Αριθμός Κλάσεων: Η Εικασία του Gauss

Νίκη Σπιθάκη

Επιβλέπων καθηγητής:
Ιωάννης Α. Αντωνιάδης

Πτυχιακή Εργασία

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών,
Πανεπιστήμιο Κρήτης,
Ηράκλειο,
Ιούνιος 2020

Στη μνήμη του πρώτου μου δασκάλου, του παππού μου, Μιχάλη Σπιθάκη

Ευχαριστίες

Η παρούσα πτυχιακή εργασία δε θα μπορούσε να έχει ολοκληρωθεί χωρίς την πολύτιμη βοήθεια του κ. Ιωάννη Αντωνιάδη, ο οποίος με αστείρευτη υπομονή και ενθουσιασμό δε δίστασε στιγμή να αφιερώσει χρόνο και κόπο ούτως ώστε να έχουμε ένα άρτιο αποτέλεσμα, παρά τις αντιξοότητες της εποχής που διανύσαμε. Θα είμαι για πάντα ευγνώμων για τη διδασκαλία του και για το ενδιαφέρον που έδειξε καθόλη τη διάρκεια προετοιμασίας του έργου αυτού.

Θα ήθελα επίσης να ευχαριστήσω τον κ. Αλέξανδρο Κουβιδάκη και την κ. Μαρία Λουκάκη ως μέλη της κριτικής επιτροπής της εργασίας .

Ένα μεγάλο ευχαριστώ οφείλω και στους συμφοιτητές και φίλους που με στήριξαν και με εμψύχωσαν κατά την περίοδο συγγραφής της πτυχιακής αυτής εργασίας.

Τέλος, ευχαριστώ την οικογένειά μου, που αποτελεί το στήριγμά μου σε κάθε σημαντική πτυχή της ζωής μου. Δε θα τα είχα καταφέρει χωρίς εσάς πλάι μου.

Νίκη Σπιθάκη
Ιούνιος 2020

Περιεχόμενα

Εισαγωγή

Κατά το έτος 1801, δημοσιεύθηκε το βιβλίο Θεωρίας Αριθμών του Carl Friedrich Gauss με τον λατινικό τίτλο "*Disquisitiones Arithmeticae.*"Το βιβλίο αυτό αποτελεί ένα δοκίμιο μεγίστης σημασίας και σπουδαιότητας, καθώς ως γνωστό, σηματοδοτεί την απαρχή της μοντέρνας Αριθμοθεωρίας. Ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στο [11] της βιβλιογραφίας για μία μεταγενέστερη έκδοση του βιβλίου αυτού.

Σχήμα 1: C. F. Gauss.

Εμείς εστιάζουμε την προσοχή μας στο άρθρο 303, στο οποίο ο Gauss αναφέρεται σε υπολογισμούς του αριθμού κλάσεων πρωταρχικών θετικά ορισμένων τετραγωνικών μορφών:

"*The series of determinants corresponding to the same given classification always seems to come to an end. [...] Since the table from which we drew these examples has been extended far beyond the largest determinants that occur here, and since it furnishes no others belonging to these classes, there seems to be no doubt that the preceding series do in fact terminate, and by analogy it is permissible to extend the same conclusion to any other classifications. [...] It is extremely probable that the classifications are all complete before we reach the number -9000, or at least that they have very few determinants*

greater than -10000. However, rigorous proofs of these observations seem to be very difficult."

Ουσιαστικά, όπως φαίνεται από το παραπάνω απόσπασμα, ο Gauss διατυπώνει δύο ***εικασίες:***

Εικασία 1η. Αν h είναι ένας φυσικός αριθμός, τότε υπάρχουν πεπερασμένου πλήθους αρνητικές διακρίνουσες d, με αριθμό κλάσεων $h(d) = h$.

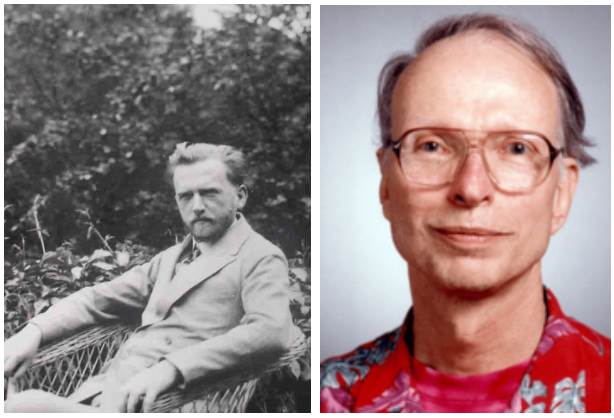
Εικασία 2η. Τα μιγαδικά τετραγωνικά σώματα αριθμών με αριθμό κλάσεων $h(d) = 1$ είναι ακριβώς αυτά που είχε υπολογίσει ο ίδιος ο Gauss. Πιο συγκεκριμένα, ισχυρίζεται ότι ισχύει η ακόλουθη ισοδυναμία:

$$h(d) = 1 \Leftrightarrow d = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Η πρώτη εικασία αποδείχθηκε από τον C. L. Siegel (βλ.[26]). Συγκεκριμένα, ο Siegel απέδειξε ότι, για κάθε $\varepsilon > 0$, υπάρχει μία σταθερά $c > 0$, η οποία δεν μπορεί να υπολογιστεί με ακρίβεια (effective) τέτοια ώστε

$$h(d) > c|d|^{\frac{1}{2}-\varepsilon}.$$

Το κύριο θέμα της παρούσας πτυχιακής εργασίας είναι η απόδειξη των Kurt Heegner και Harold M. Stark της δεύτερης εικασίας του Gauss.



(α′) K. Heegner. (β′) H. M. Stark.

Προτού φτάσουμε, όμως, στο βασικό μας στόχο, είναι απαραίτητο για τη μελέτη της απόδειξης των Heegner - Stark να αναφερθούμε σε στοιχεία διάφορων μαθηματικών εννοιών και θεωριών, η κάθε μία από τις οποίες έχει το δικό της ιδιαίτερο ρόλο στην τελική επίτευξη του σκοπού μας.

Στο πρώτο κεφάλαιο ασχολούμαστε με κάποια βασικά στοιχεία της θεωρίας των δυαδικών τετραγωνικών μορφών, και συγκεκριμένα εστιάζουμε στις πρωταρχικές, θετικά ορισμένες τετραγωνικές μορφές αρνητικής διακρίνουσας. Θα συνδέσουμε τη θεωρία αυτού του κεφαλαίου αργότερα με εκείνη των τετραγωνικών σωμάτων αριθμών.

Το δεύτερο κεφάλαιο περιλαμβάνει θεμελιώδεις έννοιες της αλγεβρικής θεωρίας αριθμών, με στόχο την εμβάθυνση στη γνώση των αλγεβρικών σωμάτων αριθμών. Εδώ διατυπώνουμε σημαντικά θεωρήματα που αφορούν τα αλγεβρικά σώματα αριθμών, παραλείποντας τις αποδείξεις, για τις οποίες παραπέμπουμε στα [2] και [3] της βιβλιογραφίας.

Ο κύριος λόγος για τον οποίο αναφερόμαστε στα θεωρήματα αυτά είναι η εφαρμογή τους στο τρίτο κεφάλαιο, το οποίο είναι αφιερωμένο στη μελέτη των τετραγωνικών σωμάτων αριθμών, δηλαδή των αλγεβρικών σωμάτων αριθμών βαθμού 2 υπέρ του $\mathbb{Q}$. Καθώς η δεύτερη εικασία του Gauss αφορά συγκεκριμένα τα μιγαδικά τετραγωνικά σώματα αριθμών, περιοριζόμαστε στην εργασία μας σε αυτά. Κλείνουμε το τρίτο κεφάλαιο με τη μελέτη των τάξεων τετραγωνικών σωμάτων αριθμών, μία έννοια που θα συμβάλλει σημαντικά στην επίτευξη του βασικού μας στόχου.

Στο τέταρτο κεφάλαιο ξεφεύγουμε ελάχιστα από το κύριο θέμα της εργασίας μας και ασχολούμαστε με το πρόβλημα ύπαρξης πολυωνυμικής συνάρτησης με διαδοχικές τιμές πρώτους αριθμούς. Εδώ παρουσιάζουμε το θεώρημα του Rabinowitsch, το οποίο συνδέει το πρόβλημα αυτό με τον αριθμό κλάσεων, καθώς και ένα γενικότερο θεώρημα από το βιβλίο του Jean - Pierre Serre, το [25] της βιβλιογραφίας. Υπολογίζουμε, τέλος, τις διακρίνουσες όλων των τάξεων τετραγωνικών σωμάτων αριθμών με αριθμό κλάσεων 1.

Στο πέμπτο κεφάλαιο εισάγουμε τις έννοιες των ελλειπτικών και modular συναρτήσεων. Η θεωρία αυτή, που περιλαμβάνει αρκετά στοιχεία Μιγαδικής Ανάλυσης, είναι ιδιαίτερα σημαντική για τον τελικό μας στόχο. Για το κεφάλαιο αυτό βασιστήκαμε κυρίως στο βιβλίο του Tom Apostol, το [4] της βιβλιογραφίας.

Η απόδειξη των Heegner - Stark και άρα το κύριο θέμα της εργασίας μας παρουσιάζεται στο έκτο και τελευταίο κεφάλαιο. Εδώ όλες οι θεωρίες με τις οποίες ασχοληθήκαμε στα προηγούμενα κεφάλαια συνδέονται αρμονικά μεταξύ τους, με αποτέλεσμα μία διοφαντική εξίσωση, οι λύσεις της οποίας δίνουν την τελική απάντηση στην εικασία του Gauss.

Ηράκλειο, Ιούνιος 2020

Κεφάλαιο 1

Τετραγωνικές Μορφές

1.1 Εισαγωγικά Στοιχεία

Ορισμός 1.1.1. *Δυαδική τετραγωνική μορφή* ονομάζεται κάθε ομογενές πολυώνυμο δευτέρου βαθμού, δύο μεταβλητών, με συντελεστές ακέραιους αριθμούς, δηλαδή κάθε πολυώνυμο της μορφής

$$f(X,Y) = aX^2 + bXY + cY^2, \quad a,b,c \in \mathbb{Z}.$$

Για λόγους ευκολίας, συχνά θα συμβολίζουμε την τετραγωνική μορφή $f(X,Y) = aX^2 + bXY + cY^2$ ως $f = [a,b,c]$. Επίσης, καθώς στο πλαίσιο αυτής της εργασίας θα ασχοληθούμε αποκλειστικά με δυαδικές τετραγωνικές μορφές, στη συνέχεια θα παραλείπουμε τον όρο "δυαδικές".

Ορισμός 1.1.2. Ως *διακρίνουσα* της τετραγωνικής μορφής $f = [a,b,c]$ ορίζουμε τον ακέραιο αριθμό

$$\Delta_f := b^2 - 4ac.$$

Στο παρόν κεφάλαιο θα μας απασχολήσουν δύο ερωτήματα:

1. Δοσμένου $\Delta \in \mathbb{Z}$, πόσες τετραγωνικές μορφές διακρίνουσας Δ υπάρχουν; Μπορούμε να τις ταξινομήσουμε;

2. Αν $f(X,Y)$ τετραγωνική μορφή, να βρεθούν οι φυσικοί αριθμοί n που παρίστανται από την f, δηλαδή εκείνοι για τους οποίους υπάρχουν ακέραιοι x,y τέτοιοι ώστε $f(x,y) = n$.

Παρατήρηση 1.1.3 Προφανώς ισχύει ότι $\Delta \equiv b^2 (mod 4)$. Στην περίπτωση που ο b είναι άρτιος αριθμός, εύκολα παρατηρούμε ότι $\Delta \equiv 0 (mod 4)$. Αν πάλι

ο b είναι περιττός αριθμός, τότε $\Delta \equiv 1(mod4)$. Επομένως, κάθε διακρίνουσα τετραγωνικής μορφής είναι ισότιμη με 0 ή 1 $(mod4)$.

Παρατήρηση 1.1.4 Ισχύει και το αντίστροφο: αν Δ ένας ακέραιος αριθμός για τον οποίο ισχύει $\Delta \equiv 0(mod4)$ ή $\Delta \equiv 1(mod4)$, τότε υπάρχει τετραγωνική μορφή με διακρίνουσα Δ. Πράγματι, αν υποθέσουμε ότι $\Delta \equiv 0(mod4)$, τότε εύκολα βλέπουμε ότι η τετραγωνική μορφή

$$X^2 - \frac{\Delta}{4}\Upsilon^2$$

έχει διακρίνουσα Δ. Αν πάλι $\Delta \equiv 1(mod4)$, τότε η τετραγωνική μορφή

$$X^2 + XY + \frac{1-\Delta}{4}Y^2$$

έχει τη ζητούμενη διακρίνουσα[1].

Ιδιαίτερα χρήσιμος στη συνέχεια θα είναι ο παρακάτω ορισμός των πρωταρχικών τετραγωνικών μορφών.

Ορισμός 1.1.5 Η τετραγωνική μορφή $f = [a, b, c]$ θα λέγεται *πρωταρχική* αν για τους συντελεστές της, a, b, c, ισχύει η σχέση $(a, b, c) = 1$.

Έστω τώρα μία τετραγωνική μορφή $f = [a, b, c]$ με $\Delta_f \neq 0$. Διακρίνουμε δύο περιπτώσεις για τη Δ_f :

Περίπτωση 1. Αν $\Delta_f < 0$, τότε κατ'ανάγκη ισχύει $a \cdot c > 0$, δηλαδή οι ακέραιοι a και c είναι ομόσημοι.

Ορισμός 1.1.6 Έστω τετραγωνική μορφή $f = [a, b, c]$. Αν ισχύουν $\Delta_f < 0$ και $a > 0$, τότε η f θα λέγεται *θετικά ορισμένη*. Αν πάλι $\Delta_f < 0$ και $a < 0$, η f θα λέγεται *αρνητικά ορισμένη*.

Είναι προφανές ότι αν η τετραγωνική μορφή $[a, b, c]$ είναι θετικά ορισμένη, τότε μπορεί να παραστήσει μόνο μη-αρνητικούς ακέραιους, ενώ αν είναι αρνητικά ορισμένη μπορεί να παραστήσει ακέραιους ≤ 0.

Επίσης, εύκολα παρατηρούμε ότι αν η $[a, b, c]$ είναι θετικά ορισμένη, τότε η $[-a, -b, -c]$ είναι αρνητικά ορισμένη. Επομένως, χωρίς βλάβη της γενικότητας, μπορούμε να περιοριστούμε, στην περίπτωση $\Delta < 0$, στις θετικά ορισμένες

[1] Οι τετραγωνικές μορφές αυτές, για $\Delta \equiv 0(mod4)$ και $\Delta \equiv 1(mod4)$ αντίστοιχα, λέγονται θεμελιώδεις τετραγωνικές μορφές διακρίνουσας Δ.

τετραγωνικές μορφές.

Περίπτωση 2. Αν $\Delta_f > 0$, η τετραγωνική μορφή παριστά τόσο θετικούς όσο και αρνητικούς ακέραιους και λέγεται *απροσδιόριστη (indefinite)*.

Παρακάτω θα περιοριστούμε σε τετραγωνικές μορφές με διακρίνουσα $\Delta < 0$, όπου η Δ δεν είναι τέλειο τετράγωνο ακεραίου.

1.2 Ισοδύναμες Τετραγωνικές Μορφές

Έστω η τετραγωνική μορφή $f(X,Y) = aX^2 + bXY + cY^2$, διακρίνουσας $\Delta_f = b^2 - 4ac$. Θεωρούμε τον πίνακα

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

και ορίζουμε

$$f(X,Y)|_T = f(X+Y, Y).$$

Παίρνουμε έτσι μία καινούρια τετραγωνική μορφή,

$$g(X,Y) = f(X+Y,Y) = aX^2 + (2a+b)XY + (a+b+c)Y^2.$$

Η διακρίνουσα της g είναι:

$$\Delta_g = (2a+b)^2 - 4a(a+b+c) = b^2 - 4ac = \Delta_f.$$

Επομένως, δρώντας στο ζεύγος $\begin{pmatrix} X \\ Y \end{pmatrix}$ με τον πίνακα T προκύπτει μέσω της f νέα τετραγωνική μορφή ίδιας διακρίνουσας.

Όμοια, θεωρώντας τώρα τον πίνακα

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

με

$$f(X,Y)|_S = f(-Y,X),$$

παίρνουμε την τετραγωνική μορφή

$$h(X,Y) = f(-Y,X) = cX^2 - bXY + aY^2.$$

Εύκολα παρατηρούμε ότι πάλι προκύπτει τετραγωνική μορφή ίδιας διακρίνουσας $\Delta_h = \Delta_f$.

Παρατήρηση 1.2.1 Για τον πίνακα T ισχύει:

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \qquad n \in \mathbb{Z}.$$

Επομένως, ο T έχει άπειρη τάξη.

Υπολογίζουμε τώρα τις δυνάμεις του πίνακα S:

$$S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2, \;\; S^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \;\; S^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

Επομένως, ο S έχει τάξη 4. Επειδή, όμως, περιοριζόμαστε σε θετικά ορισμένες τετραγωνικές μορφές, ταυτίζουμε την τετραγωνική μορφή

$$f(X,Y)|_{-I_2} = f(-X,-Y)$$

με την ταυτοτική, $f(X,Y)|_{I_2} = f(X,Y)$. Βάση αυτού, και εφόσον $S^2 = -I_2$, θεωρούμε ότι ο πίνακας S έχει τάξη 2.

Οδηγούμαστε, έτσι, στο εξής συμπέρασμα:
Η διακρίνουσα Δ παραμένει αναλλοίωτη κάτω από τη δράση της ομάδας

$$< S, T >= \{T^{n_1} S T^{n_2} S ... S T^{n_k} \text{ (πεπερασμένα γινόμενα)} \mid n_i \in \mathbb{Z}\}.$$

Παρατήρηση 1.2.2 Για τις ορίζουσες των πινάκων S και T έχουμε ότι $detS = detT = 1$. Λόγω της πολλαπλασιαστικής ιδιότητας της ορίζουσας, το ίδιο ισχύει για κάθε στοιχείο της ομάδας $< S, T >$. Από εδώ συμπεραίνουμε επίσης ότι τα στοιχεία της ομάδας έχουν ακέραιους συντελεστές. Επομένως, ισχύει ότι

$$< S, T > \leq \; SL_2(\mathbb{Z}),$$

όπου

$$SL_2(\mathbb{Z}) := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z}, \; ad - bc = 1 \right\}.$$

Το επόμενο θεώρημα μας δείχνει ότι, στην πραγματικότητα, ισχύει η ισότητα.

Θεώρημα 1.2.3 Η ομάδα $SL_2(\mathbb{Z})$ παράγεται από τους πίνακες S και T, δηλαδή

$$SL_2(\mathbb{Z}) =< S, T > .$$

Ισοδύναμα, κάθε πίνακας $A \in SL_2(\mathbb{Z})$ μπορεί να γραφεί στη μορφή

$$A = T^{n_1} S T^{n_2} S ... S T^{n_k},$$

όπου n_i ακέραιοι αριθμοί.

Απόδειξη. Αρκεί να αποδείξουμε το θεώρημα για γενικό πίνακα

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

με $c \geq 0$. Αυτό γιατί, αν έχουμε $c < 0$, τότε απλά δουλεύουμε με τον πίνακα $-A$, τον οποίο ταυτίζουμε με τον A.

Αποδεικνύουμε το θεώρημα με επαγωγή στο c.

Αν $c = 0$, τότε $detA = ad = 1$, επομένως $a = d = \pm 1$ και

$$A = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix} = \begin{pmatrix} 1 & \pm b \\ 0 & 1 \end{pmatrix} = T^{\pm b}.$$

Δηλαδή ο A είναι δύναμη του T.

Αν $c = 1$, τότε $detA = ad - b = 1$, άρα $b = ad - 1$ και

$$A = \begin{pmatrix} a & ad-1 \\ 1 & d \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} = T^a S T^d.$$

Έστω τώρα ότι το θεώρημα ισχύει για κάθε πίνακα

$$M = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(\mathbb{Z})$$

με $a_{21} < c$, όπου $c \geq 1$. Για τον πίνακα A ισχύει $detA = ad - bc = 1$, άρα $(c, d) = 1$. Διαιρώντας το d με το c έχουμε

$$d = cq + r, \quad 0 < r < c.$$

Τότε

$$AT^{-q} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -aq+b \\ c & r \end{pmatrix}$$

και

$$AT^{-q}S = \begin{pmatrix} a & -aq+b \\ c & r \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -aq+b & -a \\ r & -c \end{pmatrix}.$$

Από την επαγωγική υπόθεση, ο τελευταίος πίνακας γράφεται σαν γινόμενο του S και δυνάμεων του T, άρα το ίδιο ισχύει και για τον A. Η απόδειξη, επομένως, ολοκληρώθηκε. □

Παράδειγμα 1.2.4 Θα χρησιμοποιήσουμε τώρα τον πίνακα

$$A = \begin{pmatrix} 12 & 29 \\ 7 & 17 \end{pmatrix}$$

και θα εφαρμόσουμε την απόδειξη του θεωρήματος 1.2.3 για να βρούμε την αναπαράστασή του σε γινόμενο του S και δυνάμεων του T.

Διαιρούμε το 17 με το 7 και βρίσκουμε $17 = 7 \cdot 2 + 3$. Πολλαπλασιάζουμε, συνεπώς, τον πίνακα A με τον πίνακα T^{-2}:

$$AT^{-2} = \begin{pmatrix} 12 & 29 \\ 7 & 17 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 12 & 5 \\ 7 & 3 \end{pmatrix}.$$

Στη συνέχεια πολλαπλασιάζουμε με τον πίνακα S:

$$AT^{-2}S = \begin{pmatrix} 12 & 5 \\ 7 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 5 & -12 \\ 3 & -7 \end{pmatrix}.$$

Τώρα, $-7 = 3 \cdot (-3) + 2$, πολλαπλασιάζουμε επομένως με τον πίνακα T^3 :

$$AT^{-2}ST^3 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}.$$

Πολλαπλασιάζουμε ξανά με τον πίνακα S:

$$AT^{-2}ST^3S = \begin{pmatrix} 3 & -5 \\ 2 & -3 \end{pmatrix}.$$

Επαναλαμβάνουμε τη διαδικασία: $-3 = 2 \cdot (-2) + 1$, άρα πολλαπλασιάζουμε με τον T^2,

$$AT^{-2}ST^3ST^2 = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$$

και με τον S,

$$AT^{-2}ST^3ST^2S = \begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}.$$

Τώρα $-2 = 1 \cdot (-2) + 0$, άρα

$$AT^{-2}ST^3ST^2ST^2 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

και

$$AT^{-2}ST^3ST^2ST^2S = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = -T \equiv T.$$

Λύνοντας ως προς A έχουμε:

$$A = TST^{-2}ST^{-2}ST^{-3}ST^{2}.$$

Παρατήρηση 1.2.5 Η αναπαράσταση ενός πίνακα σε γινόμενο της παραπάνω μορφής δεν είναι μοναδική. Αυτό γιατί θα μπορούσαμε, αντί να επιλέγουμε κάθε φορά το αντίθετο του πηλίκου της διαίρεσης ως δύναμη του πίνακα T, να επιλέξουμε οποιαδήποτε δύναμη τέτοια ώστε, μετά και τον πολλαπλασιασμό με τον πίνακα S, να προκύψει στην κάτω αριστερή θέση του νέου πίνακα αριθμός μικρότερος του προηγούμενου στην ίδια θέση.

Ορισμός 1.2.6 Έστω $f(X,Y)$, $g(X',Y')$ δύο τετραγωνικές μορφές. Θα λέμε ότι οι f, g είναι *ισοδύναμες*, $f \sim g$, αν υπάρχει πίνακας

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

τέτοιος ώστε

$$g(X',Y') = f(X,Y)|_A = f\Big(A\begin{pmatrix} X \\ Y \end{pmatrix}\Big) = f(aX+bY, cX+dY).$$

Είναι φανερό ότι η παραπάνω σχέση αποτελεί σχέση ισοδυναμίας. Επομένως, οι τετραγωνικές μορφές χωρίζονται σε κλάσεις ισοδυναμίας.

Πρόταση 1.2.7 Αν η $f(X,Y)$ είναι τετραγωνική μορφή και $A \in SL_2(\mathbb{Z})$, τότε οι τετραγωνικές μορφές $f(X,Y)$ και $f(X,Y)|_A$ παριστούν τους ίδιους ακέραιους.

Απόδειξη. Αν $f(x,y) = n$ για $n, x, y \in \mathbb{Z}$, επειδή και ο A^{-1} ανήκει στην ομάδα $SL_2(\mathbb{Z})$, έχουμε ότι

$$f\Big|_A\Big(A^{-1}\begin{pmatrix} x \\ y \end{pmatrix}\Big) = f\Big(AA^{-1}\begin{pmatrix} x \\ y \end{pmatrix}\Big) = f(x,y) = n,$$

δηλαδή η $f(X,Y)|_A$ παριστά τον n. Αντίστροφα, αν $f(x,y)|_A = n$, τότε

$$f\Big(A\begin{pmatrix} x \\ y \end{pmatrix}\Big) = n,$$

δηλαδή η $f(X,Y)$ παριστά τον n. □

Πρόταση 1.2.8 Αν Δ_f, Δ_g οι διακρίνουσες των ισοδύναμων τετραγωνικών μορφών f, g αντίστοιχα, τότε ισχύει $\Delta_f = \Delta_g$.

Απόδειξη. Αν $A \in SL_2(\mathbb{Z})$, τότε ισχύει

$$\Delta_{f|_A} = \Delta_f \cdot (detA)^2 = \Delta_f.$$

Αν τώρα $f \sim g$, υπάρχει $A \in SL_2(\mathbb{Z})$ τέτοιος ώστε $g = f|_A$, επομένως η πρόταση είναι αληθής. □

Παρατήρηση 1.2.9 Το αντίστροφο της προηγούμενης πρότασης δεν ίσχυει. Αν, δηλαδή, δύο τετραγωνικές μορφές έχουν ίσες διακρίνουσες, τότε αυτές δεν είναι κατ'ανάγκη ισοδύναμες.

Για παράδειγμα, οι τετραγωνικές μορφές $X^2 + 10Y^2$ και $2X^2 + 5Y^2$ έχουν και οι δύο διακρίνουσα $\Delta = -40$. Παρόλα αυτά δεν είναι ισοδύναμες, αφού η πρώτη παριστά τον ακέραιο αριθμό 1, ενώ η δεύτερη όχι.

Θα δώσουμε τώρα απάντηση στο πρώτο ερώτημα που θέσαμε στην αρχή αυτού του κεφαλαίου, υπολογίζοντας το πλήθος των κλάσεων ισοδυναμίας τετραγωνικών μορφών δοσμένης διακρίνουσας Δ.

Όπως είπαμε, περιοριζόμαστε στην περίπτωση όπου έχουμε $\Delta < 0$ και οι τετραγωνικές μορφές είναι θετικά ορισμένες. Θα αποδείξουμε ότι το πλήθος των $SL_2(\mathbb{Z})-$ κλάσεων ισοδυναμίας τετραγωνικών μορφών με διακρίνουσα $\Delta < 0$ είναι πάντοτε πεπερασμένο.

Δίνουμε πρώτα έναν ορισμό:

Ορισμός 1.2.10 Η τετραγωνική μορφή $f = [a, b, c]$ θα λέγεται *σχεδόν ανάγωγη* αν $a \leq c$ και $|b| \leq a$.

Πρόταση 1.2.11 Κάθε τετραγωνική μορφή διακρίνουσας Δ είναι ισοδύναμη με κάποια σχεδόν ανάγωγη.

Απόδειξη. Ας υποθέσουμε ότι για την τετραγωνική μορφή

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

ισχύει $a > c$. Τότε

$$f(X, Y)|_S = f(-Y, X) = cX^2 - bXY + aY^2 = a'X^2 + b'XY + c'Y^2,$$

όπου $a' = c,\ b' = -b,\ c' = a$ και $a' = c < a = c'$. Επομένως, μπορούμε να βρούμε ισοδύναμη τετραγωνική μορφή της f που να ικανοποιεί $a \leq c$.

Υποθέτουμε τώρα ότι $|b| > a$. Έστω T_n ο πίνακας

$$T_n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \qquad n \in \mathbb{Z}.$$

Τότε

$$g(X,Y) = f(X,Y)|_{T_n} = aX^2 + (2an+b)XY + (an^2+bn+c)Y^2.$$

Για να είναι η g σχεδόν ανάγωγη, πρέπει να ισχύει $|2an+b| \leq a$, δηλαδή

$$n \in \Big[-\frac{a+b}{2a}, \frac{a-b}{2a}\Big].$$

Το μήκος αυτού του διαστήματος είναι

$$\frac{a-b}{2a} - \Big(-\frac{a+b}{2a}\Big) = 1,$$

επομένως πάντα υπάρχει τουλάχιστον ένα $n \in \mathbb{Z}$ που ανήκει σε αυτό. Επιλέγοντας ένα τέτοιο n, παίρνουμε μία ισοδύναμη τετραγωνική μορφή που ικανοποιεί την ανισότητα $|b| \leq a$. Αν τώρα για την $g(X,Y)$ δεν ισχύει η ανισότητα $a \leq (an^2+bn+c)$, τότε απλώς ξαναχρησιμοποιούμε τον πίνακα S. Το $2an+b$ θα αλλάξει μόνο κατά πρόσημο, επομένως η $|b| \leq a$ εξακολουθεί να ισχύει. □

Πρόταση 1.2.12 Το πλήθος των σχεδών ανάγωγων τετραγωνικών μορφών διακρίνουσας Δ είναι πεπερασμένο.

Απόδειξη. Έστω $f(X,Y) = aX^2+bXY+cY^2$ μία σχεδόν ανάγωγη τετραγωνική μορφή διακρίνουσας $\Delta_f = b^2-4ac$. Έχουμε:

$$a \leq c \Rightarrow 4a^2 \leq 4ac \Rightarrow 4a^2 \leq b^2 - \Delta \Rightarrow 4a^2 \leq a^2 - \Delta \Rightarrow |a| \leq \sqrt{\frac{|\Delta|}{3}},$$

δηλαδή το a μπορεί να λάβει πεπερασμένου πλήθους τιμές. Το ίδιο ισχύει και για το b, καθώς $-a \leq b \leq a$. Τέλος, για το c ισχύει

$$c = \frac{b^2-\Delta}{4a},$$

επομένως το c ορίζεται μονοσήμαντα μέσω των $a,\ b$. □

Οι Προτάσεις 1.2.11 και 1.2.12 μας δίνουν ακριβώς ότι το πλήθος των κλάσεων ισοδυναμίας τετραγωνικών μορφών διακρίνουσας Δ είναι πεπερασμένο. Πράγματι, από την Πρόταση 1.2.11 συμπεραίνουμε ότι κάθε κλάση ισοδυναμίας περιέχει τουλάχιστον μία σχεδόν ανάγωγη τετραγωνική μορφή, το πλήθος των οποίων είναι πεπερασμένο από την Πρόταση 1.2.12.

Το επόμενο ερώτημα που τίθεται τώρα φυσιολογικά είναι αν για κάθε κλάση ισοδυναμίας υπάρχει μοναδικός αντιπρόσωπος. Στο τέλος της παρούσας παραγράφου θα δώσουμε την απάντηση.

Ορισμός 1.2.13 Η τετραγωνική μορφή $f = [a, b, c]$ θα λέγεται *ανηγμένη (reduced)* αν $|b| \leq a \leq c$ και επιπλέον, όταν ισχύει μία από τις δύο ισότητες, δηλαδή όταν $|b| = a$ ή $a = c$, επιλέγουμε $b \geq 0$.

Η παρακάτω πρόταση, την οποία θα αποδείξουμε στην επόμενη ενότητα, δίνει απάντηση στο ερώτημά μας.

Πρόταση 1.2.14 Κάθε κλάση ισοδυναμίας θετικά ορισμένων τετραγωνικών μορφών περιέχει ακριβώς μία ανηγμένη τετραγωνική μορφή.

Παρατήρηση 1.2.15 Από την πρόταση 1.2.14 συμπεραίνουμε ότι το πλήθος των κλάσεων ισοδυναμίας τετραγωνικών μορφών διακρίνουσας Δ ισούται με το πλήθος των θετικά ορισμένων ανηγμένων τετραγωνικών μορφών διακρίνουσας Δ.

Παράδειγμα 1.2.16 Θα υπολογίσουμε το πλήθος των κλάσεων ισοδυναμίας τετραγωνικών μορφών διακρίνουσας $\Delta = -20$, δηλαδή το πλήθος των ανηγμένων τετραγωνικών μορφών διακρίνουσας -20.

Έστω λοιπόν $f(X, Y) = aX^2 + bXY + cY^2$ μία ανηγμένη τετραγωνική μορφή. Από την απόδειξη της πρότασης 1.2.12 έχουμε την σχέση

$$a^2 \leq \frac{|\Delta|}{3} \Rightarrow a^2 \leq \frac{20}{3}.$$

Εφόσον το a είναι ένας θετικός ακέραιος αριθμός, αναγκαστικά θα ισχύει $a = 1$ ή $a = 2$.

Αν $a = 1$, από την ανισότητα $|b| \leq a$ έπεται ότι $b \in \{-1, 0, 1\}$. Στην περίπτωση $|b| = 1 = a$, από τον ορισμό της ανηγμένης επιλέγουμε $b = 1$. Τώρα το c ορίζεται μονοσήμαντα μέσω της διακρίνουσας:

$$c = \frac{-\Delta + b^2}{4a} = \frac{21}{4}.$$

Όμως $\frac{21}{4} \notin \mathbb{Z}$, επομένως αυτή η περίπτωση απορρίπτεται. Αν τώρα $b = 0$, βρίσκουμε ότι $c = 5$, επομένως μία ανηγμένη διακρίνουσας -20 είναι η

$$f(X, Y) = X^2 + 5Y^2.$$

Αν $a = 2$, με τον ίδιο τρόπο βρίσκουμε ότι $b \in \{0, \pm 1, \pm 2\}$. Αν $|b| = 2 = a$, επιλέγουμε $b = 2$. Έπεται ότι $c = 3$, άρα μία άλλη ανηγμένη διακρίνουσας -20 είναι η

$$g(X, Y) = 2X^2 + 2XY + 3Y^2.$$

Οι περιπτώσεις $|b| = 1$ και $b = 0$ δίνουν c που δεν είναι ακέραιος, επομένως απορρίπτονται.

