4.3.1. Η συνάρτηση $\wp$ του Weierstrass ορίζεται μέσω της σειράς

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L(\omega_1, \omega_2)} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

ΘΕΩΡΗΜΑ 4.3.2. *Η συνάρτηση $\wp$, όπως ορίστηκε ανωτέρω, έχει περιόδους ω_1 και ω_2. Είναι αναλυτική συνάρτηση εκτός από ένα διπλό πόλο που έχει σε κάθε περίοδο $\omega \in L(\omega_1, \omega_2)$. Επιπροσθέτως, η $\wp(z)$ είναι άρτια συνάρτηση του z.*

Απόδειξη. Η συνάρτηση του Weierstrass ορίζεται μέσω του τύπου

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L(\omega_1, \omega_2)} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Κάθε όρος της σειράς έχει μέτρο

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega^2 - (z-\omega)^2}{\omega^2 (z-\omega)^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right|.$$

Θεωρούμε κάποιο συμπαγή δίσκο $|z| \leq R$, τότε σε αυτόν υπάρχουν πεπερασμένο πλήθος περιόδων ω για οποιαδήποτε επιλογή του R. Εάν εξαιρέσουμε τους όρους της ακολουθίας που περιέχουν αυτές τις περιόδους λαμβάνουμε, όπως και στην απόδειξη του λήμματος 4.2.6, την ανισότητα

$$\left| \frac{1}{(z-\omega)^2} \right| \leq \frac{M}{|\omega|^2},$$

για κάποια συγκεκριμένη σταθερά M, η οποία εξαρτάται από το R. Η ανισότητα αυτή μας δίνει μία εκτίμηση για το μέτρο των όρων της σειράς. Με άλλα λόγια, ισχύει ότι

$$\left|\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right| = \left|\frac{z(2\omega-z)}{\omega^2(z-\omega)^2}\right| \leq \frac{2MR(2|\omega|+R)}{|\omega|^4} \leq \frac{2MR(2+\frac{R}{|\omega|})}{|\omega|^3} \leq \frac{3MR}{|\omega^3|},$$

αφού για κάθε περίοδο ω εκτός του δίσκου $|z| \leq R$ ισχύει ότι $|\omega| > R$. Η σειρά, λοιπόν, που εναπομένει αν εξαιρέσουμε τους όρους που εμπλέκουν τις περιόδους ω για τις οποίες ισχύει ότι $|\omega| \leq R$ συγκλίνει απόλυτα και ομοιόμορφα στο δίσκο $|z| \leq R$, άρα είναι αναλυτική σε αυτόν. Εάν, τώρα, προσμετρήσουμε και τους όρους που εξαιρέσαμε, ώστε να έχουμε τη συνάρτηση $\wp$, λαμβάνουμε ότι σε κάθε περίοδο έχουμε διπλό πόλο, ήτοι η συνάρτηση μας είναι μερόμορφη.

Σε αυτό το σημείο θα δείξουμε ότι η συνάρτηση του Weierstrass είναι άρτια. Πράγματι, ισχύει ότι

$$\begin{aligned}
\wp(-z) &= \frac{1}{(-z)^2}+\sum_{0\neq\omega\in L(\omega_1,\omega_2)}\left(\frac{1}{(-z-\omega)^2}-\frac{1}{\omega^2}\right) = \frac{1}{z^2}+\sum_{0\neq\omega\in L(\omega_1,\omega_2)}\left(\frac{1}{(z-(-\omega))^2}-\frac{1}{\omega^2}\right)\\
&= \frac{1}{z^2}+\sum_{0\neq-\omega\in L(\omega_1,\omega_2)}\left(\frac{1}{(z-(-\omega))^2}-\frac{1}{\omega^2}\right) = \frac{1}{z^2}+\sum_{0\neq\omega\in L(\omega_1,\omega_2)}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)\\
&= \wp(z).
\end{aligned}$$

Τέλος, εξετάζουμε την περιοδικότητα της $\wp$. Ήδη γνωρίζουμε ότι η παράγωγος αυτής, ήτοι η συνάρτηση $\wp'$ είναι διπλά περιοδική συνάρτηση, με περιόδους ω_1 και ω_2. Ισχύει επομένως ότι $\wp'(z) = \wp'(z+\omega)$, για κάθε $\omega \in L(\omega_1,\omega_2)$. Αυτό όμως σημαίνει ότι η συνάρτηση $\wp(z)-\wp(z+\omega)$ είναι μία σταθερή συνάρτηση. Για $z=-\omega/2$, γνωρίζουμε ότι $\wp(-\omega/2)-\wp(\omega/2)=0$. Άρα ισχύει ότι $\wp(z)=\wp(z+\omega)$, για κάθε $\omega\in L(\omega_1,\omega_2)$, ήτοι η $\wp$ είναι και διπλά περιοδική. Βάσει, λοιπόν, όλων των παραπάνω η συνάρτηση του Weierstrass είναι ελλειπτική. □

Το ερώτημα που εγείρεται φυσικά, είναι αν υπάρχουν και άλλες ελλειπτικές συναρτήσεις τάξης 2. Η απάντηση σε αυτό το ερώτημα δίνεται από το παρακάτω θεώρημα:

ΘΕΩΡΗΜΑ 4.3.3. *Το σύνολο των ελλειπτικών συναρτήσεων τάξεως 2 ταυτίζεται με το σώμα* $\mathbb{C}(\wp,\wp')$.

Απόδειξη. Έστω f τυχούσα ελλειπτική συνάρτηση με περιόδους ω_1 και ω_2. Γράφουμε την f υπό τη μορφή

$$f(z) = \frac{f(z)+f(-z)}{2}+\frac{f(z)-f(-z)}{2},$$

ήτοι ως άθροισμα μίας άρτιας και μίας περιττής ελλειπτικής συνάρτησης. Αυτό σημαίνει ότι αντί να δείξουμε το ζητούμενο για τυχούσα ελλειπτική συνάρτηση, αρκεί να ελέγξουμε την περίπτωση όπου η f είναι είτε άρτια, είτε περιττή. Εάν υποθέσουμε ότι η f είναι περιττή συνάρτηση, τότε η $f\wp'$ θα είναι άρτια συνάρτηση και σαφώς ελλειπτική. Μπορούμε, επομένως, χ.β.τ.γ. να υποθέσουμε ότι η f είναι άρτια ελλειπτική συνάρτηση. Τότε θα ισχύει ότι

$$f(z) = f(-z),$$

για κάθε $z\in\mathbb{C}$. Από τη σχέση αυτή έπεται άμεση την

$$f^{(k)}(z) = (-1)^k\cdot f^{(k)}(-z).$$

Αυτό σημαίνει ότι εάν η f έχει το u ως σημείο μηδενισμού πολλαπλότητας m, τότε και το $-u$ θα είναι σημείο μηδενισμού πολλαπλότητας m. Το αυτό θα ισχύει και για τους πόλους. Θα δείξουμε, τώρα, ότι εάν $2u\in L(\omega_1,\omega_2)$, τότε η f έχει σημείο μηδενισμού άρτιας πολλαπλότητας, ή εάν το u είναι πόλος

και $2u \in L(\omega_1, \omega_2)$ τότε η f έχει πόλο άρτιας τάξης. Ξεκινάμε με την ιδιότητα $2u \in L(\omega_1, \omega_2)$. Τα σημεία ενός παραλληλογράμμου περιόδων που έχουν αυτή την ιδιότητα είναι τα παρακάτω τέσσερα:

$$0\,,\,\frac{\omega_1}{2}\,,\,\frac{\omega_2}{2}\,,\,\frac{\omega_1+\omega_2}{2}.$$

Η συνάρτηση f εξ υποθέσεως είναι άρτια άρα η παράγωγος αυτής, ήτοι η f', θα είναι περιττή συνάρτηση. Επομένως θα έχουμε ότι

$$f'(z) = -f'(-z),$$

για κάθε $z \in \mathbb{C}$. Εάν εφαρμόσουμε την ιδιότητα αυτή για $z = u$, θα έχουμε ότι

$$f'(u) + f'(-u) = 0.$$

Όμως ισχύει ότι $2u \in L(\omega_1, \omega_2) \Rightarrow u \equiv -u \pmod{L(\omega_1, \omega_2)}$ [3]. Άρα έχουμε ότι

$$f'(u) = 0.$$

Αυτό σημαίνει ότι εάν το u είναι σημείο μηδενισμού της f, τότε θα είναι πολλαπλότητας τουλάχιστον 2. Διακρίνουμε, τώρα, τις εξής περιπτώσεις:

- Εάν $u \notin L(\omega_1, \omega_2)$ το ανωτέρω επιχείρημα εφαρμοσμένο στη συνάρτηση $g(z) := \wp(z) - \wp(u)$ μας πληροφορεί ότι η g έχει σημείο μηδενισμού το u, πολλαπλότητας τουλάχιστον 2. Όμως από το 4.2.3 και το γεγονός ότι η $\wp$ έχει πόλο τάξης 2 σε κάθε περίοδο, έπεται άμεσα ότι το u είναι σημείο μηδενισμού πολλαπλότητας ίσης με 2. Εξ ορισμού της η g είναι άρτια ελλειπτική συνάρτηση άρα το αυτό ισχύει και για το πηλίκο f/g. Μάλιστα, η f/g θα είναι ολόμορφη συνάρτηση στο u. Εάν $f(u)/g(u) \neq 0$, τότε πράγματι η πολλαπλότητα του u στην f είναι ίση με 2. Εάν $f(u)/g(u) = 0$, τότε η f/g έχει ως σημείο μηδενισμού το u, οπότε επαναλαμβάνουμε τη διαδικασία.

- Εάν $u \in L(\omega_1, \omega_2)$ τότε ως g επιλέγουμε τη συνάρτηση $1/\wp$ και εφαρμόζουμε το επιχείρημα της προηγούμενης περίπτωσης.

Έτσι, δείξαμε ότι η f έχει σημείο μηδενισμού άρτιας πολλαπλότητας στο u. Θεωρούμε την οικογένεια $\{u_i \mid i = 1, 2, \ldots, r\}$ σημείων, τα οποία είναι είτε σημεία μηδενισμού είτε πόλοι της f και, επιπροσθέτως, έχουν την ιδιότητα

$$u_i \neq -u_j\,,\,\forall\, i \neq j,$$

όπου $i, j \in \{1, 2, \ldots, r\}$. Τότε ορίζουμε

$$m_i := \begin{cases} ord_f(u_i) & ,\text{αν } \ 2u_i \notin L(\omega_1, \omega_2) \\ \frac{1}{2} ord_f(u_i) & ,\text{αν } \ 2u_i \in L(\omega_1, \omega_2) \end{cases},$$

όπου ως $ord_f(u_i)$ συμβολίζουμε την πολλαπλότητα του u_i όταν αυτό είναι σημείο μηδενισμού της f, ή την τάξη του u_i όταν αυτό είναι πόλος της f. Επί τη βάσει των όσων μέχρι τώρα έχουμε αποδείξει, για τυχόντα $a \in \mathbb{C}$ το να ισχύει ότι $2a \in L(\omega_1, \omega_2)$ είναι ισοδύναμο με το ότι η συνάρτηση $\wp(z) - \wp(a)$ έχει στο a πόλο τάξης 2 ή σημείο μηδενισμού πολλαπλότητας 2. Αν από την άλλη ισχύει ότι $2a \notin$

[3] Με την ισοτιμία αυτή εννοούμε ότι τα u και $-u$ βρίσκονται στην ίδια κλάση ισοδυναμίας, που ορίζεται μέσω της σχέσης ισοδυναμίας

$$\alpha \sim_{L(\omega_1,\omega_2)} \beta :\Leftrightarrow \alpha - \beta \in L(\omega_1, \omega_2).$$

Ουσιαστικά έχουμε υποθέσει ότι το u δεν είναι απλά ένας μιγαδικός αριθμός, αλλά είναι στοιχείο του του πηλίκου $\mathbb{C}/L(\omega_1, \omega_2)$.

$L(\omega_1, \omega_2)$, τότε η συνάρτηση $\wp(z) - \wp(a)$ παρουσιάζει στα σημεία a και $-a$ πόλο τάξης 1 η σημείο μηδενισμού πολλαπλότητας 1. Κατά συνέπεια για κάθε $z \notin L(\omega_1, \omega_2)$ ισχύει ότι η συνάρτηση

$$\prod_{i=1}^{r} \left(\wp(z) - \wp(u_i)\right)^{m_i},$$

έχει την ίδια τάξη στο z με την f. Τελικά, εάν υποθέσουμε τη συνάρτηση πηλίκο της f δια το ανωτέρω γινόμενο τότε αυτή είναι μία ελλειπτική συνάρτηση χωρίς σημεία μηδενισμού ή πόλους, ήτοι σταθερή συνάρτηση. Με αυτή τη διαπίστωση ολοκληρώνεται η απόδειξη του θεωρήματος. □

Από αυτό το σημείο και μέχρι το τέλος της παραγράφου αυτής θα δώσουμε κάποια επιπρόσθετα στοιχεία για τη συνάρτηση του Weierstrass. Έχουμε ήδη αναφέρει ότι η $\wp$ έχει ανάπτυγμα Laurent. Χωρίς απόδειξη αναφέρουμε το παρακάτω θεώρημα το οποίο προσδιορίζει πλήρως τη μορφή του αναπτύγματος.

ΠΡΟΤΑΣΗ 4.3.4. *Εστω* $r = min\{|\omega| \ : \ 0 \neq \omega \in L(\omega_1, \omega_2)\}$. *Τότε στο δακτύλιο* $0 < |z| < r$ *ισχύει ότι*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{+\infty} \left((2n+1) \cdot G_{2n+2} \cdot z^{2n}\right),$$

όπου ως G_n *συμβολίζουμε τη* σειρά Eisenstein τάξης n, *ήτοι τη σειρά*

$$G_n := \sum_{0 \neq \omega \in L(\omega_1, \omega_2)} \frac{1}{\omega^n}, \ n \geq 3.$$

Απόδειξη. (βλ. [3], σελ.11, Θεώρ.1.11.) □

ΠΡΟΤΑΣΗ 4.3.5. *Η συνάρτηση* $\wp$ *ικανοποιεί τη μη γραμμική διαφορική εξίσωση*

$$\left(\wp'(z)\right)^2 = 4\wp^3(z) - 60G_4 \cdot \wp(z) - 140G_6$$

Απόδειξη. Η απόδειξη βασίζεται στην κατασκευή ενός γραμμικού συνδυασμού δυνάμεων των συναρτήσεων $\wp$ και $\wp'$ με σκοπό να εξαλείψουμε τον πόλο στη θέση $z = 0$. Η διαδικασία αυτή θα μας δώσει μία ελλειπτική συνάρτηση χωρίς πόλους και κατά συνέπεια σταθερή. Κοντά στο $z = 0$ έχουμε ότι

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + \cdots.$$

Αυτή είναι μία ελλειπτική συνάρτηση τάξης 3. Το τετράγωνο αυτής είναι ελλειπτική συνάρτηση τάξης 6. Πράγματι,

$$\left(\wp'(z)\right)^2 = \frac{4}{z^6} + \frac{24G_4}{z^2} - 80G_6 + \cdots,$$

όπου στο $+\cdots$ υπάρχει μία δυναμοσειρά, η οποία μηδενίζεται για $z = 0$. Έχουμε, τώρα, ότι

$$4\wp^3(z) = \frac{4}{z^6} + \frac{36G_4}{z^2} + 6 - G_6 + \cdots,$$

άρα

$$\left(\wp'(z)\right)^2 - 4\wp^3(z) = -\frac{60G_4}{z^2} - 140G_6 + \cdots.$$

Επομένως

$$\left(\wp'(z)\right)^2 - 4\wp^3(z) + 60G_4 \cdot \wp(z) = -140G_6 + \cdots.$$

Το αριστερό μέλος είναι ελλειπτική συνάρτηση χωρίς πόλο στο σημείο $z = 0$, το οποίο σημαίνει ότι είναι μία σταθερή συνάρτηση. Κατ' ανάγκη, λοιπόν, θα ισούται με $-140G_6$. □

Στην πορεία θα δούμε ότι η εν λόγω διαφορική εξίσωση μας επιτρέπει να συσχετίσουμε τη συνάρτηση του Weierstrass με τις ελλειπτικές καμπύλες. Περαιτέρω αναφορά θα γίνει στο επόμενο κεφάλαιο. Το δεύτερο μέλος της διαφορικής εξίσωσης ουσιαστικά είναι ένα πολυώνυμο τρίτου βαθμού. Επιθυμούμε, όπως είναι λογικό, την παραγοντοποίηση αυτού. Θα δείξουμε ότι πράγματι το πολυώνυμο αυτό επιδέχεται παραγοντοποίηση και μάλιστα σε γινόμενο αναγώγων πολυωνύμων. Προς απόδειξη αυτού δίνουμε τον παρακάτω ορισμό:

ΟΡΙΣΜΟΣ 4.3.6. Ως e_1, e_2 και e_3 συμβολίζουμε τις τιμές τις συνάρτησης του Weierstrass στις μη μηδενικές ημιπεριόδους $\omega_1/2$, $\omega_2/2$ και $(\omega_1+\omega_2)/2$ αντιστοίχως. Με άλλα λόγια, έχουμε ότι

$$e_1 = \wp\left(\frac{\omega_1}{2}\right) \ , \ e_2 = \wp\left(\frac{\omega_2}{2}\right) \ , \ e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right).$$

ΘΕΩΡΗΜΑ 4.3.7. *Ισχύει ότι*

$$4\wp^3(z) - g_2\wp(z) - g_3 = \big(\wp(z)-e_1\big)\big(\wp(z)-e_2\big)\big(\wp(z)-e_3\big),$$

όπου

$$g_2 := 60G_4 \ \textit{και} \ \ g_3 := 140G_6.$$

Επιπλέον, τα σημεία μηδενισμού e_1, e_2 και e_3 του πολυωνύμου είναι διακεκριμένα, ήτοι ισχύει ότι ${g_2}^3 - 27\cdot {g_3}^2 \neq 0$.

Απόδειξη. Εφόσον η $\wp$ είναι άρτια συνάρτηση η $\wp'$, όπως έχουμε ήδη επισημάνει. θα είναι περιττή συνάρτηση. Επομένως θα ισχύει ότι

$$\wp(z) = -\wp(-z),$$

για κάθε μιγαδικό αριθμό z. Όμως η $\wp'$ είναι ελλειπτική συνάρτηση και κατά συνέπεια και διπλά περιοδική με περιόδους τις ω_1 και ω_2, δηλαδή τις ίδιες με την $\wp$. Άρα θα ισχύει ότι

$$\wp(z+\omega_1) = \wp(z).$$

Εάν επιλέξουμε $z = -\omega_1/2$, τότε θα έχουμε ότι

$$\wp\left(-\frac{\omega_1}{2}+\omega_1\right) = \wp\left(-\frac{\omega_1}{2}\right) \Rightarrow \wp\left(\frac{\omega_1}{2}\right) = \wp\left(-\frac{\omega_1}{2}\right) = -\wp\left(\frac{\omega_1}{2}\right) \Rightarrow 2\wp\left(\frac{\omega_1}{2}\right) = 0 \Rightarrow$$

$$\wp\left(\frac{\omega_1}{2}\right) = 0.$$

Ομοίως δείχνουμε και ότι

$$\wp\left(\frac{\omega_2}{2}\right) = 0 = \wp\left(\frac{\omega_1+\omega_2}{2}\right).$$

Άρα αυτά είναι τα σημεία μηδενισμού του πολυωνύμου $4\wp^3(z) - g_2\wp(z) - g_3$ σε κάποιο παραλληλόγραμμο περιόδων. Θα δείξουμε, τώρα, ότι οι αριθμοί e_1, e_2 και e_3 είναι διακεκριμένοι. Η ελλειπτική συνάρτηση $\wp(z)-e_1$ έχει ως σημείο μηδενισμού το $z=\omega_1/2$. Το σημείο αυτό έχει πολλαπλότητα ίση με 2 (βλ. απόδειξη του θεωρήματος 4.3.3). Ομοίως η συνάρτηση $\wp(z)-e_2$ έχει ως διπλό σημείο μηδενισμού το $z=\omega_2/2$. Εάν υποθέσουμε ότι $e_1=e_2$, αυτό θα σήμαινε ότι η ελλειπτική συνάρτηση $\wp(z)-e_1$ θα είχε ως διπλό σημείο μηδενισμού και το e_1 και το e_2. Επομένως το πλήθος των σημείων μηδενισμού προσμετρώντας και τις πολλαπλότητες θα ήταν ≥ 4. Όμως αφού η $\wp$ σε κάθε παραλληλόγραμμο τετραγώνων έχει ένα πόλο τάξης 2, από την πρόταση 4.2.3 καταλήγουμε σε αντίφαση. Άρα θα ισχύει ότι $e_1 \neq e_2$. Με όμοιο τρόπο αποδεικνύουμε και ότι $e_2 \neq e_3$ και $e_3 \neq e_1$. □

4.4 $\mathcal{J}$- αναλλοίωτος και unimodular μετασχηματισμοί

Το τελευταίο θεώρημα της προηγούμενης παραγράφου μας πληροφορεί ότι ${g_2}^3 - 27{g_3}^2 \neq 0$. Στο επόμενο κεφάλαιο πρόκειται να δούμε ότι η πληροφορία αυτή έχει ιδιαίτερη σημασία. Εάν δούμε το $4\wp^3(z) - g_2\wp(z) - g_3$ ως πολυώνυμο μεταβλητής $\wp(z)$, τότε η ποσότητα ${g_2}^3 - 27{g_3}^2$ εκφράζει πολλαπλάσιο της διακρίνουσας του πολυωνύμου και προς τούτο θα καλείται *διακρίνουσα* και θα συμβολίζεται ως Δ. Εάν δούμε τη διακρίνουσα ως συνάρτηση μεταβλητών ω_1 και ω_2, ήτοι $\Delta = \Delta(\omega_1, \omega_2)$, τότε δεδομένου ότι οι g_2 και g_3 είναι ομογενείς συναρτήσεις βαθμού -4 και -6, αντιστοίχως, συμπεραίνουμε ότι η διακρίνουσα είναι ένα ομογενές πολυώνυμο βαθμού -12. Επομένως, για τυχαίο μιγαδικό αριθμό $\lambda \neq 0$ ισχύει ότι

$$\Delta(\lambda\omega_1, \lambda\omega_2) = \lambda^{-12} \cdot \Delta(\omega_1, \omega_2).$$

Επιλέγουμε, τώρα, ως λ το μιγαδικό αριθμό $1/\omega_1$ και θέτουμε $\tau := \omega_2/\omega_1$. Τότε θα ισχύει ότι

$$\Delta(1, \tau) = \Delta\left(\frac{1}{\omega_1} \cdot \omega_1, \frac{1}{\omega_1} \cdot \omega_2\right) = \left(\frac{1}{\omega_1}\right)^{-12} \cdot \Delta(\omega_1, \omega_2) = {\omega_1}^{12} \cdot \Delta(\omega_1, \omega_2).$$

Ομοίως μπορούμε να πράξουμε και για τις συναρτήσεις $g_2 = g_2(\omega_1, \omega_2)$ και $g_3 = g_3(\omega_1, \omega_2)$ αφού και αυτές είναι εξ ορισμού ομογενή πολυώνυμα βαθμών 4 και 6 αντιστοίχως. Τότε θα έχουμε

$$g_2(1, \tau) = {\omega_1}^4 \cdot g_2(\omega_1, \omega_2),$$

$$g_3(1, \tau) = {\omega_1}^6 \cdot g_3(\omega_1, \omega_2).$$

Αυτό σημαίνει ότι με κατάλληλη κανονικοποίηση μπορούμε να υποθέσουμε ότι οι συναρτήσεις g_2, g_3 και Δ είναι συναρτήσεις μίας μόνο μιγαδικής μεταβλητής, της τ. Μάλιστα, μπορούμε χ.β.τ.γ. να υποθέσουμε ότι το φανταστικό μέρος της μεταβλητής $\tau = \omega_2/\omega_1$ είναι θετικό και έτσι να μελετάμε τις συναρτήσεις αυτές στο *άνω μιγαδικό ημιεπίπεδο*, ήτοι στο

$$\mathcal{H} := \{z \in \mathbb{C} \mid Im(z) > 0\}.$$

Σε αυτή την περίπτωση οι συναρτήσεις g_2, g_3 και Δ παίρνουν τη μορφή

$$g_2(\tau) = 60 \cdot \sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(m+n\tau)^4},$$

$$g_3(\tau) = 140 \cdot \sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(m+n\tau)^6}$$

και

$$\Delta(\tau) = {g_2}^3(\tau) - 27{g_3}^2(\tau).$$

Το θεώρημα 4.3.7 μας πληροφορεί ότι

$$\Delta(\tau) \neq 0 \ , \ \forall\, \tau \in \mathcal{H}.$$

Ορισμος 4.4.1. Εάν ισχύει ότι $\omega_2/\omega_1 \in \mathbb{C} \setminus \mathbb{R}$, ορίζουμε τη συνάρτηση

$$\mathcal{J} := 1728\frac{{g_2}^3}{\Delta} = 12^3\frac{{g_2}^3}{\Delta},$$

η οποία καλείται *συνάρτηση του Klein*, ή *$\mathcal{J}$-αναλλοίωτος του Klein*, ή πιο απλά *$\mathcal{J}$-αναλλοίωτος*.

Είναι απλό να ελέγξουμε ότι εξ ορισμού της, η $\mathcal{J}$-αναλλοίωτος είναι ομογενές πολυώνυμο βαθμού 0, ήτοι ισχύει ότι

$$\mathcal{J}(1,\tau) = \mathcal{J}(\omega_1,\omega_2).$$

Για το λόγο αυτό θα γράφουμε $\mathcal{J}(\tau)$ αντί για $\mathcal{J}(\omega_1,\omega_2)$.