Τελικά, το πλήθος των κλάσεων ισοδυναμίας τετραγωνικών μορφών διακρίνουσας $\Delta = -20$ ισούται με 2 και οι αντιπρόσωποι των δύο κλάσεων είναι οι ανηγμένες $f = [1, 0, 5]$ και $g = [2, 2, 3]$.

1.3 Παράσταση Ακεραίων από Τετραγωνικές Μορφές

Ορισμός 1.3.1 Έστω $n \in \mathbb{Z}$ και τετραγωνική μορφή $f(X, Y)$. Θα λέμε ότι ο n *παρίσταται* μέσω της f αν υπάρχει $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ τέτοια ώστε

$$f(x, y) = n.$$

Ορισμός 1.3.2 Θα λέμε ότι ο $n \in \mathbb{Z}$ *παρίσταται γνήσια* μέσω της f αν υπάρχει $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ με $MK\Delta(x, y) = 1$ τέτοια ώστε $f(x, y) = n$.

Παρατήρηση 1.3.3 Αν $n = f(x, y)$ για κάποιους ακέραιους $x,\ y$ και $(x, y) = d$, τότε $(x/d, y/d) = 1,\ d^2 \mid n$ και ο n/d^2 παρίσταται γνήσια από την f.

Επομένως, αν P το σύνολο των ακεραίων που παρίστανται γνήσια από την f και A το σύνολο των ακεραίων που παρίστανται από την f, ισχύει:

$$A = \{l \cdot d^2 \mid l \in P,\ d \in \mathbb{Z},\ d \neq 0\}.$$

Παρατήρηση 1.3.4 Αν ο ακέραιος n παρίσταται από την $f(X, Y)$, τότε παρίσταται από κάθε ισοδύναμή της.

Πράγματι, έστω ότι $f \sim g$, δηλαδή υπάρχει πίνακας

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

τέτοιος ώστε $g(X, Y) = f(aX + bY, cX + dY)$. Ο n παρίσταται από την f, άρα $n = f(x, y)$ για κάποια $x, y \in \mathbb{Z}$. Ψάχνουμε κατάλληλα $X,\ Y$ τέτοια ώστε $f(aX + bY, cX + dY) = n$. Λύνουμε το σύστημα

$$\begin{cases} x = aX + bY \\ y = cX + dY \end{cases}$$

και βρίσκουμε $X = xd - yb,\ Y = ay - cx$. Επομένως, $g(xd - yb, ay - cx) = n$.

Παρατήρηση 1.3.5 Αν $f = [a, b, c] \sim g = [n, k, l]$, δηλαδή υπάρχει πίνακας

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$$

τέτοιος ώστε $g = f|_M$, τότε $n = f(\alpha, \gamma)$ και μάλιστα η παράσταση είναι γνήσια. Με άλλα λόγια, η f παριστά γνήσια το συντελεστή του X^2 κάθε ισοδύναμής της.

Πράγματι,

$$g(X, Y) = f(\alpha X+\beta Y, \gamma X+\delta Y) \Rightarrow nX^2+kXY+lY^2 = (a\alpha^2+b\alpha\gamma+c\gamma^2)X^2+...,$$

δηλαδή

$$n = a\alpha^2 + b\alpha\gamma + c\gamma^2 = f(\alpha, \gamma).$$

Η παράσταση είναι γνήσια γιατί η ορίζουσα του πίνακα είναι $\alpha\delta - \beta\gamma = 1$, από όπου άμεσα προκύπτει $(\alpha, \gamma) = 1$.

Παρατήρηση 1.3.6 Ισχύει και το αντίστροφο της προηγούμενης παρατήρησης:

Έστω ότι ο n παρίσταται γνήσια από την $f = [a, b, c]$. Τότε υπάρχουν $\alpha,\ \gamma \in \mathbb{Z}$ με $(\alpha, \gamma) = 1$ τέτοια ώστε $n = f(\alpha, \gamma)$.

Αφού $(\alpha, \gamma) = 1$ υπάρχουν $\beta, \delta \in \mathbb{Z}$ τέτοια ώστε $\alpha\delta - \beta\gamma = 1$. Επομένως, η τετραγωνική μορφή $g = f|_M$, όπου

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$$

είναι ισοδύναμη της f και μάλιστα

$$g(X, Y) = f(\alpha X + \beta Y, \gamma X + \delta Y) = (a\alpha^2 + b\alpha\gamma + c\gamma^2)X^2 + ... = nX^2 + ...,$$

δηλαδή η g έχει συντελεστή του X^2 το n.

Από τις παρατηρήσεις 1.3.5 και 1.3.6 προκύπτει η ακόλουθη πρόταση:

Πρόταση 1.3.7 Το σύνολο των ακεραίων που παρίστανται γνήσια από την τετραγωνική μορφή $f = [a, b, c]$ ταυτίζεται με το σύνολο των ακεραίων που εμφανίζονται ως συντελεστές του X^2 για όλες τις τετραγωνικές μορφές που είναι ισοδύναμες με την f.

Παρατήρηση 1.3.8 Έστω $C(\Delta)$ το σύνολο των κλάσεων πρωταρχικά ορισμένων τετραγωνικών μορφών διακρίνουσας Δ. Μπορούμε τότε να ορίσουμε

σύνθεση μεταξύ των τετραγωνικών μορφών. Βασικά εργαζόμαστε με αντιπροσώπους των κλάσεων, δηλαδή το σύνολο των ανηγμένων τετραγωνικών μορφών διακρίνουσας Δ. Έτσι το σύνολο $C(\Delta)$ αποκτά δομή πεπερασμένης αβελιανής ομάδας τάξης ίσης με το πλήθος των κλάσεων τετραγωνικών μορφών διακρίνουσας Δ.

Το μοναδιαίο στοιχείο της ομάδας είναι η κλάση της θεμελιώδους τετραγωνικής μορφής

$$f(X,Y) = X^2 - \frac{\Delta}{4}Y^2, \text{ αν } \Delta \equiv 0(mod 4)$$

ή της θεμελιώδους τετραγωνικής μορφής

$$f(X,Y) = X^2 + XY + \frac{1-\Delta}{4}Y^2, \text{ αν } \Delta \equiv 1(mod 4).$$

Τέλος, η αντίστροφη κλάση της τετραγωνικής μορφής $f(X,Y) = aX^2+bXY+cY^2$ είναι η κλάση της τετραγωνικής μορφής $g(X,Y) = aX^2 - bXY + cY^2$.

Είμαστε τώρα σε θέση να αποδείξουμε την Πρόταση 1.2.14.

Απόδειξη. Έστω $f = [a,b,c],\ g = [a',b',c']$ δύο ανηγμένες θετικά ορισμένες τετραγωνικές μορφές, οι οποίες είναι ισοδύναμες. Αρκεί να δείξουμε ότι

$$a = a',\ b = b',\ c = c'.$$

Σαν πρώτο βήμα θα δείξουμε ότι οι μικρότεροι θετικοί ακέραιοι που παρίστανται γνήσια από μία ανηγμένη θετικά ορισμένη τετραγωνική μορφή $f = [a,b,c]$ είναι οι a, c και $a + c - |b|$ (όχι απαραίτητα διαφορετικοί μεταξύ τους).

Ισχύει ότι:

$$f(X,Y) = aX^2 + bXY + cY^2 = a\Big(X + \frac{b}{2a}Y\Big)^2 + \frac{4ac-b^2}{4a}Y^2.$$

Επειδή $a > 0$, ισχύει $a(x + \frac{b}{2a}y)^2 \geq 0$ για κάθε $x, y \in \mathbb{Z}$. Από τις ανισότητες $|b| \leq a \leq c \Rightarrow |b| \leq a,\ |b| \leq c$ προκύπτει $b^2 \leq ac \Rightarrow ac - b^2 \geq 0$.

Διακρίνουμε, τώρα, τρεις περιπτώσεις:

- Αν $|y| \geq 2$, έχουμε:

$$f(x,y) \geq \frac{4ac-b^2}{4a}y^2 = \frac{ac-b^2}{4a}y^2 + \frac{3ac}{4a}y^2 \geq 3c = c + 2c > c + a,$$

αφού $a \leq c \Rightarrow a < 2c$. Επομένως, ισχύει $f(x,y) > a + c$.

- Αν $y = \pm 1,\ |x| \geq 2$, τότε $f(x, \pm 1) = ax^2 \pm bx + c$. Επειδή $-a \leq b \leq a$, έχουμε

$$f(x, \pm 1) \geq a|x|^2 - a|x| + c = a|x|(|x| - 1) + c \geq 2a + c > a + c.$$

- Στις περιπτώσεις $y = 0$ και x οποιοσδήποτε ακέραιος ή $y = \pm 1$ και $|x| \leq 1$:

  Επειδή ενδιαφερόμαστε μόνο για γνήσιες παραστάσεις, δηλαδή $(x, y) = 1$, η πρώτη συνθήκη μας δίνει $(x, 0) = |x| = 1 \Rightarrow x = \pm 1$, δηλαδή το ζεύγος $(\pm 1, 0)$. Από τη δεύτερη συνθήκη έχουμε $(x, \pm 1) = 1$, συνεπώς για $x = 0$ παίρνουμε το $(0, \pm 1)$, ενώ για $x = \pm 1$ τα $(1, \pm 1),\ (-1, \pm 1)$. Τα ζευγάρια αυτά παριστούν τους ακέραιους αριθμούς $a,\ c,\ a \pm b + c,\ a \mp b + c$ αντίστοιχα.

Επομένως, οι τρεις πιο μικροί θετικοί ακέραιοι που η τετραγωνική μορφή f παριστά γνήσια είναι οι $a \leq c \leq a + c - |b|$. Παρατηρούμε, ακόμη, ότι όταν ισχύει $a < c$, τότε

$$ax^2 + bxy + cy^2 = a \Leftrightarrow x = \pm 1, y = 0$$

και επίσης $f(0, \pm 1) \neq a$. Ανάλογα, οι μικρότεροι θετικοί ακέραιοι που παριστά η g γνήσια είναι οι $a' \leq c' \leq a' + c' - |b'|$ και ισχύει η ίδια παρατήρηση.

Τώρα, εφόσον $f \sim g$, υπάρχει πίνακας

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$$

τέτοιος ώστε $g = f|_A$. Επίσης, ως ισοδύναμες, οι $f,\ g$ παριστούν γνήσια τους ίδιους ακεραίους, άρα και τους ελάχιστους, $a,\ a'$. Από αυτό προκύπτει αναγκαστικά ότι $a = a'$.

Η Παρατήρηση 1.3.5 και η τελευταία ισότητα μας δίνουν τη σχέση

$$a = a\alpha^2 + b\alpha\gamma + c\gamma^2 \tag{1.1}$$

Διακρίνουμε ξανά τρεις περιπτώσεις:

- Αν $a < c$, τότε $-a < b \leq a < c$. Από τη σχέση 1.1 συμπεραίνουμε ότι $\alpha = \pm 1,\ \gamma = 0$ και αφού $\alpha\delta - \beta\gamma = 1$ θα ισχύει $\delta = \alpha = \pm 1$. Επομένως,

$$\begin{pmatrix} x \\ y \end{pmatrix} = A \cdot \begin{pmatrix} x' \\ y' \end{pmatrix},$$

όπου

$$A = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \text{ ή } A = \begin{pmatrix} -1 & \beta \\ 0 & -1 \end{pmatrix}.$$

Από την ισότητα $g(X,Y) = f(\alpha X + \beta Y, \gamma X + \delta Y)$ για το b' προκύπτει

$$b' = 2a\alpha\beta + b\alpha\delta = \pm 2a\beta + b \Rightarrow |b' - b| = 2a|\beta|.$$

Όμως $-a < b, b' \leq a \Rightarrow |b' - b| < 2a$. Επομένως $2a|\beta| < 2a \Rightarrow |\beta| < 1 \Rightarrow \beta = 0$. Για τον πίνακα A, συνεπώς, θα ισχύει

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ ή } A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

δηλαδή $A = I_2$ ή $A = -I_2$. Και οι δύο αυτοί πίνακες δίνουν $b = b',\ c = c'$.

- Η περίπτωση $a' < c'$ είναι συμμετρική της προηγούμενης.
- Έστω, τέλος, $a = c$ και $a' = c'$. Η ισότητα $a = a'$ αποδείχθηκε ανεξάρτητα της περιπτωσιολογίας παραπάνω, συνεπώς $f = [a,b,c] \sim g = [a,b',c']$. Αμέσως έχουμε ότι $c = c'$ και $b, b' > 0$. Αν $\Delta_f,\ \Delta_g$ οι διακρίνουσες των $f,\ g$ αντίστοιχα, λόγω της ισοδυναμίας των τετραγωνικών μορφών έχουμε ότι $\Delta_f = \Delta_g \Rightarrow b^2 - 4ac = b'^2 - 4a'c' \Rightarrow b = b'$.

Η απόδειξη, λοιπόν, ολοκληρώθηκε. □

Ακολουθεί ένα κριτήριο που μας λέει πότε ένας ακέραιος αριθμός παρίσταται από μία τετραγωνική μορφή.

Θεώρημα 1.3.9

1. Έστω ότι ο $n \in \mathbb{Z}$ παρίσταται γνήσια από την $f = [a,b,c]$, διακρίνουσας $\Delta_f = b^2 - 4ac$. Τότε η Δ_f είναι τετραγωνικό υπόλοιπο $mod 4|n|$, δηλαδή η ισοτιμία $x^2 \equiv \Delta_f (mod 4|n|)$ έχει λύση.
2. Αν ο αριθμός Δ είναι τετραγωνικό υπόλοιπο $mod 4|n|$, δηλαδή η ισοτιμία $x^2 \equiv \Delta (mod 4|n|)$ έχει λύση, τότε ο n παρίσταται γνήσια από κάποια τετραγωνική μορφή διακρίνουσας Δ.

Απόδειξη. 1. Αφού ο n παρίσταται γνήσια από την f, από την Παρατήρηση 1.3.6 υπάρχει τετραγωνική μορφή $g = [n,k,l]$ με $f \sim g$. Επομένως, θα ισχύει $\Delta_f = \Delta_g \Rightarrow \Delta_f = k^2 - 4nl \Rightarrow k^2 = \Delta_f + 4nl \equiv \Delta_f (mod 4|n|)$, δηλαδή η ισοτιμία $x^2 \equiv \Delta_f (mod 4|n|)$ έχει λύση, $x = k$. Επομένως, η Δ_f είναι τετραγωνικό υπόλοιπο $mod|4n|$.

2. Γνωρίζουμε ότι υπάρχει $t \in \mathbb{Z}$ τέτοιο ώστε $t^2 \equiv \Delta(mod4|n|)$, δηλαδή $t^2 = \Delta + 4|n|l \Rightarrow \Delta = t^2 - 4|n|l,\ l \in \mathbb{Z}$. Τότε η τετραγωνική μορφή $g = nX^2 + tXY + lY^2$ έχει διακρίνουσα Δ και παριστά γνήσια τον n, αφού $g(1,0) = n$.

□

Πόρισμα 1.3.10 Αν όλες οι τετραγωνικές μορφές διακρίνουσας Δ είναι μεταξύ τους ισοδύναμες (αν, δηλαδή, $h(\Delta) = 1$), τότε η ύπαρξη λύσης της ισοτιμίας $x^2 \equiv \Delta(mod4|n|)$ για $n \in \mathbb{Z}$ είναι ισοδύναμη με το ότι ο n παρίσταται γνήσια από κάθε τετραγωνική μορφή διακρίνουσας ίσης με Δ.

Τελειώνοντας αυτή την ενότητα και κλείνοντας, έτσι, το κεφάλαιο των τετραγωνικών μορφών, θα δώσουμε κάποιες πιο ειδικές προτάσεις σχετικά με την παράσταση ακεραίων από τετραγωνικές μορφές.

Πρόταση 1.3.11 Κάθε πρώτος αριθμός $p \equiv 1(mod4)$ παρίσταται ως άθροισμα δύο τετραγώνων.

Απόδειξη. Έστω ότι υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε $p = x^2 + y^2 = f(x,y)$, όπου $f = [1,0,1]$. Η διακρίνουσα της f είναι $\Delta = -4$. Καταρχήν θα δείξουμε ότι $h(-4) = 1$.

Έστω λοιπόν $aX^2 + bXY + cY^2$ τυχαία ανηγμένη θετικά ορισμένη τετραγωνική μορφή διακρίνουσας -4. Έχουμε ότι $0 < a^2 \leq \frac{4}{3}$, άρα $a = 1$. Επομένως, $|b| \leq 1 \Rightarrow b \in \{-1, 0, 1\}$. Αν $|b| = 1 = a$, επιλέγουμε $b = 1$. Τότε $c = \frac{5}{4} \notin \mathbb{Z}$, δηλαδή η περίπτωση αυτή απορρίπτεται. Αν τώρα $b = 0$, βρίσκουμε $c = 1$, άρα έχουμε μοναδική ανηγμένη την $f = [1,0,1]$ και $h(-4) = 1$.

Τώρα, η παράσταση του p από την f είναι γνήσια, γιατί, αν $(x,y) = d$, δηλαδή $x = dx_1,\ y = dy_1$, έπεται ότι $p = d^2(x_1^2 + y_1^2)$, δηλαδή $d^2 \mid p \Rightarrow d = 1$.

Απομένει να δείξουμε ότι θα πρέπει $p \equiv 1(mod4)$. Από το Πόρισμα 1.3.10 ο p παρίσταται από την f αν και μόνο αν η ισοτιμία

$$x^2 \equiv (-4)(mod4p)$$

έχει λύση. Πρέπει, δηλαδή, να ισχύει $x = 2x_1$, όπου το x_1 είναι λύση της ισοτιμίας

$$x^2 \equiv (-1)(modp).$$

Αυτή η ισοτιμία έχει λύση αν και μόνο αν το σύμβολο του Legendre, $(\frac{-1}{p})$, ισούται με 1, δηλαδή αν και μόνο αν

$$(-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p \equiv 1(mod4).$$

□

Θεώρημα 1.3.12 Έστω $n = a^2 \cdot b$, όπου ο b είναι ελεύθερος τετραγώνων. Τότε ο n γράφεται ως άθροισμα δύο τετραγώνων αν και μόνο αν δεν υπάρχει p πρώτος αριθμός, με $p \equiv 3(mod4)$, που διαιρεί τον b.

Απόδειξη. Έστω ότι $n = x^2 + y^2$ και ότι υπάρχει p πρώτος αριθμός, $p \equiv 3(mod4)$, που διαιρεί τον b. Τότε $n = a^2 \cdot b = a^2pk \Rightarrow x^2 + y^2 = a^2pk$, όπου $k \in \mathbb{Z}$. Ισχύει, επομένως,

$$x^2 \equiv -y^2(modp) \tag{1.2}$$

Αν $y \not\equiv 0(modp)$, τότε η ισοτιμία $y\varphi \equiv 1(modp)$ έχει λύση, έστω $\varphi = y^{-1}$. Οπότε

$$(x \cdot y^{-1})^2 \equiv -1(modp),$$

δηλαδή η ισοτιμία $z^2 \equiv -1(modp)$ έχει λύση. Αυτό σημαίνει ότι το σύμβολο του Legendre $(\frac{-1}{p})$ ισούται με 1. Αυτό όμως είναι άτοπο, καθώς $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = -1$, αφού $p \equiv 3(mod4)$. Επομένως, η ισοτιμία $z^2 \equiv -1(modp)$ δεν έχει λύση. Άρα $y \equiv 0(modp) \Rightarrow p \mid y$, και από την σχέση 1.2 προκύπτει $p \mid x$. Συνεπώς, $p^2 \mid n$ και

$$\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2.$$

Αν τώρα $p \mid \frac{n}{p^2}$, επαναλαμβάνουμε τη διαδικασία. Τελικά προκύπτει ότι η μέγιστη δύναμη του p που διαιρεί το n είναι άρτια, το οποίο είναι άτοπο, καθώς υποθέσαμε ότι $p \mid b$ και ο b είναι ελεύθερος τετραγώνων.

Αντίστροφα, έστω ότι δεν υπάρχει πρώτος αριθμός $p \equiv 3(mod4)$ που διαιρεί τον b.

Παρατηρούμε το εξής: Αν έχουμε δύο ακέραιους αριθμούς που γράφονται ως άθροισμα δύο τετραγώνων, έστω $a^2+b^2,\ c^2+d^2$, τότε για το γινόμενό τους ισχύει:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

δηλαδή και το γινόμενό τους γράφεται ως άθροισμα δύο τετραγώνων. Επαγωγικά, το ίδιο ισχύει για γινόμενο κ ακεραίων.

Τώρα,

$$n = a^2 \cdot b = 2^r q_1^{2s_1} q_2^{2s_2} ... q_k^{2s_k} \cdot p_1 p_2 ... p_m,$$

όπου $p_i \equiv 1(mod4), p_i \neq p_j$ για $i \neq j$.

Τότε $q_i^{2s_i} = (q_i^{s_i})^2 + 0$, δηλαδή τα $q_i^{2s_i}$ γράφονται σαν άθροισμα δύο τετραγώνων. Επίσης, $p_i \equiv 1(mod4)$, άρα από την Πρόταση 1.3.11 γράφονται και αυτοί ως άθροισμα δύο τετραγώνων. Τέλος, $2 = 1^2 + 1^2$, άρα και ο 2^r γράφεται ως άθροισμα δύο τετραγώνων.

Συμπεραίνουμε ότι ο n γράφεται ως άθροισμα δύο τετραγώνων ως γινόμενο αριθμών που γράφονται ως άθροισμα δύο τετραγώνων. □

Πρόταση 1.3.13 Αν p πρώτος αριθμός, τότε ο p μπορεί να παρασταθεί από την τετραγωνική μορφή X^2+2Y^2 αν και μόνο αν $p \equiv 1(mod8)$ ή $p \equiv 3(mod8)$.

Απόδειξη. Έστω ότι υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε $p = x^2 + 2y^2 = f(x, y)$. Η διακρίνουσα της f είναι $\Delta = -8$. Θα αποδείξουμε, καταρχήν, ότι $h(-8) = 1$.

Έστω λοιπόν $aX^2 + bXY + cY^2$ τυχαία ανηγμένη θετικά ορισμένη τετραγωνική μορφή διακρίνουσας -8. Έχουμε ότι $0 < a^2 \leq \frac{8}{3}$, άρα $a = 1$. Επομένως, $|b| \leq 1 \Rightarrow b \in \{-1, 0, 1\}$. Αν $|b| = 1 = a$, επιλέγουμε $b = 1$. Τότε $c = \frac{9}{4} \notin \mathbb{Z}$, δηλαδή η περίπτωση αυτή απορρίπτεται. Αν τώρα $b = 0$, βρίσκουμε $c = 2$, άρα έχουμε μοναδική ανηγμένη την $f = [1, 0, 2]$ και $h(-8) = 1$.

Από το Πόρισμα 1.3.10, ο p παρίσταται από την f αν και μόνο αν η ισοτιμία

$$x^2 \equiv (-8)(mod4p)$$

έχει λύση, δηλαδή αν και μόνο αν $x = 2x_1$ με x_1 λύση της ισοτιμίας

$$\chi^2 \equiv (-2)(modp).$$

Η ισοτιμία αυτή έχει λύση αν και μόνο αν

$$\left(\frac{-2}{p}\right) = 1 \Leftrightarrow \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = 1.$$

Επομένως, έχουμε δύο περιπτώσεις:

- Έστω $(-1)^{\frac{p-1}{2}} = 1$ και $(-1)^{\frac{p^2-1}{8}} = 1$. Η πρώτη ισότητα μας δίνει την ισοτιμία $p \equiv 1(mod4)$, ενώ από τη δεύτερη προκύπτει $p \equiv 1(mod8)$ ή $p \equiv 7(mod8)$. Από την $p \equiv 1(mod4)$ συνεπάγεται $p \equiv 1(mod8)$ ή $p \equiv 5(mod8)$. Συνδυάζοντας τις ισοτιμίες συμπεραίνουμε ότι σε αυτή την περίπτωση πρέπει να ισχύει $p \equiv 1(mod8)$.

- Έστω $(-1)^{\frac{p-1}{2}} = -1$ και $(-1)^{\frac{p^2-1}{8}} = -1$. Έπεται από την πρώτη σχέση $p \equiv 3(mod4) \Leftrightarrow p \equiv 3(mod8)$ ή $p \equiv 7(mod8)$ και από τη δεύτερη προκύπτουν οι ισοτιμίες $p \equiv 3(mod8)$ ή $p \equiv 5(mod8)$. Επομένως, σε αυτή την περίπτωση θα πρέπει να ισχύει $p \equiv 3(mod8)$.

□

1.4 Σημειώσεις

Η θεωρία των (θετικά ορισμένων) τετραγωνικών μορφών αποτελεί μέρος του περιεχομένου κάθε βιβλίου στοιχειώδους Θεωρίας Αριθμών. Ενδεικτικά αναφέρουμε τα [1],[8],[23] και [31].

Για την απόδειξη του Θεωρήματος 1.2.3 συμβουλευτήκαμε το άρθρο του Keith Conrad, $SL_2(\mathbb{Z})$. Ο ενδιαφερόμενος αναγνώστης μπορεί επίσης να ανατρέξει στο [4] (σελ.26-30).

Τέλος, στην απόδειξη της Πρότασης 1.3.7 ακολουθήσαμε το [15].

Κεφάλαιο 2

Στοιχεία Αλγεβρικής Θεωρίας Αριθμών

2.1 Εισαγωγικά Στοιχεία

Πριν προχωρήσουμε στη μελέτη των τετραγωνικών σωμάτων αριθμών, θα αναφερθούμε σε κάποια βασικά στοιχεία αλγεβρικής θεωρίας αριθμών, που θα χρησιμοποιήσουμε παρακάτω.

Ορισμός 2.1.1 Ο μιγαδικός αριθμός α θα λέγεται *αλγεβρικός* όταν αποτελεί ρίζα ενός πολυωνύμου $f(x) \in \mathbb{Q}[x],\ f \neq 0$.

Το σύνολο των αλγεβρικών αριθμών αποτελεί υπόσωμα του $\mathbb{C}$. Λέγεται *αλγεβρική θήκη* του $\mathbb{Q}$ και συμβολίζεται με $\widetilde{\mathbb{Q}}$.

Ορισμός 2.1.2 Ο $\alpha \in \widetilde{\mathbb{Q}}$ θα λέγεται *ακέραιος αλγεβρικός* όταν το ανάγωγο πολυώνυμο του α, $Irr(\alpha, \mathbb{Q})$, έχει ακέραιους συντελεστές, δηλαδή

$$Irr(\alpha, \mathbb{Q}) \in \mathbb{Z}[x].$$

Παρατήρηση 2.1.3 Αν συμβολίσουμε $\widetilde{\mathbb{Z}}$ το σύνολο των ακέραιων αλγεβρικών αριθμών, αυτό αποτελεί ακέραια περιοχή της οποίας το σώμα πηλίκων είναι το $\widetilde{\mathbb{Q}}$.

Παρατήρηση 2.1.4 Κάθε αλγεβρικός αριθμός μπορεί να παρασταθεί ως πηλίκο ενός ακέραιου αλγεβρικού με ένα φυσικό αριθμό. Πράγματι, αν $\alpha \in \widetilde{\mathbb{Q}}$ και $Irr(\alpha, \mathbb{Q}) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \ \in \mathbb{Q}[x]$, θέτουμε $m \in \mathbb{N}$ το γινόμενο των παρονομαστών των a_i. Τότε ο αριθμός $b = \alpha m$ είναι ρίζα του πολυωνύμου

$m^n f(x/m)$, το οποίο είναι μονικό και έχει ακέραιους συντελεστές. Επομένως, $\alpha = b/m,\ b \in \widetilde{\mathbb{Z}},\ m \in \mathbb{N}$.

2.2 Αλγεβρικά Σώματα Αριθμών

Ορισμός 2.2.1 Ένα *αλγεβρικό σώμα αριθμών* K είναι μία πεπερασμένη επέκταση του $\mathbb{Q}$ που περιέχεται στο $\mathbb{C}$.

Προφανώς η επέκταση $K/\mathbb{Q}$ είναι πεπερασμένη (άρα και αλγεβρική) και διαχωρίσιμη, επομένως είναι απλή. Υπάρχει, δηλαδή, ένα στοιχείο $\theta \in K$ τέτοιο ώστε $K = \mathbb{Q}(\theta)$. Λόγω της Παρατήρησης 2.1.4, μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι ο θ είναι ακέραιος αλγεβρικός.

Είναι γνωστό ότι ο βαθμός της επέκτασης $n = [K : \mathbb{Q}]$ ισούται με τον βαθμό του πολυωνύμου $p(x) := Irr(\theta, \mathbb{Q})$. Αν $\theta^{(1)} =: \theta, \theta^{(2)}, ..., \theta^{(n)}$ οι ρίζες του ανάγωγου πολυωνύμου $p(x)$ του θ υπέρ του $\mathbb{Q}$, υπάρχουν ακριβώς n $\mathbb{Q}-$μονομορφισμοί του σώματος K στο $\mathbb{C}$, έστω $\sigma_1, \sigma_2, ..., \sigma_n$.

Ορισμός 2.2.2 Τα σώματα

$$K^{(i)} = \sigma_i(K) = \mathbb{Q}(\theta^{(i)})$$

για $i = 1, 2, ..., n$ λέγονται *συζυγή σώματα* του K. Επίσης, για κάθε $\alpha \in K$, οι αριθμοί $\alpha^{(i)} = \sigma_i(\alpha),\ i = 1, 2, ..., n$, λέγονται *συζυγείς αριθμοί* του α.

Αν το ανάγωγο πολυώνυμο $p(x) := Irr(\theta, \mathbb{Q})$ έχει r_1 πραγματικές ρίζες και $2r_2$ μιγαδικές ρίζες, τότε ισχύει:

$$n = r_1 + 2r_2.$$

Επομένως, r_1 από τα συζυγή σώματα του K περιέχονται στο $\mathbb{R}$ και $2r_2$ από αυτά είναι μιγαδικά υποσώματα του $\mathbb{C}$.

Ορισμός 2.2.3 Η εμφύτευση σ_i θα λέγεται *πραγματική* όταν

$$K^{(i)} = \mathbb{Q}(\theta^{(i)}) \leq \mathbb{R},$$

διαφορετικά θα λέγεται *μιγαδική*. Το διατεταγμένο ζεύγος $[r_1, r_2]$ θα λέγεται *ταυτότητα* του σώματος K.

Οι δύο οριακές περιπτώσεις είναι όταν $r_1 = 0$ ή $r_2 = 0$. Αν η ταυτότητα του σώματος K είναι $[r_1, 0]$, τότε λέμε ότι το σώμα είναι *πλήρως (ή ολικά) πραγματικό*. Αν, πάλι, η ταυτότητα του K είναι $[0, r_2]$, τότε το σώμα K θα λέγεται

πλήρως μιγαδικό.

Αν $\sigma_1, \sigma_2, ..., \sigma_{r_1}$ είναι οι πραγματικές εμφυτεύσεις του σώματος K, τότε το στοιχείο $\alpha \in K$ θα λέγεται *πλήρως θετικό* όταν $\sigma_i(\alpha) > 0$, για κάθε $\sigma_i,\ i = 1, 2, ..., r_1$.

Παρατήρηση 2.2.4 Αν $\alpha \in K = \mathbb{Q}(\theta)$, οι συζυγείς αριθμοί του α είναι οι ρίζες του $Irr(\alpha, \mathbb{Q}) =: f(x)$, αφού

$$f(\alpha^{(i)}) = f(\sigma_i(\alpha)) = \sigma_i(f(\alpha)) = \sigma_i(0) = 0.$$

Αν $degf(x) = degIrr_{\mathbb{Q}}(\alpha) < n = [K : \mathbb{Q}]$, τότε οι συζυγείς του α δεν είναι όλοι διαφορετικοί μεταξύ τους.

Ορισμός 2.2.5 Έστω $K = \mathbb{Q}(\theta)$ αλγεβρικό σώμα αριθμών με $[K : \mathbb{Q}] = n$ και $\alpha \in K$. Ορίζουμε το *ίχνος* του α ως

$$S_K(\alpha) := \alpha^{(1)} + \alpha^{(2)} + ... + \alpha^{(n)}$$

και τη *norm* του α ως

$$N_K(\alpha) := \alpha^{(1)} \cdot \alpha^{(2)} \cdot ... \cdot \alpha^{(n)}.$$

Ισχύει το εξής:

Αν $\alpha \in K,\ Irr(\alpha, \mathbb{Q}) = a_0 + a_1 x + ... + a_{m-1}x^{m-1} + x^m$ και $s = n/m$, όπου $[K : \mathbb{Q}] = n$, τότε:

$$S_K(\alpha) = -sa_{m-1}, \quad N_K(\alpha) = (-1)^n a_0^s.$$

Προφανώς, για κάθε $\alpha \in K$ ισχύει $S_K(\alpha), N_K(\alpha) \in \mathbb{Q}$. Μάλιστα, αν α ακέραιος αλγεβρικός, τότε $S_K(\alpha), N_K(\alpha) \in \mathbb{Z}$.

Ισχύουν, τέλος, τα ακόλουθα:
Έστω $\alpha \in K = \mathbb{Q}(\theta)$. Τότε

$$\alpha \in \mathbb{Q} \Longleftrightarrow \sigma_1(\alpha) = \sigma_2(\alpha) = ... = \sigma_n(\alpha).$$

Επίσης,

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\theta) \Longleftrightarrow \sigma_i(\alpha) \neq \sigma_j(\alpha),$$

για κάθε $i, j \in \{1, 2, ..., n\}, i \neq j$.