Θεωρημα 4.4.2. *Οι συναρτήσεις $g_2(\tau)$, $g_3(\tau)$, $\Delta(\tau)$ και $\mathcal{J}(\tau)$ είναι αναλυτικές στο $\mathcal{H}$.*

Απόδειξη. Έχουμε ήδη παρατηρήσει ότι

$$\Delta(\tau) \neq 0\ ,\ \forall\, \tau \in \mathcal{H}.$$

Επομένως αρκεί να δείξουμε μόνο ότι οι g_2 και g_3 είναι αναλυτικές συναρτήσεις στο $\mathcal{H}$. Άρα εξ ορισμού της και η $\mathcal{J}$ είναι αναλυτική στο $\mathcal{H}$. Τα g_2 και g_2 ορίζονται μέσω σειρών της μορφής

$$\sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(m+n\tau)^a},$$

για κάποιο $a > 2$. Έστω ότι $\tau = x + iy$, όπου $y > 0$. Θα δείξουμε ότι για $a > 2$ η ανωτέρω σειρά συγκλίνει απόλυτα για οποιοδήποτε $\tau \in \mathcal{H}$ και ομοιόμορφα σε κάθε λωρίδα S της μορφής

$$S = \{x + iy \in \mathbb{C}\ :\ |x| < A\ ,\ y \geq \delta > 0\}.$$

Προς τούτο θα δείξουμε ότι υπάρχει μία σταθερά που εξαρτάται μονάχα από τους αριθμούς A και δ, και ικανοποιεί την ανισότητα

$$\frac{1}{|m+n\tau|^a} \leq \frac{M}{|m+in|^a},$$

για κάθε $\tau \in S$ και $(m,n) \neq (0,0)$. Εάν το καταφέρουμε αυτό τότε το ζητούμενο έπεται άμεσα από το λήμμα 4.2.5. Άρα αρκεί να βρούμε μία σταθερά $K > 0$, η οποία να εξαρτάται μονάχα από τους αριθμούς δ και A και να ικανοποιεί τη σχέση

$$|m+n\tau|^2 > K|m+ni|^2.$$

Ισοδυνάμως, επιθυμούμε η K να ικανοποιεί την ανισότητα

$$(m+nx)^2 + (ny)^2 > K(m^2+n^2).$$

Εάν $n = 0$ τότε η ανωτέρω ανισότητα είναι αληθής για οποιαδήποτε επιλογή του K στο διάστημα $(0,1)$. Εάν $n \neq 0$, τότε θέτουμε $q = m/n$ και έχουμε ότι

$$(m+nx)^2 + (ny)^2 > K(m^2+n^2) \Leftrightarrow \frac{(q+x)^2+y^2}{1+q^2} > K.$$

Επιλέγουμε τον αριθμό

$$K = \frac{\delta^2}{1+(A+\delta)^2} > 0,$$

εάν $|x| < A$ και $|y| \geq \delta$. Διακρίνουμε τις περιπτώσεις:

- Αν ισχύει ότι $|q| \leq A + \delta$, τότε $(q+x)^2 \geq 0$ και $y^2 \geq \delta^2$. Επομένως είναι προφανές ότι

$$\frac{(q+x)^2+y^2}{1+q^2} \geq \frac{\delta^2}{1+(A+\delta)^2} = K$$

- Αν, από την άλλη ισχύει ότι $|q| > A + \delta$, τότε

$$\left|\frac{x}{q}\right| < \frac{|x|}{|A+\delta|} \leq \frac{A}{A+\delta} < 1,$$

άρα

$$\left|1 + \frac{x}{q}\right| \geq 1 - \left|\frac{x}{q}\right| \geq 1 - \frac{A}{A+\delta} = \frac{\delta}{A+\delta} \Rightarrow |q+x| \geq \frac{q\delta}{A+\delta}.$$

Συνεπώς έχουμε και ότι

$$\frac{(q+x)^2 + y^2}{1+q^2} > \frac{\delta^2}{(A+\delta)^2} \cdot \frac{q^2}{1+q^2}.$$

Όμως η συνάρτηση $q^2/(1+q^2)$ είναι αύξουσα συνάρτηση του q. Αυτό σημαίνει ότι

$$|q| > A + \delta \Rightarrow \frac{q^2}{1+q^2} \geq \frac{(A+\delta)^2}{1+(\delta+A)^2}.$$

Άρα έχουμε ότι

$$\frac{(q+x)^2 + y^2}{1+q^2} > \frac{\delta^2}{(A+\delta)^2} \cdot \frac{q^2}{1+q^2} \geq \frac{\delta^2}{(A+\delta)^2} \cdot \frac{(A+\delta)^2}{1+(A+\delta)^2} = \frac{\delta^2}{1+(A+\delta)^2} =: K.$$

Έτσι, δείξαμε τη ζητούμενη ανισότητα, άρα και το ζητούμενο! □

Εισάγουμε, τώρα, δυο νέες περιόδους ω_1' και ω_2', για τις οποίες ισχύει ότι

$$\omega_2' = a\omega_2 + b\omega_1$$

$$\omega_1' = c\omega_2 + d\omega_1,$$

όπου οι a, b, c και d είναι ακέραιοι αριθμοί με την ιδιότητα $ad - bc = 1$. Τότε τα ζεύγη (ω_1, ω_2) και (ω_1', ω_2') είναι ισοδύναμα. Επομένως τα κιγκλιδώματα των ζευγών αυτών ταυτίζονται, ήτοι

$$L(\omega_1, \omega_2) = L(\omega_1', \omega_2').$$

Αυτό σημαίνει ότι ισχύουν οι ισότητες

$$g_2(\omega_1, \omega_2) = g_2(\omega_1', \omega_2'),$$

$$g_3(\omega_1, \omega_2) = g_3(\omega_1', \omega_2'),$$

$$\Delta(\omega_1, \omega_2) = \Delta(\omega_1', \omega_2')$$

και

$$\mathcal{J}(\omega_1, \omega_2) = \mathcal{J}(\omega_1', \omega_2').$$

Για το λόγο τ' των νέων περιόδων ισχύει ότι

$$\tau' = \frac{\omega_2}{\omega_1} = \frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1} = \frac{a\tau + b}{c\tau + d},$$

όπου $\tau = \omega_2/\omega_1$. Μία γρήγορη παρατήρηση που απορρέει από την παραπάνω σχέση είναι ότι ισχύει η ισοδυναμία

$$\tau' \in \mathcal{H} \Leftrightarrow \tau \in \mathcal{H}.$$

ΟΡΙΣΜΟΣ 4.4.3. Η σχέση

$$\tau' = \frac{a\tau + b}{c\tau + d}$$

ονομάζεται *unimodular μετασχηματισμός*, εάν οι αριθμοί a, b, c και d είναι ακέραιοι και ισχύει ότι $ad - bc = 1$.

Επί τη βάσει των όσων έχουμε ήδη αναφέρει ισχύει το παρακάτω θεώρημα.

ΘΕΩΡΗΜΑ 4.4.4. *Εάν $\tau \in \mathcal{H}$ και a, b, c και d ακέραιοι για τους οποίους ισχύει ότι $ad - bc = 1$, τότε ισχύει ότι*

$$\frac{a\tau + b}{c\tau + d} \in \mathcal{H},$$

και μάλιστα, ισχύει ότι

$$\mathcal{J}(\tau) = \mathcal{J}\left(\frac{a\tau + b}{c\tau + d}\right).$$

Πριν κλείσουμε αυτή την παράγραφο παρατηρούμε ότι μία επιτρεπτή επιλογή για τους a, b, c, και d είναι η $a = b = d = 1$ και $c = 0$. Τότε ισχύει ότι

$$\mathcal{J}(\tau) = \mathcal{J}\left(\frac{1 \cdot \tau + 1}{0 \cdot \tau + 1}\right) = \mathcal{J}(\tau + 1).$$

Επομένως η συνάρτηση του Klein είναι περιοδική με περίοδο ίση με 1.

4.5 Τα αναπτύγματα Fourier των g_2, g_3, Δ και $\mathcal{J}$.

Κάθε σειρά Eisenstein

$$\sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(m + n\tau)^k}$$

είναι μία περιοδική συνάρτηση με περίοδο 1. Ιδιαιτέρως, οι συντελεστές $g_2(\tau)$ και $g_3(\tau)$ είναι συναρτήσεις περιόδου 1. Για να προσδιορίσουμε πλήρως τους συντελεστές Fourier αυτών θα χρειαστούμε το παρακάτω λήμμα

ΛΗΜΜΑ 4.5.1. *Εάν $\tau \in \mathcal{H}$ και $n > 0$, τότε ισχύει ότι*

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m + n\tau)^4} = \frac{8\pi^4}{3} \sum_{r=1}^{+\infty} r^3 e^{2\pi r n \tau}$$

και

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m + n\tau)^6} = -\frac{8\pi^6}{15} \sum_{r=1}^{+\infty} r^5 e^{2\pi r n \tau}.$$

Απόδειξη. (βλ.[3], σελ.19, Λήμ. 3) □

ΠΡΟΤΑΣΗ 4.5.2. *Εάν $\tau \in \mathcal{H}$, τότε λαμβάνουμε τα αναπτύγματα Fourier*

$$g_2(\tau) = \frac{4\pi^4}{3}\left(1 + 240 \sum_{k=1}^{\infty} \sigma_3(k) e^{2\pi i k \tau}\right)$$

και

$$g_3(\tau) = \frac{8\pi^6}{27}\left(1 - 504\sum_{k=1}^{\infty}\sigma_5(k)e^{2\pi ik\tau}\right),$$

όπου

$$\sigma_\alpha(k) = \sum_{d|k} d^\alpha.$$

Απόδειξη. Ισχύει ότι

$$\begin{aligned} g_2(\tau) &= 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{+\infty} \frac{1}{(m+n\tau)^4} \\ &= 60\left(\sum_{m\neq 0}^{+\infty}\frac{1}{m^4} + \sum_{n=1}^{+\infty}\sum_{m=-\infty}^{+\infty}\left(\frac{1}{(m+n\tau)^4} + \frac{1}{(m-n\tau)^4}\right)\right) \\ &= 60\left(2\zeta(4) + 2\sum_{n=1}^{+\infty}\sum_{m=-\infty}^{+\infty}\frac{1}{(m+n\tau)^4}\right) \\ &= 60\left(\frac{2\pi^4}{90} + \frac{16\pi^4}{3}\sum_{m=1}^{+\infty}\sum_{n=1}^{+\infty} r^3 q^{nr}\right), \end{aligned}$$

όπου $q = e^{2\pi i\tau}$. Ο υπολογισμός τελειώνει συγκεντρώνοντας όλους τους όρους, για τους οποίους το γινόμενο nr είναι σταθερό. Ο τύπος για το $g_3(\tau)$ αποδεικνύεται ανάλογα. □

ΠΡΟΤΑΣΗ 4.5.3. *Εάν $\tau \in \mathcal{H}$, τότε ισχύει ότι*

$$\Delta(\tau) = (2\pi)^{12}\sum_{n=1}^{+\infty}\tau(n)e^{2\pi in\tau},$$

όπου οι συντελεστές $\tau(n)$[4] είναι ακέραιοι, με $\tau(1) = 1$ και $\tau(2) = -24$.

Απόδειξη. Θέτουμε

$$q := e^{2\pi i\tau}\ ,\ A := \sum_{n=1}^{+\infty}\sigma_3(n)q^n\ ,\ B := \sum_{n=1}^{+\infty}\sigma_5(n)q^n.$$

Τότε

$$\Delta(\tau) = {g_2}^3(\tau) - 27{g_3}^3(\tau) = \frac{64\pi^{12}}{27}\big((1+240A)^3 - (1-504B)^2\big).$$

Τα A και B είναι δυναμοσειρές με ακέραιους συντελεστές και ισχύει ότι

$$(1+240A)^3 - (1-504B)^2 = 12^2(5A+7B) + 12^3(100A^2 - 147B^2 + 8000A^3).$$

Όμως

$$5A + 7B = \sum_{n=1}^{+\infty}\big(5\sigma_3(n) + 7\sigma_5(n)\big)q^n$$

[4] Η αριθμητική συνάρτηση $\tau(n)$ ονομάζεται *τ συνάρτηση του Ramanujan.*

και

$$5d^3 + 7d^5 = d^3(5 + 7d^2) \equiv \begin{cases} d^3(d^2 - 1) \equiv 0 \pmod 3 \\ d^3(1 - d^2) \equiv 0 \pmod 4 \end{cases}.$$

Αυτό σημαίνει ότι $12 \mid 5A + 7B$, ήτοι το 12^3 είναι διαιρέτης κάθε συντελεστή της δυναμοσειράς του $(1 + 240A)^3 - (1 - 504B)^2$. Επομένως,

$$\Delta(\tau) = \frac{64\pi^{12}}{27}\left(12^3 \sum_{n=1}^{+\infty} \tau(n) e^{2\pi i n\tau}\right) = (2\pi)^{12} \sum_{n=1}^{+\infty} \tau(n) e^{2\pi i n\tau},$$

όπου $\tau(n) \in \mathbb{Z}$, για κάθε $n \in \mathbb{N}$. Ο συντελεστής του $q = e^{2\pi i\tau}$ είναι $12^2(5 + 7) = 12^3$, ήτοι $\tau(1) = 1$. Ομοίως, υπολογίζουμε και το $\tau(2)$. □

ΠΡΟΤΑΣΗ 4.5.4. *Εάν $\tau \in \mathcal{H}$, τότε ισχύει ότι*

$$\mathcal{J}(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{+\infty} c(n) e^{2\pi i n\tau},$$

όπου $c(n) \in \mathbb{Z}$ για κάθε $n \in \mathbb{N}$.

Απόδειξη. Κάνουμε τη σύμβαση να συμβολίζουμε ως I κάθε δυναμοσειρά του q με ακέραιους συντελεστές. Έτσι, εάν $q := e^{2\pi i\tau}$, έχουμε ότι

$$g_2{}^3(\tau) = \frac{64\pi^{12}}{27}(1 + 240q + I)^3 = \frac{64\pi^{12}}{27}(1 + 720q + I)^3$$

$$\Delta(\tau) = \frac{64\pi^{12}}{27}\big(12^3 q(1 - 24q + I)\big).$$

Επομένως, έχουμε ότι

$$\mathcal{J}(\tau) = 12^3 \cdot \frac{g_2{}^3(\tau)}{\Delta(\tau)} = 12^3 \frac{1 + 720q + I}{12^3 q(1 - 24q + I)} = \frac{1}{q}(1 + 720q + I)(1 + 24q + I).$$

Άρα

$$\mathcal{J}(\tau) = \frac{1 + 744q + I}{q}.$$

Έτσι, αποδείξαμε το ζητούμενο. □

4.6 Η modular ομάδα Γ και η θεμελιώδης περιοχή R_Γ

Στην προηγούμενη παράγραφο ασχοληθήκαμε με τους unimodular μετασχηματισμούς. Τώρα πρόκειται να εμβαθύνουμε σε αυτούς και να τους χρησιμοποιήσουμε για τον ορισμό και τη μελέτη της modular ομάδας.

Αρχικά, θεωρούμε το unimodular μετασχηματισμό

$$\varphi(z) = \frac{az + b}{cz + d}.$$

Οι αριθμοί a, b, c και d είναι τυχόντες μιγαδικοί αριθμοί. Επιθυμούμε να μελετήσουμε τη συνάρτηση αυτή. Παρατηρούμε ότι η δοθείσα συνάρτηση δεν ορίζεται για $z = -d/c$ και για $z = \infty$. Για το λόγο αυτό, θέτουμε

$$\varphi\left(\frac{-d}{c}\right) = \infty \text{ και } \varphi(\infty) = \frac{a}{c}.$$

Με άλλα λόγια, θεωρούμε τον unimodular μετασχηματισμό φ ως συνάρτηση επί του $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. Έτσι, έχουμε καταφέρει να ορίσουμε τη φ σε ολόκληρη τη σφαίρα του Riemann. Ακόμα, παρατηρούμε ότι

$$\varphi(z) - \varphi(w) = \frac{(ad-bc)(w-z)}{(cw+d)(cz+d)},$$

άρα η φ είναι σταθερή συνάρτηση εάν ισχύει ότι $ad - bc = 0$. Συνεπώς για να αποφύγουμε εκφυλισμένες περιπτώσεις όταν κάνουμε λόγο για unimodular μετασχηματισμούς, θα λαμβάνουμε πάντα ως δεδομένο ότι $ad - bc \neq 0$. Η φ, λοιπόν, είναι μία συνάρτηση αναλυτική παντού στο $\mathbb{C}^*$, εκτός από το σημείο $z = -d/b$ που εμφανίζει απλό πόλο. Από τη μιγαδική μας ανάλυση γνωρίζουμε ότι η φ, αφού είναι ένας μετασχηματισμός Möbius, απεικονίζει κύκλους σε κύκλους,[5], ήτοι η εικόνα ενός κύκλου μέσω της φ είναι ένας κύκλος. Είναι εύκολο να διαπιστώσουμε ότι εάν πολλαπλασιάσουμε καθένα από τους αριθμούς a, b, c και d με μία μη μηδενική σταθερά η φ θα παραμείνει αμετάβλητη. Για το λόγο αυτό μπορούμε χ.β.τ.γ. να υποθέσουμε ότι για τη φ όπως ορίστηκε, ισχύει ότι $ad-bc = 1$.

Έτσι, μπορούμε να ταυτίσουμε κάθε unimodular μετασχηματισμό

$$\varphi(z) = \frac{az+b}{cz+d}$$

με έναν 2×2 πίνακα

$$A := A_\varphi := \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

για τον οποίο ισχύει $\det A = 1$, αφού έχουμε υποθέσει ότι $ad - bc = 1$. Με άλλα λόγια, έχουμε ότι $A \in SL_2(\mathbb{C})$. Η σύνθεση $\varphi \circ \psi$ δύο unimodular μετασχηματισμών φ και ψ είναι επίσης ένας unimodular μετασχηματισμός και μάλιστα, για τους αντίστοιχους πίνακες ισχύει η σχέση

$$A_{\varphi\circ\psi} = A_\varphi \cdot A_\psi.$$

Μάλιστα, ο ταυτοτικός πίνακας $I_2 \in SL_2(\mathbb{C})$ αντιστοιχεί στο unimodular μετασχηματισμό $id(z) = z$, ήτοι στον ταυτοτικό unimodular μετασχηματισμό. Μπορούμε, επομένως, δοθέντος unimodular μετασχηματιμού φ, να βρούμε έναν unimodular μετασχηματισμό ψ τέτοιο, ώστε

$$\varphi \circ \psi = id.$$

Σε επίπεδο πινάκων η σχέση αυτή γράφεται ως εξής:

$$A_\varphi \cdot A_\psi = I_2.$$

Άρα διαπιστώνουμε ότι ισχύει η σχέση

$$A_{\varphi^{-1}} = {A_\varphi}^{-1}.$$

Τελικά, συμπεραίνουμε ότι το σύνολο των πινάκων που αντιστοιχούν σε κάποιο unimodular μετασχηματισμό, με πράξη τον πολλαπλασιασμό πινάκων, αποτελούν ομάδα. Κατά συνέπεια το αυτό θα ισχύει και για τους unimodular μετασχηματισμούς.

Είναι σαφές ότι εάν κάνουμε λόγο για unimodular μετασχηματισμούς, ότι ειπώθηκε ανωτέρω εξακολουθεί να έχει ισχύ, ήτοι οι unimodular μετασχηματισμούς με πράξη τη σύνθεση απεικονίσεων δημιουργούν ομάδα.

ΟΡΙΣΜΟΣ 4.6.1. Θεωρούμε το σύνολο

$$\mathbf{\Gamma} := \left\{ \frac{a\tau+b}{c\tau+d} \ : \ \tau \in \mathcal{H} \text{ και } a,b,c,d \in \mathbb{Z} \text{ , με } ad-bc = 1 \right\}.$$

Όπως έχουμε ήδη αναφέρει αυτό αποτελεί ομάδα με πράξη τη σύνθεση απεικονίσεων. Η ομάδα αυτή καλείται *modular ομάδα* και είναι ισόμορφη, σύμφωνα με όλα τα παραπάνω, με την ομάδα $\mathbb{P}SL_2(\mathbb{Z})$.

[5]Για να είμαστε ακριβείς, κάθε μετασχηματισμός Möbius απεικονίζει ευθεία ή κύκλο σε ευθεία ή κύκλο. Απλά θεωρούμε την ευθεία ως έναν εκφυλισμένο κύκλο, μιας και το σώμα στο οποίο εργαζόμαστε είναι το $\mathbb{C}$.

Ορίσαμε την modular ομάδα ως ένα σύνολο κάποιων μετασχηματισμών στοιχείων του $\mathcal{H}$. Σε επίπεδο θεωρίας ομάδων αυτό σημαίνει ότι η modular ομάδα ουσιαστικά πρόκειται για δράση της ομάδας $SL_2(\mathbb{Z})$ στο σύνολο $\mathcal{H}$. Η παρατήρηση αυτή μας βοηθάει στην απόδειξη του παρακάτω θεωρήματος, που προσδιορίζει πλήρως τους γεννήτορες της **Γ**.

ΘΕΩΡΗΜΑ 4.6.2. *Ισχύει ότι*

$$\mathbf{\Gamma} = \langle t(\tau), s(\tau) \rangle,$$

όπου

$$t(\tau) = \tau + 1 \ \textit{και} \ \ s(\tau) = -\frac{1}{\tau}.$$

Απόδειξη. Συμβολίζουμε ως G την ομάδα που παράγεται από τους πίνακες

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \ \text{και} \ T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

ήτοι

$$G = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle.$$

Οι πίνακες S και T αντιστοιχούν στους unimodular μετασχηματισμούς $s(\tau)$ και $t(\tau)$ αντίστοιχα. Επομένως είναι αρκετό να δείξουμε ότι $G = SL_2(\mathbb{Z})$. Αρχικά, παρατηρούμε ότι εάν επιλέξουμε τυχόν στοιχείο A της $SL_2(\mathbb{Z})$, τότε έχουμε

$$S \cdot A = S \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

και

$$T^n \cdot A = T^n \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + nc & b + nd \\ c & d \end{pmatrix},$$

για οποιοδήποτε $n \in \mathbb{Z}$. Υποθέτουμε ότι $c \neq 0$. Εάν ισχύει ότι $|a| \geq |c|$, τότε από την ευκλείδια διαίρεση μπορούμε $q, r \in \mathbb{Z}$ τέτοιους ώστε να ισχύει ότι

$$a = cq + r \ \text{, με } 1 \leq r < |c|.$$

Τότε

$$T^{-q} \cdot A = \begin{pmatrix} * & a - qc \\ * & * \end{pmatrix}.$$

Επομένως το πάνω αριστερά στοιχείο του πίνακα $T^{-q}A$ είναι κατ' απόλυτη τιμή μικρότερο από το κάτω αριστερά στοιχείο του A, δηλαδή το c. Πολλαπλασιάζουμε εξ αριστερών με τον πίνακα S και έτσι έχουμε εναλλαγή των σειρών του πίνακα $T^{-q}A$ και αλλαγή προσήμου στην πρώτη σειρά. Κοιτάζουμε ξανά την τιμή στο κάτω αριστερά στοιχείο του πίνακα $ST^{-q}A$. Συνεχίζουμε τη διαδικασία αυτή, ήτοι το διαδοχικό πολλαπλασιασμό εξ αριστερών του A με δυνάμεις του T και το S, και αναπόφευκτα σε κάποιο βήμα καταλήγουμε σε ένα πίνακα με το κάτω αριστερά στοιχείο να είναι ίσο με 0. Κι εφόσον ο πίνακας αυτός έχει ακέραια στοιχεία και διακρίνουσα ίση με 1, θα είναι κατ' ανάγκη της μορφής

$$\pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix},$$

για κάποιο $m \in \mathbb{Z}$. Όμως ο πίνακας αυτός είναι ο $\pm T^{\pm m}$ [6], γεγονός που ολοκληρώνει την απόδειξη μας □

Η απόδειξη του παραπάνω θεωρήματος είναι καθαρά αλγοριθμική. Υπάρχει απόδειξη η οποία βασίζεται μόνο στη γεωμετρική έννοια της modular ομάδας, αλλά δε θα επεκταθούμε σε αυτή καθώς είναι εκτενέστερη.

[6] Έχουμε την ίδια επιλογή προσήμου για τη δύναμη του T και για τον εκθέτη.

Πορισμα 4.6.3. *Κάθε στοιχείο της ομάδας* $\mathbf{\Gamma}$ *γράφεται υπό τη μορφή*

$$t^{n_1}st^{n_2}s\cdots t^{n_k-1}st^{n_k},$$

όπου $k\in\mathbb{N}$ *και* $n_i\in\mathbb{Z}$*, για κάθε* $i=1,2,\ldots,k$*.*

Από αυτό το σημείο θα υιοθετήσουμε το συμβολισμό

$$A\tau=\frac{a\tau+b}{c\tau+d},$$

όπου

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z}).$$

Ο συμβολισμός αυτός ουσιαστικά εκφράζει τον πολλαπλασιασμό εξ αριστερών με τον πίνακα A, πράξη η οποία αποτελεί και τη δράση της ομάδας $SL_2(\mathbb{Z})$ στο σύνολο $\mathcal{H}$. Θεωρούμε μία υποομάδα G της $\mathbf{\Gamma}$. Δύο σημεία $\tau,\tau'\in\mathcal{H}$ λέγονται *ισοδύναμα* εάν υπάρχει $A\in G$ με την ιδιότητα $\tau'=A\tau$. Εύκολα μπορούμε να διαπιστώσουμε ότι η εν λόγω ισοδυναμία σημείων είναι σχέση ισοδυναμίας. Αυτό σημαίνει ότι το άνω ημιεπίπεδο $\mathcal{H}$ γράφεται ως ξένη ένωση κλάσεων ισοδυναμίας, τις οποίες θα ονομάζουμε *τροχιές*[7]. Κάθε τροχιά είναι της μορφής $G\tau$, ήτοι περιέχει μιγαδικούς αριθμούς της μορφής $A\tau$ για κάποιο πίνακα $A\in G$. Επιλέγουμε, τώρα, ένα σημείο από κάθε τροχιά. Η ένωση αυτών καλείται *θεμελιώδες σύνολο της* G. Όμως εμείς θα επιθυμούσαμε το εν λόγω θεμελιώδες σύνολο να έχει κάποιες καλές τοπολογικές ιδιότητες. Προς τούτο τροποποιούμε ελαχίστως την ιδέα του θεμελιώδους συνόλου και δίνουμε τον κατωτέρω ορισμό:

Ορισμος 4.6.4. Έστω G μία υποομάδα της της modular ομάδας $\mathbf{\Gamma}$. Ένα ανοιχτό υποσύνολο R_G του $\mathcal{H}$ καλείται *θεμελιώδης περιοχή της* G εάν έχει τις εξής δύο ιδιότητες

(i) Εάν δύο σημεία της R_G είναι ισοδύναμα τότε κατ' ανάγκη ταυτίζονται.

(ii) Εάν $\tau\in\mathcal{H}$, τότε υπάρχει ένα σημείο τ' στην κλειστότητα του R_G τέτοιο ώστε τα τ και τ' να είναι ισοδύναμα.

Επί τη βάσει αυτού του ορισμού επιθυμούμε να προσδιορίσουμε τη θεμελιώδη περιοχή ολόκληρης της ομάδας $\mathbf{\Gamma}$. Χωρίς απόδειξη αναφέρουμε τα παρακάτω λήμματα:

Λημμα 4.6.5. *Δοθέντων μιγαδικών αριθμών* ω_1' *και* ω_2' *με* $\omega_2'/\omega_1'\in\mathbb{C}\setminus\mathbb{R}$*, υπάρχει πάντα ένα θεμελιώδες ζεύγος περιόδων* (ω_1,ω_2) *ισοδύναμο προς το* $(\omega_1'\omega_2')$ *για το οποίο ισχύει ότι*

$$\begin{pmatrix}\omega_2\\ \omega_1\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\omega_2'\\ \omega_1'\end{pmatrix},$$

με $ad-bc=1$*, και επιπλέον*

$$|\omega_2|\geq|\omega_1|\ ,\ |\omega_1+\omega_2|\geq|\omega_2|\ ,\ |\omega_1-\omega_2|\geq|\omega_2|.$$

Απόδειξη. (βλ. [3], σελ.31, Λήμ.1) □

Λημμα 4.6.6. *Εάν* $\tau'\in\mathcal{H}$*, τότε υπάρχει ένας μιγαδικός αριθμός* $\tau\in\mathcal{H}$ *ισοδύναμος προς τον* τ' *με τις ιδιότητες*

$$|\tau|\geq 1\ ,\ |\tau+1|\geq|\tau|\ ,\ |\tau-1|\geq|\tau|.$$

Απόδειξη. (βλ. [3], σελ.32, Θεώρ.2.2.) □

[7]Η ορολογία "τροχιές" συμφωνεί με την ομαδοθεωρητική της έννοια.

ΘΕΩΡΗΜΑ 4.6.7. *Το ανοιχτό σύνολο*

$$R_{\mathbf{\Gamma}} = \{\tau \in \mathcal{H} \, : \, |\tau| > 1 \, , \, |\tau + \overline{\tau}| < 1\}$$

είναι μία θεμελιώδης περιοχή της ομάδας $\mathbf{\Gamma}$. *Επιπροσθέτως, εάν* $A \in \mathbf{\Gamma}$ *και ισχύει ότι* $A\tau = \tau$, *για κάποιο* $\tau \in R_{\mathbf{\Gamma}}$, *τότε κατ'ανάγκη θα έχουμε ότι* $A = I_2$. *Με άλλα λόγια, μόνο το ταυτοτικό στοιχείο της* $\mathbf{\Gamma}$ *αφήνει αναλλοίωτα τα σημεία της* $R_{\mathbf{\Gamma}}$.