2.3 Βάση Ακεραιότητας και Διακρίνουσα

Ορισμός 2.3.1 Έστω $K = \mathbb{Q}(\theta)$ αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$ και $a_1, a_2, ..., a_n$ μία $n-$άδα στοιχείων του σώματος K. Συμβολίζουμε τους συζυγείς του a_i με $a_i^{(1)} = a_i, a_i^{(2)}, ..., a_i^{(n)},\ i = 1, 2, ..., n$. Ορίζουμε ως *διακρίνουσα* της $n-$άδας $(a_1, a_2, ..., a_n)$ τον αριθμό

$$d(a_1, a_2, ..., a_n) = \begin{vmatrix} a_1^{(1)} & a_1^{(2)} & \dots & a_1^{(n)} \\ a_2^{(1)} & a_2^{(2)} & \dots & a_2^{(n)} \\ \vdots & \vdots & \dots & \vdots \\ a_n^{(1)} & a_n^{(2)} & \dots & a_n^{(n)} \end{vmatrix}^2 .$$

Επειδή ισχύει

$$d(a_1, a_2, ..., a_n) = \begin{vmatrix} S_K(a_1^2) & S_K(a_1a_2) & \dots & S_K(a_1a_n) \\ S_K(a_2a_1) & S_K(a_2^2) & \dots & S_K(a_2a_n) \\ \vdots & \vdots & \dots & \vdots \\ S_K(a_na_1) & S_K(a_na_2) & \dots & S_K(a_n^2) \end{vmatrix},$$

έπεται ότι $d(a_1, a_2, ..., a_n) \in \mathbb{Q}$. Μάλιστα, αν $a_1, a_2, ..., a_n$ ακέραιοι αλγεβρικοί, τότε $d(a_1, a_2, ..., a_n) \in \mathbb{Z}$.

Ως διακρίνουσα ενός $\alpha \in K$ ορίζεται η διακρίνουσα $d(1, \alpha, ..., \alpha^{n-1})$. Εδώ έχουμε μία ορίζουσα Vandermonde:

$$d(\alpha) := d(1, \alpha, ..., \alpha^{n-1}) = \prod_{i>j} (\alpha^{(i)} - \alpha^{(j)})^2.$$

Είναι φανερό ότι $K = \mathbb{Q}(\alpha) \Leftrightarrow d(\alpha) \neq 0$.

Πρόταση 2.3.2 Αν $K = \mathbb{Q}(\theta)$ αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$ και $\alpha \in K$ με $degIrr(\alpha, \mathbb{Q}) < n$, τότε $d(\alpha) = 0$. Αν πάλι $degIrr(\alpha, \mathbb{Q}) = degf(x) = n$, τότε ισχύει η ισότητα:

$$d(\alpha) = (-1)^{\frac{n(n-1)}{2}} N_K(f'(\alpha)),$$

όπου f' η παράγωγος του πολυωνύμου $f(x) = Irr(\alpha, \mathbb{Q})$.

Αν, τώρα, $\{\omega_1, \omega_2, ..., \omega_n\}$ μία βάση της επέκτασης $K/\mathbb{Q}$ και

$$\alpha_i = \sum_{j=1}^{n} a_{ij}\omega_j, \quad a_{ij} \in \mathbb{Q},\ i = 1, 2, ..., n,$$

τότε

$$d(\alpha_1, \alpha_2, ..., \alpha_n) = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}^2 \cdot d(\omega_1, \omega_2, ..., \omega_n).$$

Ορισμός 2.3.3 Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$ και $\{\omega_1, \omega_2, ..., \omega_n\}$ μία $n-$άδα ακέραιων αλγεβρικών αριθμών του σώματος K. Το σύνολο $\{\omega_1, \omega_2, ..., \omega_n\}$ θα λέγεται *βάση ακεραιότητας* του K αν:

1. είναι ένα $\mathbb{Q}-$γραμμικά ανεξάρτητο σύνολο και
2. κάθε ακέραιος αλγεβρικός αριθμός $\alpha \in K$ έχει μία (μονοσήμαντη) παράσταση της μορφής $\alpha = a_1\omega_1 + a_2\omega_2 + ... + a_n\omega_n,\ a_i \in \mathbb{Z}$.

Προκύπτει λογικά το ερώτημα αν υπάρχει πάντοτε μία βάση ακεραιότητας. Η απάντηση σε αυτό το ερώτημα είναι θετική. Συγκεκριμένα, ισχύει το εξής:

Θεώρημα 2.3.4 Κάθε αλγεβρικό σώμα αριθμών έχει μία τουλάχιστον βάση ακεραιότητας. Επιπλέον, όλες οι βάσεις ακεραιότητας ενός αλγεβρικού σώματος έχουν ίσες διακρίνουσες.

Ορισμός 2.3.5 Η διακρίνουσα μιας βάσης ακεραιότητας ενός αλγεβρικού σώματος αριθμών θα λέγεται *διακρίνουσα του σώματος*.

Διατυπώνουμε, τέλος, την ακόλουθη πρόταση:

Πρόταση 2.3.6 Η διακρίνουσα μίας $\mathbb{Q}-$γραμμικά ανεξάρτητης $n-$άδας ακέραιων αλγεβρικών στοιχείων ενός αλγεβρικού σώματος αριθμών ισούται με την διακρίνουσα του σώματος επί το τετράγωνο ενός φυσικού αριθμού.

2.4 Μονάδες

Ορισμός 2.4.1 Αν ε ακέραιος αλγεβρικός αριθμός, $\varepsilon \in \widetilde{\mathbb{Z}}$, τότε ο ε θα λέγεται *μονάδα* αν και ο αντίστροφός του, ε^{-1}, είναι ακέραιος αλγεβρικός, δηλαδή αν ο ε είναι μονάδα του δακτυλίου $\widetilde{\mathbb{Z}}$ των ακέραιων αλγεβρικών αριθμών.

Έστω τώρα $E(K)$ το σύνολο των μονάδων του $\widetilde{\mathbb{Z}}$, $E(\widetilde{\mathbb{Z}})$, που ανήκουν στο αλγεβρικό σώμα αριθμών K. Είναι προφανές ότι η $E(K)$ αποτελεί αντιμεταθετική υποομάδα της $E(\widetilde{\mathbb{Z}})$.

Πρόταση 2.4.2 Έστω $\varepsilon \in K$. Τότε:

$$\varepsilon \in E(K) \iff \text{ο } \varepsilon \text{ είναι ακέραιος αλγεβρικός και } N_K(\varepsilon) = \pm 1.$$

Παρατήρηση 2.4.3 Η ομάδα των ριζών της μονάδας ενός αλγεβρικού σώματος αριθμών είναι κυκλική πεπερασμένης τάξης, η οποία τάξη διαιρεί τον αριθμό $2d(K)$, όπου $d(K)$ η διακρίνουσα του σώματος K.

Θεώρημα 2.4.4 (Θεώρημα μονάδων του Dirichlet) Έστω K ένα αλγεβρικό σώμα αριθμών διακρίνουσας $d(K)$ και ταυτότητας $[r_1, r_2]$. Υπάρχουν r μονάδες του σώματος K, έστω $\varepsilon_1, \varepsilon_2, ..., \varepsilon_r$,[1] όπου $r = r_1 + r_2 - 1$, και μία ρίζα της μονάδας $\zeta \in K$ μέγιστης τάξης $m \mid 2d(K)$, έτσι ώστε κάθε μονάδα του σώματος, ε, να γράφεται μονοσήμαντα στη μορφή

$$\varepsilon = \zeta^s \varepsilon_1^{s_1} \varepsilon_2^{s_2} ... \varepsilon_r^{s_r}$$

με $0 \leq s < m$ και $s_1, s_2, ..., s_r \in \mathbb{Z}$.

Πιο συγκεκριμένα, αυτό σημαίνει ότι η ομάδα των μονάδων του K είναι το ευθύ γινόμενο

$$E(K) = < \zeta > \otimes < \varepsilon_1 > \otimes ... \otimes < \varepsilon_r >$$

μιας κυκλικής ομάδας $< \zeta >$ τάξης m και r κυκλικών ομάδων $< \varepsilon_1 >, ..., < \varepsilon_r >$ άπειρης τάξης. Είναι, δηλαδή, μία πεπερασμένα παραγόμενη αβελιανή ομάδα βαθμού $r = r_1 + r_2 - 1$.

2.5 Ο δακτύλιος R_K. Ιδεώδη

Έστω K ένα αλγεβρικό σώμα αριθμών. Συμβολίζουμε με R_K το σύνολο των ακέραιων αλγεβρικών αριθμών του σώματος K. Τότε το R_K είναι δακτύλιος και, μάλιστα, ακέραια περιοχή.

Για το σώμα K, ο δακτύλιος R_K είναι το αντίστοιχο του $\mathbb{Z}$ για το $\mathbb{Q}$, με μία σημαντική διαφορά: ο $\mathbb{Z}$ είναι περιοχή μονοσήμαντης ανάλυσης, δεν ισχύει όμως το ίδιο, εν γένει, και για τον R_K.

Πρόταση 2.5.1 Ο δακτύλιος R_K είναι περιοχή Dedekind με την ιδιότητα της πεπερασμένης norm. Αυτό σημαίνει ότι:

1. Ο R_K είναι ακέραια κλειστός, δηλαδή αν $\alpha \in K$ ακέραιο υπέρ του R_K, τότε $\alpha \in R_K$.

[1] Οι $\varepsilon_1, ..., \varepsilon_r$ λέγονται θεμελιώδεις μονάδες του σώματος K.

2. Ο R_K είναι περιοχή της Noether. Αυτό σημαίνει ότι ο R_K είναι ακέραια περιοχή και επίσης ισχύουν οι ακόλουθες, ισοδύναμες μεταξύ τους, προτάσεις:

   (α′) Κάθε αύξουσα ακολουθία ιδεωδών του R_K γίνεται τελικά σταθερή.

   (β′) Κάθε, διάφορο του κενού, σύνολο ιδεωδών του R_K περιέχει maximal στοιχεία.

   (γ′) Κάθε ιδεώδες του R_K είναι πεπερασμένα παραγόμενο.

3. Κάθε, μη-μηδενικό, πρώτο ιδεώδες του R_K είναι και maximal.

Παρατήρηση 2.5.2 Από την ιδιότητα (2) έπεται ότι κάθε στοιχείο $a \in R_K$ αναλύεται, όχι κατ'ανάγκη μονοσήμαντα, σε γινόμενο ανάγωγων στοιχείων.

Η πιο σημαντική ιδιότητα, από τη σκοπιά της Θεωρίας Αριθμών, που έχουν οι δακτύλιοι R_K είναι ότι κάθε μη-μηδενικό ιδεώδες του R_K αναλύεται μονοσήμαντα σε γινόμενο πρώτων (δηλαδή maximal) ιδεωδών.

Πρόταση 2.5.3 (Η ιδιότητα της πεπερασμένης norm) Αν $A \neq \{0\}$ ιδεώδες του R_K, τότε ο δακτύλιος πηλίκων R_K/A έχει πεπερασμένη τάξη.

Από εδώ και στο εξής δεν θεωρούμε το μηδενικό ιδεώδες του R_K ως ιδεώδες.

Ορισμός 2.5.4 Η τάξη του δακτυλίου R_K/A λέγεται *norm* του ιδεώδους A και συμβολίζεται $N_K(A)$.

Για κάθε ιδεώδες A του R_K ισχύει

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

Επίσης, ισχύει η πλήρως πολλαπλασιαστική ιδιότητα της norm: Αν A, B ιδεώδη του R_K, τότε

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

Η έννοια είναι συμβατή με την έννοια της norm στοιχείου του R_K. Συγκεκριμένα, αν $a \in R_K$, τότε ισχύει:

$$N_K(< a >) = |N_K(a)|.$$

Ιδιαίτερα, αν $A = P$ πρώτο ιδεώδες, τότε, αφού το P είναι και maximal, το πηλίκο R_K/P είναι πεπερασμένο σώμα. Επομένως, έχουμε ότι

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

για κάποιο πρώτο αριθμό p και φυσικό $f \geq 1$. Εύκολα συμπεραίνουμε με βάση τα προηγούμενα ότι $p \in P$. Αυτό σημαίνει ότι ένα πρώτο ιδεώδες περιέχει έναν πρώτο αριθμό, και μάλιστα αποδεικνύεται ότι ο πρώτος αυτός είναι μοναδικός.

Άλλη μία σημαντική ιδιότητα του R_K είναι ότι είναι ένα ελεύθερο $\mathbb{Z}-$module βαθμού $n = [K : \mathbb{Q}]$.

Θα γενικεύσουμε, τώρα, την έννοια του ιδεώδους.

Ορισμός 2.5.5 Ένα υποσύνολο A του αλγεβρικού σώματος K λέγεται *ιδεώδες* του σώματος K αν ισχύουν οι ακόλουθες ιδιότητες:

1. Αν $\alpha, \beta \in A$, τότε και $\alpha - \beta \in A$. Με άλλα λόγια, το A αποτελεί αβελιανή ομάδα ως προς την πρόσθεση του σώματος.
2. αν $\alpha \in A$ και $r \in R_K$, τότε και το $r\alpha \in A$.
3. Υπάρχει $\alpha \in A,\ \alpha \neq 0$, δηλαδή $A \neq < 0 >$.
4. Υπάρχει $\delta \in K,\ \delta \neq 0$ τέτοιο ώστε $\delta A \subseteq R_K$.

Αν ισχύει $A \subseteq R_K$, το A θα λέγεται *ακέραιο ιδεώδες* του K, διαφορετικά θα λέγεται *κλασματικό ιδεώδες* του K.

Σε πιο μοντέρνα γλώσσα, ένα ιδεώδες του K είναι ένα μη-μηδενικό πεπερασμένα παραγόμενο R_K-submodule του K.

Ορισμός 2.5.6 Αν $\alpha \in K,\ \alpha \neq 0$, τότε το σύνολο

$$< \alpha >= R_K\alpha = \{r\alpha \mid r \in R_K\}$$

είναι ιδεώδες του K και θα λέγεται *κύριο ιδεώδες* του K.

2.6 Αριθμός Κλάσεων Ιδεωδών

Έστω K αλγεβρικό σώμα αριθμών και R_K ο δακτύλιος των ακέραιων αλγεβρικών αριθμών αυτού. Έστω επίσης $n = [K : \mathbb{Q}]$.

Το σύνολο I_K των ιδεωδών του K αποτελεί αβελιανή, πολλαπλασιαστική ομάδα. Το σύνολο $H_K = \{< \alpha >= R_K\alpha \mid \alpha \in K^*\}$ αποτελεί υποομάδα της ομάδας I_K. Η ομάδα πηλίκων

$$\mathcal{R}_K := \frac{I_K}{H_K}$$

λέγεται *ομάδα κλάσεων ιδεωδών* του σώματος K.

Θεώρημα 2.6.1 Η ομάδα κλάσεων ιδεωδών οποιουδήποτε αλγεβρικού σώματος αριθμών είναι *πεπερασμένη* (αβελιανή) ομάδα.

Ορισμός 2.6.2 Η τάξη της ομάδας $\mathcal{R}_K$ λέγεται *αριθμός κλάσεων ιδεωδών* του σώματος K και συμβολίζεται h_K.

Συχνά θα συμβολίζουμε τον αριθμό κλάσεων ιδεωδών και ως $h(d(K))$, όπου $d(K)$ η διακρίνουσα του σώματος K.

Δύο ιδεώδη A, B του K ανήκουν στην ίδια κλάση ιδεωδών, $A \sim B$, αν υπάρχει αριθμός $\delta \neq 0$ του K τέτοιος ώστε να ισχύει $B =< \delta > A$.

Είναι προφανές ότι, αν $A^m =< \alpha >$, $\alpha \in K^*$ είναι κύριο ιδεώδες του K και $(m, h_K) = 1$, τότε κατ'ανάγκη το A είναι κύριο ιδεώδες του K. Επίσης, ισχύει $h_K = 1$ αν και μόνο αν ο δακτύλιος R_K είναι περιοχή μονοσήμαντης ανάλυσης (δηλαδή η έννοια της περιοχής κυρίων ιδεωδών συμπίπτει με την έννοια της περιοχής μονοσήμαντης ανάλυσης στη Θεωρία Αριθμών).

Στο ερώτημα υπολογισμού του αριθμού κλάσεων ιδεωδών ενός αλγεβρικού σώματος αριθμών, μία πρώτη απάντηση μας δίνει το ακόλουθο θεώρημα του Minkowski:

Θεώρημα 2.6.3 Έστω K αλγεβρικό σώμα αριθμών με $[K : \mathbb{Q}] = n$ και ταυτότητα $[r_1, r_2]$. Σε κάθε κλάση $\mathcal{K} \in \mathcal{R}_K$ υπάρχει ένα ιδεώδες $A \in \mathcal{K}$ με $N_K(A) \leq C_K$, όπου

$$C_K = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d(K)|^{1/2}.$$

Είναι, λοιπόν, αρκετό να καταγράψουμε όλα τα πρώτα ιδεώδη P με $N_K(P) \leq C_K$ και στη συνέχεια να ελέγξουμε ποια και πόσα από αυτά ανήκουν σε διαφορετικές κλάσεις.

Δύο σημαντικές συνέπειες του θεωρήματος του Minkowski είναι τα ακόλουθα δύο θεωρήματα:

Θεώρημα 2.6.4 (Hermite) Υπάρχουν το πολύ πεπερασμένου πλήθους αλγεβρικά σώματα αριθμών που έχουν κάποιο δοσμένο ακέραιο αριθμό ως διακρίνουσα.

Θεώρημα 2.6.5 Για κάθε αλγεβρικό σώμα αριθμών $K \neq \mathbb{Q}$ ισχύει:

$$|d(K)| > 1.$$

2.7 Νόμος Ανάλυσης και Θεωρία Διακλαδώσεως

Έστω K αλγεβρικό σώμα αριθμών και R_K ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του K. Αν p πρώτος αριθμός, τότε το κύριο ιδεώδες $< p >= R_K p$ του K αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών του K,

$$< p >= P_1^{e_1} P_2^{e_2} ... P_s^{e_s}, \quad e_i \in \mathbb{N}.$$

Μάλιστα, τα P_i είναι τα μόνα ιδεώδη του K που περιέχουν τον πρώτο p.

Ορισμός 2.7.1 Ο αριθμός s λέγεται *αριθμός αναλύσεως* του p στο K.

Ο αριθμός $e_i,\ i = 1, ..., s$, λέγεται *δείκτης διακλαδώσεως* του πρώτου ιδεώδους P_i στο K.

- Αν $e_i = 1$, λέμε ότι το P_i *δεν διακλαδίζεται* στο K. Αν $e_i > 1$, λέμε ότι το P_i *διακλαδίζεται* στο K.

- Αν $e_1 = e_2 = ... = e_s = 1$, τότε λέμε ότι ο πρώτος p *δεν διακλαδίζεται* στο K. Αν υπάρχει τουλάχιστον ένα $e_i > 1$, τότε λέμε ότι ο p *διακλαδίζεται* στο K.

Έστω $f_1, ..., f_s$ οι *βαθμοί αδρανείας* των πρώτων ιδεωδών $P_1, ..., P_s$, δηλαδή $N_K(P_i) = p^{f_i},\ i = 1, 2, ..., s$.

- Αν $f_i = 1$ λέμε ότι το πρώτο ιδεώδες P_i είναι *αδρανές* στο K.

- Αν $f_1 = ... = f_s = 1$, λέμε ότι ο πρώτος αριθμός p είναι *αδρανής* στο K.

Η εύρεση της ανάλυσης ενός πρώτου αριθμού σε γινόμενο πρώτων ιδεωδών του K λέγεται *νόμος ανάλυσης* για το σώμα K.

Θεώρημα 2.7.2 Έστω K αλγεβρικό σώμα αριθμών, R_K ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του K και $[K : \mathbb{Q}] = n$ ο βαθμός της επέκτασης $K/\mathbb{Q}$. Αν p πρώτος αριθμός και $< p >= P_1^{e_1} P_2^{e_2} ... P_s^{e_s}$, με $N_K(P_i) = p^{f_i}$, τότε ισχύει:

$$e_1 f_1 + e_2 f_2 + ... + e_s f_s = n.$$

Ειδικότερα, αν η επέκταση $K/\mathbb{Q}$ είναι επέκταση Galois, τότε ισχύουν

$$e_1 = e_2 = ... = e_s =: e, \quad f_1 = f_2 = ... = f_s =: f.$$

Συνεπώς, $e \cdot f \cdot s = n$, όπου $n = [K : \mathbb{Q}]$.

Ορισμός 2.7.3 Έστω p πρώτος αριθμός, $n = [K : \mathbb{Q}]$. Αν $< p >= P^n$, λέμε ότι ο p *διακλαδίζεται πλήρως* στο K. Αν $< p >= P_1 P_2 ... P_n$, λέμε ότι ο p *αναλύεται πλήρως* στο K.

Πώς, όμως, θα βρούμε τα πρώτα ιδεώδη που εμφανίζονται στην ανάλυση ενός πρώτου αριθμού p, καθώς και τους γεννήτορές αυτών; Απάντηση σε αυτό το ερώτημα μας δίνει το ακόλουθο θεώρημα.

Θεώρημα 2.7.4 (Dedekind) Έστω $K = \mathbb{Q}(\theta)$, $\theta \in R_K$, αλγεβρικό σώμα αριθμών βαθμού $[K : \mathbb{Q}] = n$. Υποθέτουμε ότι $R_K = \mathbb{Z}[\theta]$. Έστω επίσης p πρώτος αριθμός και $f(x) := Irr(\theta, \mathbb{Q})$.

Θεωρούμε την ανάλυση του πολυωνύμου $\overline{f}(x)$ που προκύπτει αν αντικαταστήσουμε τους συντελεστές του $f(x)$ με τις κλάσεις υπολοίπων τους $mod p$. Ισχύει, δηλαδή, $\overline{f}(x) \in \mathbb{F}_p[x]$. Αφού το $\mathbb{F}_p$ είναι σώμα, το $\overline{f}(x)$ θα έχει μονοσήμαντη ανάλυση της μορφής

$$\overline{f}(x) = \overline{f_1}(x)^{e_1} \overline{f_2}(x)^{e_2} ... \overline{f_s}(x)^{e_s}$$

σε γινόμενο ανάγωγων πολυωνύμων $\overline{f_i}(x) \in \mathbb{F}_p[x]$.

Τότε τα ιδεώδη

$$P_i =< p, f_i(\theta) >= R_K p + R_K f_i(\theta), \quad i = 1, 2, ..., s$$

είναι πρώτα ιδεώδη του K και ισχύει

$$< p >= R_K p = P_1^{e_1} P_2^{e_2} ... P_s^{e_s}, \quad N_K(P_i) = p^{f_i},$$

όπου $f_i = deg(\overline{f_i}(x))$.

Οφείλουμε να παρατηρήσουμε εδώ ότι το θεώρημα του Dedekind δεν είναι δυνατό να εφαρμοστεί σε οποιοδήποτε αλγεβρικό σώμα αριθμών, καθώς δεν είναι πάντοτε δυνατή η εύρεση ενός ακέραιου αλγεβρικού αριθμού θ τέτοιου ώστε οι δυνάμεις $1, \theta, ..., \theta^{n-1}$ (όπου n ο βαθμός της επέκτασης $K/\mathbb{Q}$) να αποτελούν βάση ακεραιότητας του K. Παρόλα αυτά, το θεώρημα εφαρμόζεται στα τετραγωνικά σώματα αριθμών, με τα οποία θα ασχοληθούμε στο επόμενο κεφάλαιο.

Διατυπώνουμε, τέλος, ένα ακόμη σημαντικό θεώρημα, γνωστό ως το Θεώρημα της Διακρίνουσας.

Θεώρημα 2.7.5 Έστω K αλγεβρικό σώμα αριθμών, p πρώτος αριθμός. Τότε ο p διακλαδίζεται στο K αν και μόνο αν ισχύει $p \mid d(K)$.

Άμεση συνέπεια αυτού του θεωρήματος είναι ότι το πλήθος των διακλαδιζόμενων πρώτων αριθμών στην επέκταση $K/\mathbb{Q}$ είναι *πεπερασμένο*.

Κεφάλαιο 3

Τετραγωνικά Σώματα Αριθμών

Θα εφαρμόσουμε την προηγούμενη θεωρία στα τετραγωνικά σώματα αριθμών, δηλαδή τα αλγεβρικά σώματα αριθμών K με $[K : \mathbb{Q}] = 2$.

3.1 Εισαγωγικά Στοιχεία

Έστω $K = \mathbb{Q}(\theta)$, όπου θ ακέραιος αλγεβρικός. Τότε το ανάγωγο πολυώνυμο του θ είναι της μορφής $Irr(\theta, \mathbb{Q}) = x^2 - ax + b$, όπου $a,\ b \in \mathbb{Z}$. Επομένως,

$$\theta = \frac{a \pm \sqrt{a^2 - 4b}}{2}.$$

Έστω $a^2 - 4b = mr^2$, με $m,\ r \in \mathbb{Z}$ και m ελεύθερος τετραγώνων. Τότε ισχύει $m \neq 1$, γιατί διαφορετικά το θ θα ήταν στοιχείο του $\mathbb{Q}$ και θα είχαμε $\mathbb{Q}(\theta) = \mathbb{Q}$. Συνεπώς,

$$\theta = \frac{a \pm r\sqrt{m}}{2}$$

και

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

Αποδείξαμε το εξής:

Πρόταση 3.1.1 Αν K τετραγωνικό σώμα αριθμών, τότε υπάρχει $m \neq 1$ ελεύθερος τετραγώνων τέτοιος ώστε $K = \mathbb{Q}(\sqrt{m})$.

Το σύνολο $\{1, \sqrt{m}\}$ είναι μία βάση της επέκτασης $K/\mathbb{Q}$, επομένως

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

Αν $m > 0$, το σώμα λέγεται *τετραγωνικό πραγματικό σώμα αριθμών*.
Αν $m < 0$, λέγεται *τετραγωνικό μιγαδικό σώμα αριθμών*.

Η επέκταση $K/\mathbb{Q}$ είναι κανονική και διαχωρίσιμη, επομένως είναι επέκταση Galois. Η ομάδα Galois είναι η $\{Id_K, \sigma\}$, όπου $\sigma : K \to K$ με

$$\sigma(a + b\sqrt{m}) = a - b\sqrt{m}.$$

Οι συζυγείς αριθμοί του $\alpha = \sqrt{m}$ είναι οι $\alpha^{(1)} = \alpha = \sqrt{m}$ και $\alpha^{(2)} = -\sqrt{m}$.

Από τον ορισμό του ίχνους και της norm που δώσαμε στην προηγούμενη ενότητα, έπεται ότι το ίχνος ενός αριθμού $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ ισούται με

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

ενώ η norm του α είναι ίση με

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

Πρόταση 3.1.2 Αν $\alpha \in \mathbb{Q}(\sqrt{m}) = K$, τότε $\alpha \in R_K$ αν και μόνο αν $S_K(\alpha),\ N_K(\alpha) \in \mathbb{Z}$, όπου R_K ο δακτύλιος των ακέραιων αλγεβρικών του σώματος K.

Απόδειξη. Αν $\alpha = a + b\sqrt{m} \in R_K$, γνωρίζουμε ότι οι συζυγείς του $\alpha^{(1)} = \alpha,\ \alpha^{(2)}$ ανήκουν επίσης στον R_K. Συνεπώς, $S_K(\alpha) = \alpha^{(1)} + \alpha^{(2)} = 2a,\ N_K(\alpha) = \alpha^{(1)} \cdot \alpha^{(2)} = a^2 + b^2 m \in \mathbb{Z}$.

Αντίστροφα, αν $S_K(\alpha),\ N_K(\alpha) \in \mathbb{Z}$, έπεται άμεσα ότι $\alpha \in R_K$, γιατί είναι ρίζα του πολυωνύμου $x^2 - S_K(\alpha)x + N_K(\alpha) \in \mathbb{Z}[x]$. □

3.2 Βάση Ακεραιότητας, Διακρίνουσα

Θα υπολογίσουμε τώρα τη βάση ακεραιότητας και τη διακρίνουσα του σώματος $\mathbb{Q}(\sqrt{m})$. Ξεκινάμε με την ακόλουθη πρόταση:

Πρόταση 3.2.1 Ο αριθμός

$$\alpha = \frac{a + b\sqrt{m}}{2} \in \mathbb{Q}(\sqrt{m}), \quad a,\ b \in \mathbb{Q}$$

είναι ακέραιος αλγεβρικός αν και μόνο αν:

1. $a,\ b \in \mathbb{Z}$
2. $a \equiv b(mod 2)$ για $m \equiv 1(mod 4)$ και $a \equiv b \equiv 0(mod 2)$ για $m \equiv 2,\ 3(mod 4)$.

Απόδειξη. ($\Leftarrow$) Έστω ότι για τον α ισχύουν οι δύο συνθήκες. Τότε $S_K(\alpha) = a \in \mathbb{Z}$ από τη συνθήκη 1, και

$$N_K(\alpha) = \frac{a^2 - b^2 m}{4}.$$

Αρκεί να δείξουμε ότι $N_K(\alpha) \in \mathbb{Z}$. Τότε θα έχουμε το ζητούμενο από την Πρόταση 3.1.2.

Διακρίνουμε δύο περιπτώσεις:

- Αν $m \equiv 1(mod4)$ και $a \equiv b \equiv 0(mod2)$, έστω $a = 2s,\ b = 2t,\ s,\ t \in \mathbb{Z}$, τότε $N_K(\alpha) = s^2 - mt^2 \in \mathbb{Z}$. Αν πάλι $a \equiv b \equiv 1(mod2)$, τότε έχουμε $a^2 \equiv b^2 \equiv mb^2 \equiv 1(mod4)$, συνεπώς $a^2 - b^2 m \equiv 0(mod4)$ και άρα $N_K(\alpha) \in \mathbb{Z}$.

- Αν $m \equiv 2,\ 3(mod4)$, οι $a,\ b$ είναι άρτιοι από τη συνθήκη 2, επομένως $a^2 \equiv b^2 \equiv 0(mod4)$ και άρα $N_K(\alpha) \in \mathbb{Z}$.

($\Rightarrow$) Έστω τώρα $\alpha = \frac{a+b\sqrt{m}}{2} \in R_K$. Τότε από την Πρόταση 3.1.2 έχουμε

$$S_K(\alpha) = a,\ N_K(\alpha) = \frac{a^2 - b^2 m}{4} \in \mathbb{Z},$$

άρα

$$a^2 - 4\frac{a^2 - b^2 m}{4} = mb^2 \in \mathbb{Z}.$$

Επειδή ο m είναι ελεύθερος τετραγώνων, προκύπτει ότι $b \in \mathbb{Z}$. Ισχύει, επομένως, η συνθήκη 1.

Τώρα, $N_K(\alpha) \in \mathbb{Z} \Rightarrow a^2 \equiv mb^2(mod4)$.

- Αν $m \equiv 1(mod4)$, τότε:

$$ma^2 \equiv mb^2(mod4) \Rightarrow a^2 \equiv b^2(mod4) \Rightarrow a \equiv b(mod2).$$

- Στην περίπτωση $m \equiv 2,\ 3(mod4)$, αν $m \equiv 2(mod4)$, τότε:

$$a^2 m \equiv 2mb^2(mod4) \Rightarrow a^2 \equiv 2b^2(mod4).$$

Αν ίσχυε $b \equiv 1(mod2)$, τότε θα είχαμε

$$b^2 \equiv 1(mod4) \Rightarrow 2b^2 \equiv 2(mod4) \Rightarrow a^2 \equiv 2(mod4).$$

Αυτό όμως είναι άτοπο, αφού για κάθε $n \in \mathbb{Z}$ ισχύει $n^2 \equiv 0(mod4)$ ή $n^2 \equiv 1(mod4)$. Επομένως,

$$b \equiv 0(mod2) \Rightarrow b^2 \equiv 0(mod4) \Rightarrow a^2 \equiv 0(mod4) \Rightarrow a \equiv 0(mod2).$$

Στην περίπτωση $m \equiv 3(mod4)$ έχουμε αντίστοιχα

$$a^2m \equiv 3mb^2(mod4) \Rightarrow a^2 \equiv 3b^2(mod4).$$

Αν $b \equiv 1(mod2)$, τότε θα έπρεπε $a^2 \equiv 3(mod4)$, που είναι άτοπο για τον ίδιο λόγο όπως προηγουμένως. Συνεπώς, πάλι ισχύει $b \equiv a \equiv 0(mod2)$.

□

Θεώρημα 3.2.2 Έστω

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2}, & \text{αν } m \equiv 1(mod4) \\ \sqrt{m}, & \text{αν } m \equiv 2,3(mod4). \end{cases}$$

Τότε το σύνολο $\{1, \omega\}$ αποτελεί βάση ακεραιότητας του τετραγωνικού σώματος $K = \mathbb{Q}(\sqrt{m})$. Η διακρίνουσα του K είναι

$$d(K) = \begin{cases} m, & \text{αν } m \equiv 1(mod4) \\ 4m, & \text{αν } m \equiv 2,3(mod4). \end{cases}$$

Απόδειξη. Καταρχήν, εύκολα παρατηρούμε ότι $1, \omega \in R_K$. Δείχνουμε τώρα ότι τα 1,ω είναι γραμμικά ανεξάρτητα. Έστω λοιπόν $a, b \in \mathbb{Q}$ τέτοια ώστε $a \cdot 1 + b \cdot \omega = 0$.

- Αν $\omega = \frac{1+\sqrt{m}}{2}$, τότε η παραπάνω σχέση γίνεται $a \cdot 1 + \frac{b+b\sqrt{m}}{2} = 0$. Από εδώ έπεται άμεσα ότι $b = 0$, καθώς διαφορετικά θα προέκυπτε ότι $\sqrt{m} \in \mathbb{Q}$. Συνεπώς ισχύει και $a = 0$.

- Αν $\omega = \sqrt{m}$, δηλαδή $a \cdot 1 + b\sqrt{m} = 0$, πάλι βρίσκουμε $a = b = 0$. Επομένως, και στις δύο περιπτώσεις έχουμε γραμμική ανεξαρτησία.

Απομένει να δείξουμε ότι κάθε $\lambda \in R_K$ γράφεται συναρτήσει των 1,ω με ακέραιους συντελεστές. Έστω λοιπόν $\lambda = \frac{a+b\sqrt{m}}{2} \in R_K$.

- Αν $m \equiv 1(mod4)$, το λ γράφεται ως

$$\lambda = \frac{a-b}{2} + b \cdot \frac{1+\sqrt{m}}{2}.$$

Εδώ οι a, b από την Πρόταση 3.2.1 είναι είτε και οι δύο άρτιοι είτε και οι δύο περιττοί, επομένως σε κάθε περίπτωση ισχύει $\frac{a-b}{2} \in \mathbb{Z}$.

- Αν $m \equiv 2,\ 3(mod4)$, το λ γράφεται ως

$$\lambda = \frac{a}{2} + \frac{b}{2} \cdot \sqrt{m}.$$

Πάλι από την Πρόταση 3.2.1 έχουμε ότι οι a, b είναι άρτιοι, άρα $\frac{a}{2}, \frac{b}{2} \in \mathbb{Z}$.

Συμπεραίνουμε ότι η $\{1, \omega\}$ αποτελεί βάση ακεραιότητας του $K = \mathbb{Q}(\sqrt{m})$.

Η διακρίνουσα, τέλος, προκύπτει εύκολα από τη σχέση

$$d(K) = \begin{vmatrix} 1 & 1 \\ \omega^{(1)} & \omega^{(2)} \end{vmatrix}^2,$$

αντικαθιστώντας κατάλληλα το ω ανάλογα με το m. □

Διατυπώνουμε, τέλος, την ακόλουθη πρόταση που μας δίνει μία διαφορετική μορφή του τετραγωνικού σώματος K και του δακτυλίου R_K, την οποία θα χρησιμοποιήσουμε παρακάτω.

Πρόταση 3.2.3 Έστω K τετραγωνικό σώμα αριθμών διακρίνουσας $d(K)$. Τότε ισχύει ότι $K = \mathbb{Q}(\sqrt{d(K)})$ και

$$R_K = \mathbb{Z}\left[\frac{d(K) + \sqrt{d(K)}}{2}\right].$$

Απόδειξη. Έστω $K = \mathbb{Q}(\sqrt{m})$. Αφού η διακρίνουσα $d(K)$ του σώματος είναι ίση είτε με m είτε με $4m$, εύκολα βλέπουμε ότι

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

Τώρα,

$$\frac{d(K) + \sqrt{d(K)}}{2} = \begin{cases} \frac{m+\sqrt{m}}{2} = \frac{m-1}{2} + \frac{1+\sqrt{m}}{2}, & \text{αν } m \equiv 1 (mod 4) \\ 2m + \sqrt{m}, & \text{αν } m \equiv 2, 3 (mod 4). \end{cases}$$

Διακρίνουμε τις δύο περιπτώσεις:

- Αν $m \equiv 2, 3 (mod 4)$, τότε $d(K) = 4m$ και

  $$\mathbb{Z}\left[\frac{d(K) + \sqrt{d(K)}}{2}\right] = \mathbb{Z}[2m + \sqrt{m}].$$

  Αρκεί να δείξουμε ότι

  $$\mathbb{Z}[2m + \sqrt{m}] = \mathbb{Z}[\sqrt{m}] = R_K.$$

  Καταρχάς, προφανώς ισχύει

  $$\mathbb{Z}[2m + \sqrt{m}] \subseteq \mathbb{Z}[\sqrt{m}].$$

  Έστω τώρα $\alpha \in \mathbb{Z}[\sqrt{m}]$, δηλαδή $\alpha = a + b\sqrt{m},\ a, b \in \mathbb{Z}$. Ψάχνουμε ακέραιους αριθμούς c, d τέτοιους ώστε $\alpha = c + d2m + d\sqrt{m}$. Εύκολα βλέπουμε ότι για $c = a - 2mb$ και $d = b$ έχουμε το ζητούμενο, άρα

  $$\mathbb{Z}[\sqrt{m}] \subseteq \mathbb{Z}[2m + \sqrt{m}]$$

  και συνεπώς ισχύει η ισότητα.

- Αν $m \equiv 1(mod4)$, τότε $d(K) = m$ και

$$\mathbb{Z}\left[\frac{d(K)+\sqrt{d(K)}}{2}\right] = \mathbb{Z}\left[\frac{m+\sqrt{m}}{2}\right].$$

Αρκεί να δείξουμε ότι

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

Αρχικά γράφουμε

$$A := \mathbb{Z}\left[\frac{m+\sqrt{m}}{2}\right] = \mathbb{Z}\left[\frac{m-1}{2} + \frac{1+\sqrt{m}}{2}\right],\ B := \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$$

και παρατηρούμε ότι

$$\frac{m-1}{2} \in \mathbb{Z}.$$

Έστω τώρα $\alpha \in A$, δηλαδή

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

Τότε προφανώς $\alpha \in B$, άρα $A \subseteq B$. Αντίστροφα, αν $\alpha \in B$, δηλαδή

$$\alpha = a + b\frac{1+\sqrt{m}}{2},$$

τότε μπορούμε να γράψουμε το α ως

$$\alpha = c + \frac{m-1}{2}d + \frac{1+\sqrt{m}}{2}d$$

για $d = b$ και $c = a - \frac{m-1}{2}b$ ακέραιους αριθμούς. Επομένως $\alpha \in A$, δηλαδή ισχύει $B \subseteq A$ και άρα η ισότητα.

□

3.3 Μονάδες

Θα μελετήσουμε την ομάδα των μονάδων του R_K, όπου $K = \mathbb{Q}(\sqrt{m})$. Περιοριζόμαστε στην περίπτωση $m < 0$, δηλαδή το K είναι μιγαδικό τετραγωνικό σώμα αριθμών. Συμβολίζουμε την ομάδα των μονάδων του R_K ως $E(R_K)$.

Έχουμε δει ότι ένα στοιχείο ε ανήκει στην ομάδα των μονάδων αν και μόνο αν $N_K(\varepsilon) = \pm 1$. Διακρίνουμε δύο περιπτώσεις, για $m \equiv 1(mod4)$ και $m \equiv 2,\ 3(mod4)$.

1. Ξεκινάμε με την περίπτωση $m \equiv 2, 3(mod4)$. Τότε ο δακτύλιος R_K είναι ο $\mathbb{Z}[\sqrt{m}]$ και για το τυχαίο στοιχείο του δακτυλίου $\varepsilon = a + b\sqrt{m}$ έχουμε:

$$\varepsilon \in E(R_K) \Leftrightarrow N_K(\varepsilon) = a^2 - b^2 m = \pm 1 \overset{m<0}{\Longleftrightarrow} a^2 + |m|b^2 = 1.$$

   (α′) Αν $|m| > 1$, τότε κατ'ανάγκη $b = 0$, άρα $a = \pm 1$. Επομένως, βρίσκουμε $\varepsilon = \pm 1$.

   (β′) Αν $m = -1$, δηλαδή $a^2 + b^2 = 1$, βρίσκουμε $\varepsilon \in \{\pm 1, \pm i\}$.

2. Στην περίπτωση $m \equiv 1(mod4)$, ισχύει ότι $R_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Το τυχαίο στοιχείο του δακτυλίου είναι της μορφής

$$\varepsilon = a + b \cdot \frac{1 + \sqrt{m}}{2} \tag{3.1}$$

   και έπεται όπως πριν ότι

$$\varepsilon \in E(R_K) \Leftrightarrow N_K(\varepsilon) = a^2 + ab + \frac{1-m}{4} \cdot b^2 = \pm 1.$$

   Επειδή όμως

$$a^2 + ab + \frac{1-m}{4} \cdot b^2 = \left(a + \frac{b}{2}\right)^2 - \frac{m}{4} \cdot b^2$$

   και $m < 0$, τελικά

$$\varepsilon \in E(R_K) \Leftrightarrow \left(a + \frac{b}{2}\right)^2 + \frac{|m|}{4} \cdot b^2 = 1.$$

   (α′) Αν $|m| > 4$, πάλι προκύπτει $b = 0$, δηλαδή $a = \pm 1$ και $\varepsilon = \pm 1$.

   (β′) Αν $|m| \leq 4$, από τις υποθέσεις μας η μόνη πιθανή τιμή του m είναι η $m = -3$. Τότε έχουμε

$$\left(a + \frac{b}{2}\right)^2 + \frac{3}{4} \cdot b^2 = 1. \tag{3.2}$$

   Αν $|b| \geq 2$, όπως και προηγουμένως εύκολα βλέπουμε ότι δεν υπάρχουν λύσεις για την παραπάνω σχέση. Επομένως, $b \in \{-1, 0, 1\}$. Για $b = 0$ βρίσκουμε $a = \pm 1$, για $b = 1$ έπεται $a \in \{-1, 0\}$ και τέλος για $b = -1$ ισχύει $a \in \{0, 1\}$. Αντικαθιστώντας όλα τα παραπάνω αποτελέσματα στη (2.1) βρίσκουμε

$$\varepsilon \in \left\{\pm 1, \frac{\pm 1 \pm \sqrt{3}}{2}\right\}.$$

Αποδείξαμε, συνεπώς, το ακόλουθο θεώρημα:

Θεώρημα 3.3.1 Έστω $K = \mathbb{Q}(\sqrt{m})$ τετραγωνικό μιγαδικό σώμα αριθμών. Η ομάδα των μονάδων $E(R_K)$ της περιοχής R_K είναι:

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

3.4 Διακλάδωση και Νόμος Ανάλυσης

Τελειώνοντας τη μελέτη μας πάνω στα τετραγωνικά σώματα αριθμών, θα διατυπώσουμε και θα αποδείξουμε τον νόμο ανάλυσης στο σώμα $K = \mathbb{Q}(\sqrt{m})$.

Έχουμε ήδη δει ότι η επέκταση $K/\mathbb{Q}$ είναι επέκταση Galois και $[K : \mathbb{Q}] = 2$, επομένως από τη γενική θεωρία για το νόμο ανάλυσης σε αλγεβρικό σώμα αριθμών προκύπτει ότι $e \cdot f \cdot s = 2$. Διακρίνουμε, συνεπώς, τις ακόλουθες τρεις περιπτώσεις:

1. Αν $e = f = 1,\ s = 2$, τότε

   $$< p >= P_1 P_2,$$

   όπου $P_1,\ P_2$ πρώτα ιδεώδη, $N_K(P_i) = p,\ i = 1, 2$. Σε αυτή την περίπτωση, ο πρώτος αριθμός p *αναλύεται* (πλήρως) στο K.

2. Αν $e = s = 1,\ f = 2$, τότε

   $$< p >= P$$

   πρώτο ιδεώδες με $N_K(P) = p^2$. Εδώ ο πρώτος p είναι *αδρανής* στο K.

3. Αν $s = f = 1,\ e = 2$, τότε

   $$< p >= P^2,$$

   όπου P πρώτο ιδεώδες με $N_K(P) = p$, δηλαδή ο p *διακλαδίζεται* (πλήρως) στο K.

Ορισμός 3.4.1 Έστω $a \in \mathbb{Z},\ p$ πρώτος αριθμός. Συμβολίζουμε με $\left(\frac{a}{p}\right)$ το *σύμβολο του Kronecker* και το ορίζουμε ως εξής:

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

Θεώρημα 3.4.2 *(Νόμος Ανάλυσης)* Έστω $K = \mathbb{Q}(\sqrt{m}),\ p$ πρώτος αριθμός. Τότε:

1. Αν $p \neq 2$:

   (α′) $(\frac{m}{p}) = 1 \Longleftrightarrow < p >= P_1P_2$ με $N_K(P_i) = p,\ i = 1, 2.$

   (β′) $(\frac{m}{p}) = -1 \Longleftrightarrow < p >= P$ πρώτο ιδεώδες με $N_K(P) = p^2.$

   (γ′) $(\frac{m}{p}) = 0 \Longleftrightarrow < p >= P^2$ με $N_K(P) = p.$

2. Αν $p = 2$:

   (α′) Αν $m \equiv 1(mod 8)$, τότε $< 2 >= P_1P_2.$

   (β′) Αν $m \equiv 5(mod 8)$, τότε $< 2 >= P$ πρώτο ιδεώδες.

   (γ′) Αν $m \equiv 2, 3(mod 4)$, τότε $< 2 >= P^2.$

Απόδειξη. Για την απόδειξη θα χρησιμοποιήσουμε το θεώρημα του Dedekind. Θα ασχοληθούμε πρώτα με την περίπτωση $p \neq 2$.

- Αν $m \equiv 2, 3(mod 4)$, το σύνολο $\{1, \sqrt{m}\}$ αποτελεί βάση ακεραιότητας του σώματος K. Τότε

  $$f(x) = Irr(\sqrt{m}, \mathbb{Q}) = x^2 - m \ \in \mathbb{Z}[x]$$

  και ορίζουμε το πολυώνυμο

  $$\overline{f}(x) = x^2 - \overline{m} \ \in \mathbb{F}_p[x].$$

  Αν $(\frac{m}{p}) = 1$, η ισοτιμία $x^2 \equiv m(mod p)$ έχει λύση, έστω $\overline{x_0} = x_0(mod p)$. Ισχύει, δηλαδή, $\overline{x_0}^2 = \overline{m}$. Επομένως,

  $$\overline{f}(x) = x^2 - \overline{m} = (x - \overline{x_0})(x + \overline{x_0})$$

  και άρα από το θεώρημα Dedekind έχουμε ότι $< p >= P_1P_2$, όπου

  $$P_1 =< p, \sqrt{m} + x_0 >,\ P_2 =< p, \sqrt{m} - x_0 > .$$

  Αν $(\frac{m}{p}) = -1$, η ισοτιμία $x^2 \equiv m(mod p)$ δεν έχει λύση. Συμπεραίνουμε ότι το πολυώνυμο $\overline{f}(x) = x^2 - \overline{m}$ είναι ανάγωγο στο δακτύλιο $\mathbb{F}_p[x]$, διότι αν ίσχυε $x^2 - \overline{m} = (x - \overline{a})(x - \overline{b})$, τότε θα έπρεπε $\overline{b} = -\overline{a}$ και $\overline{a}^2 = \overline{m}$, δηλαδή η ισοτιμία $x^2 \equiv m(mod p)$ θα είχε λύση, άτοπο. Άρα το ιδεώδες

  $$P =< p, (\sqrt{m})^2 - m >=< p >$$

  είναι πρώτο.

  Αν, τέλος, $(\frac{m}{p}) = 0$, τότε το πολυώνυμο $\overline{f}$ παίρνει τη μορφή $\overline{f}(x) = x^2$ και έπεται ότι

  $$< p >= P^2, \quad P =< p, \sqrt{m} > .$$

- Αν, τώρα, $m \equiv 1(mod4)$, το σύνολο

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

αποτελεί βάση ακεραιότητας του σώματος K. Το ελάχιστο πολυώνυμο τότε είναι το

$$f(x) = Irr(\omega, \mathbb{Q}) = x^2 - x - \frac{m-1}{4}$$

και

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

Αν $(\frac{m}{p}) = 1$, η ισοτιμία $x^2 \equiv m(modp)$ έχει λύση, έστω $\overline{x_0} = x_0(modp)$. Τότε βλέπουμε ότι

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

και από το θεώρημα του Dedekind, προκύπτει $< p >= P_1 P_2$, με

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

Αν $(\frac{m}{p}) = -1$, η ισοτιμία $x^2 \equiv m(modp)$ δεν έχει λύση. Όπως προηγουμένως, συμπεραίνουμε ότι το πολυώνυμο $\overline{f}$ είναι ανάγωγο στο δακτύλιο $\mathbb{F}_p[x]$, αφού αν είχαμε μία ανάλυση του $\overline{f}$ της μορφής $\overline{f}(x) = (x-\overline{a})(x-\overline{b})$, τότε θα έπρεπε να ισχύουν οι σχέσεις

$$\overline{a} + \overline{b} = 1$$

και

$$\overline{ab} = \overline{\left(-\frac{m-1}{4}\right)}.$$

Αν, όμως, θέσουμε $\overline{a} = \overline{\frac{1+x_0}{2}}$ για τυχαίο x_0, προκύπτει ότι $\overline{b} = \overline{\frac{1-x_0}{2}}$, και άρα $x_0^2 \equiv m(modp)$, άτοπο. Επομένως, το ιδεώδες

$$P = \left\langle p, \left(\frac{1+\sqrt{m}}{2}\right)^2 - \frac{1+\sqrt{m}}{2} - \frac{m-1}{4}\right\rangle =< p >$$

είναι πρώτο.

Αν, τέλος, $(\frac{m}{p}) = 0$, τότε $\overline{f}(x) = (x-\overline{a})^2$, όπου το a είναι λύση της ισοτιμίας $2x \equiv 1(modp)$. Συνεπώς,

$$< p >= P^2, \quad P = \left\langle p, \frac{1+\sqrt{m}}{2} - a\right\rangle.$$

Περνάμε, τώρα, στην περίπτωση $p = 2$.

- Αν $m \equiv 2, 3(mod4)$, όπως προηγουμένως το σύνολο $\{1, \sqrt{m}\}$ αποτελεί βάση ακεραιότητας του σώματος K και

$$f(x) = Irr(\sqrt{m}, \mathbb{Q}) = x^2 - m.$$

Για $m \equiv 2(mod4)$, προκύπτει ότι

$$\overline{f}(x) = x^2 - \overline{m} = x^2$$

και άρα $< 2 >= P^2$, όπου $P =< 2, \sqrt{m} >$.

Αν πάλι $m \equiv 3(mod4)$, τότε

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

άρα $< 2 >= P^2$, όπου $P =< 2, \sqrt{m} + 1 >$.

- Τελειώνουμε με την περίπτωση $m \equiv 1(mod4)$, οπότε το σύνολο

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

αποτελεί βάση ακεραιότητας του σώματος K και

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

Αν $m \equiv 1(mod8)$, τότε εύκολα παρατηρούμε ότι

$$\overline{f}(x) = x^2 - x = x(x - \bar{1}),$$

άρα $< 2 >= P_1 P_2$, όπου

$$P_1 = \left\langle 2, \frac{\sqrt{m} + 1}{2} \right\rangle,\ P_2 = \left\langle 2, \frac{\sqrt{m} - 1}{2} \right\rangle.$$

Αν, τέλος, $m \equiv 5(mod8)$, τότε το πολυώνυμο

$$\overline{f}(x) = x^2 - x - \bar{1}$$

είναι ανάγωγο στο δακτύλιο $\mathbb{F}_2[x]$, συνεπώς το $< 2 >$ είναι πρώτο ιδεώδες.

Η απόδειξη, λοιπόν, ολοκληρώθηκε. □

Αν θέλουμε να έχουμε για το δεύτερο μέρος του παραπάνω θεωρήματος μία αναλογία με το πρώτο μέρος, επεκτείνουμε το σύμβολο του Legendre στο σύμβολο του Kronecker, το οποίο για ακέραιο $d \equiv 0, 1(mod 4)$ ορίζεται ως εξής:

$$\left(\frac{d}{2}\right) = \begin{cases} 0, & \text{αν } d \equiv 0(mod 4) \\ 1, & \text{αν } d \equiv 1(mod 8) \\ -1, & \text{αν } d \equiv 5(mod 8). \end{cases}$$

Επομένως, έχουμε το ακόλουθο:

Θεώρημα 3.4.3 Έστω $K = \mathbb{Q}(\sqrt{d})$ τετραγωνικό σώμα αριθμών διακρίνουσας d και p ένας πρώτος αριθμός. Ισχύουν:

1. $< p >= P_1 P_2$, με $N_K(P_1) = N_K(P_2) = p \Longleftrightarrow (\frac{d}{p}) = 1$.
2. $< p >= P$, με $N_K(P) = p^2 \Longleftrightarrow (\frac{d}{p}) = -1$.
3. $< p >= P^2$, με $N_K(P) = p \Longleftrightarrow (\frac{d}{p}) = 0$.

Θα διατυπώσουμε, τώρα, ένα θεώρημα από το οποίο φαίνεται η αντιστοιχία μεταξύ των κλάσεων τετραγωνικών μορφών και των κλάσεων ιδεωδών ενός τετραγωνικού σώματος αριθμών K.

Δίνουμε πρώτα τον ακόλουθο ορισμό της θεμελιώδους διακρίνουσας μιας τετραγωνικής μορφής.

Ορισμός 3.4.4 Μία διακρίνουσα λέγεται *θεμελιώδης* διακρίνουσα όταν:

1. Αν $d \equiv 1(mod 4)$, τότε ο d είναι ελεύθερος τετραγώνων.
2. Αν $d \equiv 0(mod 4)$, τότε ο αριθμός $\frac{d}{4}$ είναι ελεύθερος τετραγώνων και επιπλέον ισχύει $\frac{d}{4} \equiv 2$ ή $3(mod 4)$.

Αξίζει να τονίσουμε εδώ ότι η διακρίνουσα ενός τετραγωνικού σώματος αριθμών είναι πάντα θεμελιώδης.

Θεώρημα 3.4.5 Έστω K ένα τετραγωνικό σώμα αριθμών διακρίνουσας $d(K) < 0$. Τότε:

1. Αν $f(X, Y) = aX^2 + bXY + cY^2$ μία πρωταρχική θετικά ορισμένη τετραγωνική μορφή διακρίνουσας $d(K)$, τότε το

$$\left[a, \frac{-b + \sqrt{d(K)}}{2}\right] = a\mathbb{Z} + \left(\frac{-b + \sqrt{d(K)}}{2}\right)\mathbb{Z}$$

είναι ένα ιδεώδες του R_K.

2. Η απεικόνιση
$$f(X,Y) \mapsto \left[a, \frac{-b+\sqrt{d(K)}}{2}\right]$$
επάγει έναν ισομορφισμό ομάδων μεταξύ της ομάδας $C(d(K))$ των κλάσεων ισοδυναμίας πρωταρχικών τετραγωνικών μορφών διακρίνουσας $d(K)$ και της ομάδας κλάσεων ιδεωδών $\mathcal{R}_K = I_K/H_K$ του σώματος K.

3.5 Τάξεις τετραγωνικών σωμάτων αριθμών

Εντελώς φυσιολογικά τίθεται τώρα το εξής ερώτημα: Τι συμβαίνει με τις κλάσεις τετραγωνικών μορφών των οποίων η διακρίνουσα δεν είναι θεμελιώδης;

Για να απαντήσουμε, χρειαζόμαστε μία καινούρια έννοια, αυτή της *τάξης* ενός τετραγωνικού σώματος αριθμών.

Έστω K ένα τετραγωνικό σώμα αριθμών. Είδαμε σε προηγούμενη ενότητα ότι, αν $d(K)$ η διακρίνουσα του σώματος, τότε ισχύει $K = \mathbb{Q}(\sqrt{d(K)})$ και ο δακτύλιος των ακέραιων αλγεβρικών R_K έχει βάση ακεραιότητας το σύνολο $\{1, \omega_K\}$, όπου
$$\omega_K = \frac{d(K)+\sqrt{d(K)}}{2}.$$

Ορισμός 3.5.1 Μία *τάξη* $\mathcal{O}$ του K είναι ένα υποσύνολο $\mathcal{O} \subseteq K$ τέτοιο ώστε:

1. Το $\mathcal{O}$ είναι υποδακτύλιος του K που περιέχει το 1.
2. Το $\mathcal{O}$ είναι πεπερασμένα παραγόμενο $\mathbb{Z}-$module.
3. Το $\mathcal{O}$ περιέχει μία $\mathbb{Q}-$βάση του K.

Προφανώς, το $\mathcal{O}$ είναι ελεύθερο στρέψεως (torsion free). Επειδή ισχύει ότι κάθε πεπερασμένα παραγόμενο, ελεύθερο στρέψεως $R-$module ως προς μια περιοχή κύριων ιδεωδών R είναι ελεύθερο module, από την ιδιότητα 2 εύκολα συμπεραίνουμε ότι η τάξη $\mathcal{O}$ είναι ένα ελεύθερο $\mathbb{Z}-$module.

Μάλιστα, από την ιδιότητα 3 έπεται ότι το $\mathcal{O}$ είναι ένα ελεύθερο $\mathbb{Z}-$module βαθμού 2, και το σώμα πηλίκων του είναι το σώμα K.

Είναι φανερό ότι και ο ίδιος ο δακτύλιος R_K είναι μία τάξη του σώματος K. Ισχύει το εξής:

Πρόταση 3.5.2 Έστω $\alpha \in \mathbb{C}$. Υποθέτουμε ότι υπάρχει ένα πεπερασμένα παραγόμενο $\mathbb{Z}-$submodule $M \subseteq \mathbb{C},\ M \neq \{0\}$, τέτοιο ώστε $\alpha M \subseteq M$. Τότε ισχύει $\alpha \in \widetilde{\mathbb{Z}}$.

Απόδειξη. Έστω ότι $M = \mathbb{Z} < b_1, ..., b_n >$, με τα b_i όχι όλα ίσα με μηδέν. Από τη σχέση $\alpha M \subseteq M$ έπεται ότι $\alpha b_i \in M$ για κάθε $i = 1, ..., n$, δηλαδή το στοιχείο αb_i γράφεται ως $\mathbb{Z}-$γραμμικός συνδυασμός των $b_1, ..., b_n$. Αυτό σημαίνει ότι υπάρχει πίνακας $C = (c_{ij}) \in M_n(\mathbb{Z})$ τέτοιος ώστε $\alpha b = Cb$, όπου $b = (b_1, ..., b_n)^T$. Συμπεραίνουμε ότι το α είναι ιδιοτιμή του πίνακα C, δηλαδή είναι ρίζα του χαρακτηριστικού πολυωνύμου του C, $\chi_C(x)$. Το $\chi_C(x)$ είναι μονικό και, αφού $C \in M_n(\mathbb{Z})$, έχει ακέραιους συντελεστές. Επομένως, προκύπτει άμεσα ότι $\alpha \in \widetilde{\mathbb{Z}}$. □

Αν εφαρμόσουμε την παραπάνω πρόταση για $M = \mathcal{O}$ και σε συνδυασμό με τις ιδιότητες 1 και 2 προκύπτει ότι $\mathcal{O} \subseteq R_K$. Με άλλα λόγια, κάθε τάξη του K περιέχεται στον δακτύλιο των ακέραιων αλγεβρικών R_K. Για αυτό το λόγο, συχνά ο R_K λέγεται η maximal τάξη του K.

Πρόταση 3.5.3 Έστω $\mathcal{O}$ μία τάξη του τετραγωνικού σώματος αριθμών K διακρίνουσας $d(K)$. Τότε η $\mathcal{O}$ είναι πεπερασμένου δείκτη στον R_K. Αν $f := [R_K : \mathcal{O}]$, τότε ισχύει

$$\mathcal{O} = \mathbb{Z} + fR_K = [1, f\omega_K].$$

Απόδειξη. Αφού τα $R_K, \mathcal{O}$ είναι και τα δύο ελεύθερα $\mathbb{Z}-$modules με τον ίδιο βαθμό (εδώ 2), έπεται ότι $[R_K : \mathcal{O}] < \infty$. Έστω λοιπόν $f = [R_K : \mathcal{O}]$. Ισχύει $fR_K \subseteq \mathcal{O}$, οπότε και $\mathbb{Z} + fR_K \subseteq \mathcal{O}$. Αφού $R_K = [1, \omega_K]$, έπεται ότι $\mathbb{Z} + fR_K = [1, f\omega_K] \subseteq \mathcal{O}$. Αρκεί, επομένως, να αποδείξουμε ότι το $[1, f\omega_K]$ έχει δείκτη f στον R_K. Αυτό όμως είναι προφανές, αφού ο f είναι ο ελάχιστος φυσικός τέτοιος ώστε $f\omega_K \in [1, f\omega_K]$. □

Από εδώ και στο εξής, στην παρούσα παράγραφο, την τάξη θα τη συμβολίζουμε R_f και το δακτύλιο R_K με R_1.

Ορισμός 3.5.4 Ο φυσικός αριθμός f λέγεται *οδηγός* (conductor) της τάξης R_f.

Ισχύει, μάλιστα, το εξής:

$$R_f \subseteq R_{f'} \Longleftrightarrow f'|f.$$

Η διακρίνουσα μιας τάξης ορίζεται, κατ'αναλογία προς τη διακρίνουσα του R_1, ως το τετράγωνο της ορίζουσας μιας οποιασδήποτε βάσης αυτής. Αν θεωρήσουμε την τάξη R_f με βάση την $\{1, f\omega_K\}$, τότε εύκολα βρίσκουμε ότι η διακρίνουσά της d_f ισούται με

$$d_f = f^2 d(K).$$

Υπενθυμίζουμε ότι η διακρίνουσα $d(K)$ είναι θεμελιώδης ως διακρίνουσα σώματος.

Θα επιθυμούσαμε, τώρα, να αναπτύξουμε μία αριθμητική για κάθε τάξη, δηλαδή να ορίσουμε μία θεωρία ιδεωδών του R_f.

Αν A είναι ένα μη-μηδενικό ιδεώδες της τάξης R_f, τότε, όπως και στην περίπτωση του R_1, ο δακτύλιος πηλίκων R_f/A είναι πεπερασμένος. Ορίζουμε, όπως και στον R_1, τη norm του ιδεώδους $A, N_f(A)$, ως το πλήθος των στοιχείων του R_f/A.

Αποδεικνύεται ότι ο δακτύλιος R_f είναι περιοχή της Noether και ότι κάθε, μη-μηδενικό, πρώτο ιδεώδες αυτού είναι maximal. Για $f > 1$ όμως δεν είναι δακτύλιος του Dedekind, αφού δεν είναι ακέραια κλειστός. Αυτό σημαίνει ότι πλέον, για $f > 1$, δεν έχουμε μονοσήμαντη ανάλυση των ιδεωδών της R_f σε γινόμενο πρώτων ιδεωδών. Θα πρέπει, λοιπόν, να περιοριστούμε σε μικρότερες κλάσεις ιδεωδών του R_f.

Αν A ιδεώδες της τάξης R_f, τότε από τον ορισμό του ιδεώδους, έπεται ότι $R_f A \subseteq A$. Επομένως, ισχύει:

$$R_f \subseteq \{a \in K \mid aA \subseteq A\}. \tag{3.3}$$

Ορισμός 3.5.5 Ένα ιδεώδες A της τάξης R_f θα λέγεται *γνήσιο (proper)* όταν στη σχέση (3.3) ισχύει η ισότητα, δηλαδή

$$R_f = \{a \in K \mid aA \subseteq A\}.$$

Η έννοια επεκτείνεται ανάλογα και στα κλασματικά ιδεώδη της R_f, δηλαδή υποσύνολα του K τα οποία είναι πεπερασμένα παραγόμενα R_f-modules.

Πρόταση 3.5.6 Έστω R_f μια τάξη του K και A ένα R_f-ιδεώδες του K. Τότε το A είναι γνήσιο ιδεώδες αν και μόνο αν το A είναι αντιστρέψιμο.

Δυστυχώς, η παραπάνω πρόταση δεν είναι αρκετή για να έχουμε μονοσήμαντη ανάλυση σε γινόμενο πρώτων ιδεωδών. Για να το πετύχουμε αυτό, θα πρέπει να θεωρήσουμε το σύνολο των γνήσιων R_f- ιδεωδών του K τα οποία είναι πρώτα προς τον οδηγό f. Αυτό θα πει ότι ισχύει η ισότητα:

$$A + fR_f = R_f.$$

Πρόταση 3.5.7 Ένα R_f-ιδεώδες A του K είναι πρώτο προς τον αριθμό f ακριβώς όταν η norm του $A, N_f(A)$, είναι σχετικά πρώτη προς τον f. Μάλιστα, κάθε R_f-ιδεώδες του K πρώτο προς τον f είναι γνήσιο.

Όπως και στην περίπτωση του R_1 και με βάση τις παραπάνω προτάσεις, έχουμε:

Το σύνολο των R_f-ιδεωδών του K που είναι πρώτα προς το f αποτελεί πολλαπλασιαστική ομάδα και θα τη συμβολίζουμε $I_f(K)$.

Το σύνολο των R_f-κύριων ιδεωδών του K τα οποία παράγονται από στοιχεία $a \in R_f$ τέτοια ώστε $(N_f(a), f) = 1$ αποτελεί υποομάδα της $I_f(K)$ και θα συμβολίζεται $H_f(K)$.

Η ομάδα πηλίκων $I_f(K)/H_f(K)$ είναι πεπερασμένη και θα λέγεται *ομάδα κλάσεων ιδεωδών* της τάξης R_f. Η τάξη αυτής,

$$h_f(K) := \#\frac{I_f(K)}{H_f(K)}$$

θα λέγεται *αριθμός κλάσεων ιδεωδών* της τάξης R_f του τετραγωνικού σώματος αριθμών K.

Για τη σχέση αυτού του αριθμού κλάσεων με τον αριθμό κλάσεων h_K ισχύει η ισότητα:

$$h_f(K) = \frac{h_K f}{[E(R_1) : E(R_f)]} \cdot \prod_{p|f}\Big(1 - \Big(\frac{d(K)}{p}\Big)\frac{1}{p}\Big), \tag{3.4}$$

όπου $E(R_f)$ είναι η ομάδα των μονάδων του R_f και $(\frac{d(K)}{p})$ το σύμβολο του Kronecker.

Παράδειγμα 3.5.8 Έστω $K = \mathbb{Q}(\sqrt{-3})$. Τότε ο δακτύλιος των ακεραίων αλγεβρικών είναι ο

$$R_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right].$$

Έστω το γνήσιο υποσύνολο του R_K, $\mathbb{Z}[\sqrt{-3}]$. Μπορούμε εύκολα να δούμε ότι το σύνολο αυτό αποτελεί τάξη του σώματος K, και μάλιστα, αν $\mathbb{Z}[\sqrt{-3}] = \mathcal{O}$, τότε ισχύει $[R_K : \mathcal{O}] = 2$. Επομένως, η διακρίνουσα της τάξης είναι

$$d_f = f^2 d(K) = 2^2(-3) = -12.$$

Επίσης, καθώς ισχύει $[E(R_K) : E(\mathcal{O})] = 3$, ο αριθμός κλάσεων της τάξης $\mathcal{O}$ θα ισούται από τη σχέση (3.4) με $h_f = 1$.

Ισχύει, τώρα, η εξής πρόταση: Αν η ιδιότητα της μονοσήμαντης παραγοντοποίησης ισχύει για τα γνήσια $\mathcal{O}-$ιδεώδη, τότε η τάξη $\mathcal{O}$ είναι Περιοχή Μονοσήμαντης Ανάλυσης.

Στο παράδειγμά μας, όμως, η τάξη μας δεν είναι ΠΜΑ, καθώς μπορούμε εύκολα να δείξουμε ότι τα στοιχεία

$$2,\ 1+\sqrt{-3},\ 1-\sqrt{-3} \in \mathcal{O}$$

είναι ανάγωγα και για το στοιχείο $4 \in \mathcal{O}$ ισχύει

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3}).$$

Αυτό σημαίνει, από το αντιστροφοαντίθετο της προηγούμενης παρατήρησής μας, ότι δεν ισχύει η μονοσήμαντη παραγοντοποίηση για τα γνήσια $\mathcal{O}-$ιδεώδη του σώματος K.

Διατυπώνουμε, τέλος, το ακόλουθο θεώρημα, το οποίο αποτελεί γενίκευση του Θεωρήματος 3.4.5.

Θεώρημα 3.5.9 Έστω R_f μία τάξη διακρίνουσας $d_f = f^2 d(K)$ ενός μιγαδικού τετραγωνικού σώματος αριθμών K.