Απόδειξη. Από το λήμμα 4.6.6 εφαρμοσμένο για την ίδια την ομάδα $\mathbf{\Gamma}$, έχουμε ότι για τυχόν $\tau' \in \mathcal{H}$ υπάρχει τ στην κλειστότητα της θεμελιώδους περιοχής $R_{\mathbf{\Gamma}}$ ώστε τα τ και τ' να είναι ισοδύναμα. Υποθέτουμε, λοιπόν, ότι

$$\tau' = A\tau,$$

όπου

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Ύστερα από απλές πράξεις έπεται ότι

$$Im(\tau') = \frac{Im(\tau)}{|c\tau + d|^2}.$$

Εάν υποθέσουμε ότι $\tau \in R_{\mathbf{\Gamma}}$ και $c \neq 0$, έχουμε ότι

$$|c\tau + d|^2 = c^2\tau\overline{\tau} + cd(\tau + \overline{\tau}) + d^2 > c^2 - |cd| + d^2.$$

Αν $d = 0$, παρατηρούμε ότι $|c\tau + d|^2 \geq c^2 \geq 1$. Εάν ισχύει ότι $d \neq 0$, τότε έχουμε

$$c^2 - |cd| + d^2 = (|c| - |d|)^2 + |cd| \geq |cd| \geq 1,$$

οπότε και πάλι ισχύει ότι $|c\tau + d|^2 > 1$. Αυτό σημαίνει ότι εάν $\tau \in R_{\mathbf{\Gamma}}$ και $c \neq 0$ τότε ισχύει ότι $Im(\tau') < Im(\tau)$. Με άλλα λόγια, κάθε στοιχείο $A\tau \in \mathbf{\Gamma}$ με $c \neq 0$ μειώνει το φανταστικό μέρος του τ, όταν αυτό ανήκει στην $R_{\mathbf{\Gamma}}$. Γνωρίζουμε, όμως, ότι

$$\tau' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau \Rightarrow \tau = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \tau'.$$

Εάν υποθέσουμε ότι $c \neq 0$, τότε η σχέση

$$\tau' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau,$$

μας πληροφορεί ότι $Im(\tau') < Im(\tau)$, ενώ η σχέση

$$\tau = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \tau'$$

ότι $Im(\tau) < Im(\tau')$. Αυτό σημαίνει ότι $c = 0$. Τότε, όμως, ισχύει ότι $ad = 1$ και $a, d \in \mathbb{Z}$. Κατά συνέπεια θα έχουμε ότι $a = d = \pm 1$. Άρα

$$A = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix} = T^{\pm b}.$$

Επομένως θα έχουμε ότι $\tau' = \tau \pm b$. Έχουμε υποθέσει ότι $\tau \in R_{\mathbf{\Gamma}}$. Αν υποθέσουμε και ότι $\tau' \in R_{\mathbf{\Gamma}}$, τότε παρατηρούμε ότι από την ανισότητα $|\tau + \overline{\tau}| < 1$, λαμβάνουμε ότι η οριζόντια απόσταση δύο σημείων της $R_{\mathbf{\Gamma}}$ είναι < 1. Όμως

$$\tau' = \tau \pm b \Rightarrow Re(\tau') = Re(\tau) \pm b \Rightarrow |b| = |Re(\tau') - Re(\tau)| < 1 \Rightarrow b = 0.$$

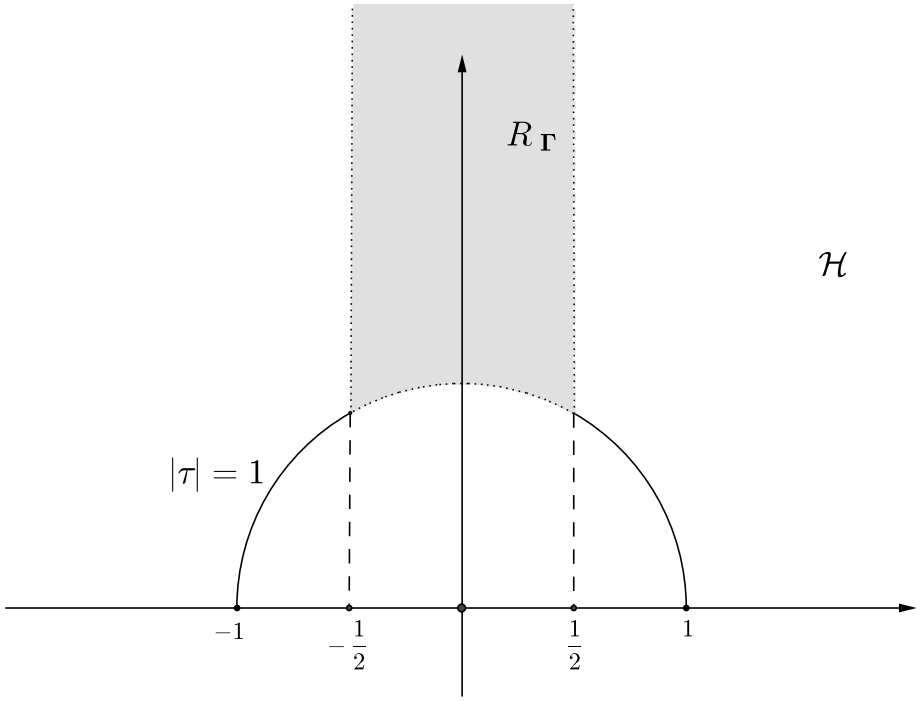
Άρα $A = \pm I_2 \Rightarrow \tau = \tau'$. Αποδείξαμε, λοιπόν, ότι δύο διακεκριμένα σημεία της $R_{\mathbf{\Gamma}}$ είναι αδύνατο να είναι ισοδύναμα.

Το ανωτέρω επιχείρημα μας υποδεικνύει ότι εάν υποθέσουμε τη σχέση $A\tau = \tau$, όπου ξανά

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

τότε $c = 0$. Συνεπώς, θα έχουμε $a = d = \pm 1$, ήτοι $A = \pm I_2$. Έτσι, δείχνουμε ότι μονάχα ο ταυτοτικός unimodular μετασχηματισμός διατηρεί τα σημεία της $R_{\mathbf{\Gamma}}$. □

Μια εικόνα της θεμελιώδους περιοχής $R_{\mathbf{\Gamma}}$ της modular ομάδας $\mathbf{\Gamma}$ φαίνεται στο σχήμα που ακολουθεί.



Η θεμελιώδης περιοχή είναι το γραμμοσκιασμένο χωρίο. Πρέπει να προσέξουμε ότι εξ ορισμού της, η θεμελιώδης περιοχή είναι ανοιχτό σύνολο, επομένως το σύνορο δε λογίζεται σε αυτή. Γι΄αυτό και στο ανωτέρω σχήμα έχουμε διακεκομμένη γραμμή στο σύνορο.

4.7 Modular συναρτήσεις

ΟΡΙΣΜΟΣ 4.7.1. Μία μιγαδική συνάρτηση f ονομάζεται *modular* εάν ικανοποιεί τις παρακάτω τρεις συνθήκες:

(i) Η f είναι μερόμορφη στο $\mathcal{H}$.

(ii) Ισχύει ότι $f(A\tau) = f(\tau)$, για κάθε στοιχείο A της ομάδας $SL_2(\mathbb{Z})$.

(iii) Το ανάπτυγμα Fourier της f έχει τη μορφή

$$f(\tau) = \sum_{k=-m}^{+\infty} a(k) e^{2\pi i k \tau}.$$

Η πρώτη ιδιότητα των modular συναρτήσεων ουσιαστικά μας πληροφορεί ότι είναι αναλυτικές συναρτήσεις στο $\mathcal{H}$, εκτός από κάποιους πόλους που εμφανίζουν. Από τη δεύτερη ιδιότητα συνεπάγεται ότι οι modular συναρτήσεις παραμένουν αναλλοίωτες από τη δράση των μετασχηματισμών της $\mathbf{\Gamma}$. Τέλος, η μορφή της σειράς Fourier της f μας δίνει πληροφορία για το σημείο $\tau = i\infty$. Προφανώς, εάν θέσουμε $x := e^{2\pi i\tau}$, τότε λαμβάνουμε το ανάπτυγμα Laurent της f ως προς το x. Τότε μπορούμε να αποφανθούμε για τη συμπεριφορά της f στο σημείο $\tau = i\infty$ μελετώντας το ανάπτυγμα Laurent γύρω από το 0. Από τη μιγαδική ανάλυση γνωρίζουμε ότι εάν $m > 0$, τότε η συνάρτηση f παρουσιάζει πόλο, ενώ εάν $m \geq 0$, τότε η συνάρτηση είναι αναλυτική στο $\tau = i\infty$. Άρα η ιδιότητα (iii) του ορισμού ισοδυναμεί με το ότι μια modular συνάρτηση, στη χειρότερη των περιπτώσεων, μπορεί να έχει πόλο τάξης m στη θέση $z = i\infty$.

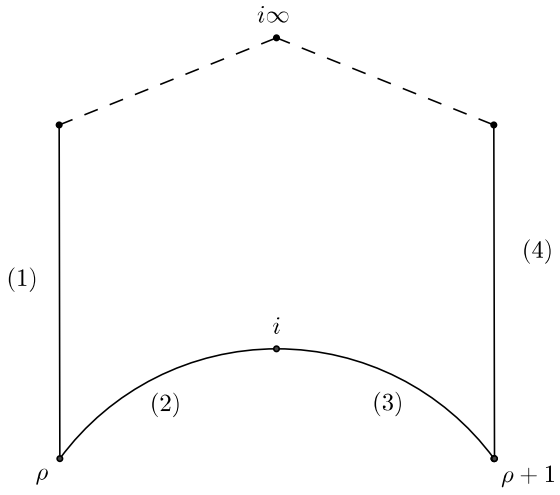
Γνωρίζουμε ήδη μια modular συνάρτηση. Αυτή είναι η $\mathcal{J}$-αναλλοίωτος, η οποία παρουσιάζει στο $\tau = i\infty$ απλό πόλο, ήτοι πόλο τάξης 1. Μάλιστα, θα τη χρησιμοποιήσουμε για να δείξουμε ότι κάθε modular συνάρτηση εκφράζεται ως ρητή συνάρτηση της $\mathcal{J}$.

Ακολουθεί ένα θεώρημα με το οποίο κατ' ουσία βρίσκουμε το πλήθος των πόλων και των σημείων μηδενισμού κάποιας μη μηδενικής modular συνάρτησης f. Λόγω της έκτασης της απόδειξης θα την παραλείψουμε. Παρ' όλα αυτά θα κάνουμε κάποια σχόλια πάνω στι θεώρημα αυτό.

Θεωρημα 4.7.2. *Θεωρούμε μία μη μηδενική modular συνάρτηση f. Τότε στην κλειστότητα της θεμελιώδους περιοχής $R_{\mathbf{\Gamma}}$ το πλήθος των σημείων μηδενισμού της f ισούται με το πλήθος των πόλων αυτής.*

Απόδειξη. (βλ. [3], σελ.34, Θεώρ. 2.4.) □

Για να έχει ισχύ το παραπάνω θεώρημα θα πρέπει να κάνουμε κάποιες συμβάσεις για το σύνορο της θεμελιώδους περιοχής. Θεωρούμε, λοιπόν, το σύνορο όπως φαίνεται στο ακόλουθο σχήμα.



Οι πλευρές (1) και (4), ενώ στην πραγματικότητα είναι παράλληλες, θεωρούμε ότι τέμνονται στο σημείο $\tau = i\infty$[8]. Ακόμα, χωρίζουμε το τόξο του κύκλου σε δυο ίσα μέρη και θεωρούμε ως διαφορετική πλευρά το καθένα. Το ρ είναι συγκεκριμένο και ισούται με $e^{2\pi i/3}$. Ο τρόπος με τον οποίο έγινε διαχωρισμός του συνόρου σε πλευρές βασίζεται στο ότι ανά ζεύγη οι πλευρές είναι ισοδύναμες, υπό την έννοια ότι κάθε σημείο της πλευράς (1) έχει ισοδύναμο στην πλευρά (4) και κάθε σημείο στο τόξο (2) έχει ισοδύναμο προς το τόξο (3). Επομένως, εάν κάποιο σημείο της πλευράς (2) είναι σημείο μηδενισμού της f ή πόλος, τότε και το ισοδύναμο αυτού θα είναι σημείο μηδενισμού ή πόλος.

[8]Ουσιαστικά, εξετάζουμε το σχήμα ως αντικείμενο της υπερβολικής γεωμετρίας.

ΠΟΡΙΣΜΑ 4.7.3. *Θεωρούμε μία μη τετριμμένη modular συνάρτηση f. Τότε γι' αυτήν ισχύει ότι*

$$ord_{i\infty}(f) + \frac{1}{3}ord_{\rho}(f) + \frac{1}{2}ord_{i}(f) + \sum_{z\neq i,\rho,i\infty} ord_z(f) = 0,$$

όπου $\rho := e^{2\pi i/3}$.

Απόδειξη. (βλ. [15], σελ.279, Πρ. 9.16) □

ΠΟΡΙΣΜΑ 4.7.4. *Εάν η f είναι μία μη σταθερή modular συνάρτηση, τότε για κάθε $z \in \mathbb{C}$ η συνάρτηση $f - z$ έχει το ίδιο πλήθος πόλων και σημείων μηδενισμού στην κλειστότητα του $R_{\mathbf{\Gamma}}$.*

ΠΟΡΙΣΜΑ 4.7.5. *Εάν η f είναι modular συνάρτηση και φραγμένη στο $\mathcal{H}$, τότε είναι σταθερή.*

Το τελευταίο θεώρημα αυτής της παραγράφου ουσιαστικά προσδιορίζει τη μορφή όλων των modular συναρτήσεων. Πρωτού, όμως, περάσουμε στο θεώρημα χρειάζεται να υπολογίσουμε την τιμή της συνάρτησης του Klein σε κάποια σημείο. Έτσι, έχουμε την παρακάτω πρόταση:

ΠΡΟΤΑΣΗ 4.7.6. *Η $\mathcal{J}$-αναλλοίωτος λαμβάνει κάθε τιμή ακριβώς μία φορά στην κλειστότητα της θεμελιώδους περιοχής $R_{\mathbf{\Gamma}}$. Ιδιαίτερα, στις κορυφές ισχύει ότι*

$$\mathcal{J}(\rho) = 0 \ , \ \mathcal{J}(i) = 1728 \ , \ \mathcal{J}(i\infty) = \infty.$$

Στο σημείο $\tau = i\infty$ έχουμε πόλο τάξης 1. Στο $\tau = \rho$ έχουμε σημείο μηδενισμού τάξης 3 και η συνάρτηση $\mathcal{J}(\tau) - 1728$ έχει διπλό σημείο μηδενισμού το $\tau = i$.

Απόδειξη. Αρχικά θα δείξουμε ότι η $\mathcal{J}$-αναλλοίωτος λαμβάνει όλες τις τιμές στην κλειστότητα της περιοχής $R_{\mathbf{\Gamma}}$, ήτοι ότι για κάθε μιγαδικό αριθμό $z \in \mathbb{C}$ υπάρχει $\tau_0 \in R_{\mathbf{\Gamma}} \cup \partial R_{\mathbf{\Gamma}}$ με την ιδιότητα $\mathcal{J}(\tau_0) = z$. Υποθέτουμε ότι αυτό δεν ισχύει, ήτοι υπάρχει κάποιος μιγαδικός αριθμός $z \in \mathbb{C}$ για τον οποίο ισχύει ότι

$$\mathcal{J}(\tau) \neq z \, , \forall \tau \in R_{\mathbf{\Gamma}} \cup \partial R_{\mathbf{\Gamma}}.$$

Θεωρούμε τη συνάρτηση $f(\tau) := J(\tau) - z$. Εφόσον η $\mathcal{J}$ έχει ένα τουλάχιστον πόλο τάξης 1 στο σημείο $\tau = i\infty$, βάσει του πορίσματος 4.7.4 η f θα έχει και ένα τουλάχιστον σημείο μηδενισμού στην κλειστότητα της περιοχής $R_{\mathbf{\Gamma}}$. Αυτό, όμως, αντίκειται στην υπόθεση

$$\mathcal{J}(\tau) \neq z \, , \forall \tau \in R_{\mathbf{\Gamma}} \cup \partial R_{\mathbf{\Gamma}},$$

το οποίο είναι άτοπο. Ακόμα, για ένα μιγαδικό αριθμό $z \in \mathbb{C}$, υποθέτουμε ότι υπάρχουν δύο μιγαδικοί τ_1 και τ_2 που ανήκουν στην κλειστότητα της $R_{\mathbf{\Gamma}}$ τέτοιοι, ώστε $\mathcal{J}(\tau_1) = z = \mathcal{J}(\tau_2)$. Τότε, αν θεωρήσουμε ξανά τη συνάρτηση $f(\tau) := \mathcal{J}(\tau) - z$, αυτή έχει ως σημεία μηδενισμού της τα τ_1 και τ_2. Σύμφωνα με το πόρισμα 4.7.4 αυτό σημαίνει ότι στην κλειστότητα της $R_{\mathbf{\Gamma}}$ η f έχει είτε δύο απλούς πόλους, είτε ένα διπλό. Αυτό όμως είναι άτοπο, μιας και γνωρίζουμε ότι η $\mathcal{J}$ έχει ένα απλό πόλο στη θέση $\tau = i\infty$. Θα δείξουμε, τώρα, ότι

$$\mathcal{J}(\rho) = 0 \ , \ \mathcal{J}(i) = 1728 \ , \ \mathcal{J}(i\infty) = \infty.$$

Επαληθεύουμε ότι $g_2(\rho) = 0 = g_3(i)$. Εφόσον $\rho = e^{2\pi i/3} \Rightarrow \rho^3 = 1 \Rightarrow \rho^2 + \rho + 1 = 0$, έχουμε ότι

$$\begin{aligned}
\frac{1}{60}g_2(\rho) &= \sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(m+n\rho)^4} = \sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(m\rho^3+n\rho)^4} \\
&= \frac{1}{\rho^4} \sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(m\rho^2+n)^4} = \frac{1}{\rho} \sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(n-m-m\rho)^4} \\
&= \frac{1}{\rho} \sum_{(0,0)\neq(M,N)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(N+M\rho)^4} = \frac{1}{60\rho}g_2(\rho).
\end{aligned}$$

Άρα $g_2(\rho) = 0$. Όμοίως πράττουμε για το $g_3(i) = 0$. Επομένως εύκολα προκύπτει ότι

$$\mathcal{J}(\rho) = 12^3 \cdot \frac{{g_2}^3(\rho)}{\Delta(\rho)} = 0 \text{ και } \mathcal{J}(i) = 12^3 \cdot \frac{{g_2}^3(i)}{{g_2}^3(i)} = 1728.$$

Για να δούμε τι γίνεται στο σημείο $\tau = i\infty$, χρησιμοποιούμε το ανάπτυγμα Laurent της συνάρτησης $\mathcal{J}$. Έτσι, από την πρόταση 4.5.4, έχουμε ότι

$$\mathcal{J}(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{+\infty} c(n)e^{2\pi in\tau},$$

όπου οι συντελεστές $c(n)$ είναι ακέραιοι αριθμοί. Εάν θέσουμε $\tau = i\infty$, τότε παρατηρούμε ότι

$$e^{-2\pi i(i\infty)} = e^{2\pi\infty} = \infty$$

και

$$e^{2\pi i(i\infty)} = e^{-2\pi\infty} = 0.$$

Άρα

$$\mathcal{J}(i\infty) = \infty + 744 + \sum_{n=1}^{+\infty} c(n) \cdot 0 = \infty \Rightarrow \mathcal{J}(i\infty) = \infty.$$

Οι πολλαπλότητες και οι τάξεις υπολογίζονται από το θεώρημα 4.7.2. □

Θεωρημα 4.7.7. *Κάθε ρητή συνάρτηση της $\mathcal{J}$-αναλλοιώτου είναι modular συνάρτηση. Αντιστρόφως, κάθε modular συνάρτηση μπορεί να εκφραστεί ως ρητή συνάρτηση της $\mathcal{J}$-αναλλοιώτου. Με άλλα λόγια, το σώμα των modular συναρτήσεων είναι το $\mathbb{C}(\mathcal{J})$.*

Απόδειξη. Θεωρούμε τη συνάρτηση

$$f(\tau) = \frac{P(\mathcal{J}(\tau))}{Q(\mathcal{J}(\tau))},$$

όπου τα P και Q είναι πολυώνυμα μεταβλητής $\mathcal{J}(\tau)$. Εφόσον το $\mathbb{C}$ είναι σώμα αλγεβρικά κλειστό, μπορούμε να υποθέσουμε ότι

$$P(\mathcal{J}(\tau)) = \prod_{i=1}^{m} \big(\mathcal{J}(\tau) - \alpha_i\big) \text{ και } Q(\mathcal{J}(\tau)) = \prod_{j=1}^{n} \big(\mathcal{J}(\tau) - \beta_j\big).$$

όπου τα α_i και β_j είναι τα σημεία μηδενισμού των πολυωνύμων P και Q, αντιστοίχως. Έτσι, η συνάρτηση f γράφεται υπό τη μορφή

$$f(\tau) = \frac{\prod_{i=1}^{m} \big(\mathcal{J}(\tau) - \alpha_i\big)}{\prod_{j=1}^{n} \big(\mathcal{J}(\tau) - \beta_j\big)}.$$

Μάλιστα, επί τη βάσει του θεωρήματος 4.7.2, ισχύει ότι $m = n$, ήτοι

$$f(\tau) = \prod_{i=1}^{n} \frac{\mathcal{J}(\tau) - \alpha_i}{\mathcal{J}(\tau) - \beta_i}.$$

Έστω $z_1, z_2, \ldots, z_n$ τέτοια ώστε

$$\mathcal{J}(z_i) = \alpha_i \,, \forall\, i = 1, 2, \ldots, n$$

και $p_1, p_2, \ldots, p_n$ σημεία τέτοια, ώστε

$$\mathcal{J}(p_i) = \beta_i \, , \forall \, i = 1, 2, \ldots, n.$$

Τότε τα $p_1, p_2, \ldots, p_n$ αποτελούν πόλους της f, ήτοι η f είναι μερόμορφη συνάρτηση. Ακόμα, εφόσον η $\mathcal{J}$-αναλλοίωτος είναι modular συνάρτηση, για αυτήν ισχύει ότι

$$\mathcal{J}(\tau) = \mathcal{J}(A\tau) \, , \forall \, A \in SL_2(\mathbb{Z}).$$

Κατά συνέπεια,

$$f(A\tau) = \prod_{i=1}^{n} \frac{\mathcal{J}(A\tau) - \alpha_i}{\mathcal{J}(A\tau) - \beta_i} = \prod_{i=1}^{n} \frac{\mathcal{J}(\tau) - \alpha_i}{\mathcal{J}(\tau) - \beta_i} = f(\tau) \, , \forall \, A \in SL_2(\mathbb{Z}).$$

Τέλος, τα σημεία $p_1, p_2, \ldots, p_n$ αποτελούν πόλους πεπερασμένης τάξης, μιας και είναι απλά σημεία μηδενισμού του πολυωνύμου $Q(\mathcal{J}(\tau))$. Από όλα τα παραπάνω έπεται ότι η f είναι modular συνάρτηση.
Σε ότι αφορά στο δεύτερο σκέλος, θωρούμε μία modular συνάρτηση g. Υποθέτουμε ότι τα $z_1, z_2, \ldots, z_n$ είναι σημεία μηδενισμού αυτής και τα $p_1, p_2, \ldots, p_n$ είναι πόλοι αυτής. Θεωρούμε τη συνάρτηση

$$h(\tau) := \prod_{k=1}^{n} \frac{\mathcal{J}(\tau) - \mathcal{J}(z_k)}{\mathcal{J}(\tau) - \mathcal{J}(p_k)},$$

αντικαθιστώντας την τιμή της $\mathcal{J}$ με 1, όταν $p_k = \infty$ ή $z_k = \infty$ σύμφωνα με την πρόταση 4.7.6. Τότε η συνάρτηση h, η οποία είναι modular συνάρτηση βάσει του πρώτου σκέλους του θεωρήματος, έχει τους ίδιους πόλους και τα ίδια σημεία μηδενισμού με την g. Αυτό σημαίνει ότι η συνάρτηση g/h δεν έχει πόλους ή σημεία μηδενισμού. Άρα η g/h είναι αναλυτική συνάρτηση και συνεπώς σταθερή από το θεώρημα Liouville. Επομένως το ζητούμενο δείχθηκε! □

Κεφάλαιο 5

Ελλειπτικές Καμπύλες και Μιγαδικός Πολλαπλασιασμός

5.1 Εισαγωγικά στοιχεία

Αρχικά υποθέτουμε ένα σώμα στο οποίο θα ορίσουμε τις ελλειπτικές μας καμπύλες και γενικά θα δομήσουμε τα αποτελέσματα μας. Επιλέγουμε το σώμα αυτό να είναι το $\mathbb{C}$. Η επιλογή του σώματος των μιγαδικών αριθμών είναι αρκετά βολική καθώς πρόκειται για αλγεβρικά κλειστό σώμα χαρακτηριστικής μηδέν. Εκτός αυτού, θα δούμε ότι στο $\mathbb{C}$ τα αποτελέσματα σχετίζονται με όσα έχουμε ήδη ασχοληθεί.

Όταν κάνουμε χρήση του συμβόλου $\mathbb{A}^2_{\mathbb{C}}$ εννοούμε το καρτεσιανό γινόμενο του $\mathbb{C}$ με τον εαυτό του. Με άλλα λόγια, το $\mathbb{A}^2_{\mathbb{C}}$ είναι το σύνολο όλων των ζευγών με συντεταγμένες από το $\mathbb{C}$. Το $\mathbb{A}^2_{\mathbb{C}}$ ονομάζεται *δισδιάστατος συσχετικός (ή αφφινικός) χώρος υπεράνω του σώματος* $\mathbb{C}$, ή πιο απλά *συσχετικό επίπεδο*. Αναλόγως ορίζουμε το *συσχετικό χώρο* $\mathbb{A}^3_{\mathbb{C}}$ και γενικότερα τον n-διάστατο συσχετικό χώρο $\mathbb{A}^n_{\mathbb{C}}$.

Εάν θεωρήσουμε ένα πολυώνυμο $F \in \mathbb{C}[X, Y]$, τότε αυτό ορίζει ένα σύνολο που αποτελείται από όλα τα σημεία μηδενισμού αυτού, τα ανήκοντα στον $\mathbb{A}^2_{\mathbb{C}}$. Το σύνολο αυτό, ήτοι το

$$\mathbf{V}(F) := \{(x, y) \in \mathbb{A}^2_{\mathbb{C}} \mid F(x, y) = 0\},$$

αποτελεί ουσιαστικά μία *καμπύλη* εντός του $\mathbb{A}^2_{\mathbb{C}}$. Όταν δε, συμβεί το πολυώνυμο F να είναι βαθμού 3, τότε η καμπύλη ονομάζεται *συσχετική κυβική καμπύλη*.