1. Αν $f(X,Y) = aX^2 + bXY + cY^2$ είναι μία πρωταρχική θετικά ορισμένη τετραγωνική μορφή διακρίνουσας d_f, τότε το

$$\left[a, \frac{-b+\sqrt{d_f}}{2}\right] = a\mathbb{Z} + \left(\frac{-b+\sqrt{d_f}}{2}\right)\mathbb{Z}$$

είναι ένα γνήσιο (proper) ιδεώδες της R_f.

2. Η απεικόνιση

$$f(X,Y) \mapsto \left[a, \frac{-b+\sqrt{d_f}}{2}\right]$$

επάγει έναν ισομορφισμό ομάδων μεταξύ της ομάδας $C(d_f)$ των κλάσεων ισοδυναμίας πρωταρχικών τετραγωνικών μορφών διακρίνουσας d_f και της ομάδας κλάσεων ιδεωδών της τάξης R_f.

3.6 Σημειώσεις

Οι βασικές έννοιες αλγεβρικής θεωρίας αριθμών περιέχονται σε κάθε εισαγωγικό βιβλίο αντίστοιχου περιεχομένου. Συγκεκριμένα, συνιστούμε τα [2] και [3]. Επίσης, ιδιαίτερα για τις παρατηρήσεις της σελίδας 51, προτείνουμε στον ενδιαφερόμενο αναγνώστη να ανατρέξει στο [20] (σελ.71-75). Τέλος, για τη θεωρία των τάξεων παραπέμπουμε στα [6],[8] και [31].

Κεφάλαιο 4

Πολυώνυμα και Πρώτοι Αριθμοί

Ξεφεύγουμε λίγο από την κύρια κατεύθυνση του σκοπού αυτής της εργασίας για να ασχοληθούμε με ένα πρόβλημα σχετιζόμενο με το κύριο θέμα μας και εξαιρετικά ενδιαφέρον.

4.1 Εισαγωγικά Στοιχεία

Ένα από τα προβλήματα που απασχολεί ακόμα και σήμερα εκείνους που ασχολούνται με τη Θεωρία Αριθμών είναι το εξής:

Υπάρχουν συναρτήσεις $f(n)$, ορισμένες για όλους τους φυσικούς $n \geq 1$, που υπολογίζονται σχετικά εύκολα και δίνουν τιμές ορισμένους ή όλους τους πρώτους αριθμούς;

Λογικό ήταν αρχικά να θεωρηθεί η περίπτωση πολυωνυμικών συναρτήσεων. Το πρόβλημα, όμως, που προκύπτει είναι ότι αν $f(x)$ είναι ένα μη σταθερό πολυώνυμο με ακέραιους συντελεστές, τότε υπάρχουν άπειροι το πλήθος ακέραιοι αριθμοί n τέτοιοι ώστε η τιμή $|f(n)|$ να είναι σύνθετος. Επομένως, δεν υπάρχει πολυώνυμο $f(x) \in \mathbb{Z}[x]$, βαθμού $deg f(x) > 1$, για το οποίο οι τιμές $f(m)$, για κάθε $m \in \mathbb{N}$, να είναι πρώτοι αριθμοί. Η παραπάνω πρόταση προέρχεται από επιστολή του Goldbach στον Euler στις 28 Σεπτεμβρίου 1743. Εμείς παραπέμπουμε επίσης στο [22] (σελ.142).

Στην παρούσα ενότητα θα περιορίσουμε το πρόβλημα και θα εξετάσουμε αν υπάρχουν πολυώνυμα $f(x) \in \mathbb{Z}[x]$ τέτοια ώστε για κάποιες διαδοχικές τιμές της μεταβλητής $n \in \mathbb{N}_0$ να δίνουν τιμές πρώτους αριθμούς.

Ας πάρουμε πρώτα ένα πολυώνυμο πρώτου βαθμού, έστω $f(x) = ax + b$, με $a > 1, b > 1, (a, b) = 1$. Αν $f(0) \in \mathbb{P}$ πρώτος αριθμός, τότε ο $b = f(0) \in \mathbb{P}$. Συνεπώς, το πολυώνυμο έχει τη μορφή $f(x) = ax + p,\ p \in \mathbb{P}$. Τότε όμως, $f(p) = ap + p = p(a + 1)$ είναι σύνθετος.
Επομένως, για πολυώνυμα πρώτου βαθμού υπάρχουν το πολύ p διαδοχικές τιμές της μεταβλητής έτσι ώστε η τιμή του πολυωνύμου να είναι πρώτος αριθμός.

Το πρόβλημα αν, δοθέντος κάποιου πρώτου p, υπάρχει $a \in \mathbb{Z}, a \geq 1$ τέτοιο ώστε όλοι οι ακέραιοι της μορφής $p, a + p, 2a + p, ..., (p - 1)a + p$ να είναι πρώτοι, παραμένει μέχρι σήμερα *ανοιχτό*. Παρόλα αυτά, μπορεί να επαληθευτεί για μικρές τιμές του p. Για παράδειγμα, για $p = 3$ και $a = 6$ λαμβάνουμε τις διαδοχικές τιμές 3,5,7, ενώ για $p = 5$ και $a = 6$ παίρνουμε τους διαδοχικούς πρώτους 5,11,17,23,29.

Σημειώνουμε ακόμη ότι ο Lagrange έχει αποδείξει ότι αν υπάρχει τέτοιο a, για δοσμένο $p \in \mathbb{P}$, τότε αυτό θα είναι πολλαπλάσιο του γινομένου

$$\prod_{\substack{q<p \\ q\in\mathbb{P}}} q.$$

Θεωρούμε τώρα πολυώνυμα δευτέρου βαθμού.

Ορισμός 4.1.1 Ένα πολυώνυμο $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ με $a, c \geq 1$ θα λέγεται πολυώνυμο που *παράγει (γεννάει) πρώτους αριθμούς*, όταν υπάρχει ακέραιος $l > 2$ τέτοιος ώστε οι διαδοχικές τιμές $f(0), f(1), ..., f(l - 1)$ να είναι πρώτοι αριθμοί.

Από τα προηγούμενα έπεται ότι το l είναι φραγμένο. Η μέγιστη από τις τιμές του θα λέγεται *μήκος παραγωγής πρώτων αριθμών* του πολυωνύμου $f(x)$.

Το 1772 ο Euler παρατήρησε ότι το πολυώνυμο

$$f(x) = x^2 - x + 41$$

δίνει για $x = 1, 2, ..., 40$, δηλαδή για 40 διαδοχικές τιμές του x, πρώτους αριθμούς. Συγκεκριμένα, παίρνουμε τους εξής πρώτους: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601. Φυσικά, $f(41) = 1681 = 41^2$ σύνθετος.

Το πρόβλημα απασχόλησε και τον Legendre, ο οποίος το 1798 ανακοίνωσε ότι το πολυώνυμο

$$f(x) = x^2 + x + 41$$

δίνει τιμές πρώτους για $x = 0, 1, ..., 39$. Και εδώ $f(40) = 41^2$ σύνθετος.

Παρατηρούμε επίσης ότι, για $n > 0$,

$$f(-n) = (-n)^2 + (-n) + 41 = (n-1)^2 + (n-1) + 41.$$

Επομένως, το $f(x) = x^2 + x + 41$ δίνει τιμές πρώτους και για $-40 \leq x \leq -1$.

Προκύπτει φυσιολογικά το ερώτημα αν υπάρχουν άλλα πολυώνυμα με ανάλογες ιδιότητες.

Ας πάρουμε πάλι το πολυώνυμο $f(x) = x^2 + x + 41$. Μπορούμε να θέσουμε στη θέση του x το $x - a$, με $a \in \mathbb{Z}, a \geq 1$. Παίρνουμε τότε το πολυώνυμο

$$(x-a)^2 + (x-a) + 41 = x^2 - (2a-1)x + (a^2 - a + 41).$$

Για $a = 1$ προκύπτει το πολυώνυμο $f(x) = x^2 - x + 41$, το οποίο λαμβάνει τιμές πρώτους αριθμούς για $-39 \leq x \leq 40$.

Αν θέσουμε, για παράδειγμα, $a = 40$, προκύπτει το πολυώνυμο $f(x) = x^2 - 79x + 1601$, το οποίο λαμβάνει τιμές πρώτους αριθμούς για $0 \leq x \leq 79$, που είναι όμως οι ίδιες τιμές του $x^2 - x + 41$ οι οποίες λαμβάνονται δύο φορές.

Στο πολυώνυμο του Euler η σταθερά είναι ένας πρώτος αριθμός, ο 41. Στη γενική περίπτωση, αν έχουμε το πολυώνυμο $f(x) = x^2 + x + p$, με p πρώτο, τότε προφανώς $f(0) = p \in \mathbb{P}$ και $f(p) = p(p+2)$ σύνθετος. Επίσης, $f(p-1) = p^2$, που είναι επίσης σύνθετος.

Το βέλτιστο, επομένως, αποτέλεσμα που ελπίζουμε να έχουμε εδώ είναι οι τιμές του πολυωνύμου $f(x)$ για $0 \leq x \leq p-2$ να είναι πρώτοι αριθμοί, όπως και στην περίπτωση του $p = 41$. Κάτι τέτοιο, για παράδειγμα, ισχύει αν επιλέξουμε $p = 2, 3, 5, 11, 17, 41$, ενώ δεν ισχύει για $p = 7, 13, 19, 23, 29, 31, 37$. Η επαλήθευση είναι εύκολη.

Λογικό είναι να αναρωτηθεί κανείς αν υπάρχει πολυώνυμο $f(x) = x^2 + x + p$, με $p \in \mathbb{P},\ p > 41$, που να δίνει τιμές πρώτους αριθμούς για $0 \leq x \leq p-2$. Η απάντηση σε αυτό το ερώτημα είναι αρνητική. Είναι αξιοσημείωτο ότι η απάντηση σχετίζεται άμεσα με το πρόβλημα του Gauss για τον αριθμό κλάσεων. Συγκεκριμένα, ισχύει το θεώρημα του Rabinowitsch, το οποίο θα διατυπώσουμε και θα αποδείξουμε στη συνέχεια.

4.2 Το θεώρημα του Rabinowitsch

Θεώρημα 4.2.1 (Rabinowitsch,1913) Αν $d < 0, d \equiv 1(mod4)$, τότε το πολυώνυμο

$$x^2 - x + \frac{1+|d|}{4}$$

δίνει τιμές πρώτους αριθμούς για $1 \leq x \leq \frac{|d|-3}{4}$ αν και μόνο αν $h_K = 1$, όπου h_K ο αριθμός κλάσεων ιδεωδών του τετραγωνικού μιγαδικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{d})$, διακρίνουσας d.

Θα αποδείξουμε το θεώρημα παρακάτω.

Αποδεικνύεται, με χρήση της θεωρίας γένους, ότι

$$2^{t-1} \mid h_K,$$

όπου $t = \#\{p : p \mid d(K)\}$. Εμείς θέλουμε να μελετήσουμε τα μιγαδικά τετραγωνικά σώματα αριθμών με $h_K = 1$. Επομένως, από την προηγούμενη σχέση προκύπτει αναγκαστικά $t = 1$, δηλαδή υπάρχει ακριβώς ένας πρώτος που διαιρεί τη διακρίνουσα.

Διατυπώνουμε τώρα το ακόλουθο λήμμα:

Λήμμα 4.2.2 Έστω K ένα αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$, με αριθμό κλάσεων ιδεωδών $h_K = 1$. Έστω επίσης $p \in \mathbb{P}$ για τον οποίο υπάρχει $a \in R_K$ τέτοιο ώστε $p^s \mid\mid N_K(a)$, για κάποιο φυσικό s, όπου R_K ο δακτύλιος των ακέραιων αλγεβρικών του σώματος K. Τότε υπάρχει ένα ανάγωγο στοιχείο $b \in R_K$ τέτοιο ώστε $|N_K(b)| = p^t$, για $t \leq max\{s, n\}$.

Έστω τώρα K ένα τετραγωνικό μιγαδικό σώμα αριθμών με $h_K = 1$, διακρίνουσας $d \neq -3, -4, -8$. Αυτό σημαίνει ότι $d \equiv 1(mod4)$, και μάλιστα, καθώς γνωρίζουμε ότι υπάρχει μοναδικός πρώτος αριθμός που διαιρεί τη διακρίνουσα από προηγούμενη παρατήρησή μας, θα ισχύει $d = -p,\ p \in \mathbb{P},\ p \equiv 3(mod4)$. Επιλέγουμε τη βάση $\{1, \omega\}$ του δακτυλίου R_K, όπου

$$\omega = \frac{\sqrt{d}-1}{2} = \frac{\sqrt{-p}-1}{2}.$$

Για το τυχαίο στοιχείο $a + b\omega \in R_K$ έχουμε:

$$N_K(a+b\omega) = N_K\left(a - \frac{b}{2} + \frac{b}{2}\sqrt{d}\right) = a^2 - ab + b^2 \cdot \frac{1-d}{4}.$$

Ειδικότερα, για το στοιχείο $x+\omega$ ισχύει:

$$N_K(x+\omega) = x^2 - x + \frac{1-d}{4} = x^2 - x + \frac{1+|d|}{4}.$$

Παρατηρούμε ότι για κάθε $x = 1, 2, ..., \frac{|d|-3}{4}$,

$$N_K(x+\omega) = x^2 - x + \frac{1+|d|}{4} < \left(\frac{1+|d|}{4}\right)^2 - \frac{1+|d|}{4} + \frac{1+|d|}{4} = \frac{(1+|d|)^2}{16}.$$

Παρατήρηση 4.2.3 Για $x = 1, 2, ..., \frac{|d|-3}{4}$, τα $x+\omega$ είναι ανάγωγα στοιχεία του δακτυλίου R_K. Η παρατήρηση αυτή είναι ανεξάρτητη της υπόθεσης για τον αριθμό κλάσεων, $h_K = 1$.

Απόδειξη. Έστω ότι το στοιχείο $x+\omega$ γραφόταν ως $x+\omega = \alpha\beta$, με α, β όχι μονάδες του R_K. Τότε

$$N_K(x+\omega) = N_K(\alpha) \cdot N_K(\beta) < \frac{(1+|d|)^2}{16}.$$

Αυτό σημαίνει ότι η norm ενός τουλάχιστον από τους παράγοντες α, β θα είναι μικρότερη του $\frac{1+|d|}{4}$. Χωρίς βλάβη της γενικότητας, έστω

$$N_K(\beta) < \frac{1+|d|}{4}.$$

Αν, όμως, $r+s\omega$ είναι ένα οποιοδήποτε άρρητο στοιχείο του R_K (δηλαδή $s \neq 0$), με $r, s \in \mathbb{Z}$, τότε:

$$N_K(r+s\omega) = r^2 - rs + \frac{(1+|d|)s^2}{4} = \left(r - \frac{s}{2}\right)^2 + \frac{|d|s^2}{4} \geq \frac{1+|d|}{4}.$$

Αυτό ισχύει, γιατί:

- Αν $s = \pm 1$, τότε για κάθε $r \in \mathbb{Z}$,

$$\left(r + \frac{|s|}{2}\right)^2 = \left(r + \frac{1}{2}\right)^2 \geq \frac{1}{4},$$

οπότε

$$N_K(r+s\omega) \geq \frac{1}{4} + \frac{|d|}{4} = \frac{1+|d|}{4}.$$

- Αν $|s| \geq 2$, τότε

$$N_K(r+s\omega) \geq \frac{|d|s^2}{4} \geq \frac{4|d|}{4} \geq \frac{1+|d|}{4}.$$

Επομένως, αφού

$$N_K(\beta) < \frac{1+|d|}{4},$$

έπεται ότι $\beta = r + s\omega$, με $s = 0$, δηλαδή ότι $\beta \in \mathbb{Z}$. Εύκολα, όμως, βλέπουμε ότι το στοιχείο $x + \omega$ δεν μπορεί να έχει ακέραιους διαιρέτες διάφορους των ± 1. Συνεπώς, το β είναι μονάδα και άρα το $x + \omega$ είναι ανάγωγο στο δακτύλιο R_K. □

Είμαστε τώρα έτοιμοι να αποδείξουμε το θεώρημα του Rabinowitsch.

Απόδειξη. (Rabinowitsch) Υποθέτουμε ότι $h_K = 1$. Τα στοιχεία $x + \omega \in R_K$ είναι ανάγωγα για $x = 1, 2, ..., \frac{|d|-3}{4}$ από την προηγούμενη παρατήρησή μας, άρα τα ιδεώδη $< x + \omega >$ είναι πρώτα. Συνεπώς, εφόσον το K είναι τετραγωνικό σώμα, η norm των ιδεωδών είναι

$$N_K(< x + \omega >) = p \ \ \acute{\eta} \ \ p^2, \quad p \in \mathbb{P}.$$

Αν $N_K(< x+\omega >) = p^2$, τότε το $< x+\omega >$ θα ήταν πρώτο ιδεώδες παραγόμενο από κάποιον πρώτο αριθμό, δηλαδή το $x+\omega$ θα ήταν ρητός πρώτος αριθμός, το οποίο είναι άτοπο. Επομένως,

$$|N_K(x + \omega)| = N_K(< x + \omega >) = p \in \mathbb{P} \Longrightarrow x^2 - x + \frac{1+|d|}{4} = p$$

πρώτος αριθμός για κάθε $x = 1, 2, ..., \frac{|d|-3}{4}$.

Αντίστροφα, έστω τώρα ότι $d \equiv 1(mod 4)$, $d \neq -3$ (συνεπώς θα ισχύει $|d| > 7$), και ότι το πολυώνυμο $f(x) = x^2 - x + \frac{1+|d|}{4}$ δίνει τιμή πρώτο αριθμό για κάθε $x = 1, 2, ..., \frac{|d|-3}{4}$. Θα υποθέσουμε ότι $h_K \neq 1$ και θα καταλήξουμε σε άτοπο.

Αφού $h_K \neq 1$, υπάρχει τουλάχιστον ένα (ακέραιο) ιδεώδες του K το οποίο δεν είναι κύριο. Από το σύνολο αυτών των ιδεωδών επιλέγουμε ένα, έστω A, που να έχει την ελάχιστη norm. Αυτό θα είναι προφανώς πρώτο ιδεώδες, οπότε γράφουμε $A = P$, και μάλιστα η norm του θα είναι πρώτος αριθμός.

Εφαρμόζουμε τώρα το Θεώρημα 2.6.3 του Minkowski για $K = \mathbb{Q}(\sqrt{|d|})$. Η σταθερά Minkowski είναι ίση με $2\sqrt{d}/\pi$, επομένως για την κλάση ιδεώδους που έχουμε επιλέξει ισχύει

$$N_K(P) = p \leq \frac{2\sqrt{|d|}}{\pi}.$$

Το $\{1, \omega\}$ είναι βάση του R_K, επομένως $R_K = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \omega$. Αφού $f(x) = Irr(\omega, \mathbb{Q})$ και από το νόμο ανάλυσης στο σώμα K προκύπτει ότι

$$< p >= pR_K = I \cdot J$$

με $I = pR_K + (\omega - \omega_1)R_K,\ J = pR_K + (\omega - \omega_2)R_K$, όπου ω_1, ω_2 είναι οι ρίζες του $f(x)(modp)$, οι οποίες λαμβάνονται από το διάστημα $[0, p-1]$.

Τώρα, προφανώς ισχύει $I = pR_K + (\omega + p - \omega_1)R_K$. Ο αριθμός $\omega + p - \omega_1$ έχει norm

$$N_K(\omega + p - \omega_1) = (p - \omega_1)^2 - (p - \omega_1) + \frac{1 + |d|}{4}.$$

Εύκολα βλέπουμε ότι ισχύει

$$0 < p - \omega_1 \leq p \leq \frac{2\sqrt{|d|}}{\pi}.$$

Επίσης για $|d| \geq 7$ έχουμε

$$\frac{2\sqrt{|d|}}{\pi} < \frac{1 + |d|}{4} \Leftrightarrow \frac{|d| - 3}{4} < \frac{2\sqrt{|d|}}{\pi}.$$

Από τα παραπάνω βλέπουμε ότι ο $p - \omega_1$ ικανοποιεί τις υποθέσεις μας και άρα $N_K(\omega + p - \omega_1) = q \in \mathbb{P}$. Όμως $\omega + p - \omega_1 \in P$, συνεπώς $N_K(\omega + p - \omega_1) = q \mid N_K(P) = p$ και άρα $q = p$. Συμπεραίνουμε ότι το $\omega + p - \omega_1$ παράγει το ιδεώδες P, δηλαδή το P είναι κύριο ιδεώδες, άτοπο. □

Θα δώσουμε τώρα ένα ακόμα θεώρημα που σχετίζεται με το θεώρημα του Rabinowitsch.

Για τα παρακάτω υποθέτουμε ότι ο p είναι ένας πρώτος αριθμός, $p > 3$ και $p \equiv 3(mod4)$.

Θεώρημα 4.2.4 Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες:

1. $h(-p) = 1$.
2. (α′) Ισχύει $(\frac{q}{p}) = -1$ για όλους τους πρώτους $q < \frac{p}{4}$.
   (β′) Ισχύει $(\frac{q}{p}) = -1$ για όλους τους πρώτους $q < \sqrt{\frac{p}{3}}$.
3. Αν $p > 7$, ισχύει $p \equiv 3(mod8)$ και $R_p - N_p = 3$ στο διάστημα $[1, \frac{p-1}{2}]$, όπου R_p το πλήθος των τετραγωνικών υπολοίπων $modp$ και N_p το πλήθος των μη-τετραγωνικών υπολοίπων $modp$.
4. (α′) Οι ακέραιοι
   $$x^2 + x + \frac{p+1}{4}$$
   είναι πρώτοι για
   $$0 \leq x \leq \frac{p-7}{4}.$$

(β′) Ισχύει το ίδιο για

$$0 \leq x \leq \frac{1}{2}\Big(\sqrt{\frac{p}{3}} - 1\Big).$$

Απόδειξη. (1. $\Rightarrow$ 2.(α')) Ο αριθμός $d := -p$ είναι θεμελιώδης διακρίνουσα. Θεωρούμε τη μιγαδική τετραγωνική επέκταση $K/\mathbb{Q}$, όπου $K = \mathbb{Q}(\sqrt{-p})$.

Είναι γνωστό ότι ισχύει

$$\Big(\frac{q}{p}\Big) = -1$$

αν και μόνο αν ο q αδρανεί στην επέκταση $K/\mathbb{Q}$. Επομένως, αν $q < \frac{p}{4}$, αρκεί να δείξουμε ότι ο q αδρανεί στο σώμα K. Επειδή, από το θεώρημα της διακρίνουσας, ο μόνος πρώτος που διακλαδίζεται στο K είναι ο p, αρκεί να δείξουμε ότι, αν ο πρώτος αριθμός q αναλύεται στο K, τότε αναγκαστικά θα ισχύει $q \geq \frac{p}{4}$.

Αν, λοιπόν, ο q αναλύεται στο K, δηλαδή ισχύει

$$\Big(\frac{q}{p}\Big) = 1,$$

τότε έπεται ότι

$$< q >= qR_K = P_1P_2,$$

όπου P_1, P_2 πρώτα ιδεώδη του R_K και $N_K(P_1) = N_K(P_2) = q$. Καθώς έχουμε υποθέσει ότι $h(-p) = 1$, το ιδεώδες P_1 είναι κύριο, δηλαδή υπάρχει $\alpha \in R_K$ τέτοιο ώστε $P_1 =< \alpha >$ και $|N_K(\alpha)| = q$.

Αν γράψουμε το α ως $\alpha = x + y\sqrt{-p}$, με $x, y \in \frac{1}{2}\mathbb{Z}$, τότε έχουμε ότι $N_K(\alpha) = x^2 + py^2 = q$. Το q δεν είναι τέλειο τετράγωνο, άρα $y \neq 0$. Συνεπώς, $q \geq py^2 \geq \frac{p}{4}$ και άρα δείξαμε το ζητούμενο.

(2.(α') $\Rightarrow$ 2.(β')) Η κατεύθυνση αυτή είναι προφανής.

(2.(β') $\Rightarrow$ 1.) Έστω P ένα πρώτο ιδεώδες του δακτυλίου R_K με norm $N_K(P) < \sqrt{\frac{p}{3}}$ και q ο (μοναδικός) πρώτος που ανήκει στο P. Εξ υποθέσεως γνωρίζουμε ότι

$$\Big(\frac{q}{p}\Big) = -1,$$

άρα από το νόμο ανάλυσης στο σώμα $K = \mathbb{Q}(\sqrt{-p})$ θα ισχύει ότι $N_K(P) = q^2$ και $P =< q >$ κύριο ιδεώδες. Είναι φανερό ότι και κάθε ιδεώδες A του R_K που ικανοποιεί $N_K(A) < \sqrt{\frac{p}{3}}$ είναι επίσης κύριο.

Τώρα, από το θεώρημα Minkowski γνωρίζουμε ότι κάθε κλάση ιδεωδών του K περιέχει ένα τουλάχιστον ιδεώδες, έστω A, με $N_K(A) \leq C$, όπου C η σταθερά Minkowski. Στην περίπτωσή μας, η σταθερά είναι ίση με

$$C = \frac{2}{\pi}\sqrt{|d|}.$$

Επειδή οι πραγματικοί αριθμοί $2/\pi$ και $1/\sqrt{3}$ είναι σχετικά κοντά μεταξύ τους, μπορούμε να συμπεράνουμε από τα παραπάνω ότι σε κάθε κλάση ιδεωδών του K υπάρχει τουλάχιστον ένα ιδεώδες A τέτοιο ώστε $N_K(A) < \sqrt{\frac{p}{3}}$. Από εδώ συμπεραίνουμε ότι $h(-p) = 1$.

(1. $\Leftrightarrow$ 3.) Ο Jacobi απέδειξε ότι ισχύει η σχέση

$$R_p - N_p = 3h(-p).$$

Η απόδειξη είναι αναλυτική και δε θα αναφερθεί στην παρούσα εργασία.

Τώρα, αν ισχύει $p > 7$ με $h(-p) = 1$, τότε αναγκαστικά $p \equiv 3(mod 8)$. Από την παραπάνω σχέση προκύπτει άμεσα ότι $R_p - N_p = 3$. Αντίστροφα, αν $p \equiv 3(mod 8)$, $p > 7$, και ισχύει $R_p - N_p = 3$, πάλι από την παραπάνω ισότητα έπεται ότι $h(-p) = 1$.

(2.(α') $\Rightarrow$ 4.(α')) Έστω $m = \frac{p+1}{4}$, $f_p(x) = x^2 + x + m$. Για τις τιμές $0 \leq x \leq m - 2 = \frac{p-7}{4}$ ισχύει

$$2 \leq f_p(x) < m^2.$$

Πράγματι, από τις υποθέσεις μας $p \equiv 3(mod 8)$ και $p > 3$ προκύπτει $m \geq 2$, άρα για τη μικρότερη τιμή του πολυωνύμου, $f_p(0)$, ισχύει $f_p(0) = m \geq 2$. Επίσης, για την μεγαλύτερη τιμή, $f_p(m-2)$, έχουμε ότι $f_p(m-2) = m^2 - 2m + 2 < m^2$.

Τώρα, αν για κάποια τιμή του x, έστω x_0, με $0 \leq x_0 \leq m - 2$, ο ακέραιος $f_p(x_0)$ είναι σύνθετος, τότε υπάρχει $q \in \mathbb{P}$ με $q < m$, που διαιρεί τον $f_p(x_0)$, δηλαδή υπάρχει $t \in \mathbb{Z}$, $t > 1$ με $f_p(x_0) = qt$ και $q < f_p(x_0) < m^2$. Με άλλα λόγια, προκύπτει ότι η ισοτιμία

$$x^2 + x + m \equiv 0(mod q)$$

έχει λύση, το παραπάνω x_0.

Η διακρίνουσα του $f_p(x)$ είναι ίδη με $\Delta_p = 1 - 4m = -p$. Καθώς η παραπάνω ισοτιμία έχει λύση, συμπεραίνουμε ότι ισχύει

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

Τότε, όμως, από το νόμο τετραγωνικής αντιστροφής προκύπτει ότι

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

το οποίο είναι άτοπο από τις υποθέσεις μας. Συνεπώς, οι τιμές $f_p(x)$ είναι πρώτοι αριθμοί για κάθε $0 \leq x \leq m - 2$.

$(4.(\alpha') \Rightarrow 4.(\beta'))$ Η κατεύθυνση είναι προφανής.

$(4.(\beta') \Rightarrow 2.(\beta'))$ Έστω ότι δεν ισχύει η $2(\beta')$. Τότε υπάρχει $q \in \mathbb{P},\ q < \sqrt{\frac{p}{3}}$, τέτοιος ώστε

$$\left(\frac{q}{p}\right) = 1.$$

Παρατηρούμε, καταρχάς, ότι αναγκαστικά ισχύει $q \neq 2$. Αυτό γιατί, αν $q = 2$, τότε καθώς

$$\left(\frac{2}{p}\right) = 1 \text{ και } p \equiv 3(mod 4)$$

έπεται $p \equiv 7(mod 8)$. Τότε, όμως, οι τιμές του πολυωνύμου $f_p(x) = x^2 + x + \frac{p+1}{4}$ θα ήταν άρτιοι αριθμοί μεγαλύτεροι του 2 για κάθε x με

$$1 \leq x \leq \frac{1}{2}\Big(\sqrt{\frac{p}{3}} - 1\Big),$$

δηλαδή όχι πρώτοι, άτοπο.

Τώρα, ισχύει

$$\left(\frac{q}{p}\right) = 1 \Rightarrow \left(\frac{-p}{q}\right) = 1.$$

Αυτό σημαίνει ότι η ισοτιμία

$$x^2 + x + m \equiv 0(mod q)$$

έχει δύο λύσεις, έστω x_1, x_2, και μάλιστα οι δύο λύσεις έχουν άθροισμα

$$x_1 + x_2 \equiv (q-1)(mod q).$$

Μπορούμε, επομένως, να επιλέξουμε μία λύση, έστω $x_1 := x$, τέτοια ώστε $0 \leq x \leq \frac{q-1}{2}$. Για το x αυτό, καθώς $q < \sqrt{\frac{p}{3}}$, έπεται

$$x \leq \frac{q-1}{2} < \frac{1}{2}\Big(\sqrt{\frac{p}{3}} - 1\Big).$$

Επίσης, γνωρίζουμε ότι $q \mid f_p(x)$, και καθώς ισχύει προφανώς $q < \frac{p+1}{4}$, έπεται $f_p(x) \geq \frac{p+1}{4} > q$. Συνεπώς, προκύπτει ότι ο αριθμός $f_p(x)$ είναι σύνθετος, που είναι άτοπο στην υπόθεση της πρότασης $4.(\beta')$.

Δείξαμε, επομένως, όλες τις ισοδυναμίες, και άρα η απόδειξη του θεωρήματος έχει ολοκληρωθεί. □

4.3 Οι διακρίνουσες των τάξεων με class number 1

Για τις ανάγκες της παρούσας ενότητας, υποθέτουμε ότι γνωρίζουμε τις διακρίνουσες όλων των μιγαδικών τετραγωνικών σωμάτων αριθμών με class number 1, δηλαδή θεωρούμε δεδομένο ότι

$$h(d(K)) = 1 \Leftrightarrow d(K) = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Το παραπάνω θα αποδειχθεί στη συνέχεια.

Θα υπολογίσουμε τώρα όλες τις διακρίνουσες των τάξεων μιγαδικών σωμάτων αριθμών με class number 1. Συγκεκριμένα, θα δείξουμε το εξής:

Θεώρημα 4.3.1 Αν $d \equiv 0, 1(mod 4)$, $d < 0$, τότε ισχύει $h(d) = 1$ αν και μόνο αν

$$d = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

Απόδειξη. Έστω ότι $h(d) = 1$. Η διακρίνουσα d γράφεται

$$d = d_f = f^2 d(K),$$

όπου $d(K)$ η διακρίνουσα του τετραγωνικού σώματος K στο οποίο ανήκει η τάξη. Γνωρίζουμε ότι ισχύει η σχέση

$$h(d_f) = \frac{h(d(K))f}{[E(R_K) : E(\mathcal{O}_f)]} \cdot \prod_{p|f} \left(1 - \left(\frac{d(K)}{p}\right)\frac{1}{p}\right). \tag{4.1}$$

Συνεπώς $h(d(K)) \mid h(d_f) = 1$, δηλαδή $h(d(K)) = 1$. Έτσι, έχουμε τις τιμές

$$d(K) = -3, -4, -7, -8, -11, -19, -43, -67, -163$$

και τα $h(d(K))$ είναι οι αριθμοί κλάσεων όλων των μέγιστων τάξεων (δηλαδή των δακτυλίων ακεραίων αλγεβρικών αριθμών) των αντίστοιχων σωμάτων διακρίνουσας $d(K)$, δηλαδή όλων των τάξεων με οδηγό $f = 1$.

Υποθέτουμε τώρα ότι $f > 1$ και ξεχωρίζουμε διάφορες περιπτώσεις:

- Έστω ότι $E(R_K) = \{\pm 1\}$. Αυτό σημαίνει, αν θυμηθούμε το Θεώρημα 3.3.1, ότι $K \neq \mathbb{Q}(\sqrt{-1})$ και $K \neq \mathbb{Q}(\sqrt{-3})$. Επιπλέον, για κάθε τάξη του σώματος K θα ισχύει επίσης $E(\mathcal{O}_f) = \{\pm 1\}$. Προκύπτει, λοιπόν, ότι $[E(R_K) : E(\mathcal{O}_f)] = 1$, δηλαδή η (4.1) γίνεται

$$h(d_f) = h(d(K))f \cdot \prod_{p|f} \left(1 - \left(\frac{d(K)}{p}\right)\frac{1}{p}\right).$$

Αφού έχουμε υποθέσει $h(d_f) = 1$, δηλαδή και $h(d(K)) = 1$, θα πρέπει να ισχύει

$$A := f \cdot \prod_{p|f} \left(1 - \left(\frac{d(K)}{p}\right)\frac{1}{p}\right) = 1.$$

Παρατηρούμε, όμως, ότι αν $f > 2$, τότε $A > 1$, όποια κι αν είναι η τιμή του σύμβολου Legendre. Συνεπώς, η μοναδική δυνατότητα που έχουμε για το f είναι η $f = 2$. Τότε έπεται

$$A = 2 \cdot \left(1 - \left(\frac{d(K)}{2}\right)\frac{1}{2}\right) = 1 \Leftrightarrow \left(\frac{d(K)}{2}\right) = 1 \Leftrightarrow d(K) \equiv 1(mod 8).$$

Καθώς ισχύει επίσης $h(d(K)) = 1$, η μόνη διακρίνουσα που προκύπτει είναι η $d(K) = -7$. Συνεπώς,

$$d_f = 2^2(-7) = -28.$$

- Υποθέτουμε τώρα ότι $d(K) = -4$ και $K = \mathbb{Q}(i)$. Σε αυτή την περίπτωση, $E(R_K) = \{\pm 1, \pm i\}$.