Για τη μελέτη μας, αλλά και για πολλά θέματα των μαθηματικών, είναι ανάγκη η εισαγωγή της έννοιας του προβολικού χώρου. Γενικά, δοθέντος τυχόντος σώματος μπορούμε πάντα να ορίσουμε τον προβολικό χώρο διάστασης n, όπου $n \in \mathbb{N}$. Εδώ, εφόσον κάνουμε λόγο για επίπεδο, θα επιμείνουμε στον ορισμό του *προβολικού επιπέδου υπεράνω του σώματος* $\mathbb{C}$, ή πιο απλά *μιγαδικό προβολικό επίπεδο*. Προς τούτο, για δύο σημεία (x_1, y_1, z_2) και (x_2, y_2, z_2) του $\mathbb{C}^3$ ορίζουμε τη σχέση

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) :\Leftrightarrow \exists \lambda \in \mathbb{C}^\times : x_1 = \lambda x_2 \, , \, y_1 = \lambda y_2 \text{ και } z_1 = \lambda z_2.$$

Αυτή προφανώς είναι μία σχέση ισοδυναμίας. Καθεμία από τις κλάσεις ισοδυναμίας που ορίζει η $\sim$ συμβολίζεται ως $[x : y : z]$. Με άλλα λόγια, ισχύει ότι

$$[x_1 : y_1 : z_1] = [x_2 : y_2 : z_2] \Leftrightarrow \exists \lambda \in \mathbb{C}^\times : x_1 = \lambda x_2 \, , \, y_1 = \lambda y_2 \text{ και } z_1 = \lambda z_2.$$

Έτσι, ορίζουμε το μιγαδικό προβολικό επίπεδο ως εξής:

$$\mathbb{P}^2_{\mathbb{C}} := \left(\mathbb{A}^3_{\mathbb{C}} \setminus \{0\}\right) / \sim .$$

Βάσει του ορισμού αυτού, η πλήρης περιγραφή του προβολικού επιπέδου $\mathbb{P}^2_{\mathbb{C}}$ είναι η κάτωθι:

$$\mathbb{P}^2_{\mathbb{C}} = \mathbb{P}(\mathbb{C}^3) := \{[x : y : z] \mid (x, y, z) \in \mathbb{A}^3_{\mathbb{C}} \setminus \{(0, 0, 0)\}\}.$$

Εάν υποθέσουμε, τώρα, ένα σημείο $[x : y : z] \in \mathbb{P}^2_{\mathbb{C}}$ τέτοιο ώστε $z \neq 0$, τότε εξ ορισμού του προβολικού επιπέδου έχουμε ότι

$$[x : y : z] = [\frac{x}{z} : \frac{y}{z} : \frac{z}{z}] = [\frac{x}{z} : \frac{y}{z} : 1].$$

Η παρατήρηση αυτή μας οδηγεί στη συνολοθεωρητική σχέση

$$\mathbb{P}^2_{\mathbb{C}} = \{[x : y : 1] \mid (x, y) \in \mathbb{A}^2_{\mathbb{C}}\} \cup \{[x : y : 0] \mid (x, y) \in \mathbb{A}^2_{\mathbb{C}}\}.$$

Μάλιστα, το σύνολο

$$\{[x : y : 0] \mid (x, y) \in \mathbb{A}^2_{\mathbb{C}}\},$$

ονομάζεται *επ' άπειρον ευθεία του προβολικού επιπέδου* και συμβολίζεται ως $\mathbb{H}_\infty$.

Είδαμε ότι οι κυβικές καμπύλες, και γενικότερα οι καμπύλες, επί του συσχετικού επιπέδου $\mathbb{A}^2_{\mathbb{C}}$ ορίζονται μέσω πολυωνύμων του δακτυλίου $\mathbb{C}[X, Y]$. Στο προβολικό επίπεδο ο ορισμός των καμπυλών διαφέρει στο ότι τα πολυώνυμα που χρησιμοποιούμε είναι ομογενή. Έτσι, εάν υποθέσουμε ένα πολυώνυμο $F \in \mathbb{C}[X, Y]$ βαθμού n, τότε μέσω της σχέσης

$$\bar{F}(X, Y, Z) = Z^n \cdot F\left(\frac{X}{Z}, \frac{Y}{Z}\right),$$

ορίζεται ένα νέο πολυώνυμο, το $\bar{F}$, το οποίο είναι ομογενές βαθμού n. Η διαδικασία αυτή καλείται *ομογενοποίηση*. Το σύνολο των σημείων μηδενισμού του $\bar{F}$, όταν αυτά ειδωθούν όχι ώς σημεία με τη συνήθη έννοια, αλλά ως σημεία του προβολικού χώρου, συμβολίζεται ως $\mathbf{V}_+(\bar{F})$ και αποτελεί καμπύλη εντός του $\mathbb{P}^2_{\mathbb{C}}$. Ως *βαθμό* της καμπύλης $\mathbf{V}_+(\bar{F})$ ορίζουμε το βαθμό ομογένειας του $\bar{F}$. Δοθέντος, τώρα, του ομογενούς πολυωνύμου $\bar{F}$, μπορούμε εύκολα να ορίσουμε ένα μη ομογενές πολυώνυμο του $\mathbb{C}[X, Y]$ μέσω της σχέσης

$$F(X, Y) = \bar{F}(X, Y, 1).$$

Αυτό το πολυώνυμο ονομάζεται *αποομογενοποίηση του* $\bar{F}$.

ΟΡΙΣΜΟΣ 5.1.1. *Επίπεδη προβολική κυβική καμπύλη* καλείται μια καμπύλη της μορφής $\mathbf{V}_+(\bar{F})$ εντός του $\mathbb{P}^2_{\mathbb{C}}$, όπου το $\bar{F}$ είναι ομογενές πολυώνυμο βαθμού 3.

Ο ορισμός των ελλειπτικών καμπυλών απαιτεί την έννοια της ομαλότητας μίας καμπύλης. Μια καμπύλη ονομάζεται *ομαλή* ή *μη ιδιάζουσα* όταν δεν έχει ιδιάζοντα σημεία. Ένα σημείο $P \in \mathbb{P}^2_{\mathbb{C}}$ καλείται ιδιάζον σημείο της καμπύλης $\mathbf{V}_+(\bar{F})$, όταν ισχύει ότι

$$\bar{F}(P) = \left(\frac{\partial \bar{F}}{\partial X}\right)(P) = \left(\frac{\partial \bar{F}}{\partial Y}\right)(P) = \left(\frac{\partial \bar{F}}{\partial Z}\right)(P) = 0.$$

Οι καμπύλες που έχουν τουλάχιστον ένα ιδιάζον σημείο λέγονται *ιδιάζουσες* ή *ανώμαλες* καμπύλες.

ΟΡΙΣΜΟΣ 5.1.2. Ονομάζουμε *ελλειπτική καμπύλη*, και τη συμβολίζουμε με E ή $E|_{\mathbb{C}}$[1], κάθε μη ιδιάζουσα επίπεδη προβολική κυβική καμπύλη.

Το παρακάτω αποτέλεσμα είναι μία ένδειξη ότι μπορούμε πράγματι να συνδέσουμε έννοιες του προηγούμενου κεφαλαίου με τις ελλειπτικές καμπύλες.

[1] Όταν ειδωθεί η ελλειπτική καμπύλη ως σύνολο σημείων, και όχι ως γεωμετρικό αντικείμενο, θα προτιμούμε το συμβολισμό $E(\mathbb{C})$.

ΠΡΟΤΑΣΗ 5.1.3. *Κάθε ελλειπτική καμπύλη είναι καμπύλη της μορφής* $\mathbf{V}_+(Y^2Z - X^3 - g_2XZ^2 - g_3Z^3)$*, για κάποια επιλογή των μιγαδικών αριθμών* g_2 *και* g_3*, ώστε να ισχύει ότι* ${g_2}^3 - 27{g_3}^2 \neq 0$*.*

Απόδειξη. (βλ. [6], σελ.131, Πρ. 4.23.) □

Επί τη βάσει της ανωτέρω προτάσεως διαπιστώνουμε ότι για οποιαδήποτε επιλογή των g_2 και g_3 το σημείο $[0 : 1 : 0] \in \mathbb{H}_\infty$ θα είναι πάντα σημείο της ελλειπτικής καμπύλης $E = \mathbf{V}_+(Y^2Z - X^3 - g_2XZ^2 - g_3Z^3)$. Το σημείο αυτό θα το ονομάζουμε *επ' άπειρον σημείο της ελλειπτικής καμπύλης* E και θα το συμβολίζουμε ως ∞. Το επ' άπειρον σημείο είναι ένα νοητό σημείο της γραφικής παράστασης της ελλειπτικής καμπύλης, στο οποίο βέβαια συνίσταται και η διαφοροποίηση της ελλειπτικής καμπύλης από τη γραφική παράσταση μίας συνάρτησης. Εάν, τώρα, $Z \neq 0$, τότε χ.β.τ.γ μπορούμε να θέσουμε $Z = 1$. Από τα παραπάνω συμπεραίνουμε ότι η ελλειπτική καμπύλη E μπορεί να ειδωθεί ως η γραφική παράσταση του πολυωνύμου $Y^2 = 4X^3 - g_2X - g_3$ συνυπολογίζοντας και το νοητό σημείο ∞. Με άλλα λόγια έχουμε ότι

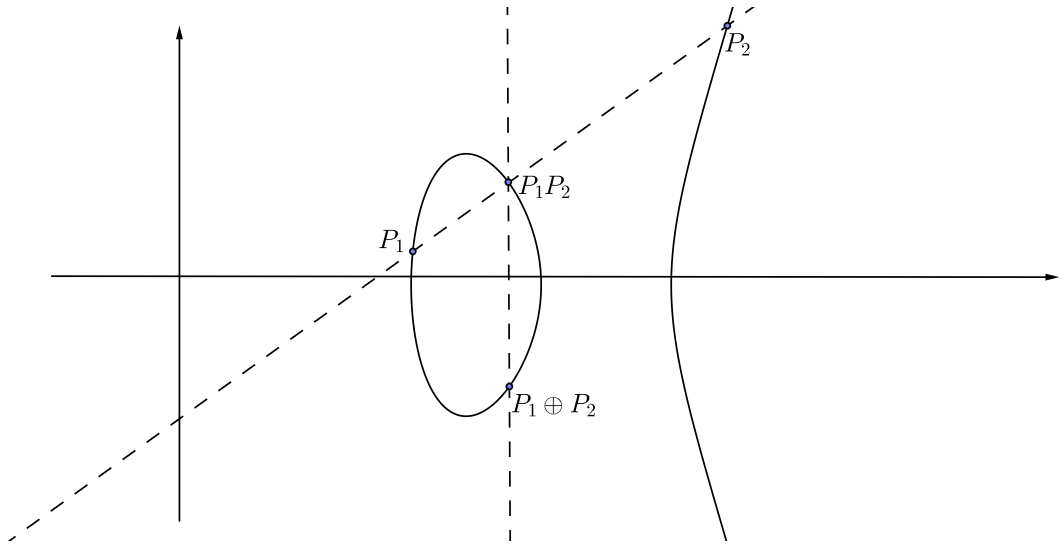
$$E(\mathbb{C}) = \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\}.$$

Άρα θα θεωρούμε για κάποια επιλογή των g_2 και g_3 την ελλειπτική καμπύλη E, ορισμένη στο σώμα των μιγαδικών αριθμών, ήτοι $g_2, g_3 \in \mathbb{C}$, γράφοντας ότι

$$E|_{\mathbb{C}} = \mathbf{V}_+(Y^2Z - X^3 - g_2XZ^2 - g_3Z^3).$$

Με το συμβολισμό αυτό υπονοούμε και την ύπαρξη του επ' άπειρον σημείου. Η μορφή αυτή της ελλειπτική καμπύλης ονομάζεται *κανονική μορφή Weierstrass* και είναι αρκετά σημαντική και χρήσιμη στη μελέτη των ελλειπτικών καμπυλών.

Εάν θεωρήσουμε τυχούσα ελλειπτική καμπύλη E, τότε αυτή, ειδωθείσα ως σύνολο σημείων, αποκτά τη δομή της ομάδας με πράξη αυτή της *πρόσθεσης σημείων επί της* E, την οποία θα συμβολίζουμε ως $\oplus$. Για να ορίσουμε την πράξη της πρόσθεσης σημείων επιλέγουμε αρχικά ένα σημείο της ελλειπτικής καμπύλης, το οποίο θα είναι και το ουδέτερο στοιχείο της πράξης. Συνηθίζεται, και αυτό θα υιοθετήσουμε και εμείς στα πλαίσια της μελέτης μας, ως ουδέτερο στοιχείο να επιλέγουμε το ∞. Ο λόγος είναι ότι για να επιτυγχάνεται δομή ομάδας πρέπει το σημείο που επειλέγουμε ως ουδέτερο να είναι σημείο καμπής. Έτσι, εάν έχουμε δύο σημεία $P_1, P_2 \in E$, τότε το $P_1 \oplus P_2$ υπολογίζεται, όπως φαίνεται στο παρακάτω σχήμα.



Η διαδικασία εύρεσης του αθροίσματος περιγράφεται γεωμετρικά. Εάν τα δυο σημεία είναι διακεκριμένα φέρουμε την ευθεία που τα ενώνει. Αυτή τέμνει την ελλειπτική καμπύλη κατ' ανάγκη και

σε ένα τρίτο σημείο, το οποίο ονομάζουμε P_1P_2. Από αυτό το σημείο φέρουμε κατακόρυφη ευθεία η οποία τέμνει την ελλειπτική καμπύλη σε κάποιο σημείο, το οποίο είναι το $P_1 \oplus P_2$. Εάν η ευθεία που ενώνει τα δυο σημεία είναι κάθετη στον οριζόντιο άξονα, τότε ως τρίτο σημείο θεωρούμε το ∞ και το άθροισμα $P_1 \oplus P_2$ ισούται με το επ' άπειρον σημείο. Τότε λέμε ότι το P_2 είναι το αντίθετο του P_1 και αντίστροφα. Εάν τα P_1 και P_2 ταυτίζονται, τότε φέρουμε εφαπτομένη και συνεχίζουμε την κατασκευή όπως παραπάνω.

Η παραπάνω διαδικασία αποδεικνύεται ότι είναι μία καλώς ορισμένη διμελής πράξη (βλ. [6], σελ.136, §4.4) και ότι, πράγματι, με αυτή το σύνολο των σημείων της ελλειπτικής καμπύλες E αποτελεί αβελιανή ομάδα. Έτσι, καταφέραμε να προσδώσουμε αλγεβρική δομή σε ένα γεωμετρικό αντικείμενο.

5.2 Ελλειπτικές καμπύλες και η συνάρτηση $\wp$ του Weierstrass.

Στο προηγούμενο κεφάλαιο, κάνοντας λόγο για διπλά περιοδικές συναρτήσεις συναντήσαμε την έννοια του πλέγματος $L := L(\omega_1, \omega_2)$ που σχηματίζουν δύο περίοδοι ω_1 και ω_2. Το σύνολο $\mathbb{C}/L$ μπορούμε να δείξουμε ότι ταυτίζεται τοπολογικά με τον τόρο στις δύο διαστάσεις. Επομένως, από αυτό το σημείο το σύνολο $\mathbb{C}/L$ θα καλείται *μιγαδικός τόρος*.

Δοθέντος κιγκλιδώματος $L := L(\omega_1, \omega_2)$ μπορούμε να ορίσουμε σε αυτό τη συνάρτηση $\wp$ του Weierstrass ως εξής:

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L(\omega_1, \omega_2)} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Τότε, όπως έχουμε ήδη αναφέρει, ισχύει ότι

$$\big(\wp'(z)\big)^2 = 4\wp^3(z) - g_2\wp(z) - g_3,$$

όπου

$$g_2 := g_2(L) := g_2(\omega_1, \omega_2)$$

και

$$g_3 := g_3(L) := g_3(\omega_1, \omega_2).$$

Αυτό σημαίνει ότι για $z \notin L$ έχουμε ότι $(\wp(z), \wp'(z)) \in E(\mathbb{C})$, όπου

$$E|_{\mathbb{C}} \ : \ Y^2 = 4X^3 - g_2X - g_3.$$

Από αυτό συνεπάγεται ότι ο λόγος

$$\frac{g_2}{{g_2}^3 - 27{g_3}^2}$$

είναι μη μηδενικός. Άρα μπορούμε να βρούμε κάποιο κιγκλίδωμα L, το οποίο να έχει ως $\mathcal{J}$-αναλλοίωτο το λόγο αυτό, ή με άλλα λόγια να ισχύει ότι

$$g_2 = g_2(L) \ \text{ και } g_3 = g_3(L).$$

Επομένως η ελλειπτική καμπύλη θα έχει τη μορφή

$$E|_{\mathbb{C}} \ : \ Y^2Z = 4X^3 - g_2(L)XZ^2 - g_3(L)Z^3.$$

Όλα τα παραπάνω είναι προάγγελος του ακόλουθου αποτελέσματος, το οποίο αποδεικνύει τον ισομορφισμό

$$\mathbb{C}/L \cong E(\mathbb{C}).$$

ΘΕΩΡΗΜΑ 5.2.1. *Η απεικόνιση*

$$\begin{aligned}\psi \;:\; & \mathbb{C}/L \longrightarrow E(\mathbb{C}) \\ & z \pmod L \longmapsto \big(\wp(z), \wp'(z)\big)\ ,\ z \notin L \\ & 0 \pmod L \longmapsto \infty,\end{aligned}$$

όπου

$$E|_{\mathbb{C}} \;:\; Y^2 = 4X^3 - g_2(L)X - g_3(L),$$

είναι αναλυτική συνάρτηση και, μάλιστα, είναι ισομορφισμός ομάδων.

Απόδειξη. Είναι σαφές εξ ορισμού της απεικόνισης ότι

$$\psi\big(z \pmod L\big) = \infty \;\Leftrightarrow\; z \equiv 0 \pmod L.$$

Ακόμα σαφές είναι και ότι η απεικόνιση ψ είναι καλώς ορισμένη.

Θα δείξουμε ότι η απεικόνιση ψ είναι επιμορφισμός. Θεωρούμε ένα ζεύγος $(x, y) \in E(\mathbb{C})$. Πρέπει να βρούμε $z_0 \in \mathbb{C}/L$, η πιο απλά $z_0 \in \mathbb{C}$ με την ιδιότητα

$$\psi\big(z_0 \pmod L\big) = (x, y) \Rightarrow \big(\wp(z_0), \wp'(z_0)\big) = (x, y).$$

Αρχικά εξετάζουμε τη συνάρτηση $\wp(z) - x$. Αυτή έχει διπλό πόλο άρα επί τη βάσει της προτάσεως 4.2.3 έχει και δύο σημεία μηδενισμού. Άρα υπάρχει κάποιο z_0, για την οποία ισχύει ότι $\wp(z_0) = x$. Τότε από τον ορισμό της ελλειπτικής καμπύλης θα έχουμε ότι

$$\wp'(z_0)^2 = y^2 \Rightarrow \wp'(z_0) = \pm y.$$

Αν $\wp'(z_0) = y$, τότε $\psi\big(z_0 \pmod L\big) = (x, y)$. Εάν, από την άλλη, έχουμε ότι $\wp'(z_0) = -y$, τότε εφόσον η $\wp'$ είναι περιττή θα ισχύει ότι

$$\psi\big(-z_0 \pmod L\big) = \big(\wp(-z_0), \wp'(-z_0)\big) = \big(\wp(z_0), -\wp'(z_0)\big) = (x, y).$$

Αποδεικνύουμε τώρα ότι η απεικόνιση μας είναι μονομορφισμός. Προς τούτο, θεωρούμε δύο μιγαδικούς αριθμούς z_1 και z_2 τέτοιους ώστε $\psi(z_1) = \psi(z_2)$ και $z_1 \not\equiv z_2 \pmod L$. Γνωρίζουμε ότι οι μοναδικοί πόλοι που εμφανίζει η συνάρτηση $\wp(z)$ είναι τα σημεία $z \in L$. Έτσι, εάν το z_1 είναι πόλος της $\wp$, τότε $z_1 \in L$. Λόγω της σχέσης $\psi(z_1) = \psi(z_2) \Rightarrow \wp(z_1) = \wp(z_2)$, θα έχουμε και ότι $z_2 \in L$. Επομένως $z_1 \equiv z_2 \pmod L$. Αυτό όμως αντίκειται στην υπόθεση ότι $z_1 \not\equiv z_2 \pmod L$. Υποθέτουμε, τώρα, ότι το z_1 δεν είναι πόλος της συνάρτησης $\wp$. Τότε η συνάρτηση $h(z) := \wp(z) - \wp(z_1)$ έχει διπλό πόλο στο $z = 0$ στο παραλληλόγραμμο περιόδων με κορυφές τις $0, \omega_1, \omega_2$ και $\omega_1 + \omega_2$. Άρα σε αυτό θα έχει και δύο σημεία μηδενισμού. Εάν υποθέσουμε ότι $z_1 = \omega_1/2$, τότε $h'(z_1) = \wp'(z_1) = 0$, άρα το z_1 είναι διπλό σημείο μηδενισμού της h. Σε αυτή την περίπτωση ισχύει ότι $z_1 = z_2 \Rightarrow z_1 \equiv z_2 \pmod L$. Όμοίως, εάν έχουμε ότι $z_1 = \omega_2/2$ ή $z_1 = (\omega_1 + \omega_2)/2$. Θεωρούμε, λοιπόν, ότι το z_1 δεν ισούται με κάποια από τις τρεις ημιπεριόδους του παραλληλογράμμου περιόδων στο οποίο δουλεύουμε. Τότε εφόσον η $\wp$ είναι άρτια συνάρτηση, το αυτό θα ισχύει και για την h. Αυτό σημαίνει ότι

$$h(z_1) = h(-z_1) = 0.$$

Κι αφού $2z_1 \not\equiv 0 \pmod L \Rightarrow z_1 \not\equiv -z_1 \pmod L$, τότε θα έχουμε κατ' ανάγκη ότι $z_2 \equiv -z_1 \pmod L$. Όμως

$$\wp'(z_2) = \wp'(-z_1) = -\wp'(z_1) = -\wp'(z_2) \Rightarrow \wp'(z_1) = \wp'(z_2) = 0.$$

Αυτό όμως είναι αντίφαση στο γεγονός ότι η συνάρτηση $\wp'$ έχει τρία ακριβώς σημεία μηδενισμού, τα $\omega_1/2, \omega_2/2$ και $(\omega_1 + \omega_2)/2$. Τελικά, σε κάθε περίπτωση καταλήγουμε σε αντίφαση στην υπόθεση ότι $z_1 \not\equiv z_2 \pmod L$. Επομένως έχουμε ότι

$$\psi\big(z_1 \pmod L\big) = \psi\big(z_2 \pmod L\big) \Rightarrow z_1 \equiv z_2 \pmod L,$$

ήτοι η απεικόνιση ψ είναι μονομορφισμός.

Μέχρι τώρα αποδείξαμε ότι η δοθείσα απεικόνιση είναι επιμορφισμός και μονομορφισμός χωρίς πρώτα να έχουμε δείξει ότι είναι ομομορφισμός. Έτσι, για να ολοκληρωθεί η απόδειξη πρέπει να δείξουμε ότι όντως ο ψ είναι ομομορφισμός ομάδων. Προς τούτο, θεωρούμε δύο μιγαδικούς αριθμούς $z_1, z_2 \in \mathbb{C}$ και θέτουμε

$$\psi\big(z_i \pmod L\big) = P_i = (x_i, y_i) \ , \ i = 1, 2.$$

Υποθέτουμε ότι κανένα από τα σημεία P_1 και P_2 δεν είναι το επ' άπειρον σημείο και ότι $P_1 \neq \pm P_2$, $2P_1 + P_2 \neq \infty$ και $P_1 + 2P_2 \neq \infty$. Έστω ότι η ευθεία που ενώνει τα P_1 και P_2 είναι η $y = \alpha x + \beta$. Ως $P_3 = (x_3, y_3)$ συμβολίζουμε το τρίτο σημείο τομής της ευθείας $y = \alpha x + \beta$ με την ελλειπτική καμπύλη E. Τότε θα υπάρχει κάποιο $z_3 \in \mathbb{C}$ τέτοιο ώστε $P_3 = (x_3, y_3) = \psi\big(z_3 \pmod L\big)$. Το α είναι η κλίση της ευθείς $y = \alpha x + \beta$, επομένως από την αναλυτική μας γεωμετρία έχουμε ότι

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1}.$$

Ακόμα, τα σημεία P_1, P_2 και P_3 ικανοποιούν το σύστημα

$$\begin{cases} y^2 = 4x^3 - g_2 x - g_3 \\ y = \alpha x + \beta \end{cases}$$

Άρα οι τετμημένες των σημείων της τομής της ευθείας $y = \alpha x + \beta$ με την ελλειπτική καμπύλη E ικανοποιούν την πολυωνυμική εξίσωση

$$4x^3 - g_2 x - g_3 = (\alpha x + \beta)^2 \Rightarrow 4x^3 - \alpha^2 x^2 + \cdots = 0.$$

Επομένως από τους τύπους Vieta έχουμε ότι

$$x_1 + x_2 + x_3 = \frac{\alpha^2}{4}.$$

Συνεπώς για την τετμημένη του σημείου P_3 λαμβάνουμε ότι

$$\begin{aligned} x_3 &= -x_1 - x_2 + \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \\ &= -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right)^2. \end{aligned}$$

Η συνάρτηση $l(z) := \wp'(z) - \alpha\wp(z) - \beta$ έχει τρία σημεία μηδενισμού ακριβώς, τα z_1, z_2 και z_3. Επί τη βάσει της προτάσεως 4.2.4, αφού ο πόλος της l είναι τριπλός και σημείο του L, ισχύει ότι $z_1 + z_2 + z_3 \in L$. Άρα

$$\wp(z_3) = \wp(-z_1 - z_2) = \wp(z_1 + z_2).$$

Άρα έχουμε ότι

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right)^2.$$

Λόγω συνέχειας, ο παραπάνω τύπος ισχύει όχι μόνο για τις συγκεκριμένες τιμές των z_1 και z_2, αλλά και για όλους τους μιγαδικούς z_1 και z_2 στους οποίους ορίζεται η συνάρτηση Weierstrass. Θα ασχοληθούμε τώρα με την τεταγμένη του σημείου P_3. Αυτό σημαίνει ότι επιθυμούμε να υπολογίσουμε το $\wp'(z_1 + z_2)$. Παραγωγίζοντας το $\wp(z_1 + z_2)$ ως προς z_2 λαμβάνουμε ένα τύπο ο οποίος περιέχει τους $\wp(z_1)$, $\wp(z_2)$, $\wp'(z_1)$, $\wp'(z_2)$ και το $\wp''(z_2)$. Επιθυμούμε να εκφράσουμε τη δεύτερη παράγωγο ως συνάρτηση των $\wp(z_1)$, $\wp(z_2)$, $\wp'(z_1)$ και $\wp'(z_2)$. Από τον τύπο της ελλειπτικής καμπύλης έχουμε ότι

$$2\wp''(z)\wp'(z) = \big(12\wp(z)^2 - g_2\big)\wp'(z) \Rightarrow 2\wp''(z) = 12\wp(z)^2 - g_2$$

[2]. Επομένως αντικαθιστούμε στο αποτέλεσμα της παραγώγισης το $\wp''(z_2)$ με $12\wp(z_2)^2 - g_2$. Υπολογίζοντας, τώρα, το y_3 με χρήση αναλυτικής γεωμετρίας, διαπιστώνουμε ότι $\wp'(z_1 + z_2) = -y_3 = -\wp'(z_3)$. Τελικά, από τον τρόπο που περιγράψαμε την πράξη $\oplus$ της πρόσθεσης σημείων επί κυβικής καμπύλης, έχουμε ότι

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, -y_3) \Rightarrow$$

$$\big(\wp(z_1), \wp'(z_1)\big) \oplus \big(\wp(z_2), \wp'(z_2)\big) = \big(\wp(z_3), -\wp'(z_3)\big) = \big(\wp(z_1 + z_2), \wp'(z_1 + z_2)\big) \Rightarrow$$

$$\psi\big(z_1 \pmod L\big) + \psi\big(z_1 \pmod L\big) = \psi\big((z_1 + z_2) \pmod L\big).$$

Για να ολοκληρώσουμε την απόδειξη του θεωρήματος αυτού πρέπει να δείξουμε ότι ο ψ εξακολουθεί να είναι ομομορφισμός ομάδων και στις εναπομείνασες περιπτώσεις. Εάν κάποιο από τα σημείο είναι το επ' άπειρον, το συμπέρασμα προκύπτει άμεσα. Επίσης άμεσα προκύπτει όταν ισχύει $P_1 + 2P_2 = \infty$ ή $2P_1 + P_2 = \infty$. Η περίπτωση που χρειάζεται προσοχή είναι αυτή όπου $z_1 = z_2$. Για την περίπτωση αυτή παίρνουμε το όριο $z_1 \to z_2$, ήτοι

$$\lim_{z_1 \to z_2} \wp(z_1 + z_2) = \lim_{z_1 \to z_2} \left(-\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)} \right)^2 \right) \Rightarrow$$

$$\wp(2z_2) = -2\wp(z_2) + \frac{1}{4}\left(\frac{\wp''(z_2)}{\wp'(z_2)} \right)^2 = \wp(2z_2) = -2\wp(z_2) + \frac{1}{4}\left(\frac{6\wp(z_2)^2 - \frac{g_2}{2}}{\wp'(z_2)} \right)^2.$$

Επομένως έχουμε υπολογίσει ότι $\wp(z_3) = \wp(2z_2)$. Παραγωγίζοντας ως προς z_2 τη σχέση

$$\wp(2z_2) = -2\wp(z_2) + \frac{1}{4}\left(\frac{6\wp(z_2)^2 - \frac{g_2}{2}}{\wp'(z_2)} \right)^2,$$

βρίσκουμε ότι $\wp'(z_3) = -\wp'(2z_2)$. Επομένως το συμπέρασμα αληθεύει και στην περίπτωση όπου $z_1 = z_2$. □

5.3 Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό

Μία κλάση ελλειπτικών καμπυλών είναι αυτές που έχουν μιγαδικό πολλαπλασιασμό. Ακριβή ορισμό της έννοιας αυτής θα δώσουμε παρακάτω. Για να το κάνουμε όμως αυτό, θα πρέπει να ασχοληθούμε με το *δακτύλιο των ενδομορφισμών μίας ελλειπτικής καμπύλης* E. Εάν ως $End_{\mathbb{C}}(E)$ συμβολίσουμε το σύνολο όλων των ενδομορφισμών της καμπύλης E, τότε ο $(End_{\mathbb{C}}(E), +, \circ)$ [3] είναι δακτύλιος.