  Αν $E(\mathcal{O}_f) = E(R_K)$, τότε όπως παραπάνω θα έπρεπε να ισχύει $A = 1$. Τώρα, όμως, η μόνη δυνατότητα για το f είναι $f = 1$, όποτε δεν προκύπτει κάποια καινούρια διακρίνουσα.

  Αν όμως $E(\mathcal{O}_f) = \{\pm 1\}$, τότε $[E(R_K) : E(\mathcal{O}_f)] = 2$, οπότε μπορούμε να επιλέξουμε $f = 2$. Τότε έχουμε

  $$d_f = 2^2(-4) = -16.$$

- Έστω, τέλος, ότι $d(K) = -3,\ K = \mathbb{Q}(\sqrt{-3})$. Τότε

  $$E(R_K) = \{\pm 1, \pm\omega, \pm\omega^2\},$$

  όπου ω μια πρωταρχική τρίτη ρίζα της μονάδας. Παρατηρούμε ότι αν $[E(R_K) : E(\mathcal{O}_f)] = 3$, έχουμε τις τιμές $f = 2$ και $f = 3$, οι οποίες μας δίνουν τις διακρίνουσες

  $$d_f = 2^2(-3) = -12$$

  και

  $$d_f = 3^2(-3) = -27.$$

  Αν, τέλος, $[E(R_K) : E(\mathcal{O}_f)] = 2$, τότε δεν υπάρχει άλλη δυνατότητα για το f.

□

4.4 Το θεώρημα του Landau

Το θεώρημα που ακολουθεί μας δείχνει πότε ισχύει $h(d) = 1$, στην περίπτωση $d \equiv 0(mod 4),\ d < 0$.

Θεώρημα 4.4.1 (*Landau*) Έστω $K = \mathbb{Q}(\sqrt{-4n})$ τετραγωνικό μιγαδικό σώμα αριθμών, $n \in \mathbb{N}, -4n = d(K)$ η διακρίνουσα του σώματος. Τότε:

$$h(-4n) = 1 \Longleftrightarrow n = 1, 2, 3, 4, 7 \Longleftrightarrow d = -4, -8, -12, -16, -28.$$

Παρατήρηση 4.4.2 Από τις παραπάνω διακρίνουσες, οι μόνες που είναι θεμελιώδεις είναι οι $d = -4, -8$, ενώ οι υπόλοιπες διακρίνουσες σχετίζονται με τις τάξεις του σώματος K.

Απόδειξη. Όπως είδαμε στο Θεώρημα 3.4.5, υπάρχει μία αντιστοιχία μεταξύ της ομάδας των κλάσεων ισοδυναμίας τετραγωνικών μορφών διακρίνουσας d και της ομάδας κλάσεων ιδεωδών του σώματος K. Επομένως, μπορούμε να ανάγουμε το πρόβλημα στις τετραγωνικές μορφές. Πρέπει επίσης να σημειωθεί ότι θα λαμβάνουμε υπόψη μόνο τις πρωταρχικές τετραγωνικές μορφές, δηλαδή εκείνες των οποίων οι συντελεστές είναι σχετικά πρώτοι.

Η μία κατεύθυνση είναι μία απλή επαλήθευση με τη μέθοδο που χρησιμοποιήσαμε στο Παράδειγμα 1.2.16. Για το ευθύ, θα δείξουμε ότι αν $n \notin \{1, 2, 3, 4, 7\}$, τότε μπορούμε να βρούμε δύο ανηγμένες τετραγωνικές μορφές διακρίνουσας d και άρα θα ισχύει $h(d) \geq 2$. Επειδή για οποιοδήποτε n η τετραγωνική μορφή

$$X^2 + nY^2$$

είναι πάντα ανηγμένη, αρκεί να δείξουμε ότι για n διαφορετικά από τα παραπάνω μπορούμε να βρούμε τουλάχιστον άλλη μία ανηγμένη.

Καταρχήν, αν $n = 1$, τότε έχουμε δείξει στην ανάποδη κατεύθυνση ότι $h(-4) = 1$. Θα υποθέσουμε, συνεπώς, στο εξής ότι $n > 1$.

- Έστω ότι ο n δεν είναι δύναμη πρώτου. Τότε ο n γράφεται ως $n = ac$, όπου $1 < a < c$ και $(a, c) = 1$. Μία κλάση αντιστοιχεί στην ανηγμένη μορφή $X^2 + nY^2$. Παρατηρούμε ότι και η τετραγωνική μορφή

  $$aX^2 + cY^2$$

  είναι ανηγμένη, αφού $0 = |b| \leq a \leq c$, και η διακρίνουσά της ισούται με $d = -4ac = -4n$. Συμπεραίνουμε ότι $h(d) \geq 2$, άρα για να έχουμε το ζητούμενο σίγουρα ο n πρέπει να είναι δύναμη πρώτου.

- Υποθέτουμε τώρα ότι $n = 2^r, r \in \mathbb{N}$. Αν $r \geq 4$, παρατηρούμε ότι η τετραγωνική μορφή

$$4X^2 + 4XY + (2^{r-2} + 1)Y^2$$

είναι ανηγμένη, καθώς $|b| = a$ και $a = 4 \leq 2^{r-2} + 1 = c$ για $r \geq 4$. Επιπλέον, η διακρίνουσά της είναι

$$4^2 - 4 \cdot 4 \cdot (2^{r-2} + 1) = -4 \cdot 2^2 \cdot 2^{r-2} = -4n = d.$$

Επομένως, $h(-4n) \geq 2$ όταν $n = 2^r, r \geq 4$.

Απομένει να εξετάσουμε τις περιπτώσεις $r = 1, 2, 3$.

Για $r = 1, 2$ έχουμε $n = 2, 4$ για τα οποία γνωρίζουμε ότι ισχύει $h(-4n) = 1$. Αν $r = 3$, τότε $n = 8$ και $d = -32$.

Θα δείξουμε ότι $h(-32) = 2$.

Έστω λοιπόν $aX^2 + bXY + cY^2$ μία ανηγμένη τετραγωνική μορφή διακρίνουσας $\Delta = -32$. Τότε

$$a^2 \leq \frac{32}{3} \Leftrightarrow a \in \{1, 2, 3\}.$$

  - Αν $a = 1$, τότε $b \in \{0, \pm 1\}$. Αν $|b| = a = 1$, επιλέγουμε $b = 1$. Τότε το $c = \frac{33}{4} \notin \mathbb{Z}$, άρα η περίπτωση αυτή απορρίπτεται. Αν $b = 0$, τότε $c = 8$ και παίρνουμε την ανηγμένη τετραγωνική μορφή

$$X^2 + 8Y^2.$$

  - Αν $a = 2$, τότε $b \in \{0, \pm 1, \pm 2\}$. Η περίπτωση $|b| = 2$ απορρίπτεται καθώς τότε $c \notin \mathbb{Z}$. Όμοια και η περίπτωση $|b| = 1$. Στη περίπτωση $b = 0$ βρίσκουμε την τετραγωνική μορφή $2X^2 + 4Y^2$, που όμως δεν είναι πρωταρχική και άρα δεν την λαμβάνουμε υπόψη.
  - Αν, τέλος, $a = 3$, τότε $b \in \{0, \pm 1, \pm 2, \pm 3\}$. Οι περιπτώσεις $b = 0, \pm 1, \pm 3$ απορρίπτονται, γιατί προκύπτει $c \notin \mathbb{Z}$. Αν $|b| = 2$, τότε $c = 3 = \alpha$, συνεπώς από τον ορισμό της ανηγμένης επιλέγουμε $b = 2$ και βρίσκουμε την πρωταρχική τετραγωνική μορφή

$$3X^2 + 2XY + 3Y^2.$$

Δείξαμε, επομένως, ότι $h(-32) = 2$.

- Τελειώνοντας, εξετάζουμε την περίπτωση $n = p^r$, όπου p περιττός πρώτος. Κοιτάμε τον ακέραιο $n + 1$:

  Αν το $n + 1$ γράφεται ως $n + 1 = ac, 1 < a < c, (a, c) = 1$, τότε η τετραγωνική μορφή

  $$aX^2 + 2XY + cY^2$$

  είναι ανηγμένη, αφού $2 \leq a < c$, και η διακρίνουσά της είναι ίση με $4 - 4ac = 4(1 - ac) = -4n = d$. Συνεπώς, σε αυτή την περίπτωση έχουμε πάλι $h(-4n) \geq 2$ και άρα υποθέτουμε ότι και ο $n + 1$ είναι δύναμη πρώτου. Επειδή όμως ο $n = p^r$ είναι περιττός αριθμός, ο $n + 1$ θα είναι άρτιος. Έχουμε, λοιπόν, ότι $n + 1 = 2^s, s \in \mathbb{N}$.

  Αν $s \geq 6$, τότε η πρωταρχική τετραγωνική μορφή

  $$8X^2 + 6XY + (2^{s-3} + 1)Y^2$$

  είναι ανηγμένη, αφού $8 \leq 2^{s-3} + 1$ όταν $s \geq 6$. Επίσης, η διακρίνουσά της ισούται με

  $$6^2 - 4 \cdot 8 \cdot (2^{s-3} + 1) = 4(1 - 2^s) = -4n = d.$$

  Συνεπώς, για $s \geq 6$ έχουμε $h(d) \geq 2$.

  Απομένει να εξετάσουμε τις περιπτώσεις $s = 1, 2, 3, 4, 5$, δηλαδή όταν $n = 1, 3, 7, 15, 31$.

  Για $n = 1, 3, 7$ γνωρίζουμε ότι $h(-4n) = 1$. Το $n = 15$ απορρίπτεται, αφού δεν είναι δύναμη πρώτου. Αν, τέλος, $n = 31$, τότε $d = -124$. Ακολουθώντας την ίδια διαδικασία όπως στην περίπτωση $d = -32$, βρίσκουμε τις πρωταρχικές ανηγμένες τετραγωνικές μορφές

  $$X^2 + 31Y^2, \quad 5X^2 \pm 4XY + 7Y^2$$

  διακρίνουσας -124, συνεπώς $h(-124) = 3$.

  Συμπεραίνουμε, τελικά, ότι $h(-4n) = 1 \Rightarrow n = 1, 2, 3, 4, 7$, και η απόδειξη έχει ολοκληρωθεί.

□

4.5 Σημειώσεις

Σχετικά με τα θέματα της πρώτης παραγράφου παραπέμπουμε στο [22]. Το βιβλίο αποτελεί μετάφραση από τα αγγλικά, με αρχικό τίτλο The Little Book of Bigger Primes.

Το θεώρημα του Rabinowitsch βρίσκεται στο [19]. Η μία κατεύθυνση του θεωρήματος είχε ήδη αποδειχθεί ένα χρόνο πριν από τον G. Frobenius. Η απόδειξη που παρουσιάζουμε εμείς στην εργασία μας οφείλεται στον I. G. Connell και συγκεκριμένα βρίσκεται στο [7]. Ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει και στο [17]. Φυσικά, υπάρχουν και άλλες αποδείξεις του θεωρήματος. Ενδεικτικά αναφέρουμε τα [5], [21] και [28].

Τέλος, το τελευταίο θεώρημα με τους διάφορους χαρακτηρισμούς των μιγαδικών τετραγωνικών σωμάτων αριθμών K με $h(K) = 1$, αναφέρεται στο [25], σελ.190.

Κεφάλαιο 5

Ελλειπτικές και Modular Συναρτήσεις

Σε αυτό το κεφάλαιο θα χρησιμοποιήσουμε κάποιες γνώσεις Μιγαδικής Ανάλυσης για να μελετήσουμε τις λεγόμενες ελλειπτικές και modular συναρτήσεις, οι οποίες θα συμβάλλουν σημαντικά στο βασικό μας σκοπό.

5.1 Διπλά Περιοδικές και Ελλειπτικές Συναρτήσεις

Δίνουμε πρώτα τον ορισμό της διπλά περιοδικής συνάρτησης.

Ορισμός 5.1.1 Έστω f μία μιγαδική συνάρτηση. Η f θα λέγεται *διπλά περιοδική* όταν έχει δύο περιόδους, $\omega_1, \omega_2 \in \mathbb{C}$ τέτοιες ώστε

$$f(z) = f(z + \omega_1) = f(z + \omega_2) \quad \forall z \in \mathbb{C}$$

και, επίσης,

$$Im\Big(\frac{\omega_1}{\omega_2}\Big) \neq 0^1.$$

Η τελευταία απαίτηση είναι σημαντική για την αποφυγή εκφυλισμένων περιπτώσεων. Για παράδειγμα, αν ο λόγος δύο περιόδων ω_1, ω_2 είναι ένας ρητός αριθμός, εύκολα μπορούμε να δούμε ότι τότε τα ω_1, ω_2 είναι ακέραια πολλαπλάσια της ίδιας περιόδου ω. Αν, πάλι, ο λόγος ω_1/ω_2 είναι πραγματικός άρρητος αριθμός, αποδεικνύεται ότι η συνάρτηση f έχει αυθαίρετα μικρές περιόδους και άρα

[1] Η συνθήκη $Im(\frac{\omega_1}{\omega_2}) \neq 0$ είναι ισοδύναμη με τη συνθήκη το σύνολο $\{\omega_1, \omega_2\}$ να είναι $\mathbb{R}-$γραμμικά ανεξάρτητο.

είναι σταθερή σε κάθε ανοικτό συνεκτικό χωρίο στο οποίο είναι αναλυτική.

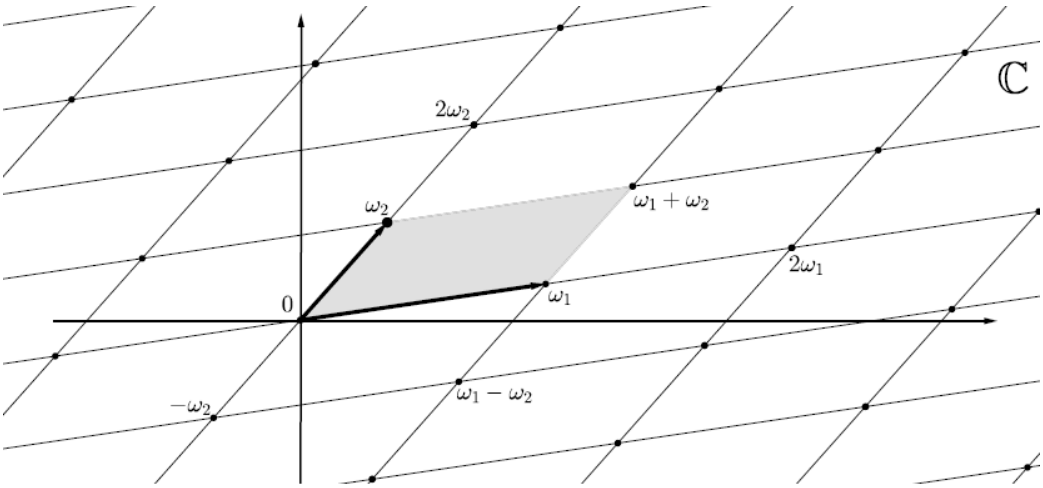
Είναι προφανές ότι όλα τα σημεία της μορφής $m\omega_1 + n\omega_2 \in \mathbb{C}$ αποτελούν περιόδους της συνάρτησης f.

Ορισμός 5.1.2 Έστω f μία διπλά περιοδική συνάρτηση με περιόδους ω_1, ω_2 τέτοιες ώστε $Im(\omega_1/\omega_2) \neq 0$. Το ζεύγος περιόδων (ω_1, ω_2) θα λέγεται *θεμελιώδες ζεύγος* αν κάθε περίοδος της f είναι της μορφής $m\omega_1 + n\omega_2,\ m, n \in \mathbb{Z}$.

Κάθε θεμελιώδες ζεύγος (ω_1, ω_2) ορίζει το σύνολο

$$L = L(\omega_1, \omega_2) := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{m\omega_1 + n\omega_2,\ m, n \in \mathbb{Z}\}.$$

Το L θα λέγεται 2−διάστατο *δικτυωτό* (lattice) του $\mathbb{C}$.



Σχήμα 5.1: Ένα δικτυωτό L.

Το σκιασμένο παραλληλόγραμμο του σχήματος λέγεται *παραλληλόγραμμο περιόδων*. Καθένα από τα ίσα προς αυτό παραλληλόγραμμα του σχήματος είναι παραληλόγραμμο περιόδων. Είναι σημαντικό να τονίσουμε ότι θεωρούμε ότι στο χρωματισμένο παραλληλόγραμμο μόνο τα σημεία των πλευρών που καταλήγουν στα ω_1, ω_2 και το σημείο 0 ανήκουν στο σύνορο. Με άλλα λόγια, ένα παραλληλόγραμμο περιόδων είναι το σύνολο

$$\{\gamma + t_1\omega_1 + t_2\omega_2 \mid \gamma \in \mathbb{C},\ 0 \leq t_i < 1, i = 1, 2\}.$$

Θα συμβολίζουμε το παραλληλόγραμμο περιόδων ως $\mathcal{F}(\gamma, L)$. Για παράδειγμα, το χρωματισμένο παραλληλόγραμμο περιόδων του σχήματος είναι το $\mathcal{F}(0, L)$.

Προφανώς, το $\mathcal{F}(\gamma, L)$ είναι ένα πλήρες σύστημα αντιπροσώπων του $\mathbb{C}modL$.

Πρόταση 5.1.3 Αν (ω_1, ω_2) είναι ένα θεμελιώδες ζεύγος περιόδων, τότε το τρίγωνο με κορυφές $0, \omega_1, \omega_2$ δεν περιέχει άλλες περιόδους στο εσωτερικό ή στο σύνορό του. Αντίστροφα, κάθε ζεύγος με αυτή την ιδιότητα είναι θεμελιώδες.

Απόδειξη. Η μία κατεύθυνση είναι προφανής. Για το αντίστροφο, έστω ότι το παραπάνω τρίγωνο δεν περιέχει άλλες περιόδους πέρα των ω_1, ω_2, και έστω ω μία περίοδος. Αρκεί να δείξουμε ότι $\omega = m\omega_1 + n\omega_2, m, n \in \mathbb{Z}$.

Εφόσον έχουμε υποθέσει ότι $Im(\omega_1/\omega_2) \neq 0$ και άρα τα ω_1, ω_2 είναι $\mathbb{R}-$γραμμικά ανεξάρτητα, για την περίοδο ω θα ισχύει ότι

$$\omega = t_1\omega_1 + t_2\omega_2, \quad t_1, t_2 \in \mathbb{R}. \tag{5.1}$$

Συμβολίζουμε τώρα με $[t]$ το ακέραιο μέρος του αριθμού t. Τότε οι αριθμοί t_1, t_2 γράφονται ως

$$t_1 = [t_1] + r_1,\ t_2 = [t_2] + r_2, \quad 0 \leq r_1, r_2 < 1$$

και άρα η σχέση (5.1) γίνεται

$$\omega - [t_1]\omega_1 - [t_2]\omega_2 = r_1\omega_1 + r_2\omega_2.$$

Ο μιγαδικός αριθμός $r_1\omega_1 + r_2\omega_2$ είναι περίοδος που ανήκει στο παραλληλόγραμμο περιόδων με κορυφές $0, \omega_1, \omega_1 + \omega_2, \omega_2$. Αν, όμως, μία περίοδος ω βρίσκεται στο εσωτερικό του παραλληλογράμμου, τότε το ίδιο ισχύει και για την περίοδο $\omega_1 + \omega_2 - \omega$, και μάλιστα αποδεικνύεται ότι μία εκ των δύο θα ανήκει είτε στο εσωτερικό του τριγώνου με κορυφές $0, \omega_1, \omega_2$ ή στη διαγώνιο που ενώνει τα σημεία ω_1, ω_2. Και από τις δύο αυτές περιπτώσεις προκύπτει κατ'ανάγκη ότι $r_1 = r_2 = 0$, και επομένως $\omega = [t_1]\omega_1 + [t_2]\omega_2$, όπως θέλαμε. □

Ορισμός 5.1.4 Δύο θεμελιώδη ζεύγη $(\omega_1, \omega_2), (\omega_1', \omega_2')$ θα λέγονται *ισοδύναμα* αν τα δικτυωτά τους ταυτίζονται, δηλαδή $L(\omega_1, \omega_2) = L(\omega_1', \omega_2')$. (Προφανώς, υποθέτουμε ότι $Im(\omega_1/\omega_2), Im(\omega_1'/\omega_2') \neq 0$.)

Το παρακάτω θεώρημα αποτελεί κριτήριο ελέγχου ισοδυναμίας δύο θεμελιωδών ζευγών.

Θεώρημα 5.1.5 Δύο θεμελιώδη ζεύγη $(\omega_1, \omega_2), (\omega_1', \omega_2')$ είναι ισοδύναμα αν και μόνο αν υπάρχει 2×2 πίνακας

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

με $a, b, c, d \in \mathbb{Z},\ detA = ad - bc = \pm 1$, τέτοιος ώστε

$$\begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}.$$

Απόδειξη. Βλ.[4], σελ.4. □

Ορισμός 5.1.6 Μία μιγαδική συνάρτηση f θα λέγεται *ελλειπτική* αν ισχύουν τα εξής:

1. Η f είναι διπλά περιοδική συνάρτηση.
2. Η f είναι μερόμορφη συνάρτηση, δηλαδή οι μοναδικές ανωμαλίες που παρουσιάζει είναι πόλοι.

Πρόταση 5.1.7 Κάθε μη-σταθερή ελλειπτική συνάρτηση έχει ένα θεμελιώδες ζεύγος περιόδων.

Απόδειξη. Αν f μία μη-σταθερή ελλειπτική συνάρτηση, τότε το σύνολο των σημείων στα οποία η f είναι αναλυτική αποτελεί ένα ανοικτό συνεκτικό χωρίο. Επίσης, η f είναι διπλά περιοδική, επομένως έχει δύο περιόδους με μη πραγματικό λόγο. Από όλες τις μη-μηδενικές περιόδους της f μπορούμε να επιλέξουμε κάποια με τη μικρότερη απόσταση από το 0. Πράγματι, αν δεν μπορούσαμε να κάνουμε αυτή την επιλογή, τότε η f θα είχε αυθαίρετα μικρές περιόδους, δηλαδή θα ήταν σταθερή. Έστω λοιπόν ω αυτή η περίοδος. Από τις περιόδους εκείνες με μέτρο $|\omega|$, επιλέγουμε αυτή με το μικρότερο μη-αρνητικό όρισμα, έστω ω_1 (μία τέτοια περίοδος υπάρχει για τον ίδιο λόγο). Αν υπάρχουν και άλλες περίοδοι μέτρου $|\omega_1|$ πέρα των $\omega_1, -\omega_1$, επιλέγουμε αυτή με το μικρότερο όρισμα μεγαλύτερο του $arg\omega_1$, έστω ω_2. Αν πάλι δεν υπάρχουν άλλες τέτοιες περίοδοι, βρίσκουμε τον επόμενο μεγαλύτερο δίσκο που περιέχει περιόδους διάφορες του $n\omega_1$ και επιλέγουμε εκείνη με το μικρότερο μη-αρνητικό όρισμα. Μία τουλάχιστον τέτοια περίοδος υπάρχει, καθώς η f έχει σίγουρα δύο ανεξάρτητες περιόδους ως διπλά περιοδική. Ονομάζουμε την τελευταία περίοδο ω_2. Εκ κατασκευής, στο τρίγωνο με κορυφές $0, \omega_1, \omega_2$ δεν υπάρχουν άλλες περίοδοι, επομένως το ζεύγος (ω_1, ω_2) είναι θεμελιώδες. □

Παρατήρηση 5.1.8 Αν f, g δύο ελλειπτικές συναρτήσεις, εύκολα διαπιστώνουμε ότι οι συναρτήσεις $f+g, f-g, f \cdot g, f/g$ είναι επίσης ελλειπτικές με τις ίδιες περιόδους. Επομένως, το σύνολο όλων των ελλειπτικών συναρτήσεων ενός δικτυωτού $L = L(\omega_1, \omega_2)$ αποτελεί σώμα και θα το συμβολίζουμε $K(L)$. Μάλιστα, ισχύει το εξής:

$$f \in K(L) \Longrightarrow f' \in K(L).$$

Λόγω περιοδικότητας, είναι αρκετό να μελετήσουμε τη συμπεριφορά μίας ελλειπτικής συνάρτησης σε ένα οποιοδήποτε παραλληλόγραμμο περιόδων. Εξάγουμε, έτσι, τα ακόλουθα συμπεράσματα:

Πρόταση 5.1.9 Αν μία ελλειπτική συνάρτηση f δεν έχει πόλους σε κάποιο παραλληλόγραμμο περιόδων, τότε είναι σταθερή.

Απόδειξη. Αφού η f δεν έχει πόλους σε ένα παραλληλόγραμμο περιόδων, συμπεραίνουμε ότι είναι συνεχής και φραγμένη στην κλειστότητα του παραλληλογράμμου. Λόγω περιοδικότητας, η f είναι συνεχής και φραγμένη σε όλο το μιγαδικό επίπεδο. Συνεπώς, από το θεώρημα του Liouville, η f είναι σταθερή. □

Από την Πρόταση 5.1.9 συμπεραίνουμε επίσης ότι, αν η f δεν παρουσιάζει σημεία μηδενισμού σε κάποιο παραλληλόγραμμο περιόδων, τότε είναι σταθερή. Αυτό προκύπτει από εφαρμογή του θεωρήματος του Liouville στη συνάρτηση $1/f$.

Από τα παραπάνω προκύπτει άμεσα ότι κάθε μη-σταθερή ελλειπτική συνάρτηση έχει πόλους. Μάλιστα, το σύνολο των πόλων μιας ελλειπτικής συνάρτησης f σε ένα παραλληλόγραμμο περιόδων θα είναι πεπερασμένο, αφού τα σημεία συσσώρευσης των πόλων είναι ουσιώδη ιδιάζοντα σημεία της f, και επιπλέον το πλήθος των πόλων δεν εξαρτάται από την επιλογή του παραλληλογράμμου περιόδων.

Παρατήρηση 5.1.10 Αν οι ελλειπτικές συναρτήσεις $f, g \in K(L)$ έχουν ακριβώς τους ίδιους πόλους και τα ίδια σημεία μηδενισμού, και μάλιστα με την ίδια πολλαπλότητα, τότε εύκολα βλέπουμε ότι είναι ανάλογες, δηλαδή υπάρχει $c \in \mathbb{C}^*$ τέτοιο ώστε $f = c \cdot g$.

Παρατήρηση 5.1.11 Κάποιες φορές η ύπαρξη πόλων ή σημείων μηδενισμού στο σύνορο ενός παραλληλογράμμου περιόδων μπορεί να μας προκαλέσει προβλήματα. Επειδή, λοιπόν, μία μερόμορφη συνάρτηση έχει πεπερασμένο πλήθος πόλων ή σημείων μηδενισμού σε κάθε φραγμένη περιοχή του $\mathbb{C}$, μπορούμε να απεικονίσουμε ένα παραλληλόγραμμο περιόδων σε ένα ισότιμο, στο σύνορο του οποίου η f δεν έχει ούτε πόλους ούτε σημεία μηδενισμού. Θα ονομάζουμε ένα τέτοιο παραλληλόγραμμο *κελί* (cell). Τα διανύσματα ενός κελιού μπορεί να μην είναι πλέον περίοδοι.

Ορισμός 5.1.12 Το πεπερασμένο σύνολο των πόλων μιας ελλειπτικής συνάρτησης σε ένα παραλληλόγραμμο περιόδων αυτής θα λέγεται *τάξη* της ελλει-

πτικής συνάρτησης.

Πρόταση 5.1.13 Το ολοκλήρωμα μιας ελλειπτικής συνάρτησης f στο σύνορο ενός κελιού ισούται με 0.

Απόδειξη. Τα ολοκληρώματα δύο απέναντι πλευρών του κελιού, λόγω περιοδικότητας, είναι ίσα κατά απόλυτη τιμή αλλά ετερόσημα, συνεπώς αλληλοαναιρούνται. □

Με χρήση της παραπάνω πρότασης και εφαρμόζοντας το θεώρημα ολοκληρωτικών υπολοίπων του Cauchy, αποδεικνύεται η ακόλουθη πρόταση:

Πρόταση 5.1.14 Το άθροισμα των ολοκληρωτικών υπολοίπων μιας ελλειπτικής συνάρτησης στους πόλους ενός παραλληλογράμμου περιόδων είναι 0.

Απόδειξη. Βλ.[4], σελ.6. □

Από την Πρόταση 5.1.14 έπεται ότι δεν υπάρχει ελλειπτική συνάρτηση τάξης 1, δηλαδή ελλειπτική συνάρτηση με μοναδικό πόλο. Πράγματι, αν η ελλειπτική συνάρτηση f παρουσίαζε μοναδικό πόλο στο $z = a$ στοιχείο του παραλληλογράμμου περιόδων, τότε το ανάπτυγμα Laurent της f κοντά στο a θα ήταν της μορφής

$$f(z) = \sum_{j=-1}^{\infty} a_j (z-a)^j,$$

όπου $a_{-1} \neq 0$. Τότε όμως το άθροισμα των ολοκληρωτικών υπολοίπων είναι ακριβώς ίσο με $a_{-1} \neq 0$, άτοπο.

Επομένως, συμπεραίνουμε από τα παραπάνω ότι κάθε μη-σταθερή ελλειπτική συνάρτηση έχει τάξη ≥ 2, δηλαδή έχει δύο τουλάχιστον πόλους ή τουλάχιστον έναν διπλό πόλο σε κάθε παραλληλόγραμμο περιόδων.

Πρόταση 5.1.15 Το πλήθος των σημείων μηδενισμού μιας ελλειπτικής συνάρτησης σε κάθε παραλληλόγραμμο περιόδων είναι ίσο με το πλήθος των πόλων αυτής, λαμβάνοντας υπόψη την πολλαπλότητα του σημείου μηδενισμού και την τάξη του πόλου.

Απόδειξη. Θεωρούμε την f σε ένα κελί. Η συνάρτηση f'/f είναι ελλειπτική και έχει τις ίδιες περιόδους με την f. Επομένως, το ολοκλήρωμα

$$\frac{1}{2\pi i} \int_C \frac{f'(z)}{f(z)} dz,$$

όπου C το σύνορο του κελιού, ισούται με 0. Το παραπάνω, όμως, ολοκλήρωμα μετράει ακριβώς τη διαφορά του πλήθους των σημείων μηδενισμού και του πλήθους των πόλων στο κελί, συνεπώς ισχύει το ζητούμενο. □

5.2 Κατασκευή Ελλειπτικών Συναρτήσεων

Θα ασχοληθούμε τώρα με το πρόβλημα κατασκευής μη-σταθερών ελλειπτικών συναρτήσεων. Επιλέγουμε έτσι ένα σταθερό θεμελιώδες ζεύγος περιόδων (ω_1, ω_2). Αφού, όπως είδαμε στα προηγούμενα, θέλουμε η τάξη της ελλειπτικής συνάρτησης να είναι μεγαλύτερη ή ίση του 2, επιθυμούμε η συνάρτηση f να έχει σε κάθε παραληλόγραμμο περιόδων είτε τουλάχιστον έναν διπλό ή τουλάχιστον δύο απλούς πόλους. Στα πλαίσια της εργασίας μας θα ακολουθήσουμε τη θεωρία του Weierstrass, ο οποίος υπέθεσε ότι η ελλειπτική συνάρτηση παρουσιάζει πόλο τάξης 2 στο $z = 0$ και άρα σε κάθε περίοδο.

Μπορούμε να επιλέξουμε μία περιοχή γύρω από κάθε περίοδο ω, χωρίς αυτήν, στην οποία η f να είναι αναλυτική. Σε κάθε τέτοια περιοχή, η συνάρτησή μας έχει ανάπτυγμα Laurent, το κύριο μέρος του οποίου σύμφωνα με τις υποθέσεις μας θα είναι της μορφής

$$\frac{A}{(z-\omega)^2} + \frac{B}{z-\omega}.$$

Για λόγους απλότητας, επιλέγουμε $A = 1, B = 0$. Εφόσον επιθυμούμε μία έκφραση της παραπάνω μορφής γύρω από κάθε περίοδο ω, θεωρούμε το άθροισμα

$$\sum_{\omega \in L(\omega_1,\omega_2)} \frac{1}{(z-\omega)^2},$$

όπου $\omega = m\omega_1 + n\omega_2$. Για σταθερό $z \neq \omega$, το παραπάνω είναι ένα διπλό άθροισμα ως προς m και n.

Λήμμα 5.2.1 Αν $a \in \mathbb{R}$, η σειρά

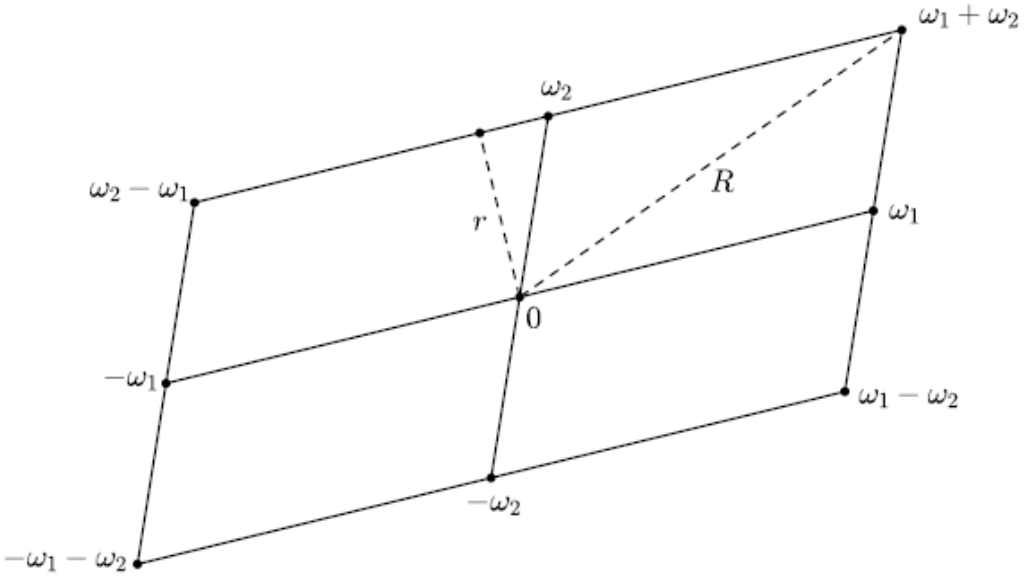
$$\sum_{\substack{\omega \in L(\omega_1,\omega_2) \\ \omega \neq 0}} \frac{1}{\omega^a}$$

συγκλίνει απόλυτα αν και μόνο αν $a > 2$.