Παραδειγμα 5.3.1. Ένα απλό παράδειγμα ενδομορφισμού είναι ο m-πολλαπλασιασμός σημείου της E, όπου $m \in \mathbb{Z}$. Πράγματι, εάν ορίσουμε την απεικόνιση

$$\begin{aligned} Mult_m \quad : \quad & E \longrightarrow E \\ & P \longmapsto mP, \end{aligned}$$

όπου

$$mP := \begin{cases} \underbrace{P \oplus P \oplus \cdots \oplus P}_{m-\text{φορές}} & , \text{αν } m > 0 \\ \infty & , \text{αν } m = 0 \\ \underbrace{(-P) \oplus (-P) \oplus \cdots \oplus (-P)}_{(-m)-\text{φορές}} & , \text{αν } m < 0 \end{cases},$$

[2]Η διαίρεση με $\wp'(z)$ είναι επιτρεπτή μόνο για τους μιγαδικούς z για τους οποίους ισχύει ότι $\wp'(z) \neq 0$. Παρά ταύτα ο τύπος γενικεύεται στο $\mathbb{C}$ λόγω συνέχειας.

[3]Ως $\circ$ συμβολίζουμε την πράξη της σύνθεσης απεικονίσεων.

τότε εύκολα διαπιστώνουμε, λόγω της μεταθετικότητας της πράξης $\oplus$, προκύπτει άμεσα ότι είναι ομομορφισμός ομάδων, άρα ενδομορφισμός της καμπύλης E. Λαμβάνοντας περιπτώσεις μπορούμε να δείξουμε ότι για δύο ακέραιους αριθμούς m και n ισχύει η σχέση

$$mP + nP = (m+n)P.$$

Πρόταση 5.3.2. *Ισχύει ότι $\mathbb{Z} \subseteq End_{\mathbb{C}}(E)$. Ιδιαίτερα, ο δακτύλιος $\mathbb{Z}$ των ακεραίων εμφυτεύεται στο δακτύλιο των ενδομορφισμών της ελλειπτικής καμπύλης E μέσω του μονομορφισμού*

$$\begin{aligned} \eta \quad : \quad & \mathbb{Z} \longrightarrow End_{\mathbb{C}}(E) \\ & m \longmapsto Mult_m. \end{aligned}$$

Απόδειξη. Θα αποδείξουμε ότι η απεικόνιση η είναι μονομορφισμός και τότε ο εγκλεισμός $\mathbb{Z} \subseteq End_{\mathbb{C}}(E)$ προκύπτει άμεσα. Αρχικά, δείχνουμε ότι ο η είναι ομομορφισμός. Θεωρούμε δύο ακέραιους αριθμούς m και n. Τότε έχουμε

$$\eta(m+n) = Mult_{m+n} = Mult_m + Mult_n = \eta(m) + \eta(n)$$

και

$$\eta(mn) = Mult_{mn} = Mult_m \cdot Mult_n = \eta(m)\eta(n)$$

Ακόμα, ισχύει ότι

$$\eta(0) = Mult_0 = \infty.$$

Επομένως η απεικόνιση η είναι ομομορφισμός. Για να δείξουμε ότι η η είναι μονομορφισμός, υπολογίζουμε τον πυρήνα αυτής. Έχουμε

$$\begin{aligned} Ker(\eta) &= \{m \in \mathbb{Z} \mid \eta(m) = Id_{End_{\mathbb{C}}(E)}\} = \{m \in \mathbb{Z} \mid Mult_m = Id_{End_{\mathbb{C}}(E)}\} \\ &= \{m \in \mathbb{Z} \mid mP = P \,, \forall\, P \in E\} = \{1\}. \end{aligned}$$

Έτσι, ολοκληρώνεται η απόδειξη της πρότασης. □

Λημμα 5.3.3. *Θεωρούμε μία ελλειπτική καμπύλη E. Ο ομομορφισμός α είναι ενδομορφισμός της E εάν, και μόνο εάν είναι της μορφής*

$$\alpha(x,y) = \big(R_1(x), yR_2(x)\big).$$

Επιθυμούμε να προσδιορίσουμε πλήρως το δακτύλιο των ενδομορφισμών $End_{\mathbb{C}}(E)$ μιας ελλειπτικής καμπύλης E. Ταυτίζουμε την ελλειπτική καμπύλη με το μιγαδικό τόρο $\mathbb{C}/L$, όπου L είναι το κιγκλίδωμα που αντιστοιχεί στην E. Θεωρούμε ένα ενδομορφισμό α. Η απεικόνιση ψ του θεωρήματος 5.2.1 είναι ισομορφισμός ομάδων. Επομένως εάν θέσουμε

$$\tilde{\alpha} := \psi^{-1} \circ \alpha \circ \psi,$$

τότε η $\tilde{\alpha} : \mathbb{C}/L \to \mathbb{C}/L$ είναι ομομορφισμός. Επιλέγουμε μία αρκούντως μικρή γειτονιά U γύρω από το σημείο $z = 0$. Τότε ισχύει ότι

$$\tilde{\alpha}(z_1 + z_2) \equiv \tilde{\alpha}(z_1) + \tilde{\alpha}(z_2) \pmod{L} \,, \forall\, z_1, z_2 \in U$$

και η απεικόνιση $\tilde{\alpha}|_U : U \to \mathbb{C}$ είναι αναλυτική. Εξ ορισμού της απεικόνισης $\tilde{\alpha}$ υπάρχει κάποιο στοιχείο του πλέγματος L τέτοιο ώστε η εικόνα του μέσω της $\tilde{\alpha}$ να είναι το ∞. Μπορούμε επομένως να το αφαιρέσουμε αυτό και να υποθέσουμε χ.β.τ.γ. ότι $\tilde{\alpha}(\infty) = \infty$. Εφόσον η $\tilde{\alpha}|_U$ είναι αναλυτική κοντά στο $z = 0$, θα είναι και συνεχής σε αυτή τη γειτονιά. Έτσι, μπορούμε χ.β.τ.γ. να επιλέξουμε τη γειτονιά U, ώστε να ισχύει ότι

$$\tilde{\alpha}(z_1 + z_2) = \tilde{\alpha}(z_1) + \tilde{\alpha}(z_2) \,, \forall\, z_1, z_2 \in U$$

[4]. Έτσι, για τυχόντα μιγαδικό αριθμό $z \in U$ έχουμε ότι

$$\tilde{\alpha}'(z) = \lim_{h\to 0} \frac{\tilde{\alpha}(z+h) - \tilde{\alpha}(z)}{h} = \lim_{h\to 0} \frac{\tilde{\alpha}(z) + \tilde{\alpha}(h) - \tilde{\alpha}(z)}{h} = \lim_{h\to 0} \frac{\tilde{\alpha}(h) - \tilde{\alpha}(0)}{h} = \tilde{\alpha}'(0).$$

Θέτοντας, λοιπόν, $\beta := \tilde{\alpha}'(0)$ λαμβάνουμε ότι

$$\tilde{\alpha}'(z) = \beta \Rightarrow \tilde{\alpha}(z) = \beta z \, , \forall \, z \in U.$$

Επιλέγουμε μιγαδικό αριθμό $z \in \mathbb{C}$. Τότε, υπάρχει ένας φυσικός αριθμός n με την ιδιότητα $z/n \in U$. Κατά συνέπεια έχουμε ότι

$$\tilde{\alpha}(z) \equiv \tilde{\alpha}\left(n \cdot \frac{z}{n}\right) \equiv n \cdot \beta \frac{z}{n} \equiv \beta z \pmod{L}.$$

Αυτό σημαίνει ότι ο ενδομορφισμός $\tilde{\alpha}$ ορίζεται μέσω του πολλαπλασιασμού με το β. Κι εφόσον ο $\tilde{\alpha}$ είναι ενδομορφισμός ισχύει ότι

$$\tilde{\alpha}(L) \subseteq L \Rightarrow \beta L \subseteq L.$$

Από την άλλη τώρα, επιλέγουμε ένα μιγαδικό αριθμό β με την ιδιότητα $\beta L \subseteq L$. Ο πολλαπλασιασμός με β προφανώς ορίζει ένα ομομορφισμό $\mathbb{C}/L \to \mathbb{C}/L$. Υπολογίζοντας τις συναρτήσεις $\wp(\beta z)$ και $\wp'(\beta z)$, παρατηρούμε ότι υπάρχουν ρητές συναρτήσεις S_1 και S_2 τέτοιες, ώστε να ισχύει ότι

$$\wp(\beta z) = S_1\big(\wp(z)\big) \;\text{ και }\; \wp'(\beta z) = \wp'(z) S_2\big(\wp(z)\big).$$

Επομένως σύμφωνα με το θεώρημα 5.2.1 και το λημμα 5.3.3 ο β ορίζει ένα εδομορφισμό.

Όλα τα παραπάνω αποδεικνύουν την ισχύ του κατωτέρω θεωρήματος:

ΘΕΩΡΗΜΑ 5.3.4. *Θεωρούμε ένα κιγκλίδωμα $L \subseteq \mathbb{C}$ και E την ελλειπτική καμπύλη που αυτό ορίζει μέσω του πηλίκου $\mathbb{C}/L$. Τότε ισχύει ότι*

$$End_{\mathbb{C}}(E) \cong \{\beta \in \mathbb{C} \mid \beta L \subseteq L\}.$$

Το παραπάνω θεώρημα δεν αποτελεί αυστηρή περιγραφή του δακτυλίου των ενδομορφισμών. Το αποτέλεσμα που καθορίζει πλήρως το τι μπορεί να είναι ο εν λόγω δακτύλιος είναι το εξής:

ΘΕΩΡΗΜΑ 5.3.5. *Έστω ελλειπτική καμπύλη E. Ο δακτύλιος $End_{\mathbb{C}}(E)$ είναι ισόμορφος είτε με το $\mathbb{Z}$, είτε με κάποια τάξη ενός μιγαδικού τετραγωνικού σώματος αριθμών.*

Απόδειξη. Θεωρούμε το πλέγμα $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ που αντιστοιχεί στην ελλειπτική καμπύλη E και το σύνολο

$$R = \{\beta \in \mathbb{C} \mid \beta L \subseteq L\}.$$

Προφανώς ισχύει ότι $\mathbb{Z} \subseteq R$, εφόσον $R \cong End_{\mathbb{C}}(E)$, και ότι το R είναι κλειστό ως προς τις πράξεις της πρόσθεσης και του πολλαπλασιασμού. Αυτό σημαίνει ότι ο R είναι δακτύλιος. Θεωρούμε ένα στοιχείο β αυτού. Τότε υπάρχουν ακέραιοι αριθμοί j, k, m και n, για τους οποίους ισχύει ότι

$$\beta\omega_1 = j\omega_1 + k\omega_2 \;\text{ και }\; \beta\omega_2 = m\omega_1 + \omega_2.$$

Οι σχέσεις αυτές μας δίνουν ότι

$$\begin{pmatrix} \beta - j & -k \\ -m & \beta - n \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = 0.$$

[4]Πράγματι, εάν τα δύο μέλη της ισότητας διαφέρουν κατά $0 \pmod{L}$, λόγω της επιλογής της γειτονιάς U, μπορούν να διαφέρουν μονάχα κατά $0 \in L$, ήτοι να ταυτίζονται.

Το σύστημα αυτό ως προς ω_1 και ω_2 έχει μη μηδενική λύση επομένως η ορίζουσα του πίνακα των συντελεστών είναι ίση με μηδέν. Αυτό σημαίνει ότι

$$\beta^2 - (j+n)\beta + (jn+km) = 0.$$

Εφόσον οι αριθμοί j, k, m και n είναι ακέραιοι ο β είναι εξ ορισμού ακέραιος αλγεβρικός αριθμός και ότι ο β είναι στοιχείο ενός τετραγωνικού σώματος αριθμών. Έστω ότι $\beta \in \mathbb{R}$. Τότε

$$\beta\omega_1 = j\omega_1 + k\omega_2 \Rightarrow (\beta - j)\omega_1 - k\omega_2 = 0.$$

Αυτό, εφόσον αποτελεί σχέση γραμμικής εξάρτησης των ω_1 και ω_1 μας πληροφορεί ότι $k = 0$ και $\beta = j \in \mathbb{Z}$. Συνεπώς $R \cap \mathbb{R} = \mathbb{Z}$. Έστω, τώρα, ότι $R \neq \mathbb{Z}$. Εάν θεωρήσουμε ότι $\beta \in R$ και $\beta \notin \mathbb{Z} \Rightarrow \beta \notin \mathbb{R}$, τότε το β είναι στοιχείο κάποιου μιγαδικού τετραγωνικού αριθμητικού σώματος, έστω του $K = \mathbb{Q}(\sqrt{d})$. Θεωρούμε ένα άλλο στοιχείο β' του R, το οποίο να μην είναι ακέραιος αριθμός. Τότε όπως και πριν υπάρχει $0 > d' \in \mathbb{Z}$ τέτοιο, ώστε να ισχύει ότι $\beta' \in K' = \mathbb{Q}(\sqrt{d'})$. Όμως $\beta + \beta' \in R$, το οποίο σημαίνει ότι και το $\beta + \beta'$ ανήκει σε κάποιο τετραγωνικό αριθμητικό σώμα, έστω το M. Όμως ισχύει ότι

$$\mathbb{Q} \leq K \leq \mathbb{Q}(\beta + \beta') \leq M \text{ και } \mathbb{Q} \leq K' \leq \mathbb{Q}(\beta + \beta') \leq M.$$

Κι εφόσον τα K, K' και M είναι τετραγωνικά σώματα αριθμών, τότε κατ' ανάγκη ισχύει ότι $K = K'$ $(= M)$. Όμως κάθε στοιχείο του R είναι ακέραιος αλγεβρικός αριθμός. Επομένως ισχύει ότι

$$R \leq R_K.$$

Έτσι, εάν $R \neq \mathbb{Z}$, τότε είναι μία τάξη ενός μιγαδικού τετραγωνικού αριθμητικού σώματος. □

ΟΡΙΣΜΟΣ 5.3.6. Θα λέμε ότι η ελλειπτική καμπύλη E έχει *μιγαδικό πολλαπλασιασμό* εάν ισχύει ότι $End_{\mathbb{C}}(E) \neq \mathbb{Z}$.

Άμεσο συμπέρασμα του θεωρήματος 5.3.5 είναι ότι ο δακτύλιος των ενδομορφισμών μας ελλειπτικής καμπύλης με μιγαδικό πολλαπλασιασμό είναι ισόμορφος με μια τάξη ενός τετραγωνικού μιγαδικού σώματος αριθμών.

5.4 $\mathcal{J}$-συνάρτηση ελλειπτικών καμπυλών με μιγαδικό πολλαπλασιασμό

Η παράγραφος αυτή έχει ως στόχο να αναδείξει κάποιες ιδιότητες της απόλυτης αναλλοιώτου μίας ελλειπτικής καμπύλης με μιγαδικό πολλαπλασιασμό, οι οποίες θα φανούν χρήσιμες στον ορισμό του σώματος του Hilbert για τετραγωνικά μιγαδικά σώματα αριθμών.

Αρχικός μας σκοπός είναι να αποδείξουμε ότι η $\mathcal{J}$-αναλλοίωτος μίας καμπύλης με μιγαδικό πολλαπλασιασμό είναι αλγεβρικός αριθμός. Σε επόμενο στάδιο, θα δείξουμε ότι είναι ακέραιος αλγεβρικός αριθμός.

ΠΡΟΤΑΣΗ 5.4.1. *Έστω O μία τάξη ενός τετραγωνικού μιγαδικού αριθμητικού σώματος K. Έστω, ακόμα, πλέγμα L για το οποίο ισχύει ότι $O = End_{\mathbb{C}}(\mathbb{C}/L)$. Τότε υπάρχει $\gamma \in \mathbb{C}^{\times}$, με την ιδιότητα το σύνολο γL να είναι ένα ιδεώδες της O. Αντιστρόφως, εάν το L είναι ένα υποσύνολο του $\mathbb{C}$ και το $\gamma \in \mathbb{C}^{\times}$ είναι τέτοιο, ώστε το γL να είναι ιδεώδες της O, τότε το L είναι πλέγμα και ισχύει ότι*

$$O \leq End_{\mathbb{C}}(\mathbb{C}/L).$$

Απόδειξη. $(\Rightarrow)$ Θεωρούμε ένα πλέγμα L. Αυτό γράφεται υπό τη μορφή

$$L = \mathbb{Z} + \tau\mathbb{Z},$$

όπου $\tau \in \mathcal{H}$. Έστω στοιχείο $\beta \in O \setminus \mathbb{Z}$. Τότε υπάρχουν αριθμοί $m, n \in \mathbb{Z}$ τέτοιοι, ώστε να ισχύει ότι

$$\beta = m \cdot 1 + n \cdot \tau \Rightarrow \tau = \frac{\beta - m}{n} \in K.$$

Παρατηρούμε ότι $n\tau = \beta - m \in R_K$, όπου ως R_K συμβολίζουμε το δακτύλιο των ακέραιων αλγεβρικών του σώματος K. Ακόμα, σύμφωνα με την πρόταση 2.5.2, ισχύει ότι $[R_K : O] < +\infty$. Έστω ότι $f := [R_K : O]$. Τότε έχουμε ότι

$$fn\tau = f\beta - fm.$$

Όμως $fm \in \mathbb{Z}$ και $\beta \in O \Rightarrow \beta \in R_K \Rightarrow f\beta \in fR_K$. Επομένως, επί τη βάσει της προτάσεως 2.5.2 ισχύει ότι

$$fn\tau \in \mathbb{Z} + fR_K = O.$$

Κι εφόσον $fn \in \mathbb{Z}$, μπορούμε να υποθέσουμε χ.β.τ.γ. ότι υπάρχει πάντα ένας ακέραιος $u \in \mathbb{Z}$ τέτοιος, ώστε $u\tau \in O$[5]. Τότε έχουμε ότι

$$L' := uL = \mathbb{Z}u + \mathbb{Z}u\tau \subseteq O.$$

Επιπροσθέτως, αφού το L είναι κλειστό ως προς την πράξη της πρόσθεσης και του πολλαπλασιασμού με στοιχείο της τάξης O, το αυτό θα ισχύει και για το L'. Συνεπώς το L' είναι ένα ιδεώδες της τάξης O.
($\Leftarrow$) Θεωρούμε το υποσύνολο L των μιγαδικών αριθμών και ένα $\gamma \in L^\times$, με την ιδιότητα το γL να είναι ιδεώδες της τάξης O. Για τυχόν $x \in \gamma L \setminus \{0\}$ ισχύει ότι

$$Ox \subseteq \gamma L \subseteq O.$$

Εφόσον η τάξη O είναι εξ ορισμού και εκ της προτάσεως 2.5.2 ένα ελεύθερο $\mathbb{Z}$-module βαθμού 2, τότε το αυτό ισχύει και για το Ox. Κατά συνέπεια, και το ιδεώδες γL είναι ένα ελεύθερο $\mathbb{Z}$-module βαθμού 2. Αυτό σημαίνει ότι υπάρχουν μιγαδικοί αριθμόι $\omega_1', \omega_2' \in L$ τέτοιοι, ώστε να ισχύει ότι

$$\gamma L = \gamma\mathbb{Z}\omega_1' + \gamma\mathbb{Z}\omega_2'.$$

Εφόσον η τάξη O περιέχει δύο $\mathbb{R}$-γραμμικώς ανεξάρτητα στοιχεία, τότε και η Ox θα περιέχει δύο τέτοια στοιχεία. Και λόγω του εγκλεισμού $Ox \subseteq \gamma L \subseteq O$, το αυτό θα ισχύει και για το γL, άρα και για το L. Η παρατήρηση αυτή οδηγεί άμεσα στο συμπέρασμα ότι τα ω_1 και ω_2 είναι $\mathbb{R}$-γραμμικώς ανεξαρτητα. Επομένως, το

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

είναι ένα πλέγμα. Κι εφόσον το γL είναι ένα ιδεώδες της O, τότε έχουμε ότι

$$O\gamma L \subseteq \gamma L \Rightarrow OL \subseteq L \Rightarrow O \subseteq End_{\mathbb{C}}(\mathbb{C}/L).$$

□

ΠΑΡΑΤΗΡΗΣΗ 5.4.2. Υπάρχουν περιπτώσεις όπου η τάξη O δεν ταυτίζεται με το δακτύλιο των ενδομορφισμών $End_{\mathbb{C}}(\mathbb{C}/L)$. Επί παραδείγματι, εάν υποθέσουμε ότι $O = \mathbb{Z}[2i]$, τότε αυτή είναι μία τάξη του τετραγωνικού μιγαδικού σώματος $\mathbb{Q}(i)$. Έστω, ακόμα, ότι $L = \mathbb{Z}[i]$. Τότε μπορούμε, πράγματι, να ελέγξουμε ότι ισχύει η σχέση

$$OL \subseteq L \Leftrightarrow \mathbb{Z}[2i]\mathbb{Z}[i] \subseteq \mathbb{Z}[i].$$

Παρα ταύτα,

$$End_{\mathbb{C}}(\mathbb{C}/L) = \mathbb{Z}[i] \neq \mathbb{Z}[2i] = O.$$

[5]Θα μπορούσαμε να θέσουμε $u := fn$ και να εξάγουμε το συμπέρασμα ότι για την επιλογή αυτή του u ισχύει ότι $u\tau \in \mathbb{Z}$. Όμως μπορούμε να θεωρήσουμε ως u και οποιοδήποτε πολλαπλάσιο του fn.

Πριν περάσουμε στο πρώτο σημαντικό αποτέλεσμα της παρούσης παραγράφου πρέπει να κάνουμε αναφορά σε κάποιες έννοιες. Δύο κιγκλιδώματα L_1 και L_2 ονομάζονται *ομοθετικά*, εάν υπάρχει ένας αριθμός $\gamma \in \mathbb{C}^\times$ τέτοιος, ώστε να ισχύει ότι

$$L_2 = \gamma L_1.$$

Εύκολα μπορούμε να διαπιστώσουμε ότι η ομοθεσία δύο κιγκλιδωμάτων αποτελεί σχέση ισοδυναμίας. Εάν θεωρήσουμε δύο ιδεώδη I_1 και I_2 μίας τάξης O ενός τετραγωνικού μιγαδικού σώματος αριθμών K, τότε αυτά καλούνται ισοδύναμα, όταν υπάρχει ένα αριθμός $\lambda \in K^\times$ με την ιδιότητα

$$I_2 = \lambda I_1.$$

Παρατηρηση 5.4.3. Αν υποθέσουμε ότι τα ιδεώδη I_1 και I_2, ως πλέγματα του $\mathbb{C}$ είναι ομοθετικά, τότε για κάποιο γ θα ισχύει ότι $I_2 = \gamma I_1$. Επιλέγουμε ένα $x \in I_1 \setminus \{0\}$. Τότε $\gamma x \in I_2$, άρα $\gamma \in K$. Επομένως τα ιδεώδη I_1 και I_2 είναι ισοδύναμα. Συνεπώς, λαμβάνουμε μία αμφιμονοσήμαντη αντιστοιχία μεταξύ του συνόλου όλων των κλάσεων ομοθεσίας των πλεγμάτων L που ικανοποιούν τον εγκλεισμό $OL \subseteq L$, και του συνόλου όλων των κλάσεων ισοδυναμίας όλων των μη τετριμμένων ιδεωδών της τάξης O. Μπορούμε να δείξουμε ότι το σύνολο των κλάσεων ισοδυναμίας των ιδεωδών έχει πεπερασμένου πλήθους στοιχεία. Αν, επί παραδείγματι, η τάξη O ταυτίζεται με το δακτύλιο R_K των ακέραιων αλγεβρικών του σώματος K , τότε το πλήθος των στοιχείων του συνόλου είναι απλά ο αριθμός κλάσεων ιδεωδών του σώματος K. Αυτό σημαίνει ότι και το σύνολο όλων των κλάσεων ομοθεσίας είναι επίσης πεπερασμένο.

Λημμα 5.4.4. *Έστω $a \in \mathbb{C}$. Εάν ισχύει ότι*

$$\#\big(\{\sigma(a) \mid \sigma \text{ αυτομορφισμός του } \mathbb{C}\}\big) < +\infty,$$

τότε ο a είναι αλγεβρικός αριθμός

Απόδειξη. (βλ. [15], σελ. 486, Πρ. C.7) □

Προταση 5.4.5. *Έστω O μία τάξη ενός μιγαδικού τετραγωνικού σώματος αριθμών και L ένα πλέγμα τέτοιο ώστε $OL \subseteq L$.Τότε ο αριθμός $\mathcal{J}(L)$ είναι αλγεβρικός.*

Απόδειξη. Έστω E η ελλειπτική καμπύλη που ορίζεται μέσω του ισομορφισμού $E \cong \mathbb{C}/L$. Έστω, ακόμα, ότι

$$E|_{\mathbb{C}} \ : \ Y^2 = 4X^3 - g_2X - g_3.$$

Θεωρούμε ένα αυτομορφισμό σ του $\mathbb{C}$. Ορίζουμε την ελλειπτική καμπύλη

$$E^\sigma|_{\mathbb{C}} \ : \ Y^2 = 4X^3 - \sigma(g_2)X - \sigma(g_3).$$

Εάν $\alpha \in End_{\mathbb{C}}(E)$, τότε ορίζουμε την απεικόνιση α^σ, η οποία δρα στον α, εφαρμόζοντας τον αυτομορφισμό σ σε κάθε συντελεστή των ρητών συναρτήσεων που περιγράφουν τον α. Τότε και ο α^σ είναι ενδομορφισμός της καμπύλης E^σ, γεγονός που υποδηλώνει ότι

$$End_{\mathbb{C}}(E) \cong End_{\mathbb{C}}(E^\sigma),$$

μέσω της απεικονίσεως

$$\begin{aligned} \xi_\sigma \ : \ & End_{\mathbb{C}}(E) \longrightarrow End_{\mathbb{C}}(E^\sigma) \\ & \alpha \longmapsto \alpha^\sigma. \end{aligned}$$

Αυτό σημαίνει ότι μπορούμε να ταξινομήσουμε τα πλέγματα L, των οποίων ο δακτύλιος των ενδομορφισμών περιέχει την τάξη O, μέχρις ομοθεσίας. Η απόλυτη αναλλοίωτος της ελλειπτικής καμπύλης E^σ είναι η $\sigma(\mathcal{J}(L))$. Όμως, εφόσον οι κλάσεις ομοθεσίας είναι πεπερασμένες στο πλήθος, σύμφωνα με την παρατήρηση 5.4.3, τότε και η $\mathcal{J}(L)$ έχει πεπερασμένου πλήθους εικόνες μέσω των αυτομορφισμών του $\mathbb{C}$. Άρα, επί τη βάσει του λήμματος 5.4.4 το ζητούμενο έπεται άμεσα. □

Θεωρημα 5.4.6. *Έστω K ένα μιγαδικό τετραγωνικό σώμα αριθμών.*

(i) Έστω $\tau \in \mathcal{H}$. Η ελλειπτική καμπύλη $\mathbb{C}/L$, όπου $L := \mathbb{Z} + \tau\mathbb{Z}$ είναι καμπύλη με μιγαδικό πολλαπλασιασμό εάν, και μόνο εάν $\tau \in K$.

(ii) Αν το $\tau \in \mathcal{H}$ είναι στοιχείο του σώματος K, τότε ο αριθμός $\mathcal{J}(\tau)$ είναι αλγεβρικός αριθμός, ήτοι $\mathcal{J}(\tau) \in \tilde{\mathbb{Q}}$.

Απόδειξη.

(i) Έχουμε ήδη αποδείξει ότι εάν η ελλειπτική καμπύλη $\mathbb{C}/L = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ είναι καμπύλη με μιγαδικό πολλαπλασιασμό τότε $\tau \in K$. Από την άλλη, τώρα, εάν $\tau \in K$, τότε το τ είναι σημείο μηδενισμού ενός πολυωνύμου βαθμού ίσου με 2 και με ακέραιους συντελεστές. Έστω, λοιπόν, ότι

$$a\tau^2 + b\tau + c = 0 \Rightarrow a\tau^2 = -b\tau - c,$$

για κάποιους ακέραιους αριθμούς a, b και c, όπου $a \neq 0$. Έτσι, εάν επιλέξουμε ένα τυχόν στοιχείο $m + n\tau \in L$, όπου $m, n \in \mathbb{Z}$, έχουμε ότι

$$a\tau(m + n\tau) = am\tau + na\tau^2 = am\tau + n(-b\tau - c) = -cn + (am - bn)\tau \in \mathbb{Z} + \tau\mathbb{Z} = L.$$

Άυτό σημαίνει ότι

$$a\tau L \subseteq L \Rightarrow a\tau \in End_{\mathbb{C}}(E) \Rightarrow End_{\mathbb{C}}(E) \neq \mathbb{Z},$$

άρα η E είναι καμπύλη με μιγαδικό πολλαπλασιασμό.

(ii) Έστω $\tau \in K$. Από το (i) αυτό σημαίνει ότι η ελλειπτική καμπύλη $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ είναι καμπύλη με μιγαδικό πολλαπλασιασμό. Οπότε ο δακτύλιος των ενδομορφισμών αυτής είναι μία τάξη O ενός μιγαδικού τετραγωνικού σώματος αριθμών, για την οποία μάλιστα ισχύει και ότι $OL \subseteq L$. Το αποτέλεσμα, τώρα, προκύπτει άμεσα από την πρόταση 5.4.5.

□

Πορισμα 5.4.7. *Έστω $\tau \in \mathcal{H}$ τέτοιο, ώστε η $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ να είναι ελλειπτική καμπύλη με μιγαδικό πολλαπλασιασμό. Τότε το $\mathbb{Q}(\tau)$ είναι ένα τετραγωνικό μιγαδικό σώμα αριθμών. Μάλιστα, ο δακτύλιος των ενδομορφισμών της εν λόγω ελλειπτικής καμπύλης είναι ισόμορφος με μία τάξη του $\mathbb{Q}(\tau)$.*

Απόδειξη. Άμεση από το θεώρημα 5.4.6. □

Το επόμενο βήμα είναι να δείξουμε ότι η απόλυτη αναλλοίωτος ελλειπτικής καμπύλης με μιγαδικό πολλαπλασιασμό είναι ακέραιος αλγεβρικός αριθμός. Προς τούτο, πρόκειται να αποδείξουμε ότι είναι σημείο μηδενισμού ενός μονικού πολυωνύμου με ακέραιους συντελεστές. Μάλιστα, η απόδειξη που θα παραθέσουμε δεν εξασφαλίζει μόνο την ύπαρξη. Το βασικό της πλεονέκτημα έναντι των υπολοίπων αποδείξεων είναι ότι προσδιορίζει πλήρως το μονικό πολυώνυμο που έχει ως σημείο μηδενισμού την απόλυτη αναλλοίωτο της ελλειπτικής καμπύλης.

Για να είναι ξεκάθαρος ο στόχος θα διατυπώσουμε το θεώρημα σε αυτό το σημείο, αλλά η απόδειξη αυτού θα παρουσιαστεί στο τέλος, όταν θα έχουμε αναφέρει και αποδείξει άλλα απαραίτητα ενδιάμεσα αποτελέσματα.

Θεωρημα 5.4.8. *Έστω R_K ο δακτύλιος των ακέραιων αλγεβρικών του τετραγωνικού μιγαδικού αριθμητικού σώματος K, μία τάξη O αυτού και L ένα πλέγμα του $\mathbb{C}$, για το οποίο ισχύει ο εγκλεισμός $OL \subseteq L$. Τότε ισχύει ότι $\mathcal{J}(L) \in \tilde{\mathbb{Z}}$. Με άλλα λόγια, η απόλυτη αναλλοίωτος κάθε ελλειπτικής καμπύλης με μιγαδικό πολλαπλασιασμό είναι ακέραιος αλγεβρικός αριθμός.*

Το πρώτο αποτέλεσμα που χρειαζόμαστε για την απόδειξη του ανωτέρω θεωρήματος είναι το παρακάτω:

Λημμα 5.4.9. *Έστω θετικός ακέραιος N και Σ_N το σύνολο όλων των πινάκων της μορφής*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \text{, όπου } a, b, d \in \mathbb{Z}$$

τέτοια, ώστε να ισχύουν οι σχέσεις

$$ad = N \text{ και } 0 \leq b < d.$$

Εάν θεωρήσουμε τυχόντα πίνακα M με στοιχεία ακέραιους αριθμούς και ορίζουσα ίση με N, τότε υπάρχει μοναδικός πίνακας $S \in \Sigma_N$, με την ιδιότητα $MS^{-1} \in SL_2(\mathbb{Z})$.

Παρατηρηση 5.4.10. Κατ' αρχάς ορίζουμε την έννοια των $SL_2(\mathbb{Z})$-ισοδύναμων πινάκων. Δύο πίνακες M_1 και M_2 καλούνται *εξ αριστερών $SL_2(\mathbb{Z})$-ισοδύναμοι*, όταν υπάρχει ένας πίνακας $X \in SL_2(\mathbb{Z})$, για τον οποίο να ισχύει ότι

$$M_2 = XM_1.$$

Προφανώς, η $SL_2(\mathbb{Z})$-ισοδυναμία είναι μία σχέση ισοδυναμίας. Έτσι, το παραπάνω λήμμα μας πληροφορεί ότι το σύνολο Σ_N περιέχει ένα ακριβώς στοιχείο κάθε κλάσης ισοδυναμίας. Την παρατήρηση αυτή πρόκειται να χρησιμοποιήσουμε στο δεύτερο σκέλος της απόδειξης του λήμματος.

Απόδειξη του λήμματος 5.4.9. Θεωρούμε τον πίνακα

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \text{, όπου } p, q, r, s \in \mathbb{Z} \text{ και } ps - qr = N.$$

Γράφουμε το κλάσμα $-p/r$ σε ανάγωγη μορφή, ήτοι υπό τη μορφή

$$-\frac{p}{r} = \frac{x}{y},$$

όπου $x, y \in \mathbb{Z}$ τέτοια, ώστε $(x, y) = 1$. Το ότι οι ακέραιοι x, y είναι πρώτοι μεταξύ τους ισοδυναμεί με την ύπαρξη ακέραιων αριθμών w, z, για τους οποίους ισχύει ότι

$$xz - wy = 1 \Leftrightarrow \begin{pmatrix} z & w \\ y & x \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Τότε ισχύει ότι

$$\begin{pmatrix} z & w \\ y & x \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Αυτό σημαίνει ότι μπορούμε εξ αρχής να υποθέσουμε ότι $r = 0$. Οπότε και $ps = N$. Ακόμα, πολλαπλασιάζοντας τον πίνακα

$$\begin{pmatrix} p & q \\ 0 & s \end{pmatrix}$$

με τον

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

αν χρειαστεί, μπορούμε να υποθέσουμε ότι $s > 0$. Επιλέγουμε, τώρα, έναν ακέραιο αριθμό $t \in \mathbb{Z}$ με την ιδιότητα

$$0 \leq q + ts < s.$$

Τότε

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ 0 & s \end{pmatrix} = \begin{pmatrix} p & q + ts \\ 0 & s \end{pmatrix} \in \Sigma_N.$$

Αυτό σημαίνει ότι το σύνολο Σ_N παριστά όλες τις κλάσεις ισοδυναμίας πινάκων του $SL_2(\mathbb{Z})$ ορίζουσας ίσης με N. Έτσι, ολοκληρώνεται η απόδειξη της ύπαρξης του πίνακα S. Για την απόδειξη της μοναδικότητας θεωρούμε δύο πίνακες

$$M_i := \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \Sigma_N \text{ , όπου } i = 1, 2,$$

οι οποίοι είναι εξ αριστερών $SL_2(\mathbb{Z})$-ισοδύναμοι. Αυτό σημαίνει ότι

$$M_1 M_2^{-1} \in SL_2(\mathbb{Z}) \Leftrightarrow \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}^{-1} \in SL_2(\mathbb{Z}) \Leftrightarrow \begin{pmatrix} \frac{a_1}{a_2} & \frac{b_1 a_2 - a_1 b_2}{N} \\ 0 & \frac{d_1}{d_2} \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Άρα έχουμε ότι

$$\frac{a_1}{a_2} \in \mathbb{Z} \ , \ \frac{d_1}{d_2} \in \mathbb{Z} \ \text{ και } \ \frac{a_1}{a_2}\frac{d_1}{d_2} = 1.$$

Μάλιστα, αφού $M_1 \in \Sigma_N$ και $M_2 \in \Sigma_N$, τότε $d_1 > 1$ και $d_2 > 0$, και από τις σχεσεις $a_1 d_1 = N = a_2 d_2$ έπεται ότι οι αριθμοί a_1/a_2 και d_1/d_2 είναι θετικοί ακέραιοι. Άρα

$$\frac{a_1}{a_2} = 1 = \frac{d_1}{d_2} \Rightarrow a_1 = a_2 \ \text{ και } \ d_1 = d_2.$$

Επιπροσθέτως, ισχύει ότι

$$\begin{pmatrix} \frac{a_1}{a_2} & \frac{b_1 a_2 - a_1 b_2}{N} \\ 0 & \frac{d_1}{d_2} \end{pmatrix} \in SL_2(\mathbb{Z}) \Rightarrow \frac{b_1 a_2 - a_1 b_2}{N} = \frac{b_1 a_1 - b_2 a_1}{a_1 d_1} = \frac{b_1 - b_2}{d_1} \in \mathbb{Z} \Rightarrow b_1 \equiv b_2 \pmod{d_1}.$$

Όμως ισχύει ότι $0 \leq b_1, b_2 < d_1 = d_2$, από το οποίο άμεσα προκύπτει ότι $b_1 = b_2$. Άρα αποδείξαμε ότι $M_1 = M_2$. □

Στο προηγούμενο κεφάλαιο, όταν κάναμε λόγο για την $\mathcal{J}$-αναλλοίωτο ενός μιγαδικού $\tau \in \mathcal{H}$, χρησιμοποιήσαμε το συμβολισμό

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d},$$

όπου

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Εδώ, διατηρούμε τον ίδιο συμβολισμό με τη διαφορά ότι η επιλογή του πίνακα γίνεται από το σύνολο Σ_N. Με άλλα λόγια, εάν

$$S := \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Sigma_N,$$

τότε

$$S\tau = \frac{a\tau + b}{d}.$$

Επί τη βάσει του συμβολισμού αυτού, ισχύει ότι

$$\mathcal{J}(S\tau) = \mathcal{J}\left(\frac{a\tau + b}{d}\right).$$

Υπενθυμίζουμε ότι η $\mathcal{J}$-αναλλοίωτος είναι αναλυτική στο $\mathcal{H}$. Ορίζουμε, τώρα, τη συνάρτηση

$$F_N(X, \tau) = \prod_{S \in \Sigma_N} \big(X - \mathcal{J}(S\tau)\big) = \sum_k a_k(\tau) X^k.$$

Συνεπώς η συνάρτηση $F_N(X, \tau)$ μπορεί να ειδωθεί ως πολυώνυμο μεταβλητής X και συντελεστών $a_k(\tau)$. Αφού η $\mathcal{J}$-αναλλοίωτος είναι αναλυτική στο $\mathcal{H}$, το αυτό θα ισχύει και για τους συντελεστές $a_k(\tau)$.

Λημμα 5.4.11. *Ισχύει ότι*

$$a_k(M\tau) = a_k(\tau)\ ,\ \forall\ M \in SL_2(\mathbb{Z}),$$

ήτοι οι συντελεστές του πολυωνύμου $F_N(X,\tau)$ παραμένουν αναλλοίωτοι από τη δράση του συνόλου $SL_2(\mathbb{Z})$.

Απόδειξη. Εάν $S \in \Sigma_N$ και $M \in SL_2(\mathbb{Z})$, τότε $\det(SM) = N$, επομένως υπάρχει πίνακας $A_S \in SL_2(\mathbb{Z})$ και ένας μονοσήμαντα ορισμένος πίνακας $M_S \in S_N$ τέτοιος, ώστε $A_S M_S = SM$. Εάν $S_1, S_2 \in \Sigma_N$ και $M_{S_1} = M_{S_2}$, τότε

$$A_{S_1}{}^{-1} S_1 M = M_{S_1} = M_{S_2} = A_{S_2}{}^{-1} S_2 M \Rightarrow A_{S_2} A_{S_1}{}^{-1} S_1 = S_2.$$

Λόγω της μοναδικότητας που έχουμε εξασφαλίσει από το λήμμα 5.4.9 ισχύει ότι $S_1 = S_2$. Αυτό σημαίνει ότι η απεικόνιση $S \longmapsto M_S$ είναι εμφύτευση του συνόλου Σ_N στον εαυτό του, ήτοι μία μετάθεση των στοιχείων του Σ_N. Επομένως έχουμε ότι

$$F_N(X, M\tau) = \prod_{S\in\Sigma_N} \big(X - \mathcal{J}(SM\tau)\big) = \prod_{S\in\Sigma_N} \big(X - \mathcal{J}(A_S M_S \tau)\big) = \prod_{S\in\Sigma_N} \big(X - \mathcal{J}(M_s\tau)\big)$$

$$= \prod_{S\in\Sigma_N} \big(X - \mathcal{J}(S\tau)\big) = F_N(X,\tau).$$

Από την ισότητα των πολυωνύμων $F_N(X, M\tau)$ και $F_N(X,\tau)$ έπεται η ισότητα των αντίστοιχων συντελεστών, γεγονός που ολοκληρώνει την απόδειξή μας. □

Λημμα 5.4.12. *Για κάθε k υπάρχει ένας ακέραιος n τέτοιος, ώστε να ισχύει ότι*

$$a_k(\tau) \in q^{-n}\mathbb{Z}[[q]],$$

όπου ως $\mathbb{Z}[[q]]$ συμβολίζουμε το σύνολο όλων των δυναμοσειρών μεταβλητής q και ακέραιων συντελεστών. Με άλλα λόγια, οι συντελεστές $a_k(\tau)$ μπορούν να εκφραστούν ως αναπτύγματα Laurent, με πεπερασμένο πλήθος αρνητικούς όρους και ακέραιους συντελεστές.

Απόδειξη. Σύμφωνα με την πρόταση 4.5.4 η $\mathcal{J}$-αναλλοίωτος έχει ανάπτυγμα Laurent το εξής:

$$\mathcal{J}(\tau) = \frac{1}{q} + 744 + \sum_{k=1}^{+\infty} c(k) q^k = \sum_{k=-1}^{+\infty} c(k) q^k =: P(q),$$

όπου οι συντελεστές $c(k)$ είναι ακέραιοι. Τότε θα έχουμε ότι

$$\mathcal{J}\left(\frac{a\tau + b}{d}\right) = \sum_{k=-1}^{+\infty} c(k)(\zeta^b e^{2\pi i a\tau/d})^k = P(\zeta^b e^{2\pi i a\tau/d}),$$

όπου $\zeta := e^{2\pi i/d}$.
Σταθεροποιούμε τα a και d ώστε να ισχύει $ad = N$. Ισχυριζόμαστε, σε αυτό το σημείο της απόδειξης, ότι το

$$\prod_{b=0}^{d-1} \big(X - P(r^b e^{2\pi i a\tau/d})\big) = \sum_{k=0}^{d} p_k(e^{2\pi i a\tau/d} X^k),$$

είναι ένα πολυώνυμο μεταβλητής X, όπου οι συντελεστές p_k αυτού είναι αναπτύγματα Laurent του $e^{2\pi i a\tau}$ με συντελεστές ακέραιους αριθμούς. Εκτός από τη συνθήκη ότι οι συντελεστές των p_k είναι ακέραιοι αριθμοί, δε χρειάζεται να αποδείξουμε τίποτα άλλο. Προς τούτο, θα δώσουμε μία απόδειξη με χρήση θεωρίας Galois. Οι συντελεστές των p_k είναι στοιχεία του $\mathbb{Z}[\zeta]$. Η ομαδα Galois

της επέκτασης $\mathbb{Q}(\zeta)/\mathbb{Q}$ μεταθέτει τους όρους του γινομένου, άρα αφήνει τους συντελεστές των p_k αναλλοίωτους. Αυτό σημαίνει ότι οι συντελεστές των p_k είναι ρητοί αριθμοί. Όμως ισχύει ότι $\mathbb{Z}[\zeta] \cap \mathbb{Q} = R_{\mathbb{Q}} = \mathbb{Z}$. Έτσι, ολοκληρώνεται η απόδειξη του ισχυρισμού.
Αφού ισχύει $ad = N$ για κάθε πίνακα του συνόλου Σ_N, έχουμε ότι

$$e^{2\pi i a\tau/d} = e^{2\pi i a^2\tau/N}.$$

Αυτό σημαίνει ότι τα $p_k(\tau)$ του ισχυρισμού μπορούν να ειδωθούν ως αναπτύγματα Laurent του $e^{2\pi i\tau/N}$, με ακέραιους συντελεστές. Επομένως οι συντελεστές $a_k(\tau)$ του $F_N(X,\tau)$ είναι σειρές Laurent με ακέραιους συντελεστές. Γνωρίζουμε ότι ο πίνακας

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$$

δρα στο $\mathcal{H}$ μέσω της απεικόνισης $\tau \longmapsto \tau + 1$. Σύμφωνα με το λήμμα 5.4.11 τα $a_k(\tau)$ παραμένουν αναλλοίωτα από τη δράση της $\tau \longmapsto \tau + 1$. Κι εφόσον για το $(e^{2\pi i\tau/N})^l$ αυτό αληθεύει μόνο όταν $N \mid l$, το ανάπτυγμα Laurent για το a_k πρέπει να είναι ανάπτυγμα Laurent του $(e^{2\pi i\tau/N})^N = e^{2\pi i\tau}$. Με αυτή την παρατήρηση ολοκληρώνεται η απόδειξη του λήμματος. □

ΠΡΟΤΑΣΗ 5.4.13. *Θεωρούμε μία αναλυτική στο $\mathcal{H}$ modular συνάρτηση f, της οποίας το ανάπτυγμα Laurent έχει ακέραιους συντελεστές. Τότε η f είναι ένα πολυώνυμο μεταβλητής $\mathcal{J}(\tau)$ με ακέραιους συντελεστές, ήτοι $f(\tau) \in \mathbb{Z}[\mathcal{J}(\tau)]$.*

Απόδειξη. Υπενθυμίζουμε ότι

$$\mathcal{J}(\tau) - \frac{1}{q} \in \mathbb{Z}[[q]].$$

Έστω ότι

$$f(\tau) = \frac{b_n}{q^n} + \cdots,$$

όπου $b_n \in \mathbb{Z}$, Τότε

$$f(\tau) - b_n\mathcal{J}^n(\tau) = \frac{b_{n-1}}{q^{n-1}} + \cdots,$$

όπου $b_{n-1} \in \mathbb{Z}$. Επομένως,

$$f(\tau) - b_n\mathcal{J}^n(\tau) - b_{n-1}\mathcal{J}^{n-1}(\tau) = \frac{b_{n-2}}{q^{n-2}} + \cdots.$$

Συνεχίζοντας κατ' αυτό τον τρόπο εξαλείφουμε ολόκληρο το κύριο μέρος του αναπτύγματος Laurent. Έτσι, μπορούμε να κατασκευάσουμε το πολυώνυμο

$$g(\tau) = f(\tau) - b_n\mathcal{J}^n(\tau) - \cdots b_0 \in q\mathbb{Z}[[q]],$$

όπου οι αριθμοί $b_0, b_1, \ldots, b_0$ είναι ακέραιοι. Η συνάρτηση g είναι αναλυτική στο $\mathcal{H}$. Κι εφόσον $g(\tau) \in q\mathbb{Z}[[q]]$, αυτό μας πληροφορεί ότι $g(i\infty) = 0$. Με άλλα λόγια ισχύει ότι $ord_{i\infty}(f) > 0$. Κι εφόσον η συνάρτηση g είναι αναλυτική η τάξη κάθε σημείου στην g είναι ένας αριθμός μη αρνητικός. Σύμφωνα, λοιπόν, με το πόρισμα 4.7.3 έχουμε ότι

$$ord_{i\infty}(f) + \frac{1}{3}ord_{\rho}(f) + \frac{1}{2}ord_{i}(f) + \sum_{z \neq i,\rho,i\infty} ord_z(f) > 0,$$

το οποίο επάγει ότι η συνάρτηση g είναι η μηδενική συνάρτηση. Κατά συνέπεια, ισχύει ότι

$$g(\tau) = f(\tau) - b_n\mathcal{J}^n(\tau) - \cdots b_0 = 0 \Rightarrow f(\tau) = b_n\mathcal{J}^n(\tau) + \cdots b_0 \in \mathbb{Z}[\mathcal{J}(\tau)].$$

□

Θεωρημα 5.4.14 (Kronecker)**.** *Έστω N ένας θετικός ακέραιος αριθμός*

(i) Υπάρχει ένα μονικό πολυώνυμο $\hat{F}(X,Y) \in \mathbb{Z}[X,Y]$ τέτοιο, ώστε να ισχύει ότι

$$F_N(X,\tau) = \hat{F}(X, \mathcal{J}(\tau)).$$

(ii) Εάν το N δεν είναι τέλειο τετράγωνο, τότε το πολυώνυμο

$$H_N(X) = \hat{F}_N(X,X) \in \mathbb{Z}[X]$$

είναι μη σταθερό και ο συντελεστής του μεγιστοβάθμιου όρου είναι ίσος με ± 1.

Απόδειξη. (i) Η απόδειξη είναι άμεση από το λήμμα 5.4.12 και την πρόταση 5.4.13.

(ii) Γνωρίζουμε ότι το

$$H_N(\mathcal{J}(\tau)) = \hat{F}_N(\mathcal{J}(\tau), \mathcal{J}(\tau)) = F_N(\mathcal{J}(\tau),\tau) = \prod_{S \in \Sigma_N} \big(\mathcal{J}(\tau) - \mathcal{J}(S\tau)\big)$$

είναι ένα πολυώνυμο με ακέραιους συντελεστές. Επιθυμούμε να προσδιορίσουμε το συντελεστή του μεγιστοβαθμίου όρου. Έστω

$$S = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Sigma_N.$$

Εάν εκφράσουμε το $J(\tau) - \mathcal{J}(S\tau)$ ως σειρά Laurent μεταβλητής $e^{2\pi i \tau/N}$, τότε ο πρώτος όρος για το $\mathcal{J}(\tau)$ είναι ο

$$e^{-2\pi i \tau} = e^{-2\pi i \tau/N)^N},$$

ενώ για το $\mathcal{J}(S\tau)$ είναι ο

$$\zeta^{-b} e^{-2\pi i a\tau/d} = \zeta^{-b} \Big(e^{-2\pi i \tau/N}\Big)^{a^2}.$$

Εφόσον το N δεν είναι τέλειο τετράγωνο, ισχύει ότι $N \neq a^2$. Συνεπώς, οι όροι αυτοί αντιπροσωπεύουν διαφορετικές δυνάμεις του $e^{2\pi i\tau/N}$, άρα δεν αλληλοαναιρούνται. Ένας εξ αυτών θα πρέπει να είναι ο πρώτος όρος του αναπτύγματος Laurent του $\mathcal{J}(\tau) - \mathcal{J}(S\tau)$. Οπότε ο συντελεστής θα είναι είτε ίσος με 1, είτε ίσος με $-\zeta^b$. Ιδιαιτέρως, όποιος και να είναι ο συντελεστής του πρώτου όρου, θα είναι σίγουρα μία ρίζα της μονάδος. Επομένως, ο συντελεστής του πολυωνύμου $H_N(X)$ θα είναι το γινόμενο όλων αυτών των ριζών της μονάδος, άρα θα είναι και ο ίδιος ρίζα της μονάδος. Μάλιστα, το γεγονός ότι οι συντελεστές των σειρών Laurent των $\mathcal{J}(\tau)$ και $\mathcal{J}(S\tau)$ δεν αλληλοαναιρούνται οδηγεί και στο ότι το ανάπτυγμα Laurent του $H_N(X)$ ως προς q έχει αρνητικές δυνάμεις. Αυτό, όμως, σημαίνει ότι το $H_N(X)$ είναι μη σταθερό πολυώνυμο. Υποθέτουμε, τώρα, ότι

$$H_N(X) = uX^l + \text{όροι χαμηλότερης τάξης},$$

όπου $u \in \mathbb{Z}$. Εφόσον η σειρά Laurent του $\mathcal{J}(\tau)$ αρχίζει με τον όρο $1/q$, έχουμε ότι

$$H_N(\mathcal{J}(\tau)) = uq^{-l} + \text{όροι υψηλότερης τάξης}.$$

Αποδείξαμε, όμως, ότι το u είναι μία ρίζα της μονάδος. Κι εφόσον $u \in \mathbb{Q}$, τότε $u = \pm 1$.

□

Ύστερα από πολλά προκαταρκτικά αποτελέσματα, είμαστε έτοιμοι να διατυπώσουμε και να αποδείξουμε ένα μεγάλης σημασίας θεώρημα για την απόλυτη αναλλοίωτο ελλειπτικής καμπύλης με μιγαδικό πολλαπλασιασμό.