Απόδειξη. Έστω r και R η ελάχιστη και η μέγιστη απόσταση αντίστοιχα του 0 από το παραλληλόγραμμο με κορυφές $\omega_1 + \omega_2, \omega_1 - \omega_2, -\omega_1 - \omega_2, \omega_2 - \omega_1$, όπως φαίνεται στο Σχήμα 5.2. Αν θέσουμε ω οποιαδήποτε από τις 8 περιόδους του παραλληλογράμμου, τότε ισχύει

$$r \leq |\omega| \leq R.$$

Κοιτάμε τώρα το αμέσως μεγαλύτερο παραλληλόγραμμο με κέντρο το 0 και κορυφές περιόδους. Αυτό θα περιέχει και τις 8 περιόδους του προηγούμενου



Σχήμα 5.2

παραλληλογράμμου. Συνολικά θα περιέχει 16 περιόδους, για κάθε μία από τις οποίες θα έχουμε

$$2r \leq |\omega| \leq 2R.$$

Επαναλαμβάνοντας αυτή τη διαδικασία, παίρνουμε τελικά την ανισότητα

$$nr \leq |\omega| \leq nR$$

για τις επόμενες $8n$ περιόδους. Ισχύει τότε ότι

$$\frac{1}{R^a} \leq \frac{1}{|\omega|^a} \leq \frac{1}{r^a} \text{ για τις πρώτες 8 περιόδους,}$$

$$\frac{1}{(2R)^a} \leq \frac{1}{|\omega|^a} \leq \frac{1}{(2r)^a} \text{ για τις επόμενες 16 περιόδους κ.ο.κ.}$$

Έτσι, αν θέσουμε

$$S(n) = \sum |\omega|^{-a}$$

για τις πρώτες $8(1 + 2 + ... + n)$ μη μηδενικές περιόδους γύρω από το 0, αυτό ικανοποιεί:

$$\frac{8}{R^a} + \frac{2 \cdot 8}{(2R)^a} + ... + \frac{n \cdot 8}{(nR)^a} \leq S(n) \leq \frac{8}{r^a} + \frac{2 \cdot 8}{(2r)^a} + ... + \frac{n \cdot 8}{(nr)^a}.$$

Ισοδύναμα,

$$\frac{8}{R^a}\sum_{k=1}^{n}\frac{1}{k^{a-1}} \le S(n) \le \frac{8}{r^a}\sum_{k=1}^{n}\frac{1}{k^{a-1}}.$$

Από την ανισότητα αυτή είναι φανερό ότι για $a > 2$ κάθε μερικό άθροισμα $S(n)$ συγκλίνει, συνεπώς σε αυτή την περίπτωση η σειρά συγκλίνει απόλυτα. Επιπλέον, κοιτώντας το κάτω φράγμα των $S(n)$ συμπεραίνουμε ότι για $a \le 2$ η σειρά αποκλίνει. □

Λήμμα 5.2.2 Αν $a > 2, R > 0$, η σειρά

$$\sum_{|\omega|>R}\frac{1}{(z-\omega)^a}$$

συγκλίνει απόλυτα και ομοιόμορφα στο δίσκο $|z| \le R$.

Απόδειξη. Για την απόδειξη θα δείξουμε ότι υπάρχει σταθερά M (που θα εξαρτάται από την επιλογή των a, R) τέτοια ώστε, αν $a \ge 1$, τότε

$$\frac{1}{|z-\omega|^a} \le \frac{M}{|\omega|^a} \tag{5.2}$$

για κάθε ω, z τέτοια ώστε $|\omega| > R$ και $|z| \le R$. Σε αυτή την περίπτωση, το ζητούμενο έπεται άμεσα από το Λήμμα 5.2.1.

Η σχέση (5.2) γίνεται

$$\Big|\frac{z-\omega}{\omega}\Big|^a \ge \frac{1}{M}, \quad |\omega| > R.$$

Επιλέγουμε ω τέτοιο ώστε το μέτρο του, $|\omega| = R + d, d > 0$, να είναι το ελάχιστο. Τότε για $|z| \le R, |\omega| \ge R + d$, έχουμε

$$\Big|\frac{z-\omega}{\omega}\Big| = \Big|1 - \frac{z}{\omega}\Big| \ge 1 - \Big|\frac{z}{\omega}\Big| \ge 1 - \frac{R}{R+d}.$$

Επομένως,

$$\Big|\frac{z-\omega}{\omega}\Big|^a \ge \Big(1 - \frac{R}{R+d}\Big)^a = \frac{1}{M},$$

όπου

$$M = \Big(1 - \frac{R}{R+d}\Big)^{-a}.$$

Συνεπώς, αποδείξαμε ότι ισχύει η σχέση (5.2) και άρα το λήμμα. □

Βλέπουμε ότι, αν προσπαθούσαμε να κατασκευάσουμε την απλούστερη ελλειπτική συνάρτηση χρησιμοποιώντας μία σειρά της μορφής

$$\sum_{\omega \in L(\omega_1,\omega_2)} \frac{1}{(z-\omega)^2},$$

η οποία εμφανίζει το κύριο μέρος που επιθυμούμε σε κάθε περίοδο, θα αποτυγχάναμε, καθώς η σειρά αυτή δεν συγκλίνει απόλυτα! Θα κατασκευάσουμε, λοιπόν, στο ακόλουθο θεώρημα μια ελλειπτική συνάρτηση με πόλο τάξης 3 αντί για 2, χρησιμοποιώντας την ίδια σειρά με εκθέτη 3. Θα χρησιμοποιήσουμε το αποτέλεσμα αυτό για να κατασκευάσουμε μία ελλειπτική συνάρτηση τάξης 2 στην επόμενη ενότητα.

Θεώρημα 5.2.3 Έστω η μιγαδική συνάρτηση f με

$$f(z) = \sum_{\omega \in L(\omega_1,\omega_2)} \frac{1}{(z-\omega)^3}.$$

Τότε η f είναι ελλειπτική συνάρτηση με περιόδους ω_1, ω_2 και πόλο τάξης 3 σε κάθε περίοδο $\omega \in L(\omega_1, \omega_2)$.

Απόδειξη. Από το Λήμμα 5.2.2, η f συγκλίνει απόλυτα και ομοιόμορφα στο δίσκο $|z| \leq R$ για $|\omega| > R$ και άρα είναι αναλυτική σε αυτόν. Οι υπόλοιποι όροι της f, που είναι πεπερασμένοι το πλήθος, αποτελούν επίσης αναλυτικές συναρτήσεις εκτός από τα σημεία των περιόδων όπου παρουσιάζουν πόλους (τάξης 3). Επομένως, η f είναι μερόμορφη συνάρτηση.

Απομένει να δείξουμε ότι η f έχει περιόδους ω_1, ω_2. Έχουμε:

$$f(z+\omega_1) = \sum_{\omega \in L(\omega_1,\omega_2)} \frac{1}{(z-\omega+\omega_1)^3} = \sum_{\omega \in L(\omega_1,\omega_2)} \frac{1}{(z-(\omega-\omega_1))^3}.$$

Η περίοδος $\omega - \omega_1$ διατρέχει επίσης όλες τις περιόδους στο $L(\omega_1, \omega_2)$, επομένως η παραπάνω σειρά είναι απλώς μία αναδιάταξη των όρων της αρχικής. Λόγω απόλυτης σύγκλισης,το όριο παραμένει σταθερό, συνεπώς

$$f(z) = f(z+\omega_1).$$

Όμοια βρίσκουμε

$$f(z) = f(z+\omega_2).$$

Επομένως, η f είναι διπλά περιοδική με περιόδους ω_1, ω_2 και άρα είναι ελλειπτική συνάρτηση. □

5.3 Η συνάρτηση $\wp$ του Weierstrass

Στην προηγούμενη ενότητα φτιάξαμε μία ελλειπτική συνάρτηση με πόλο τάξης 3 σε κάθε περίοδο. Από τη συνάρτηση αυτή του Θεωρήματος 5.2.3 θα κατασκευάσουμε μία ελλειπτική συνάρτηση τάξης 2, απλώς ολοκληρώνοντας κάθε όρο του αθροίσματός της και πολλαπλασιάζοντας με -2 για να σχηματίσουμε το ζητούμενο κύριο μέρος. Επειδή είναι βολικό να ξεκινήσουμε την ολοκλήρωση από την αρχή των αξόνων, εξαιρούμε τον όρο z^{-3} που αντιστοιχεί στην περίοδο $\omega = 0$. Η ολοκλήρωση αυτού του όρου μας δίνει $-1/2z^2$, και αφού πολλαπλασιάζουμε με -2 απλά προσθέτουμε στο ολοκλήρωμα τον όρο z^{-2}. Οδηγούμαστε έτσι στη συνάρτηση

$$\frac{1}{z^2} + \int_0^z \sum_{\omega \neq 0} \frac{-2}{(t-\omega)^3} dt, \quad \omega \in L(\omega_1, \omega_2).$$

Η κατά όρους ολοκλήρωση της συνάρτησης αυτής μας δίνει τη συνάρτηση $\wp$ του Weierstrass.

Ορισμός 5.3.1 Η συνάρτηση $\wp$ του Weierstrass ορίζεται μέσω της σειράς

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right], \quad \omega \in L(\omega_1, \omega_2).$$

Θεώρημα 5.3.2 Η συνάρτηση $\wp$ έχει περιόδους ω_1 και ω_2. Επίσης, είναι αναλυτική εκτός από ένα διπλό πόλο σε κάθε περίοδο $\omega \in L(\omega_1, \omega_2)$. Τέλος, η $\wp$ είναι άρτια συνάρτηση του z.

Απόδειξη. Κάθε όρος της σειράς που ορίζει την $\wp$ έχει μέτρο

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega^2 - (z-\omega)^2}{\omega^2 (z-\omega)^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right|.$$

Έστω τώρα ένας συμπαγής δίσκος $|z| \leq R$. Υπάρχουν πεπερασμένες το πλήθος περίοδοι στο δίσκο αυτό. Αν εξαιρέσουμε τους όρους της σειράς που περιέχουν αυτές τις περιόδους, προκύπτει από το Λήμμα 5.2.2 η σχέση

$$\left| \frac{1}{(z-\omega)^2} \right| \leq \frac{M}{|\omega|^2},$$

όπου M σταθερά που εξαρτάται από το R. Η ανισότητα αυτή μας δίνει την ακόλουθη εκτίμηση:

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right| \leq \frac{MR(2|\omega| + R)}{|\omega|^4} = \frac{MR(2 + R/|\omega|)}{|\omega|^3} \leq \frac{3MR}{|\omega|^3},$$

αφού για κάθε περίοδο ω εκτός του δίσκου $|z| \leq R$ ισχύει $|\omega| > R$. Έτσι, συμπεραίνουμε ότι η σειρά που απομένει αν εξαιρέσουμε τους όρους που περιέχουν τις περιόδους ω για τις οποίες ισχύει $|\omega| \leq R$ συγκλίνει απόλυτα και ομοιόμορφα στο δίσκο $|z| \leq R$, άρα είναι αναλυτική σε αυτόν. Οι υπόλοιποι όροι της σειράς παρουσιάζουν πόλο τάξης 2 σε κάθε περίοδο και άρα η συνάρτηση $\wp$ είναι μερόμορφη.

Τώρα, η συνάρτηση $\wp$ είναι άρτια, αφού:

$$\wp(-z) = \frac{1}{(-z)^2} + \sum_{\omega \neq 0} \left[\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2} \right] = \frac{1}{z^2} + \sum_{\omega \neq 0} \left[\frac{1}{(z-(-\omega))^2} - \frac{1}{\omega^2} \right] = \wp(z),$$

καθώς η περίοδος $-\omega$ διατρέχει επίσης όλες τις περιόδους του $L(\omega_1, \omega_2)$, όπως και η ω.

Απομένει να εξετάσουμε την περιοδικότητα της $\wp$. Η παράγωγος της $\wp$ είναι

$$\wp'(z) = \sum_{\omega \in L(\omega_1, \omega_2)} \frac{-2}{(z-\omega)^3}.$$

Έχουμε δει στο Θεώρημα 5.2.3 ότι αυτή η συνάρτηση έχει περιόδους ω_1, ω_2. Επομένως, $\wp'(z+\omega) = \wp'(z)$ για κάθε περίοδο $\omega \in L(\omega_1, \omega_2)$, δηλαδή

$$\wp(z+\omega) - \wp(z) = C,$$

όπου C σταθερά. Αν θέσουμε $z = -\omega/2$, τότε

$$\wp(\omega/2) - \wp(-\omega/2) = 0 \Rightarrow C = 0,$$

αφού η $\wp$ είναι άρτια συνάρτηση. Συνεπώς, $\wp(z+\omega) = \wp(z)$ για κάθε περίοδο $\omega \in L(\omega_1, \omega_2)$, δηλαδή η $\wp$ είναι διπλά περιοδική με περιόδους ω_1, ω_2. Από τα παραπάνω συμπεραίνουμε ότι η συνάρτηση $\wp$ είναι ελλειπτική. □

Εύλογα προκύπτει τώρα το ερώτημα, αν υπάρχουν και άλλες ελλειπτικές συναρτήσεις τάξης 2. Απάντηση εδώ μας δίνει το ακόλουθο θεώρημα.

Θεώρημα 5.3.3 Το σύνολο των ελλειπτικών συναρτήσεων ταυτίζεται με το σώμα $\mathbb{C}(\wp, \wp')$.

Απόδειξη. Έστω f ελλειπτική συνάρτηση με περιόδους ω_1, ω_2. Τότε η f γράφεται

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2},$$

δηλαδή ως άθροισμα μίας άρτιας και μίας περιττής ελλειπτικής συνάρτησης. Αρκεί, συνεπώς, να αποδείξουμε το θεώρημα στις περιπτώσεις f άρτια και f

περιττή. Αν, όμως, η f είναι περιττή συνάρτηση, τότε η συνάρτηση $f\wp'$ θα είναι άρτια και ελλειπτική και άρα μπορούμε, χωρίς βλάβη της γενικότητας, να υποθέσουμε ότι η f είναι άρτια συνάρτηση. Ισχύει, λοιπόν, ότι $f(z) = f(-z)$ για κάθε $z \in \mathbb{C}$. Έπεται άμεσα ότι

$$f^{(k)}(z) = (-1)^k f^{(k)}(-z).$$

Με άλλα λόγια, αν η f έχει ως σημείο μηδενισμού πολλαπλότητας m το u, τότε και το $-u$ θα είναι σημείο μηδενισμού της με την ίδια πολλαπλότητα. Το ίδιο θα ισχύει και για τους πόλους της f.

Ισχυριζόμαστε, τώρα, ότι αν $2u \in L(\omega_1, \omega_2)$, τότε η f έχει σημείο μηδενισμού άρτιας πολλαπλότητας και αντίστοιχα, αν το u είναι πόλος και $2u \in L(\omega_1, \omega_2)$, τότε η f παρουσιάζει πόλο άρτιας τάξης. Πράγματι, έστω ότι $2u \in L(\omega_1, \omega_2)$. Τα σημεία ενός παραλληλογράμμου περιόδων που έχουν αυτή την ιδιότητα είναι τα

$$0, \ \frac{\omega_1}{2}, \ \frac{\omega_2}{2}, \ \frac{\omega_1 + \omega_2}{2}.$$

Αφού έχουμε υποθέσει ότι η f είναι άρτια, η παράγωγός της f' θα είναι περιττή, δηλαδή για κάθε $z \in \mathbb{C}$ ισχύει $f'(z) = -f'(-z)$. Συγκεκριμένα για $z = u$, έχουμε

$$f'(u) + f'(-u) = 0.$$

Επειδή, όμως, $2u \in L(\omega_1, \omega_2)$, έπεται ότι $u \equiv -u (mod L(\omega_1, \omega_2))$, δηλαδή τα $u, -u$ ανήκουν στην ίδια κλάση ισοδυναμίας που ορίζεται ως:

$$a \sim b \Longleftrightarrow a - b \in L(\omega_1, \omega_2).$$

Συνεπώς, ισχύει η ισότητα

$$f'(u) = 0.$$

Συμπεραίνουμε, λοιπόν, ότι αν το u είναι σημείο μηδενισμού της f, τότε θα έχει πολλαπλότητα τουλάχιστον 2.

Διακρίνουμε, τώρα, δύο περιπτώσεις.

- Έστω ότι $u \notin L(\omega_1, \omega_2)$. Τότε, αν εφαρμόσουμε το παραπάνω στη συνάρτηση

  $$g(z) := \wp(z) - \wp(u),$$

  θα έχουμε ότι η g έχει σημείο μηδενισμού το u, πολλαπλότητας τουλάχιστον 2. Καθώς όμως γνωρίζουμε ότι η ελλειπτική συνάρτηση $\wp$ έχει πόλο τάξης 2 και το πλήθος των πόλων ισούται με το πλήθος των σημείων μηδενισμού από την Πρόταση 5.1.15, το u θα εμφανίζει πολλαπλότητα ακριβώς ίση με 2.

Η g είναι εξ ορισμού άρτια συνάρτηση, επομένως το ίδιο ισχύει και για τη συνάρτηση f/g. Μάλιστα, η f/g θα είναι και ολόμορφη. Αν ισχύει $f(u)/g(u) \neq 0$, τότε η πολλαπλότητα του u στην f είναι ίση με 2. Διαφορετικά, η συνάρτηση f/g έχει ως σημείο μηδενισμού το u και άρα επαναλαμβάνουμε τη διαδικασία.

- Στην περίπτωση $u \in L(\omega_1, \omega_2)$, επιλέγουμε ως g τη συνάρτηση $1/\wp$ και εφαρμόζουμε το ίδιο επιχείρημα όπως προηγουμένως.

Δείξαμε, λοιπόν, ότι η f παρουσιάζει σημείο μηδενισμού άρτιας πολλαπλότητας. Έστω τώρα $\{u_i,\ 1 \leq i \leq r\}$ μία οικογένεια σημείων, τα οποία είναι είτε σημεία μηδενισμού είτε πόλοι της f και επιπλέον ικανοποιούν τη σχέση

$$u_i \neq -u_j, \quad i \neq j,$$

με $i, j \in \{1, ..., r\}$. 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 $ord_f(u_i)$ είναι η τάξη του u_i ως πόλος ή η πολλαπλότητα του u_i ως σημείο μηδενισμού.

Σύμφωνα με τα παραπάνω, αν $a \in \mathbb{C}$ τυχαίο, τότε η σχέση $2a \in L(\omega_1, \omega_2)$ είναι ισοδύναμη με το ότι η συνάρτηση $\wp(z) - \wp(a)$ παρουσιάζει στο a σημείο μηδενισμού πολλαπλότητας 2 ή πόλο τάξης 2. Αν πάλι $2a \notin L(\omega_1, \omega_2)$, τότε η συνάρτηση $\wp(z) - \wp(a)$ παρουσιάζει στα $a, -a$ πόλο τάξης 1 ή σημείο μηδενισμού πολλαπλότητας 1. Συνεπώς, για κάθε $z \notin L(\omega_1, \omega_2)$, η συνάρτηση

$$\prod_{i=1}^{r} (\wp(z) - \wp(u_i))^{m_i}$$

έχει την ίδια τάξη στο z με την f. Αν, λοιπόν, θεωρήσουμε τη συνάρτηση f δια το παραπάνω γινόμενο, προκύπτει μία ελλειπτική συνάρτηση χωρίς πόλους ή σημεία μηδενισμού, δηλαδή μία σταθερή συνάρτηση C. Επομένως, ισχύει

$$f(z) = C \prod_{i=1}^{r} (\wp(z) - \wp(u_i))^{m_i}$$

και άρα έχουμε τελειώσει. □

Στη συνέχεια της παρούσας ενότητας θα διατυπώσουμε και θα αποδείξουμε κάποιες επιπλέον προτάσεις σχετικά με τη συνάρτηση του Weierstrass. Ξεκινάμε με την παρακάτω πρόταση, που προσδιαρίζει πλήρως τη μορφή του αναπτύγματος Laurent της συνάρτησης $\wp$ γύρω από το $z = 0$.

Πρόταση 5.3.4 Έστω $r = min\{|\omega| : \omega \neq 0\}$. Τότε, αν $0 < |z| < r$,

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n}, \tag{5.3}$$

όπου G_n είναι η σειρά Eisenstein τάξης n,

$$G_n = \sum_{\omega\neq 0}\frac{1}{\omega^n}, \quad n \geq 3.$$

Απόδειξη. Όταν $|z| < r$, από τον ορισμό του r έχουμε $|z/\omega| < 1$ και άρα

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2(1-\frac{z}{\omega})^2} = \frac{1}{\omega^2}\left(\sum_{n=0}^{\infty}\left(\frac{z}{\omega}\right)^n\right)^2 = \frac{1}{\omega^2}\left(1 + \sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n\right).$$

Επομένως,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty}\frac{n+1}{\omega^{n+2}}z^n.$$

Αθροίζοντας το παραπάνω για όλα τα $\omega \in L(\omega_1, \omega_2)$ βρίσκουμε

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)\sum_{\omega\neq 0}\frac{1}{\omega^{n+2}}z^n = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}z^n.$$

Επειδή η συνάρτηση $\wp$ είναι άρτια, οι περιττοί συντελεστές G_{2n+1} εξαφανίζονται στο άθροισμα και έτσι παίρνουμε ακριβώς τη σχέση (5.3). □

Πρόταση 5.3.5 Η συνάρτηση $\wp$ ικανοποιεί τη διαφορική εξίσωση

$$(\wp'(z))^2 = 4\wp^3(z) - 60G_4\wp(z) - 140G_6. \tag{5.4}$$

Απόδειξη. Χρησιμοποιούμε το ανάπτυγμα Laurent της συνάρτησης $\wp$ που βρήκαμε στην προηγούμενη πρόταση και προσπαθούμε με κατάλληλες προσθαφαιρέσεις των $\wp$ και $\wp'$ να εξαλείψουμε τον πόλο που εμφανίζεται στη θέση $z = 0$. Έτσι θα προκύψει μία ελλειπτική συνάρτηση χωρίς πόλους και κατά συνέπεια σταθερή. Γύρω από το $z = 0$ έχουμε, από τη σχέση (5.3),

$$\wp'(z) = \frac{-2}{z^3} + 6G_4z + 20G_6z^3 + \ldots,$$

μία ελλειπτική συνάρτηση τάξης 3. Υψώνοντας στο τετράγωνο προκύπτει μία ελλειπτική συνάρτηση τάξης 6,

$$(\wp'(z))^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \ldots,$$

όπου το παραλειπόμενο κομμάτι είναι μία δυναμοσειρά που μηδενίζεται στο $z = 0$. Τώρα,

$$4\wp^3(z) = \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + \dots,$$

συνεπώς

$$(\wp'(z))^2 - 4\wp^3(z) = -\frac{60G_4}{z^2} - 140G_6 + \dots$$

και τελικά

$$(\wp'(z))^2 - 4\wp^3(z) + 60G_4\wp(z) = -140G_6 + \dots.$$

Το αριστερό μέλος της τελευταίας ισότητας είναι μία ελλειπτική συνάρτηση χωρίς πόλο στο σημείο $z = 0$, επομένως είναι σταθερή. Κατ'ανάγκη, λοιπόν, θα ισούται με $-140G_6$ και έτσι αποδείξαμε το ζητούμενο. □

Θέτουμε τώρα

$$g_2 = 60G_4, \qquad g_3 = 140G_6.$$

Η διαφορική εξίσωση (5.4) γράφεται, με βάση τα παραπάνω,

$$(\wp'(z))^2 = 4\wp^3(z) - g_2\wp(z) - g_3. \tag{5.5}$$

Καθώς μόνο τα g_2, g_3 εμφανίζονται ως συντελεστές στη διαφορική εξίσωση, θα πρέπει να καθορίζουν την $\wp$ πλήρως. Αυτό πράγματι συμβαίνει επειδή, όπως θα δούμε στην επόμενη πρόταση, όλοι οι συντελεστές $(2n+1)G_{2n+2}$ του αναπτύγματος Laurent της συνάρτησης $\wp$ γράφονται συναρτήσει των g_2, g_3.

Πρόταση 5.3.6 Κάθε σειρά Eisenstein γράφεται ως πολυώνυμο των g_2, g_3 με ρητούς συντελεστές. Μάλιστα, αν $b(n) = (2n+1)G_{2n+2}$, προκύπτουν οι αναδρομικές σχέσεις

$$b(1) = \frac{g_2}{20}, \qquad b(2) = \frac{g_3}{28}$$

και

$$(2n+3)(n-2)b(n) = 3\sum_{k=1}^{n-2} b(k)b(n-1-k), \quad n \geq 3,$$

ή, ισοδύναμα,

$$(2m+1)(m-3)(2m-1)G_{2m} = 3\sum_{r=2}^{m-2}(2r-1)(2m-2r-1)G_{2r}G_{2m-2r},$$

για $m \geq 4$.

Απόδειξη. Βλ.[4], σελ.12-13. □

Θα δείξουμε, τέλος, ότι το πολυώνυμο που προκύπτει από τη διαφορική εξίσωση (5.5),

$$4\wp^3(z) - g_2\wp(z) - g_3,$$

αναλύεται σε γινόμενο ανάγωγων πολυωνύμων. Δίνουμε πρώτα τον ακόλουθο ορισμό:

Ορισμός 5.3.7 Συμβολίζουμε με e_1, e_2, e_3 τις τιμές της συνάρτησης $\wp$ στις ημιπεριόδους,

$$e_1 = \wp\Big(\frac{\omega_1}{2}\Big), \quad e_2 = \wp\Big(\frac{\omega_2}{2}\Big), \quad e_3 = \wp\Big(\frac{\omega_1+\omega_2}{2}\Big).$$

Θεώρημα 5.3.8 Ισχύει ότι

$$4\wp^3(z) - g_2\wp(z) - g_3 = (\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3).$$

Επιπλέον, οι ρίζες e_1, e_2, e_3 του πολυωνύμου είναι διακεκριμένες, δηλαδή η διακρίνουσα του πολυωνύμου $\Delta = g_2^3 - 27g_3^2 \neq 0$.

Απόδειξη. Όπως έχουμε ήδη δει, η $\wp$ είναι μία άρτια συνάρτηση, άρα η $\wp'$ είναι περιττή. Ισχυριζόμαστε ότι οι ημιπερίοδοι μίας περιττής ελλειπτικής συνάρτησης αποτελούν είτε σημεία μηδενισμού είτε πόλους αυτής. Συγκεκριμένα, οι ημιπερίοδοι είναι σημεία μηδενισμού της $\wp'$. Πράγματι, λογω περιοδικότητας ισχύει

$$\wp'(-\omega/2) = \wp'(\omega - \omega/2) = \wp'(\omega/2).$$

Όμως η $\wp'$ είναι περιττή, επομένως $\wp'(-\omega/2) = -\wp'(\omega/2)$ και άρα $\wp'(\omega/2) = 0$. Αφού η $\wp'$ δεν παρουσιάζει πόλους στα $\omega_1/2, \omega_2/2, \omega_1+\omega_2/2$, αυτά θα πρέπει να είναι σημεία μηδενισμού της. Επίσης, η $\wp'$ έχει τάξη 3, άρα οι ημιπερίοδοι θα είναι απλές ρίζες της και η $\wp'$ δεν μπορεί να έχει άλλες ρίζες στο παραλληλόγραμμο με κορυφές $0, \omega_1, \omega_2, \omega_1+\omega_2$. Από τη διαφορική εξίσωση (5.5) προκύπτει ότι κάθε μία από τις τιμές $\omega_1/2, \omega_2/2, \omega_1+\omega_2/2$ είναι και ρίζα του πολυωνύμου, συνεπώς έχουμε την παραπάνω παραγοντοποίηση.

Απομένει να δείξουμε ότι οι ρίζες e_1, e_2, e_3 είναι διακεκριμένες. Η ελλειπτική συνάρτηση $\wp(z) - e_1$ μηδενίζεται για $z = \omega_1/2$. Επειδή και $\wp'(\omega_1/2) = 0$, το $\omega_1/2$ είναι διπλή ρίζα της συνάρτησης. Όμοια, η συνάρτηση $\wp(z) - e_2$ έχει διπλή ρίζα για $z = \omega_2/2$. Αν, λοιπόν, είχαμε ότι $e_1 = e_2$, τότε η συνάρτηση $\wp(z) - e_1$ θα είχε διπλή ρίζα τόσο στο $\omega_1/2$ όσο και στο $\omega_2/2$, δηλαδή η τάξη της θα ήταν ≥ 4, το οποίο είναι άτοπο, καθώς η τάξη της είναι 2. Επομένως, $e_1 \neq e_2$ και όμοια δείχνουμε ότι $e_1 \neq e_3, e_2 \neq e_3$. □

5.4 $\mathcal{J}-$ αναλλοίωτος και unimodular μετασχηματισμοί

Όπως είδαμε στο τελευταίο θεώρημα της προηγούμενης παραγράφου, ο αριθμός $\Delta = g_2^3 - 27g_3^2$ είναι η διακρίνουσα του πολυωνύμου $4\wp^3(z) - g_2\wp(z) - g_3$ και θα λέγεται *διακρίνουσα*. Μπορούμε να θεωρήσουμε τη διακρίνουσα ως συνάρτηση των περιόδων ω_1, ω_2, δηλαδή

$$\Delta(\omega_1, \omega_2) = g_2^3(\omega_1, \omega_2) - 27g_3^2(\omega_1, \omega_2).$$

Οι συναρτήσεις g_2, g_3 είναι ομογενείς βαθμού -4 και -6 αντίστοιχα, δηλαδή για κάθε $\lambda \neq 0$ ισχύουν

$$g_2(\lambda\omega_1, \lambda\omega_2) = \lambda^{-4} g_2(\omega_1, \omega_2) \quad \text{και} \quad g_3(\lambda\omega_1, \lambda\omega_2) = \lambda^{-6} g_3(\omega_1, \omega_2).$$

Εύκολα συμπεραίνουμε ότι η διακρίνουσα είναι ομογενής συνάρτηση βαθμού -12, δηλαδή

$$\Delta(\lambda\omega_1, \lambda\omega_2) = \lambda^{-12}\Delta(\omega_1, \omega_2) \quad \forall \lambda \neq 0.$$

Αν επιλέξουμε ως λ τον αριθμό $1/\omega_1$ και θέσουμε $\tau = \omega_2/\omega_1$ παίρνουμε τις σχέσεις

$$g_2(1, \tau) = \omega_1^4 g_2(\omega_1, \omega_2), \quad g_3(1, \tau) = \omega_1^6 g_3(\omega_1, \omega_2), \quad \Delta(1, \tau) = \omega_1^{12}\Delta(\omega_1, \omega_2).$$

Με αυτό τον τρόπο, μπορούμε να θεωρήσουμε τις g_2, g_3 και Δ ως συναρτήσεις μίας μόνο μιγαδικής μεταβλητής, της τ. Μπορούμε, μάλιστα, χωρίς βλάβη της γενικότητας να θεωρήσουμε ότι $Im(\tau) = Im(\omega_2/\omega_1) > 0$, και άρα να μελετήσουμε αυτές τις συναρτήσεις στο άνω μιγαδικό ημιεπίπεδο, δηλαδή στο

$$\mathcal{H} := \{z \in \mathbb{C} \mid Im(z) > 0\}.$$

Για $\tau \in \mathcal{H}$, θα γράφουμε $g_2(\tau), g_3(\tau)$ και $\Delta(\tau)$ αντί για $g_2(1, \tau), g_3(1, \tau)$ και $\Delta(1, \tau)$ αντίστοιχα. Έτσι, οι συναρτήσεις μας παίρνουν τη μορφή

$$g_2(\tau) = 60 \cdot \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4},$$

$$g_3(\tau) = 140 \cdot \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^6}$$

και

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau).$$

Από το Θεώρημα 5.3.8 έπεται ότι $\Delta(\tau) \neq 0$ για κάθε $\tau \in \mathcal{H}$.

Ορισμός 5.4.1 Αν ο λόγος ω_2/ω_1 είναι μη-πραγματικός, τότε ορίζουμε τη συνάρτηση

$$\mathcal{J}(\omega_1, \omega_2) = 12^3 \cdot \frac{g_2^3(\omega_1, \omega_2)}{\Delta(\omega_1, \omega_2)}.$$

Η συνάρτηση $\mathcal{J}$ ονομάζεται $\mathcal{J}-$αναλλοίωτος του Klein ή πιο απλά $\mathcal{J}-$αναλλοίωτος.

Εξ ορισμού, η $\mathcal{J}-$αναλλοίωτος είναι ομογενής συνάρτηση βαθμού 0. Ισχύει, δηλαδή, ότι

$$\mathcal{J}(\lambda\omega_1, \lambda\omega_2) = \mathcal{J}(\omega_1, \omega_2) \quad \forall \lambda \in \mathbb{C}.$$

Συγκεκριμένα, αν $\tau = \omega_2/\omega_1 \in \mathcal{H}$, τότε

$$\mathcal{J}(1, \tau) = \mathcal{J}(\omega_1, \omega_2).$$

Θα γράφουμε $\mathcal{J}(\tau)$ αντί για $\mathcal{J}(1, \tau)$.

Θεώρημα 5.4.2 Οι συναρτήσεις $g_2(\tau), g_3(\tau), \Delta(\tau)$ και $\mathcal{J}(\tau)$ είναι αναλυτικές στο $\mathcal{H}$.

Απόδειξη. Είδαμε παραπάνω ότι $\Delta(\tau) \neq 0$ για κάθε $\tau \in \mathcal{H}$. Επομένως, αρκεί να δείξουμε ότι οι g_2 και g_3 είναι αναλυτικές στο $\mathcal{H}$. Τότε και η $\mathcal{J}$ θα είναι αναλυτική συνάρτηση εξ ορισμού.