Απόδειξη του θεωρήματος 5.4.8. Υποθέτουμε ότι το τετραγωνικό αριθμητικό σώμα K είναι της μορφής $K = \mathbb{Q}(\sqrt{-d})$ και χ.β.τ.γ. ότι το πλέγμα L που αντιστοιχεί στην ελλειπτική καμπύλη έχει τη μορφή

$$L = \mathbb{Z} + \mathbb{Z}\tau,$$

όπου $\tau \in \mathcal{H}$. Επί τη βάσει της προτάσεως 2.5.2, γνωρίζουμε ότι $n := [R_K : O] < +\infty$. Άρα ισχύει ότι $n\alpha \in O$, για κάθε $\alpha \in R_K$. Πράγματι,

$$\alpha \in R_K \Rightarrow \alpha + O \in R_K/O \Rightarrow n(\alpha + O) = O \Rightarrow n\alpha \in O.$$

Επομένως, αν $\alpha = \sqrt{-d}$ ισχύει ότι

$$n\sqrt{-d}L \subseteq L.$$

Αυτό σημαίνει ότι υπάρχουν ακέραιοι αριθμοί t, u, v και w τέτοιοι, ώστε

$$n\sqrt{-d} \cdot \tau = t\tau + u \ \text{ και } \ n\sqrt{-d} \cdot 1 = v\tau + w.$$

Διαιρώντας κατά μέλη τις εξισώσεις αυτές, λαμβάνουμε ότι

$$\tau = \frac{t\tau + u}{v\tau + w}.$$

Μάλιστα, από τις σχέσεις αυτές προκύπτει και ότι

$$(n\sqrt{-d})^2 - (t + w)(n\sqrt{-d}) + (tw - uv) = 0.$$

Με άλλα λόγια, ο αριθμός $n\sqrt{-d}$ είναι θέση μηδενισμού του πολυωνύμου

$$X^2 - (t + w)X + (tw - uv) \in \mathbb{Z}[X].$$

Γνωρίζουμε, όμως, ότι είναι και σημείο μηδενισμού του $X^2 + n^2 d \in \mathbb{Z}[X]$. Εάν τα πολυώνυμα $X^2 - (t + w)X + (tw - uv)$ και $X^2 + n^2 d$ δεν ταυτίζονται, τότε $n\sqrt{-d}$ είναι σημείο μηδενισμού της διαφοράς αυτών, ήτοι ενός πολυωνύμου βαθμού το πολύ ίσου με 1, γεγονός που είναι άτοπο. Κατά συνέπεια, τα πολυώνυμα ταυτίζονται. Άρα

$$\det \begin{pmatrix} t & u \\ v & w \end{pmatrix} = tw - uv = n^2 d.$$

Χρησιμοποιώντας το λήμμα 5.4.9 συμπεραίνουμε ότι υπάρχει ένας πίνακας $M \in SL_2(\mathbb{Z})$ και ένας $S_1 \in \Sigma_{n^2 d}$ τέτοιος, ώστε

$$\begin{pmatrix} t & u \\ v & w \end{pmatrix} = MS_1.$$

Τότε

$$\mathcal{J}(\tau) = \mathcal{J}\left(\frac{t\tau + u}{v\tau + w}\right) = \mathcal{J}(MS_1\tau) = \mathcal{J}(S_1\tau),$$

αφού η δράση στοιχείου του $SL_2(\mathbb{Z})$ αφήνει αναλλοίωτη την $\mathcal{J}$. Επομένως, έχουμε ότι

$$H_{n^2 d}(\mathcal{J}(\tau)) = \prod_{S \in \Sigma_{n^2 d}} \big(\mathcal{J}(\tau) - \mathcal{J}(S\tau)\big) = \big(\mathcal{J}(\tau) - \mathcal{J}(S_1\tau)\big) \prod_{\substack{S \in \Sigma_{n^2 d} \\ S \neq S_1}} \big(\mathcal{J}(\tau) - \mathcal{J}(S\tau)\big) = 0.$$

Εάν $d \neq 1$, το θεώρημα 5.4.14 μας εξασφαλίζει ότι ο συντελεστής του μεγιστοβαθμίου όρου του $H_{n^2 d}$ είναι ± 1. Έτσι, αλλάζοντας ίσως το πρόσημο του $H_{n^2 d}$, συμπεραίνουμε ότι το $\mathcal{J}(\tau) =: \mathcal{J}(L)$ είναι σημείο μηδενισμού ενός μονικού πολυωνύμου με ακέραιους συντελεστές, άρα είναι αλγεβρικός αριθμός. Εάν, από την άλλη, $d = 1$, ήτοι $K = \mathbb{Q}(i)$, εφαρμόζουμε το ίδιο επιχείρημα με τη διαφοροποίηση ότι θεωρούμε τον $1 + i$ αντί του i. Έτσι, το $n(1 + i)$ είναι σημείο μηδενισμού του πολυωνύμου $X^2 - 2nX + 2n^2$. Από αυτό έπεται ότι $tw - uv = 2n^2$, το οποίο δεν είναι τέλειο τετράγωνο. Οπότε εφαρμόζοντας ξανά το θεώρημα 5.4.14, δείχνουμε ότι ο $\mathcal{J}(\tau)$ είναι ακέραιος αλγεβρικός αριθμός, γεγονός που ολοκληρώνει την απόδειξη του θεωρήματος 5.4.8. □

Παραδειγμα 5.4.15. Μερικά παραδείγματα[6] υπολογισμού της $\mathcal{J}$-αναλλοιώτου μιγαδικών αριθμών

[6]Για περισσότερα παραδείγματα βλ. [4], σελ.383.

που ανήκουν στο $\mathcal{H}$ είναι:

$$\begin{aligned}
\mathcal{J}\big((1+\sqrt{-3})/2\big) &= 0 = 1728 - 3\cdot 24^2 \\
\mathcal{J}(i) &= 1728 = 1728 - 4\cdot 0^2 \\
\mathcal{J}\big((1+\sqrt{-7})/2\big) &= -3375 = (-15)^3 = 1728 - 7\cdot 27^2 \\
\mathcal{J}(\sqrt{-2}) &= 8000 = 20^3 = 1728 + 8\cdot 28^2 \\
\mathcal{J}\big((1+\sqrt{-11})/2\big) &= -32768 = (-32)^3 = 1728 - 11\cdot 56^2 \\
\mathcal{J}\big((1+\sqrt{-19})/2\big) &= -884736 = (-96)^3 = 1728 - 19\cdot 216^2 \\
\mathcal{J}\big((1+\sqrt{-43})/2\big) &= -884736000 = (-960)^3 = 1728 - 43\cdot 4536^2 \\
\mathcal{J}\big((1+\sqrt{-163})/2\big) &= -262537412640768000 = (-640320)^3 = 1728 - 163\cdot 40133016^2.
\end{aligned}$$

Μια πρόχειρη ματιά στις τιμές της $\mathcal{J}$-αναλλοιώτου οδηγούν σε κάποιες γενικές παρατηρήσεις. Αρχικά, παρατηρούμε ότι κάποιες τιμές από αυτές είναι τέλειοι κύβοι. Μία άλλη παρατήρηση είναι ότι η συνάρτηση $\mathcal{J}(\tau) - 1728$ είναι τέλειο τετράγωνο του τετραγωνικού μιγαδικού σώματος αριθμών στο οποίο ανήκει το τ. Οι παρατηρήσεις αυτές, με την υπόθεση κάποιων απαραίτητων συνθηκών, πράγματι αληθεύουν και έχουν αποδειχθεί από τους Gross και Zagier.

Κεφάλαιο 6

Το "Jugendtraum" του Kronecker

6.1 Ιστορική αναφορά

Το νεανικό όνειρο ή "Jugendtraum" του Kronecker αποτελεί ένα σημείο αναφοράς στη θεωρία του μιγαδικού πολλαπλασιασμού και για το λόγο αυτό το μελετάμε. Η έρευνα του Kronecker, πέραν της θεωρίας αριθμών, της θεωρίας των ελλειπτικών συναρτήσεων, της αλγεβρικής γεωμετρίας και πολλών άλλων κλάδων των μαθηματικών, είχε επικεντρωθεί και στη θεωρία τη μιγαδικού πολλαπλασιασμού, στην οποία συνέβαλε ουσιαστικά αποδεικνύοντας βασικά αποτελεσμάτων αυτής αλλά και διατυπώνοντας νέες ιδέες.

Στις 15 Μαρτίου, το 1880, σε γράμμα του στον Dedekind, αναφέρεται στα πρόσφατα επιτεύγματά του στην ανάπτυξη της θεωρίας του μιγαδικού πολλαπλασιασμού. Ιδιαιτέρως, πληροφορεί τον Dedekind ότι έχει καταφέρει να ξεπεράσει και τις τελευταίες δυσκολίες που έχει προκειμένου να ολοκληρώσει την έρευνά του, με την οποία έχει προσφάτως καταπιαστεί. Ύστερα γράφει:

"Es handelt sich um mein liebsten Jugendtraum, nämlich um den Nachweiss, dass die Abel'schen Gleickungen mit Quadratwurzeln rationalbar Zahlen durch Transformations-Gleickungen elliptischer Functionen mit singularen Moduln gerade so erschöpft werden, wie die ganzzahligen Abel'schen Gleickungen durch Kreistheilungs gleichungen".

"Πρόκειται για το πιο πολυπόθητο όνειρο της νεότητός μου, δηλαδή να αποδείξω ότι αβελιανές εξισώσεις με ρητές τετραγωνικές ρίζες ανάγονται σε μετασχηματισμούς ελλειπτικών συναρτήσεων με ιδιάζοντα moduli, ακριβώς όπως στην περίπτωση αναγωγής ακέραιων αβελιανών εξισώσεων σε κυκλοτομικές εξισώσεις".

Το Jugendtraum του Kronecker αναφέρεται στην επίτευξη της κατασκευής όλων των αβελιανών επεκτάσεων ενός τετραγωνικού μιγαδικού αλγεβρικού σώματος αριθμών, επισυνάπτοντας συγκεκριμένες τιμές συγκεκριμένων υπερβατικών συναρτήσεων σε τυχόντα αλγεβρικά σώματα αριθμών. Πρέπει να σημειώσουμε σε αυτό το σημείο ότι στη γενικότητά του το πρόβλημα του Jugendtraum είναι ακόμα υπό έρευνα.

Για περισσότερες πληροφορίες περί ιστορικών στοιχείων καθώς και για τα αποτελέσματα που ακολούθησαν και σχετίζονται με το Jugendtraum παραπέμπουμε στο [14], στη σελίδα 78.

6.2 Εισαγωγικά στοιχεία

Θεωρούμε την ελλειπτική καμπύλη E με μιγαδικό πολλαπλασιασμό. Τότε υπάρχει ένας μιγαδικός αριθμός $\tau \in \mathcal{H}$ τέτοιος, ώστε το $L := \mathbb{Z} + \tau\mathbb{Z}$ να είναι ένα κιγκλίδωμα του $\mathbb{C}$ και να ισχύει ότι

$$E \cong \mathbb{C}/L.$$

Σύμφωνα με το πόρισμα 5.4.7, το $\mathbb{Q}(\tau)$ είναι τετραγωνικό σώμα αριθμών. Μάλιστα, ο δακτύλιος των ενδομορφισμών $End_{\mathbb{C}}(E)$ είναι ισόμορφος με μία τάξη, έστω O, του σώματος $\mathbb{Q}(\tau)$. Σε αυτή την περίπτωση θα λέμε ότι η ελλειπτική καμπύλη E έχει μιγαδικό πολλαπλασιασμό από την O. Ιδιαίτερα, εάν ισχύει ότι $End_{\mathbb{C}}(E) \cong R_K$, τότε θα λέμε ότι η ελλειπτική καμπύλη έχει μιγαδικό πολλαπλασιασμό από το δακτύλιο των ακέραιων αλγεβρικών του K.

Στα πλαίσια της μελέτης μας προτιμούμε, αντί να κάνουμε λόγο για ελλειπτική καμπύλη, να ορίσουμε μία σχέση ισοδυναμίας, η οποία διαμερίζει το σύνολο όλων των ελλειπτικών καμπυλών σε κλάσεις, και να αναφερόμαστε σε αντιπρόσωπο μιας εκ των κλάσεων. Επί τη βάσει αυτής της ιδέας θα ταυτίζουμε την ελλειπτική καμπύλη με την κλάση ισοδυναμίας στην οποία ανήκει. Για να γίνει αυτό, πρέπει να ορίσουμε την έννοια των ισόμορφων ελλειπτικών καμπυλών.

Ορισμος 6.2.1. Οι ελλειπτικές καμπύλες $E_1 \cong \mathbb{C}/L_1$ και $E_2 \cong \mathbb{C}/L_2$ καλούνται *ισόμορφες* όταν τα κιγκλιδώματα L_1 και L_2 είναι ομοθετικά, ήτοι όταν υπάρχει $\gamma \in \mathbb{C}^\times$ με την ιδιότητα $L_2 = \gamma L_1$.

Ο ισομορφισμός ελλειπτικών καμπυλών είναι σχέση ισοδυναμίας, την οποία θα την συμβολίζουμε ως $\sim_{\text{ισομ.}}$. Με άλλα λόγια,

$$E_1 \sim_{\text{ισομ.}} E_2 \Leftrightarrow \mathbb{C}/L_1 \sim_{\text{ισομ.}} \mathbb{C}/L_2 \Leftrightarrow \exists\, \gamma \in \mathbb{C}^\times : L_2 = \gamma L_1.$$

Συμβολίζουμε ως $Ell(\mathbb{C})$ το σύνολο όλων των ελλειπτικών καμπυλών υπεράνω του σώματος $\mathbb{C}$. Έτσι, εάν θέσουμε

$$\mathfrak{Ell}(R_K) := \{E \in Ell(\mathbb{C}) \mid End_{\mathbb{C}}(E) \cong R_K\}/\sim_{\text{ισομ.}},$$

όπου το K είναι ένα τετραγωνικό μιγαδικό σώμα αριθμών, τότε το σύνολο $\mathfrak{Ell}(R_K)$ αποτελείται από όλες τις κλάσεις ισομορφίας ελλειπτικών καμπυλών με δακτύλιο ενδομορφισμών το δακτύλιο των ακέραιων αλγεβρικών αριθμών του K. Κι εφόσον έχουμε ταυτίσει τις ελλειπτικές καμπύλες με τους μιγαδικούς τόρους της μορφής $\mathbb{C}/L$, όπου το L είναι ένα μοναδικό μέχρις ομοθεσίας κιγκλίδωμα του $\mathbb{C}$, και γνωρίζουμε ότι η ομοθεσία κιγκλιδωμάτων είναι σχέση ισοδυναμίας, την οποία συμβολίζουμε ως $\sim_{\text{ομοθ.}}$, λαμβάνουμε ένα ακόμα χαρακτηρισμό για το σύνολο $\mathfrak{Ell}(R_K)$, ο οποίος είναι ο εξής:

$$\mathfrak{Ell}(R_K) = \{L \text{ κιγκλίδωμα του } \mathbb{C} \mid End_{\mathbb{C}}(\mathbb{C}/L) \cong R_K\}/\sim_{\text{ομοθ.}}$$

Συνεπώς, θα ταυτίζουμε την ελλειπτική καμπύλη $E \cong \mathbb{C}/L$ με την κλάση της $[E] \in \mathfrak{Ell}(R_K)$, ή την κλάση $[L] \in \mathfrak{Ell}(R_K)$, ανάλογα με το αν κάνουμε λόγο για ελλειπτικές καμπύλες ή μιγαδικούς τόρους.

6.3 Το βασικό θεώρημα

Το βασικό θεώρημα αυτής της παραγράφου, καθώς και ολόκληρης της παρούσας πτυχιακής εργασίας, προσδιορίζει πλήρως το σώμα του Hilbert, το οποίο μελετήσαμε στο τρίτο κεφάλαιο, ενός τετραγωνικού μιγαδικού σώματος αριθμών.

Θεωρημα 6.3.1. *Έστω K ένα τετραγωνικό μιγαδικό αριθμητικό σώμα με δακτύλιο ακέραιων αλγεβρικών το R_K και $E|_{\mathbb{C}}$ μία ελλειπτική καμπύλη με μιγαδικό πολλαπλασιασμό από το δακτύλιο R_K. Τότε το $K(\mathcal{J}(E))$ είναι το σώμα κλάσεων Hilbert του K, ήτοι $\mathscr{H}_K = K(\mathcal{J}(E))$. Μάλιστα, ισχύει ότι*

$$[K(\mathcal{J}(E) : K)] = [\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] = h_K,$$

όπου ως h_K συμβολίζουμε τον αριθμό κλάσεων ιδεωδών του σώματος K.

Παρατηρηση 6.3.2. Πρέπει σε αυτό το σημείο να τονίσουμε ότι το θεώρημα 6.3.1 απαντάει στο ερώτημα που έχουμε εξ αρχής θέσει, αλλά δε συναντάται όπως παραπάνω. Πληρέστερη διατύπωση και απόδειξη υπάρχει στο [12] (βλ. σελ. 122, Θεωρ. 4.3.).

ΠΑΡΑΤΗΡΗΣΗ 6.3.3. Το θεώρημα 6.3.1 απαιτεί την κατασκευή ελλειπτικής καμπύλης με μιγαδικό πολλαπλασιασμό από τον R_K. Από αυτό συνεπάγεται άμεσα ότι εάν ο δακτύλιος R_K ειδωθεί ως κιγκλίδωμα του $\mathbb{C}$, το οποίο είναι εφικτό καθώς το K είναι τετραγωνικό σώμα αριθμών και ο R_K είναι ένα ελεύθερο $\mathbb{Z}$-module βαθμίδας ίσης με 2, τότε η ελλειπτική καμπύλη είναι η $E \cong \mathbb{C}/R_K$. Εάν υποθέσουμε ότι $R_K = \langle 1, \omega \rangle$, όπου

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

τότε

$$\mathcal{J}(E) = \mathcal{J}(E/R_K) = \mathcal{J}(\omega).$$

Επομένως, το πρόβλημά μας ανάγεται στην κατασκευή ελλειπτικής καμπύλης με δοθείσα $\mathcal{J}$-αναλλοίωτο καθότι γνωρίζουμε το ω. Υποθέτουμε, λοιπόν, ότι $\mathcal{J}(E) = j$, όπου το j είναι γνωστό. Εάν $j = 0$, τότε η ελλειπτική καμπύλη είναι η

$$E|_{\mathbb{C}} \ : \ Y^2 = 4X^3 - g_3,$$

για τυχόν $g_3 \neq 0$, ενώ αν $j = 1728$, η ζητούμενη ελλειπτική καμπύλη είναι η

$$E|_{\mathbb{C}} \ : \ Y^2 = 4X^3 - g_2 X,$$

για αυθαίρετο $g_2 \neq 0$. Σε κάθε άλλη περίπτωση, ήτοι όταν $j \neq 0, 1728$, θεωρούμε την ελλειπτική καμπύλη

$$E|_{\mathbb{C}} \ : \ Y^2 = 4X^3 - \frac{3j}{j-1728}X - \frac{j}{j-1728},$$

για την οποία εύκολα μπορούμε να ελέγξουμε ότι ισχύει η ισότητα $\mathcal{J}(E) = j$.

Στο υπόλοιπο της παραγράφου θα ασχοληθούμε με την απόδειξη του θεωρήματος 6.3.1.

Αποδεικνύεται ότι (βλ. [12], σελ.104, Πρ. 2.1(a)) εάν ο σ είναι ένας αυτομορφισμός του $\mathbb{C}$ και η E είναι μία ελλειπτική καμπύλη ορισμένη υπεράνω του $\mathbb{C}$, τότε ισχύει ότι

$$End_{\mathbb{C}}(E^\sigma) \cong End_{\mathbb{C}}(E),$$

όπου ως E^σ συμβολίζουμε την εικόνα της ελλειπτικής καμπύλης E μέσω του αυτομορφισμού σ. Ακόμα, μπορούμε να δείξουμε (βλ. [12], σελ.104, Πρ. 2.1(c)) ότι για το σύνολο $\mathfrak{Ell}(R_K)$, όπως αυτό ορίστηκε στην παράγραφο 6.2, ισχύει ότι

$$\mathfrak{Ell}(R_K) = \frac{\{ \text{ Ελλειπτικές καμπύλες υπεράνω του } \tilde{\mathbb{Q}} \mid End_{\tilde{\mathbb{Q}}}(E) \cong R_K \}}{\text{ισομορφισμοί του } \tilde{\mathbb{Q}}}.$$

Έτσι, ταυτίζουμε το σύνολο $\mathfrak{Ell}(R_K)$ με το σύνολο όλων των $\tilde{\mathbb{Q}}$-κλάσεων ισομορφίας ελλειπτικών καμπυλών με μιγαδικό πολλαπλασιαμό.

Εάν συμβολίσουμε ως $\bar{K}$ την αλγεβρική θήκη του τετραγωνικού μιγαδικού σώματος αριθμών K, τότε η ομάδα $Gal(\bar{K}/K)$ δρα στο σύνολο $\mathfrak{Ell}(R_K)$ ως εξής:

$$\sigma([E]) = [E^\sigma].$$

ΠΑΡΑΤΗΡΗΣΗ 6.3.4. Πρέπει να σημειώσουμε εδώ, ότι η επέκταση $\bar{K}/K$ είναι άπειρη. Αυτό σημαίνει ότι για να ισχύει κάποιο θεώρημα, αντίστοιχο με αυτό του θεμελιώδους θεωρήματος της θεωρίας Galois, πρέπει να ορίσουμε μία νέα τοπολογία και να κάνουμε λόγο για κλειστές και ανοιχτές ομάδες της $Gal(\bar{K}/K)$. Σε ό,τι αφορά στη δική μας μελέτη δε θα επεκταθούμε περαιτέρω σε στοιχεία άπειρης θεωρίας Galois καθότι δεν επηρεάζουν την ισχύ των αποτελεσμάτων.

Θεωρούμε, τώρα, ένα ιδεώδες A του K. Τότε αυτό ορίζει ένα κιγκλίδωμα στο $\mathbb{C}$. Το γεγονός αυτό προκύπτει άμεσα από το ότι στην περίπτωση των τετραγωνικών μιγαδικών σωμάτων αριθμών τα ιδεώδη αυτών είναι ελεύθερα $\mathbb{Z}$-module βαθμίδας ίσης με 2. Συνεπώς, μπορούμε να ορίσουμε μία ελλειπτική καμπύλη, έστω E_A, η οποία να έχει ως δακτύλιο ενδομορφισμών τον

$$\begin{aligned} End_{\mathbb{C}}(E_A) &= \{\beta \in \mathbb{C} \mid \beta A \subseteq A\} \\ &= \{\beta \in K \mid \beta A \subseteq A\} \\ &= R_K, \end{aligned}$$

αφού $A \subseteq K$. Με άλλα λόγια, το κλασματικό ιδεώδες A του K ορίζει μία ελλειπτική καμπύλη με μιγαδικό πολλαπλασιασμό από τον R_K. Από την άλλη, εφόσον ομοθετικά κιγκλιδώματα ορίζουν ισόμορφες ελλειπτικές καμπύλες, τα ιδεώδη A και cA, όπου $c \in K^{\times}$ ορίζουν ισόμορφες ελλειπτικές καμπύλες, ήτοι

$$E_A \cong E_{cA}.$$

Η παρατήρηση αυτή μας υποδεικνύει να μελετήσουμε τα στοιχεία της ομάδας κλάσεων ιδεωδών $Cl(K)$. Προς τούτο, ορίζουμε την απεικόνιση

$$Cl(K) \longrightarrow \mathfrak{Ell}(R_K) \ , \ [A] \longmapsto E_A.$$

Γενικότερα, εάν το L είναι ένα κιγκλίδωμα του $\mathbb{C}$, τέτοιο ώστε $[L] \in \mathfrak{Ell}(R_K)$ και το A είναι ένα κλασματικό ιδεώδες του τετραγωνικού μιγαδικού σώματος αριθμών K, τότε ορίζουμε

$$AL := \{\sum_{\pi\varepsilon\pi.} \alpha_i\lambda_i \mid \alpha_i \in A \ , \ \lambda_i \in L\}.$$

Πρόταση 6.3.5. *(1) Έστω L ένα κιγκλίδωμα τέτοιο, ώστε $[L] \in \mathfrak{Ell}(R_K)$, και έστω A και B δύο κλασματικά ιδεώδη του K. Τότε*

(i) το AL είναι κιγκλίδωμα του $\mathbb{C}$,

(ii) για την ελλειπτική καμπύλη E_{AL} ισχύει ότι $End_{\mathbb{C}}(E_{AL}) \cong R_K$ και

(iii) $E_{AL} \cong E_{BL}$ εάν, και μόνο εάν $[A] = [B]$ στην ομάδα $Cl(K)$.

Συνεπώς, υπάρχει μία καλώς ορισμένη δράση της ομάδας $Cl(K)$ στο σύνολο $\mathfrak{Ell}(R_K)$, η οποία ορίζεται ως εξής:

$$[A] * E_L = E_{A^{-1}L}.$$

(2) Η δράση που περιγράφηκε στο (1) είναι απλά μεταβατική δράση. Ιδιαίτερα, ισχύει ότι

$$h_K = \#(Cl(K)) = \#(\mathfrak{Ell}(R_K)).$$

Απόδειξη.

(1) (i) Εξ υποθέσεως ισχύει ότι $End_{\mathbb{C}}(E_L) = R_K$, άρα $R_K L = L$. Επιλέγουμε έναν αριθμό $d \in \mathbb{Z}^{\times}$ τέτοιον, ώστε $dA \subseteq R_K$. Η επιλογή αυτή είναι εφικτή επί τη βάσει του ορισμού του κλασματικού ιδεώδους. Τότε

$$dAL \subseteq R_K L = L \Rightarrow AL \subseteq \frac{1}{d}L,$$

άρα το AL είναι ένα διακριτή υποομάδα του $\mathbb{C}$, εφόσον το $(1/d)L$ είναι. Επίσης, υπάρχει ένας ακέραιος αριθμός $d_1 \neq 0$, τέτοιος ώστε $d_1 R_K \subseteq A$. Άρα έχουμε ότι

$$d_1 R_K L \subseteq AL \Rightarrow d_1 L \subseteq AL.$$

Όμως εφόσον το L είναι κιγκλίδωμα, τότε και το $d_1 L$ θα είναι. Αυτό σημαίνει ότι αν $d_1 L = \langle 1, \omega, \rangle$, τότε $\mathbb{R} + \omega\mathbb{R} = \mathbb{C}$. Κι αφού ισχύει ότι $d_1 L \subseteq AL$, τότε και το αυτό ισχύει και για το AL.

(ii) Αν $\beta \in \mathbb{C}^{\times}$ και A είναι ένα κλασματικό ιδεώδες του , έχουμε ότι

$$\beta AL \subseteq AL \Leftrightarrow A^{-1}\beta AL \subseteq A^{-1}AL \Leftrightarrow \beta L \subseteq L.$$

Συνεπώς,

$$End_{\mathbb{C}}(E_{AL}) = \{\beta \in \mathbb{C} \mid \beta AL \subseteq AL\} = \{\beta \in \mathbb{C} \mid \beta L \subseteq L\} = R_K.$$

(iii) Η κλάση ισομορφίας της ελλειπτική καμπύλης E_{AL} προσδιορίζεται επακριβώς από την κλάση ομοθεσίας του κιγκλιδώματος AL. Έτσι,

$$E_{AL} \cong E_{BL} \Leftrightarrow \exists\, \gamma \in \mathbb{C}^{\times} : AL = \gamma BL \Rightarrow L = \gamma A^{-1}BL.$$

Ομοίως, πολλαπλασιάζοντας με $\gamma^{-1}AB^{-1}$, έπεται ότι

$$L = \gamma^{-1}AB^{-1}L.$$

Αυτό σημαίνει ότι τα ιδεώδη $\gamma A^{-1}B$ και $\gamma^{-1}AB^{-1}$ αφήνουν αναλλοίωτο το κιγκλίδωμα L. Επομένως,

$$\gamma^{-1}AB^{-1} = R_K \Rightarrow A = \gamma B,$$

από το οποίο προκύπτει άμεσα ότι $\gamma \in K$ και $[A] = [B]$ στην ομάδα $Cl(K)$. Έτσι, ολοκληρώνεται η απόδειξη του (iii).

Για να ελέγξουμε ότι πράγματι η

$$[A] * E_L = E_{A^{-1}L}$$

είναι δράση της ομάδας $Cl(K)$ στην $\mathfrak{Ell}(R_K)$ κάνουμε την εξής παρατήρηση:

$$[A] * ([B] * E_L) = [A] * E_{A^{-1}L} = E_{A^{-1}(B^{-1}L)} = E_{(AB)^{-1}L} = ([A][B]) * E_L.$$

(2) Θεωρούμε δυο ελλειπτικές καμπύλες E_{L_1} και E_{L_2} στο $\mathfrak{Ell}(R_K)$. Για να δείξουμε ότι η ομάδα κλάσεων ιδεωδών του K δρα μεταβατικά στο σύνολο $\mathfrak{Ell}(R_K)$ πρέπει να βρούμε ένα κλασματικό ιδεώδες A, με την ιδιότητα

$$[A] * E_{L_1} = E_{L_2}.$$

Προς τούτο, επιλέγουμε ένα μη μηδενικό αριθμό $\lambda_1 \in L_1$ και ορίζουμε το ιδεώδες του K,

$$A_1 := \frac{1}{\lambda_1}L_1.$$

Τότε αυτό είναι ένα πεπερασμένα παραγόμενο R_K-module. Ομοίως για ένα αυθαίρετα επιλεγμένο μη μηδενικό αριθμό $\lambda_2 \in L_2$ ορίζουμε το ιδεώδες

$$A_2 := \frac{1}{\lambda_2}L_2.$$

Τότε

$$\frac{\lambda_2}{\lambda_1}A_2{A_1}^{-1}L_1 = L_2.$$

Θέτοντας $A := {A_2}^{-1}A_1$, λαμβάνουμε ότι

$$[A] * E_{L_1} = E_{A^{-1}L_1} = E_{(\lambda_1/\lambda_2)L_2} \cong E_{L_2}.$$

Για να δείξουμε, τώρα, ότι η εν λόγω δράση είναι απλά μεταβατική τότε πρέπει να αποδείξουμε ότι ισχύει η συνεπαγωγή

$$A * E_L = B * E_L \Rightarrow [A] = [B],$$

το οποίο προκύπτει άμεσα από το (ii) του (1).

□

Όπως αναφέρθηκε ήδη, ταυτίζουμε το σύνολο $\mathfrak{Ell}(R_K)$ με το σύνολο όλων των κλάσεων $\tilde{\mathbb{Q}}$-ισομορφίας ελλειπτικών καμπυλών ορισμένων υπεράνω του $\tilde{\mathbb{Q}}$, οι οποίες έχουν μιγαδικό πολλαπλασιασμό από τον R_K. Έτσι, μπορούμε να ορίσουμε μία δράση της ομάδας $Gal(\bar{K}/K)$ στο σύνολο $\mathfrak{Ell}(R_K)$, στέλνοντας τον αυτομορφισμό $\sigma \in Gal(\bar{K}/K)$ στην κλάση ισομορφίας που ανήκει η E^σ στο σύνολο $\mathfrak{Ell}(R_K)$. Η παραπάνω πρόταση μας πληροφορεί ότι η δράση της ομάδας $Cl(K)$ στο σύνολο $\mathfrak{Ell}(R_K)$ είναι απλά μεταβατική, ήτοι για οποιοδήποτε αυτομορφισμό σ του $\mathbb{C}$, μπορούμε να βρούμε ένα μοναδικό στοιχείο $[A]$ της ομάδας κλάσεων ιδεωδών $Cl(K)$, με την ιδιότητα

$$[A] * E = E^\sigma.$$

Η κλάση $[A]$ προφανώς εξαρτάται από την επιλογή του αυτομορφισμού σ. Αυτό σημαίνει ότι υπάρχει μία καλά ορισμένη απεικόνιση

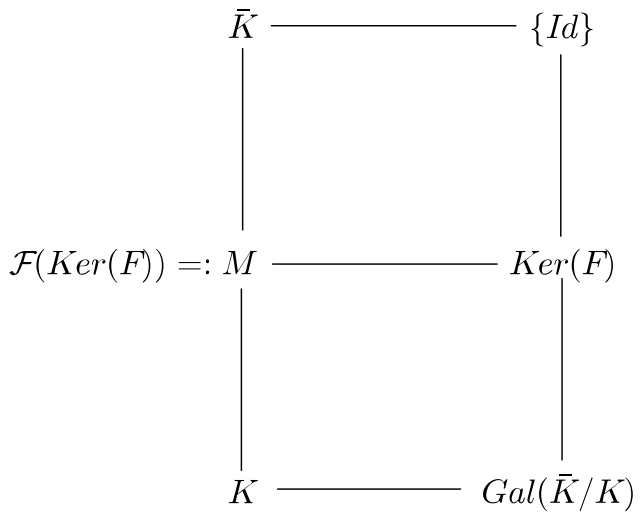
$$F : Gal(\bar{K}/K) \longrightarrow Cl(K),$$

η οποία προσδιορίζεται μέσω της σχέσης

$$E^\sigma = F(\sigma) * E \, , \forall \, \sigma \in Gal(\bar{K}/K).$$

Μελετώντας την απεικόνιση F θα διαπιστώσουμε ότι αυτή μπορεί να περιγράψει πλήρως το σώμα $K(\mathcal{J}(E))$. Εύκολα μπορούμε να αποδείξουμε ότι η F είναι ομομορφισμός ομάδων. Ακόμα, αποδεικνύεται ότι η F είναι ανεξάρτητη από την επιλογή της ελλειπτικής καμπύλης E.

Θέτουμε $M := \mathcal{F}(Ker(F))$, ήτοι το M είναι το σώμα σταθερών σημείων της υποομάδας $Ker(F)$ της $Gal(\bar{K}/K)$.



Τότε έχουμε ότι

$$\begin{aligned} Gal(\bar{K}/M) &= Ker(F) \\ &= \{\sigma \in Gal(\bar{K}/K) : F(\sigma) = 1_{Cl(K)}\} \\ &= \{\sigma \in Gal(\bar{K}/K) : F(\sigma) * E = E\} \quad \text{,σύμφωνα με την πρόταση 6.3.5(2)} \\ &= \{\sigma \in Gal(\bar{K}/K) : E^{\sigma} = E\} \\ &= \{\sigma \in Gal(\bar{K}/K) : \mathcal{J}(E^{\sigma}) = \mathcal{J}(E)\} \\ &= \{\sigma \in Gal(\bar{K}/K) : \mathcal{J}(E)^{\sigma} = \mathcal{J}(E)\} \\ &= Gal\big(\bar{K}/K(\mathcal{J}(E))\big). \end{aligned}$$

Από την ισότητα

$$Gal(\bar{K}/M) = Gal\big(\bar{K}/K(\mathcal{J}(E))\big)$$

έπεται ότι

$$M = K(\mathcal{J}(E)).$$

Πράγματι, οι ομάδες $Gal(\bar{K}/M)$ και $Gal\big(\bar{K}/K(\mathcal{J}(E))\big)$ είναι ανοιχτά σύνολα της τοπολογίας Krull, άρα είναι και κλειστά. Κι εφόσον οι επεκτάσεις M/K και $K(\mathcal{J}(E))/K$ είναι πεπερασμένες τότε η ισότητα $M = K(\mathcal{J}(E))$ προκύπτει άμεσα από το θεμελιώδες θεώρημα της θεωρίας Galois για άπειρες επεκτάσεις (βλ. [10], σελ.159, Θεωρ. 17.8). Ακόμα, εφόσον ισχύει ότι

$$Gal(M/K) \cong Gal(\bar{K}/K)/Ker(F),$$

η ομάδα $Gal(M/K)$ εμφυτεύεται στην αβελιανή ομάδα $Cl(K)$. Κατά συνέπεια η επέκταση $M = K(\mathcal{J}(E))$ είναι αβελιανή επέκταση του K.

Θεωρούμε τώρα τον οδηγό $\mathfrak{f} := \mathfrak{f}_{M/K}$ της επέκτασης M/K, όπως αυτός ορίστηκε στο θεώρημα 3.4.12 και την απεικόνιση $\Phi_{\mathfrak{f}} := \Phi_{M/K,\mathfrak{f}}$ του Artin. Σε αυτό το σημείο παρατηρούμε ότι

$$F\left(\left(\frac{M/K}{A}\right)\right) = \langle 1\rangle \text{ , } \forall\, A \in P_{K,1}(\mathfrak{f}).$$

Γνωρίζουμε ότι

$$P_{K,1}(\mathfrak{f}) = \{\langle\alpha\rangle \mid \alpha \in K^{\times} \text{ και } \alpha \equiv 1 \pmod{\mathfrak{f}}\} \subseteq Ker(\Phi_{\mathfrak{f}}).$$

Ισχυριζόμαστε, τώρα, ότι η σύνθεση $F \circ \Phi_{\mathfrak{f}}$ είναι η φυσική προβολή του $I_K(\mathfrak{f})$ στην ομάδα $Cl(K)$, ήτοι ότι ισχύει

$$(F \circ \Phi_{\mathfrak{f}})(A) = [A] \text{ , } \forall\, A \in I_K(\mathfrak{f}).$$

Για την απόδειξη του ισχυρισμού αυτού θα χρειαστούμε την παρακάτω πρόταση.

Πρόταση 6.3.6. *Υπάρχει ένα πεπερασμένο σύνολο πρώτων αριθμών $S \subseteq \mathbb{Z}$ τέτοιο, ώστε για κάθε πρώτο $p \notin S$, ο οποίος αναλύεται (πλήρως) στο K, έστω $pR_K = PP'$, να ισχύει ότι*

$$F\left(\left[\frac{L/K}{P}\right]\right) = [P] \in Cl(K).$$

Απόδειξη. (βλ. [12],σελ.122. Πρ. 4.2.) □

Ακόμα, θα χρειαστούμε το παρακάτω θεώρημα:

Θεώρημα 6.3.7 (Dirichlet)**.** *Έστω τετραγωνικό μιγαδικό σώμα αριθμών K κι ένα modulus $\mathfrak{m}$ αυτού. Τότε η γενικευμένη ομάδα κλάσεων ιδεωδών $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ περιέχει άπειρους στο πλήθος πρώτους του K, οι οποίοι έχουν βαθμό αδρανείας ίσο με* 1.

Θεωρούμε το σύνολο S της προτάσεως 6.3.6. Σύμφωνα με το θεώρημα του Dirichlet υπάρχει ένα πρώτο ιδεώδες $P \in I_K(\mathfrak{f})$, το οποίο ανήκει στην ίδια κλάση με το A και έχει βαθμό αδρανείας ίσο με 1, με την ιδιότητα $P \notin S$. Δηλαδή, υπάρχει ένα $\alpha \in K^\times$ τέτοιο, ώστε

$$\alpha \equiv 1 \pmod{\mathfrak{f}} \text{ και } A = \langle\alpha\rangle P.$$

Υπολογίζουμε, τώρα, τη σύνθεση $F \circ \Phi_\mathfrak{f}$:

$$(F \circ \Phi_\mathfrak{f})(A) = F\left(\left(\frac{M/K}{A}\right)\right) = F\left(\left(\frac{M/K}{\langle\alpha\rangle P}\right)\right) = F\left(\left(\frac{M/K}{\langle\alpha\rangle}\right)\left(\frac{M/K}{P}\right)\right) =$$

$$F\left(\left(\frac{M/K}{P}\right)\right) = [P].$$

Όμως

$$A = \langle\alpha\rangle P \Rightarrow [A] = [P]$$

στην ομάδα $Cl(K)$. Οπότε, έχουμε ότι

$$(F \circ \Phi_\mathfrak{f})(A) = [A].$$

Άμεση συνέπεια αυτού είναι ότι

$$(F \circ \Phi_\mathfrak{f})(A) = 1_{Cl(K)}\,, \forall\, A \in P_{K,1}(\mathfrak{f}).$$

Επομένως, έχουμε ότι

$$P_{K,1}(1) = P_{K,1}(\langle 1\rangle) = P_K = \{\langle\alpha\rangle \mid \alpha \in K^\times\} \subseteq Ker(\Phi_\mathfrak{f}).$$

Αυτό σημαίνει ότι $R_K = \langle 1\rangle \subseteq \mathfrak{f}$, σύμφωνα με το θεώρημα του οδηγού, ήτοι το 3.4.12. Όμως, αφού το K είναι τετραγωνικό μιγαδικό αριθμητικό σώμα, το $\mathfrak{f}$ δεν έχει ως παράγοντες άπειρους πρώτους του K. Επομένως, το $\mathfrak{f}$ είναι ακέραιο ιδεώδες του R_K, ήτοι $\mathfrak{f} \subseteq R_K$. Άρα, τελικά, ισχύει ότι

$$\mathfrak{f} = \langle 1\rangle = R_K.$$

Αυτό σημαίνει ότι η επέκταση M/K είναι μη διακλαδιζόμενη, άρα το $M = K(\mathcal{J}(E))$ περιέχεται στο σώμα του Hilbert του τετραγωνικού μιγαδικού σώματος αριθμών K, ήτοι στο $\mathscr{H}_K$.

Ο φυσικός επιμορφισμός ι που ορίζεται από την ομάδα $I_K = I_K(\langle 1\rangle)$ στην πηλικοομάδα $I_K/P_K = I_K(\langle 1\rangle)/P_{K,1}(\langle 1\rangle)$ ορίζεται ως εξής:

$$\begin{array}{rcl} \iota & : & I_K \longrightarrow Cl(K) \\ & & A \longmapsto [A]. \end{array}$$

Ο ισχυρισμός που αποδείξαμε ανωτέρω ουσιαστικά μας πληροφορεί ότι

$$\iota = F \circ \Phi_\mathfrak{f}.$$

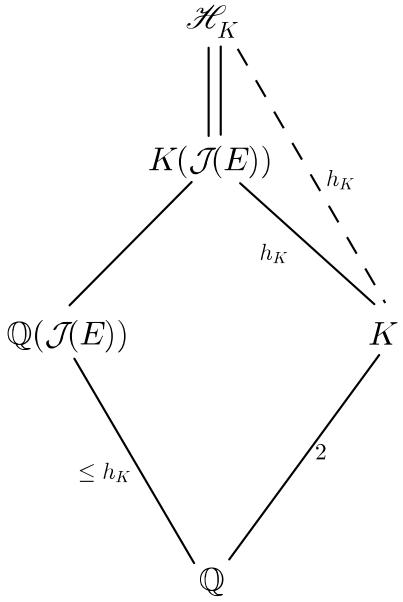
Κι εφόσον ο ι είναι επιμορφισμός, το αυτό θα ισχύει και για την F. Όμως αν ορίσουμε τον F εκ νέου, με πεδίο τιμών την ομάδα $Gal(M/K)$, τότε είναι και μονομορφισμός. Κατά συνέπεια ο F είναι ισομορφισμός. Άρα έχουμε ότι

$$Gal(M/K) \cong Cl(K) \Rightarrow [M : K] = \#(Gal(M/K)) = \#Cl(K) = h_K.$$

Άρα

$$[M : K] = [\mathscr{H}_K : K].$$

Κι αφού $M = K(\mathcal{J}(E)) \subseteq \mathscr{H}_K$, τότε $\boxed{\mathscr{H}_K = K(\mathcal{J}(E))}$. Άρα ισχύει και ότι $[K(\mathcal{J}(E) : K)] = h_K$.



Θα δείξουμε, τώρα, ότι $[\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] = h_k$. Έχουμε δει ότι για κάθε αυτομορφισμό σ του $\mathbb{C}$ ισχύει ότι

$$\mathcal{J}(E^\sigma) = \mathcal{J}(E)^\sigma.$$

Μάλιστα, εάν $End_{\mathbb{C}}(E) \cong R_K$, τότε και

$$End_{\mathbb{C}}(E^\sigma) \cong End_{\mathbb{C}}(E) \cong R_K.$$

Επομένως, η ελλειπτική καμπύλη E^σ ανήκει σε μία από της κλάσεις ισομορφίας του $\mathfrak{Ell}(R_K)$. Συνεπώς

$$[\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] \leq \#\big(\mathfrak{Ell}(R_K)\big) = h_K.$$

Το K είναι τετραγωνικό σώμα αριθμών, άρα $[K : \mathbb{Q}] = 2$. Συνεπώς, λόγω της πολλαπλασιαστικότητας των βαθμών, ισχύει ότι

$$[K(\mathcal{J}(E)) : \mathbb{Q}] = [K(\mathcal{J}(E)) : K][K : \mathbb{Q}] = 2h_K.$$

Όμως

$$[K(\mathcal{J}(E)) : \mathbb{Q}] = [K(\mathcal{J}(E)) : \mathbb{Q}(\mathcal{J}(E))][\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}].$$

Ακόμα έχουμε ότι

$$[K : \mathbb{Q}] = 2 \Rightarrow [K(\mathcal{J}(E)) : \mathbb{Q}(\mathcal{J}(E))] \leq 2.$$

Αν ισχύει ότι $[K(\mathcal{J}(E)) : \mathbb{Q}(\mathcal{J}(E))] = 1$, τότε $[\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] = 2h_K$. Αυτό αντίκειται στην ανισότητα $[\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] \leq h_K$. Άρα $[K(\mathcal{J}(E)) : \mathbb{Q}(\mathcal{J}(E))] = 2$. Χρησιμοποιώντας ξανά την πολλαπλασιαστικότητα των βαθμών έχουμε ότι

$$[K(\mathcal{J}(E)) : \mathbb{Q}] = [K(\mathcal{J}(E)) : \mathbb{Q}(\mathcal{J}(E))][\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] \Rightarrow$$

$$2h_k = 2[\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] \Rightarrow [\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] = h_k$$

Έτσι, ολοκληρώνεται η απόδειξη του θεωρήματος 6.3.1.

Παρατηρηση 6.3.8. Για παράδειγμα, εάν $m = -7$, τότε $K = \mathbb{Q}(\sqrt{-7})$. Όμως ισχύει ότι $-7 \equiv 1 \pmod 4$, οπότε έχουμε ότι

$$R_K = R_{\mathbb{Q}(\sqrt{-7})} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right].$$

Το κιγκλίδωμα από το οποίο κατασκευάζουμε την ελλειπτική καμπύλη είναι το

$$L := \mathbb{Z} + \frac{1+\sqrt{-7}}{2}\mathbb{Z} = R_K.$$

Αυτό σημαίνει ότι

$$\mathcal{J}(E) = \mathcal{J}(\mathbb{C}/L) = \mathcal{J}\left(\frac{1+\sqrt{-7}}{2}\right) = -3375 \in \mathbb{Z},$$

συμφωνα με το παράδειγμα 5.4.15.

Παρατηρηση 6.3.9. Εάν υποθέσουμε ότι $h_K = 1$, τότε βάσει του θεωρήματος 6.3.1 ισχύει ότι

$$[\mathbb{Q}(\mathcal{J}(E)) : \mathbb{Q}] = 1 \Rightarrow \mathcal{J}(E) \in \mathbb{Q}.$$

Όμως, σύμφωνα με το θεώρημα 5.4.8 ισχύει ότι $\mathcal{J}(E) \in \tilde{\mathbb{Z}}$. Επομένως,

$$\mathcal{J}(E) \in \mathbb{Q} \cap \tilde{Z} \Rightarrow \mathcal{J}(E) \in \mathbb{Z}.$$

Γνωρίζουμε ότι (βλ. [5], σελ.149, Θ. 7.30) τα μόνα τετραγωνικά μιγαδικά σώματα αριθμών με αριθμό κλάσεων ιδεωδών ίσο με 1 είναι τα $K = \mathbb{Q}(\sqrt{m})$, όπου

$$m = -1\,,\ -2\,,\ -3\,,\ -7\,,\ -11\,,\ -19\,,\ -43\,,\ -67\,,\ -163.$$

Αυτό το θεώρημα είναι η απάντηση στο πρόβλημα του Jugendtraum του Kronecker στην περίπτωση των τετραγωνικών σωμάτων αριθμών. Το θεώρημα των Kronecker και Weber μας πληροφορεί ότι εάν η $K/\mathbb{Q}$ είναι μία πεπερασμένη αβελιανή επέκταση, τότε

$$K \leq \mathbb{Q}(e^{2\pi i/n}),$$

για κάποιο ακέραιο αριθμό n. Θα μπορούσαμε να συμπεράνουμε ότι οι πεπερασμένες αβελιανές επεκτάσεις του $\mathbb{Q}$ παράγονται από συγκεκριμένες τιμές κάποιας αναλυτικής συνάρτησης, ιδιαιτέρως της $e^{2\pi iz}$. Το Jugendtraum έχει ως στόχο να γενικεύσει το αποτέλεσμα αυτό για οποιοδήποτε τετραγωνικό μιγαδικό αλγεβρικό σώμα αριθμών. Έκτος από την περίπτωση των τετραγωνικών μιγαδικών σωμάτων αριθμών, την οποία μελετήσαμε ενδελεχώς, έχει σημειωθεί πρόοδος και σε άλλες περιπτώσεις.

Παραδειγμα 6.3.10. Εάν θέσουμε $K = \mathbb{Q}(\sqrt{-6})$, τότε αποδεικνύεται ότι το σώμα Hilbert αυτού είναι το $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$, ήτοι

$$\mathscr{H}_{\mathbb{Q}(\sqrt{-6})} = \mathbb{Q}(\sqrt{2}, \sqrt{-3}) = \mathbb{Q}(\sqrt{2} + \sqrt{-3}).$$

Ακόμα, το σώμα Hilbert του $\mathbb{Q}(\sqrt{6})$ είναι γνωστό, παρόλο που δεν είναι τετραγωνικό μιγαδικό σώμα. Αυτό είναι το

$$\mathscr{H}_{\mathbb{Q}(\sqrt{6})} = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}) = \mathbb{Q}(\sqrt{-2} + \sqrt{-3}).$$

6.4 Η περίπτωση του $\mathbb{Q}(\sqrt{-163})$

Αξιοσημείωτη είναι η περίπτωση του σώματος $\mathbb{Q}(\sqrt{-163})$. Το λόγο θα τον αναλύσουμε στην πορεία της παραγράφου. Αρχικά, παρατηρούμε ότι

$$-163 \equiv -3 \equiv 1 \pmod 4,$$

από το οποίο συνεπάγεται ότι ο δακτύλιος $R_{\mathbb{Q}(\sqrt{-163})}$ των ακέραιων αλγεβρικών αριθμών του $\mathbb{Q}(\sqrt{-163})$ είναι ο

$$\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right].$$

Με άλλα λόγια, ισχύει ότι

$$R_{\mathbb{Q}(\sqrt{-163})} = \mathbb{Z} + \frac{1+\sqrt{-163}}{2} \cdot \mathbb{Z}.$$

Έχουμε δει ότι μπορούμε να θεωρήσουμε τον $R_{\mathbb{Q}(\sqrt{-163})}$ ως κιγκλίδωμα του $\mathbb{C}$. Επομένως, έχει νόημα να κάνουμε λόγο για την ελλειπτική καμπύλη $\mathbb{C}/R_{\mathbb{Q}(\sqrt{-163})}$. Αυτή είναι μία ελλειπτική καμπύλη με ελλειπτικό πολλαπλασιασμό από τον $R_{\mathbb{Q}(\sqrt{-163})}$. Πράγματι, σύμφωνα με το θεώρημα 5.3.4 ισχύει ότι

$$End_{\mathbb{C}}(\mathbb{C}/R_{\mathbb{Q}(\sqrt{-163})}) \cong \{\beta \in \mathbb{C}^{\times} \mid \beta R_{\mathbb{Q}(\sqrt{-163})} \subseteq R_{\mathbb{Q}(\sqrt{-163})}\} = R_K.$$

Χωρίς απόδειξη αναφέραμε στην παρατήρηση 6.3.9 ότι το $\mathbb{Q}(\sqrt{-163})$ είναι ένα σώμα με αριθμό κλάσεων ιδεωδών ίσο με 1. Αυτό είναι άμεσο από την απόδειξη ότι το $\mathbb{Q}(\sqrt{-163})$ είναι περιοχή κύριων ιδεωδών. Σύμφωνα με την ίδια παρατήρηση ισχύει ότι

$$\mathcal{J}(\mathbb{C}/R_{\mathbb{Q}(\sqrt{-163})}) \in \mathbb{Z}.$$

Πράγματι ισχύει ότι

$$\mathcal{J}(\mathbb{C}/R_{\mathbb{Q}(\sqrt{-163})}) = \mathcal{J}(R_{\mathbb{Q}(\sqrt{-163})}) = \mathcal{J}\left(\frac{1+\sqrt{-163}}{2}\right) = -262537412640768000 \in \mathbb{Z},$$

σύμφωνα με το παράδειγμα 5.4.15.

Επί τη βάσει της προτάσεως 3.2.5 ισχύει ότι το ανάπτυγμα Laurent της modular συνάρτησης $\mathcal{J}$ είναι της μορφής

$$\mathcal{J}(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{+\infty} c(n)e^{2\pi in\tau},$$

με $c(n) \in \mathbb{Z}$, για κάθε $n \in \mathbb{N}$. Ιδιαιτέρως, ισχύει ότι

$$\mathcal{J}(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots,$$

όπου

$$q := e^{2\pi i\tau}.$$

Στην περίπτωση του $\mathbb{Q}(\sqrt{-163})$ έχουμε ότι

$$\tau = \frac{1+\sqrt{-163}}{2} \Rightarrow q = e^{2\pi i\frac{1+\sqrt{-163}}{2}} \Rightarrow q = -e^{-\pi\sqrt{163}}.$$

Αυτό σημαίνει ότι

$$-e^{\pi\sqrt{163}} + 744 - 196884e^{-\pi\sqrt{163}} + 21493760e^{-2\pi\sqrt{163}} + \cdots \in \mathbb{Z}.$$

Εύκολα μπορούμε να ελέγξουμε ότι ισχύει η ανισότητα

$$196884e^{-\pi\sqrt{163}} - 21493760e^{-2\pi\sqrt{163}} + \cdots < 10^{-12}.$$

Κατά συνέπεια έχουμε ότι

$$|e^{\pi\sqrt{163}} - 744| < 10^{-12}.$$

Για την ακρίβεια ισχύει ότι

$$e^{\pi\sqrt{163}} = 262537412640768743,9999999999925007259\ldots.$$

Παρατηρούμε ότι κάνοντας τις πράξεις με ακρίβεια 30 ψηφίων, ήτοι 12 ψηφίων μετά την υποδιαστολή, ο αριθμός αυτός φαίνεται να είναι ακέραιος. Πράγματι, σε καιρούς κατά τους οποίους οι υπολογισμοί μεγάλης ακρίβειας δεν ήταν ευρέως διαθέσιμοι, κυκλοφορούσε ως χωρατό ότι

$$e^{\pi\sqrt{163}} \in \mathbb{Z},$$

μιας και από το θεώρημα των Gelfond και Schneider έπεται ότι θα έπρεπε να είναι υπερβατικός αριθμός. Μάλιστα, εφόσον ο αριθμός $e^{\pi\sqrt{163}}$ απέχει ελάχιστα από τον εγγύτερο ακέραιο, το αυτό θα ισχύει και για τον

$$\left(e^{\pi\sqrt{163}} - 744\right)^{1/3}.$$

Πράγματι, κάνοντας τους υπολογισμούς βλέπουμε ότι

$$\left(e^{\pi\sqrt{163}} - 744\right)^{1/3} = 640319,9999999999999999999999939031735\ldots.$$

Οι παραπάνω παρατηρήσεις καθιστούν την περίπτωση του $\mathbb{Q}(\sqrt{-163})$ αρκετά ενδιαφέρουσα γι' αυτό και αναφερθήκαμε σε αυτή.

Βιβλιογραφία

[1] Ιωάννης Αντωνιάδης, *"Αλγεβρικής Θεωρία Αριθμών"*, Χειρόγραφες σημειώσεις, Ηράκλειο, 1984

[2] Κ. Λάκκης, *"Θεωρία Αριθμών"*, Εκδόσεις Ζήτη, 6η έκδοση, Θεσσαλονίκη, 1988

[3] Tom M. Apostol, *"Modular Functions and Dirichlet Series in Number Theory"*, Springer-Verlag, vol. 2, New York, 1976

[4] Henri Cohen, *"A Course in Computational Algebraic Number Theory"*, Springer, Berlin 1993

[5] David A. Cox, *"Primes of the form $x^2 + ny^2$"*, Wiley Interscience, New York, 1989

[6] Klaus Hulek, *"Elementary Algebraic Geometry"*, American Mathematical Society, vol.20, translated by Helena Verill, 2003

[7] Gerald J. Janusz, *"Algebraic Number Fields"*, American Mathematical Society, second edition, vol. 7, New York, 1996

[8] Serge Lang, *"Elliptic Functions"*, Springer-Verlag, 2nd edition, New, York, 1999

[9] Franz Lemmermeyer, *"Class Field Theory"*, Lecture notes, 2007

[10] Patrick Morandi, *"Fields and Galois Theory"*, Springer, New York, 1996

[11] Alexander Schmidt, *"Einführung in die algebraische Zahlentheorie"*, Springer- Verlag, Berlin, 2009

[12] Joseph H. Silverman,*"Advanced Topics in the Arithmetic of Elliptic Curves"*, Springer, New York, 1999

[13] Joseph H. Silverman, *"The Arithmetic of Elliptic Curves"*, Springer, 2nd edition, Dordrecht, 2009

[14] S.G.Vladut, *"Kronecker's Jugendtraum and modular functions"*, Gordon and Breach Publishers, Second printing with revisions, Australia, 1995

[15] Lawrence C. Washington, *"Elliptic Curves, Number Theory and Cryptography"*, Chapman & Hall/CRC, 2nd edition, Boca Raton, 2008

[16] Don B. Zagier, *"Zetafunktionen und quadratische Körper, eine Einführung in die höhere Zahlentheorie"*, Springer-Verlag, Berlin, 1981