Οι συναρτήσεις g_2 και g_3 ορίζονται μέσω σειρών της μορφής

$$\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^a},$$

για κάποιο $a > 2$. Έστω $\tau = x + iy$, με $y > 0$. Θα δείξουμε ότι για $a > 2$ η σειρά συγκλίνει απόλυτα για κάθε $\tau \in \mathcal{H}$ και ομοιόμορφα σε κάθε λωρίδα S της μορφής

$$S = \{x + iy \in \mathbb{C} \ : \ |x| \leq A, y \geq \delta > 0\}.$$

Προς τούτο, θα δείξουμε ότι υπάρχει σταθερά $M > 0$ που εξαρτάται μόνο από τα A και δ, τέτοια ώστε

$$\frac{1}{|m+n\tau|^a} \leq \frac{M}{|m+in|^a}$$

για κάθε $\tau \in S$, $(m, n) \neq (0, 0)$ και έτσι θα έχουμε άμεσα το ζητούμενο από το Λήμμα 5.2.1. Αρκεί, λοιπόν, να δείξουμε ότι

$$|m + n\tau|^2 > K|m + ni|^2,$$

όπου $K > 0$ μία σταθερά που εξαρτάται μόνο από τα A, δ.

Προκύπτει ισοδύναμα η ανισότητα

$$(m + nx)^2 + (ny)^2 > K(m^2 + n^2). \tag{5.6}$$

Αν $n = 0$, η παραπάνω ανισότητα ισχύει για κάθε K στο διάστημα $(0, 1)$. Υποθέτουμε ότι $n \neq 0$. Τότε, αν θέσουμε $q = m/n$ στην (5.6) έχουμε

$$\frac{(q + x)^2 + y^2}{1 + q^2} > K, \quad K > 0. \tag{5.7}$$

Θα δείξουμε ότι η (5.7) είναι αληθής για κάθε q επιλέγοντας ως K τον αριθμό

$$K = \frac{\delta^2}{1 + (A + \delta)^2} > 0,$$

για $|x| \leq A, |y| \geq \delta$. Διακρίνουμε τις ακόλουθες περιπτώσεις:

- Αν $|q| \leq A + \delta$, τότε $(q + x)^2 \geq 0$ και $y^2 \geq \delta^2$. Επομένως, προφανώς ισχύει ότι

$$\frac{(q + x)^2 + y^2}{1 + q^2} \geq \frac{y^2}{1 + q^2} \geq \frac{\delta^2}{1 + (A + \delta)^2} = K.$$

- Αν $|q| > A + \delta$, τότε ισχύει

$$\left|\frac{x}{q}\right| < \frac{|x|}{A + \delta} \leq \frac{A}{A + \delta} < 1,$$

επομένως

$$\left|1 + \frac{x}{q}\right| \geq 1 - \left|\frac{x}{q}\right| \geq 1 - \frac{A}{A + \delta} = \frac{\delta}{A + \delta} \Rightarrow |q + x| \geq \frac{q\delta}{A + \delta}.$$

Συνεπώς, έχουμε ότι

$$\frac{(q + x)^2 + y^2}{1 + q^2} > \frac{\delta^2}{(A + \delta)^2} \cdot \frac{q^2}{1 + q^2}. \tag{5.8}$$

Όμως, η συνάρτηση $q^2/1 + q^2$ είναι αύξουσα συνάρτηση του q. Με άλλα λόγια, ισχύει

$$|q| > A + \delta \Rightarrow \frac{q^2}{1 + q^2} \geq \frac{(A + \delta)^2}{1 + (A + \delta)^2}.$$

Με βάση την παραπάνω ανισότητα, η (5.8) γίνεται

$$\frac{(q + x)^2 + y^2}{1 + q^2} \geq \frac{\delta^2}{(A + \delta)^2} \cdot \frac{(A + \delta)^2}{1 + (A + \delta)^2} = \frac{\delta^2}{1 + (A + \delta)^2} = K.$$

Δείξαμε, επομένως, ότι ισχύει η (5.7) και άρα έχουμε τελειώσει. □

Εισάγουμε τώρα δύο νέες περιόδους ω_1', ω_2', οι οποίες ικανοποιούν τις σχέσεις

$$\omega_2' = a\omega_2 + b\omega_1, \quad \omega_1' = c\omega_2 + d\omega_1,$$

όπου $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$. Αυτό σημαίνει ότι τα ζεύγη (ω_1, ω_2) και (ω_1', ω_2') είναι ισοδύναμα, δηλαδή τα δικτυωτά τους ταυτίζονται, $L(\omega_1, \omega_2) = L(\omega_1', \omega_2')$. Επομένως, 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 $\tau = \omega_2/\omega_1$. Ένας εύκολος υπολογισμός μας δίνει τη σχέση

$$Im(\tau') = \frac{Im(\tau)}{|c\tau + d|^2},$$

συνεπώς ο λόγος τ' ανήκει στο $\mathcal{H}$ αν και μόνο αν ο λόγος τ ανήκει στο $\mathcal{H}$.

Ορισμός 5.4.3 Η σχέση

$$\tau' = \frac{a\tau + b}{c\tau + d}$$

λέγεται *unimodular μετασχηματισμός* αν ισχύουν $a, b, c, d \in \mathbb{Z}$ και $ad - bc = 1$.

Το σύνολο των unimodular μετασχηματισμών αποτελεί ομάδα (με πράξη τη σύνθεση) και ονομάζεται *modular ομάδα*. Θα ασχοληθούμε περαιτέρω με την ομάδα αυτή σε επόμενη παράγραφο.

Από τις παραπάνω παρατηρήσεις μας μπορούμε να συμπεράνουμε ότι η συνάρτηση $\mathcal{J}(\tau)$ παραμένει αναλλοίωτη υπό τη δράση της modular ομάδας. Συγκεκριμένα, ισχύει το ακόλουθο:

Θεώρημα 5.4.4 Αν $\tau \in \mathcal{H}$ και $a, b, c, d \in \mathbb{Z}$ για τους οποίους ισχύει ότι $ad - bc = 1$, τότε

$$\frac{a\tau + b}{c\tau + d} \in \mathcal{H}$$

και, επιπλέον,

$$\mathcal{J}\left(\frac{a\tau + b}{c\tau + d}\right) = \mathcal{J}(\tau).$$

Παρατήρηση 5.4.5 Αν, συγκεκριμένα, επιλέξουμε $c = 0, a = b = d = 1$, τότε από το παραπάνω θεώρημα προκύπτει ότι

$$\mathcal{J}(\tau + 1) = \mathcal{J}(\tau),$$

δηλαδή η $\mathcal{J}-$αναλλοίωτος του Klein είναι περιοδική συνάρτηση με περίοδο 1.

5.5 Τα αναπτύγματα Fourier των g_2, g_3, Δ και $\mathcal{J}$.

Κάθε σειρά Eisenstein

$$\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^k}$$

είναι περιοδική συνάρτηση του τ με περίοδο 1. Ειδικότερα, οι συναρτήσεις g_2, g_3 είναι περιοδικές με περίοδο 1. Θα προσδιορίσουμε πλήρως τα αναπτύγματα Fourier των συναρτήσεων αυτών.

Υπενθυμίζουμε ότι

$$g_2(\tau) = 60 \cdot \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4}, \quad g_3(\tau) = 140 \cdot \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^6}.$$

Θα υπολογίσουμε πρώτα τα αναπτύγματα Fourier των απλούστερων σειρών,

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^4} \quad \text{και} \quad \sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^6}.$$

Λήμμα 5.5.1 Αν $\tau \in \mathcal{H}$ και $n > 0$, τότε

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^4} = \frac{8\pi^4}{3} \sum_{r=1}^{+\infty} r^3 e^{2\pi i r n \tau}$$

και

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^6} = -\frac{8\pi^6}{15} \sum_{r=1}^{+\infty} r^5 e^{2\pi i r n \tau}.$$

Απόδειξη. Βλ.[4], σελ.19. □

Πρόταση 5.5.2 Αν $\tau \in \mathcal{H}$, λαμβάνουμε τα αναπτύγματα Fourier

$$g_2(\tau) = \frac{4\pi^4}{3}\left(1 + 240\sum_{k=1}^{+\infty}\sigma_3(k)e^{2\pi ik\tau}\right)$$

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. Έχουμε:

$$g_2(\tau) = 60 \cdot \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4} =$$

$$= 60\Bigg(\sum_{\substack{m=-\infty\\m\neq 0}}^{+\infty}\frac{1}{m^4} + \sum_{n=1}^{+\infty}\sum_{m=-\infty}^{+\infty}\Big(\frac{1}{(m+n\tau)^4} + \frac{1}{(m-n\tau)^4}\Big)\Bigg) =$$

$$= 60\left(2\zeta(4) + 2\sum_{n=1}^{+\infty}\sum_{m=-\infty}^{+\infty}\frac{1}{(m+n\tau)^4}\right) = 60\left(\frac{2\pi^4}{90} + \frac{16\pi^4}{3}\sum_{m=1}^{+\infty}\sum_{n=1}^{+\infty} r^3 q^{nr}\right),$$

όπου $q = e^{2\pi i\tau}$. Συγκεντρώνουμε μαζί όλους τους όρους του τελευταίου διπλού αθροίσματος για τους οποίους το γινόμενο nr είναι σταθερό και έχουμε το ανάπτυγμα Fourier της $g_2(\tau)$. Με όμοια διαδικασία βρίσκουμε το ανάπτυγμα της $g_3(\tau)$. □

Πρόταση 5.5.3 Αν $\tau \in \mathcal{H}$, τότε ισχύει

$$\Delta(\tau) = (2\pi)^{12}\sum_{n=1}^{+\infty}\tau(n)e^{2\pi in\tau},$$

όπου $\tau(n) \in \mathbb{Z}$, με $\tau(1) = 1$ και $\tau(2) = -24$.[2]

Απόδειξη. Θέτουμε

$$q := e^{2\pi i\tau}, \quad A := \sum_{n=1}^{+\infty}\sigma_3(n)q^n, \quad B := \sum_{n=1}^{+\infty}\sigma_5(n)q^n.$$

[2]Η συνάρτηση $\tau(n)$ ονομάζεται τ συνάρτηση του Ramanujan.

Τότε έχουμε

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau) = \frac{64\pi^{12}}{27}\Big((1+240A)^3 - (1-504B)^2\Big).$$

Τώρα, 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

$$5A + 7B = \sum_{n=1}^{+\infty}(5\sigma_3(n) + 7\sigma_5(n))q^n$$

και

$$5d^3 + 7d^5 = d^3(5+7d^2) \equiv \begin{cases} d^3(d^2-1) \equiv 0(mod 3) \\ d^3(1-d^2) \equiv 0(mod 4). \end{cases}$$

Αυτό σημαίνει ότι $12 \mid 5A+7B$, συνεπώς από την παραπάνω σχέση έχουμε ότι το 12^3 διαιρεί κάθε συντελεστή της δυναμοσειράς του $(1+240A)^3-(1-504B)^2$. Έτσι προκύπτει

$$\Delta(\tau) = \frac{64\pi^{12}}{27}\left(12^3\sum_{n=1}^{+\infty}\tau(n)e^{2\pi in\tau}\right) = (2\pi)^{12}\sum_{n=1}^{+\infty}\tau(n)e^{2\pi in\tau},$$

όπου $\tau(n) \in \mathbb{Z}$ για κάθε $n \in \mathbb{N}$. Ο συντελεστής του $q = e^{2\pi i\tau}$ είναι $12^2(5+7) = 12^3$, δηλαδή $\tau(1) = 1$. Όμοια υπολογίζουμε $\tau(2) = -24$. □

Πρόταση 5.5.4 Αν $\tau \in \mathcal{H}$, τότε ισχύει

$$\mathcal{J}(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{+\infty} c(n)e^{2\pi in\tau},$$

όπου $c(n) \in \mathbb{Z}$ για κάθε $n \in \mathbb{N}$.

Απόδειξη. Θα συμβολίζουμε με I κάθε δυναμοσειρά του q με ακέραιους συντελεστές. Αν, λοιπόν, $q = e^{2\pi i\tau}$, έχουμε

$$g_2^3(\tau) = \frac{64\pi^{12}}{27}(1+240q+I)^3 = \frac{64\pi^{12}}{27}(1+720q+I)$$

και

$$\Delta(\tau) = \frac{64\pi^{12}}{27}(12^3q(1-24q+I)).$$

Επομένως,

$$\mathcal{J}(\tau) = \frac{g_2^3(\tau)}{\Delta(\tau)} = \frac{1+720q+I}{12^3q(1-24q+I)} = \frac{1}{12^3q}(1+720q+I)(1+24q+I),$$

και άρα έχουμε

$$\mathcal{J}(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{+\infty} c(n)q^n,$$

όπου $c(n) \in \mathbb{Z}$. Έτσι, το ζητούμενο αποδείχθηκε. □

5.6 Modular Συναρτήσεις

Σε αυτή την ενότητα θα εμβαθύνουμε στους unimodular μετασχηματισμούς και θα τους χρησιμοποιήσουμε για να μελετήσουμε τη modular ομάδα.

Θεωρούμε τον γενικότερο μετασχηματισμό

$$f(z) = \frac{az+b}{cz+d}, \quad a, b, c, d \in \mathbb{C}.$$

Η παραπάνω συνάρτηση ορίζεται για κάθε $z \in \mathbb{C}^* = \mathbb{C} \cup \{\infty\}$ εκτός από τα σημεία $z = -d/c$ και $z = \infty$. Θέτουμε, λοιπόν,

$$f\left(\frac{-d}{c}\right) = \infty, \quad f(\infty) = \frac{a}{c}.$$

Με αυτό τον τρόπο, έχουμε τώρα ορίσει τη συνάρτηση f σε ολόκληρο το σύνολο $\mathbb{C} \cup \{\infty\}$.

Παρατηρούμε, ακόμη, ότι

$$f(z) - f(w) = \frac{(ad-bc)(w-z)}{(cw+d)(cz+d)}. \tag{5.9}$$

Αυτό σημαίνει ότι η f είναι σταθερή συνάρτηση αν ισχύει $ad - bc = 0$. Για να αποφύγουμε, συνεπώς, τέτοιες εκφυλισμένες περιπτώσεις, θα υποθέτουμε πάντα ότι $ad - bc \neq 0$.

Η ρητή συνάρτηση που προκύπτει λέγεται *μετασχηματισμός Möbius*. Η συνάρτηση f είναι αναλυτική παντού στο $\mathbb{C}^*$, εκτός από το σημείο $z = -d/c$, όπου παρουσιάζει πόλο τάξης 1. Γνωρίζουμε από τη Μιγαδική Ανάλυση ότι οι μετασχηματισμοί Möbius απεικονίζουν κύκλους σε κύκλους (θεωρώντας την ευθεία ως εκφυλισμένο κύκλο). Εύκολα βλέπουμε ότι αν πολλαπλασιάσουμε κάθε έναν από τους αριθμούς a, b, c, d με την ίδια μη μηδενική σταθερά, τότε η f παραμένει αμετάβλητη. Συνεπώς, μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι $ad - bc = 1$. Με αυτό τον τρόπο, μπορούμε να ταυτίσουμε κάθε τέτοιο μετασχηματισμό με έναν 2×2 πίνακα

$$A = A_f = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{C}).$$

Η σύνθεση $f \circ g$ δύο μετασχηματισμών Möbius f και g είναι μετασχηματισμός Möbius, με αντίστοιχο πίνακα τον $A_f A_g$. Ο ταυτοτικός πίνακας I_2 αντιστοιχεί στον ταυτοτικό μετασχηματισμό Möbius $id(z) = z$. Τέλος, αν $f(z)$ ένας μετασχηματισμός Möbius με πίνακα

$$A_f = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

τότε η αντίστροφη απεικόνιση f^{-1} είναι επίσης μετασχηματισμός Möbius και ο αντίστοιχος πίνακας είναι ο

$$A_{f^{-1}} = (A_f)^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Από τα παραπάνω αποτελέσματα συμπεραίνουμε ότι το σύνολο των πινάκων που αντιστοιχούν σε κάποιο μετασχηματισμό Möbius αποτελεί ομάδα με πράξη τον πολλαπλασιασμό πινάκων. Κατά συνέπεια, οι μετασχηματισμοί Möbius αποτελούν ομάδα με πράξη τη σύνθεση.

Εμείς θα ασχοληθούμε με μία υποομάδα αυτής για την οποία ισχύει η επιπλέον συνθήκη ότι οι συντελεστές a, b, c, d είναι ακέραιοι αριθμοί, δηλαδή με την υποομάδα των unimodular μετασχηματισμών.

Ορισμός 5.5.1 Το σύνολο

$$\Gamma := \left\{ \frac{a\tau + b}{c\tau + d} \;\middle|\; \tau \in \mathcal{H},\ a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

αποτελεί ομάδα με πράξη τη σύνθεση απεικονίσεων και λέγεται *modular ομάδα.*

Η Γ είναι ισόμορφη, σύμφωνα και με τα παραπάνω, με την $SL_2(\mathbb{Z})$. Έτσι, η Γ μπορεί να παρασταθεί από 2×2 ακέραιους πίνακες ορίζουσας 1, με την προϋπόθεση ότι ταυτίζουμε τους πίνακες A και $-A$, καθώς αντιπροσωπεύουν τον ίδιο μετασχηματισμό. Επίσης, αν

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

γράφουμε

$$A\tau = \frac{a\tau + b}{c\tau + d}, \quad \tau \in \mathcal{H}.$$

Με άλλα λόγια, ταυτίζουμε τον πίνακα με τον αντίστοιχο unimodular μετασχηματισμό.

Το ακόλουθο θεώρημα προσδιορίζει πλήρως τους γεννήτορες της ομάδας Γ.

Θεώρημα 5.5.2 Ισχύει ότι

$$\Gamma =< T\tau, S\tau >,$$

όπου

$$T\tau = \tau + 1, \quad S\tau = -\frac{1}{\tau}.$$

Απόδειξη. Παρατηρούμε ότι

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{και} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Επομένως, η απόδειξη της παραπάνω σχέσης ανάγεται στην απόδειξη της

$$SL_2(\mathbb{Z}) =< T, S >,$$

την οποία έχουμε ήδη αποδείξει στο Θεώρημα 1.2.3. □

Θεωρούμε τώρα G μία υποομάδα της Γ. Δύο σημεία $\tau, \tau' \in \mathcal{H}$ λέγονται *ισοδύναμα* αν υπάρχει πίνακας $A \in G$ τέτοιος ώστε $\tau' = A\tau$. Εύκολα διαπιστώνουμε ότι η σχέση αυτή είναι σχέση ισοδυναμίας. Επομένως, το άνω ημιεπίπεδο $\mathcal{H}$ γράφεται ως ξένη ένωση κλάσεων ισοδυναμίας, τις οποίες θα ονομάζουμε *τροχιές*. Κάθε τροχιά είναι της μορφής $G\tau$, δηλαδή περιέχει μιγαδικούς αριθμούς της μορφής $A\tau$ για κάποιο πίνακα $A \in G$.

Επιλέγουμε τώρα ένα σημείο από κάθε τροχιά. Η ένωση των σημείων αυτών λέγεται *θεμελιώδες σύνολο* της G. Επειδή θα επιθυμούσαμε το σύνολο αυτό να έχει κάποιες καλές τοπολογικές ιδιότητες, τροποποιούμε ελάχιστα την έννοια του θεμελιώδους συνόλου και δίνουμε τον ακόλουθο ορισμό.

Ορισμός 5.5.3 Έστω G υποομάδα της modular ομάδας Γ. Ένα ανοικτό υποσύνολο R_G του $\mathcal{H}$ θα λέγεται *θεμελιώδης περιοχή* της G αν έχει τις εξής ιδιότητες:

1. Αν δύο σημεία της R_G είναι ισοδύναμα, τότε κατ'ανάγκη ταυτίζονται.
2. Αν $\tau \in \mathcal{H}$, τότε υπάρχει σημείο τ' στην κλειστότητα της R_G τέτοιο ώστε τα τ και τ' να είναι ισοδύναμα.

Παρακάτω θα προσδιορίσουμε τη θεμελιώδη περιοχή R_Γ. Θα δώσουμε πρώτα τα ακόλουθα λήμματα:

Λήμμα 5.5.4 Αν $\omega_1', \omega_2' \in \mathbb{C}$, με μη-πραγματικό λόγο, τότε υπάρχει πάντα ένα θεμελιώδες ζεύγος περιόδων (ω_1, ω_2) ισοδύναμο προς το (ω_1', ω_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 ισχύουν οι σχέσεις $|\omega_2| \geq |\omega_1|$, $|\omega_1 + \omega_2| \geq |\omega_2|$ και $|\omega_1 - \omega_2| \geq |\omega_2|$.

Απόδειξη. Βλ.[4], σελ.31-32. □

Λήμμα 5.5.5 Αν $\tau' \in \mathcal{H}$, τότε υπάρχει μιγαδικός αριθμός $\tau \in \mathcal{H}$ ισοδύναμος προς τον τ' τέτοιος ώστε $|\tau| \geq 1$, $|\tau + 1| \geq |\tau|$ και $|\tau - 1| \geq |\tau|$.

Απόδειξη. Βλ.[4], σελ.32. □

Θεώρημα 5.5.6 Το ανοικτό σύνολο

$$R_\Gamma = \{\tau \in \mathcal{H} : |\tau| > 1, |\tau + \bar{\tau}| < 1\}$$

είναι μία θεμελιώδης περιοχή της ομάδας Γ. Επιπλέον, αν $A \in \Gamma$ και $A\tau = \tau$ για κάποιο $\tau \in R_\Gamma$, τότε κατ'ανάγκη θα ισχύει $A = I_2$. Ισοδύναμα, μόνο το ταυτοτικό στοιχείο της Γ αφήνει αναλλοίωτα τα στοιχεία της R_Γ.

Απόδειξη. Από το Λήμμα 5.5.5 γνωρίζουμε ότι για το τυχαίο $\tau' \in \mathcal{H}$ υπάρχει τ στην κλειστότητα της R_Γ ισοδύναμο προς το τ' κάτω από τη δράση της ομάδας Γ. Αρκεί να δείξουμε, συνεπώς, ότι δύο διαφορετικά σημεία της R_Γ δε γίνεται να είναι ισοδύναμα υπό τη δράση της Γ.

Υποθέτουμε, λοιπόν, ότι $\tau' = A\tau$, όπου

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Από απλές πράξεις προκύπτει ότι

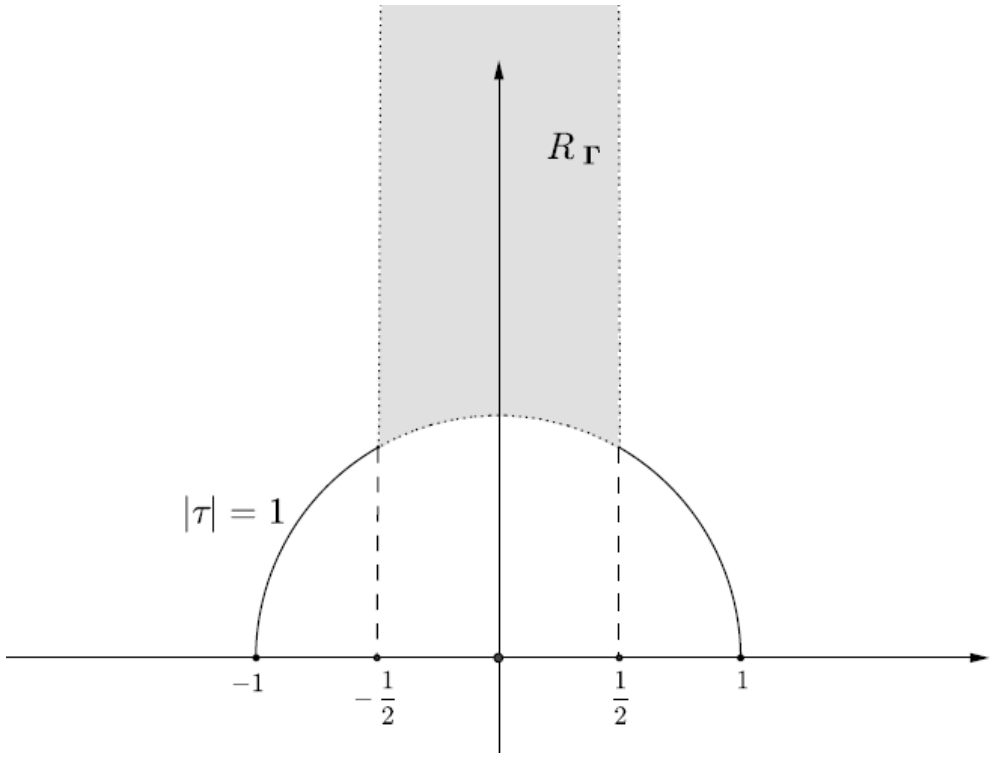
$$Im(\tau') = \frac{Im(\tau)}{|c\tau + d|^2}.$$

Αν υποθέσουμε ότι $\tau \in R_\Gamma$ και $c \neq 0$ έχουμε ότι

$$|c\tau + d|^2 = (c\tau + d)(c\bar{\tau} + d) = c^2\tau\bar{\tau} + cd(\tau + \bar{\tau}) + d^2 > c^2 - |cd| + d^2.$$

Αν $d = 0$, τότε $|c\tau + d|^2 > c^2 \geq 1$. Αν, πάλι, $d \neq 0$, τότε

$$c^2 - |cd| + d^2 = (|c| - |d|)^2 + |cd| \geq |cd| \geq 1.$$



Σχήμα 5.3: Η θεμελιώδης περιοχή R_Γ.

Σε κάθε περίπτωση, έχουμε ότι $|c\tau + d|^2 > 1$. Αυτό σημαίνει ότι αν $\tau \in R_\Gamma$ και $c \neq 0$, τότε ισχύει $Im(\tau') < Im(\tau)$. Με άλλα λόγια, κάθε στοιχείο $A \in \Gamma$ με $c \neq 0$ μειώνει το φανταστικό μέρος του $\tau \in R_\Gamma$.

Ας υποθέσουμε τώρα ότι τα τ και τ' είναι ισοδύναμα σημεία στο εσωτερικό της R_Γ. Τότε ισχύουν

$$\tau' = \frac{a\tau + b}{c\tau + d} \quad \text{και} \quad \tau = \frac{d\tau' - b}{-c\tau' + a}.$$

Αν $c \neq 0$, τότε η πρώτη σχέση μας δίνει ότι $Im(\tau') < Im(\tau)$, ενώ η δεύτερη μας πληροφορεί ότι $Im(\tau) < Im(\tau')$. Επομένως, ισχύει $c = 0$. Τότε όμως προκύπτει ότι $ad = 1$, δηλαδή $a = d = \pm 1$, και άρα

$$A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = T^b \quad \text{ή} \quad A = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} = T^{-b}.$$

Τότε $\tau' = \tau \pm b$. Επειδή έχουμε υποθέσει ότι $\tau, \tau' \in R_\Gamma$, από την ανισότητα $|\tau + \bar{\tau}| < 1$ λαμβάνουμε ότι η οριζόντια απόσταση δύο σημείων της R_Γ είναι μικρότερη του 1. Τότε όμως

$$\tau' = \tau \pm b \Rightarrow Re(\tau') = Re(\tau) \pm b \Rightarrow |b| = |Re(\tau') - Re(\tau)| < 1 \Rightarrow b = 0.$$

Επομένως, $\tau = \tau'$ και άρα δείξαμε ότι δύο διακεκριμένα σημεία της R_Γ δεν είναι δυνατό να είναι ισοδύναμα.

Χρησιμοποιώντας, τέλος, το ίδιο επιχείρημα, συμπεραίνουμε ότι αν υποθέσουμε τη σχέση $A\tau = \tau$ για κάποιο $\tau \in R_\Gamma$, όπου

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

τότε $c = 0$ και $a = d = \pm 1$, επομένως $A = \pm I_2$. Δείξαμε, έτσι, ότι μόνο ο ταυτοτικός μετασχηματισμός διατηρεί σταθερά τα σημεία της R_Γ. □

Η θεμελιώδης περιοχή R_Γ απεικονίζεται στο Σχήμα 5.3. Να παρατηρήσουμε εδώ ότι εξ ορισμού η θεμελιώδης περιοχή είναι ανοικτό σύνολο, επομένως το σύνορο δεν περιέχεται σε αυτή. Αυτός είναι και ο λόγος που το σύνορο στο σχήμα απεικονίζεται με διακεκομμένη γραμμή.

Θα ορίσουμε, τώρα, την έννοια των modular συναρτήσεων.

Ορισμός 5.5.7 Μία μιγαδική συνάρτηση f ονομάζεται *modular* αν ικανοποιεί τις παρακάτω συνθήκες:

1. Η f είναι μερόμορφη στο $\mathcal{H}$.
2. Ισχύει $f(A\tau) = f(\tau)$ για κάθε $A \in SL_2(\mathbb{Z})$.
3. Το ανάπτυγμα Fourier της f γύρω από το 0 είναι της μορφής

$$f(\tau) = \sum_{k=-m}^{+\infty} a(k) e^{2\pi i k \tau}.$$

Η πρώτη ιδιότητα μας δείχνει ότι οι modular συναρτήσεις είναι αναλυτικές στο $\mathcal{H}$, εκτός από πιθανούς πόλους. Από τη δεύτερη ιδιότητα συνεπάγεται ότι οι modular συναρτήσεις παραμένουν αναλλοίωτες υπό τη δράση των μετασχηματισμών της ομάδας Γ. Τέλος, η μορφή της σειράς Fourier μας δίνει πληροφορίες για το σημείο $\tau = i\infty$. Αν θέσουμε $x := e^{2\pi i \tau}$, τότε λαμβάνουμε το ανάπτυγμα Laurent της f ως προς το x. Η συμπεριφορά της f στο $i\infty$ περιγράφεται από τη μελέτη του αναπτύγματος Laurent γύρω από το 0: Αν $m > 0$ και $a(-m) \neq 0$, τότε η f παρουσιάζει πόλο τάξης m στο $i\infty$. Αν πάλι $m \leq 0$, τότε η f είναι αναλυτική στο $i\infty$. Η ιδιότητα 3 του ορισμού, συνεπώς, μας εξασφαλίζει ότι στη χειρότερη περίπτωση η f εμφανίζει πόλο τάξης m για $\tau = i\infty$.

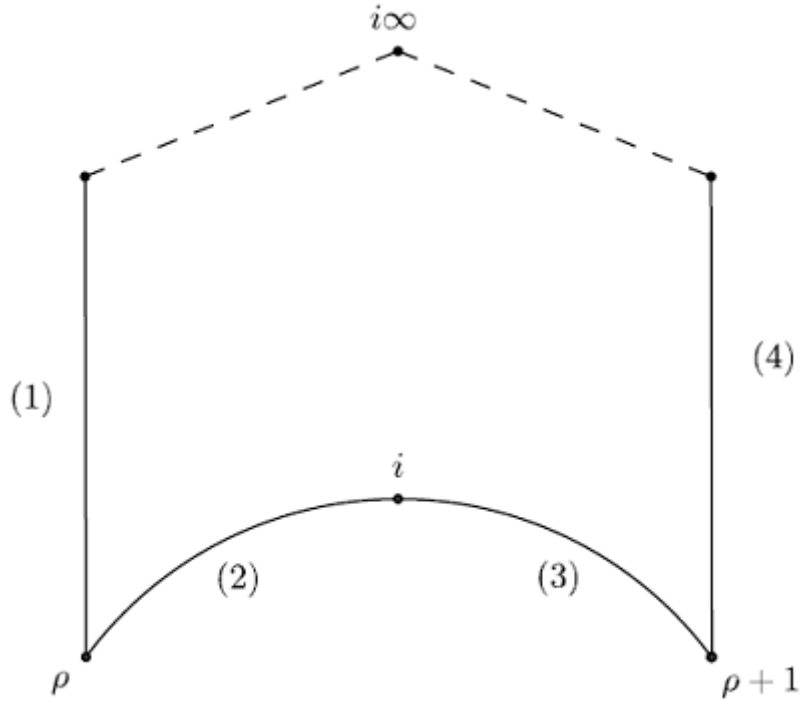
Είναι εύκολο να δούμε ότι η $\mathcal{J}-$αναλλοίωτος είναι μία modular συνάρτηση. Πράγματι, εξ ορισμού η $\mathcal{J}$ είναι αναλυτική στο $\mathcal{H}$, με μοναδικό πόλο τάξης 1 στο $i\infty$, και παραμένει αναλλοίωτη υπό τη δράση της ομάδας Γ.

Θα δείξουμε παρακάτω ότι κάθε modular συνάρτηση εκφράζεται ως ρητή συνάρτηση της $\mathcal{J}$. Η απόδειξη αυτού βασίζεται στην ακόλουθη ιδιότητα των modular συναρτήσεων.

Θεώρημα 5.5.8 Αν f μία μη-μηδενική modular συνάρτηση, τότε στην κλειστότητα της θεμελιώδους περιοχής R_Γ το πλήθος των σημείων μηδενισμού της f ισούται με το πλήθος των πόλων της.

Απόδειξη. Βλ.[4],σελ.34-39. □

Παρατήρηση 5.5.9 Για να ισχύει το παραπάνω θεώρημα θα πρέπει να κάνουμε κάποιες συμβάσεις για το σύνορο της θεμελιώδους περιοχής. Καταρχάς, θεωρούμε ότι το σύνορο της R_Γ αποτελείται από τέσσερις πλευρές που τέμνονται στα σημεία $\rho := e^{2\pi i/3}, i, \rho+1$ και $i\infty$. Οι τέσσερις αυτές πλευρές χωρίζονται στα ισοδύναμα ζεύγη (1),(4) και (2),(3), όπως φαίνεται στο Σχήμα 5.4. Έτσι, αν η f εμφανίζει σημείο μηδενισμού ή πόλο σε κάποια από τις πλευρές του συνόρου, τότε και το ισοδύναμο αυτού θα είναι σημείο μηδενισμού ή πόλος.



Σχήμα 5.4

Πόρισμα 5.5.10 Αν 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 της R_Γ.

Πόρισμα 5.5.11 Αν η f είναι μία modular και φραγμένη συνάρτηση στο $\mathcal{H}$, τότε είναι σταθερή.

Η παρακάτω πρόταση μας δίνει την τιμή της συνάρτησης $\mathcal{J}$ σε κάποια συγκεκριμένα, ειδικά σημεία.

Πρόταση 5.5.12 Η $\mathcal{J}-$αναλλοίωτος λαμβάνει κάθε τιμή ακριβώς μία φορά στην κλειστότητα της θεμελιώδους περιοχής R_Γ. Ιδιαίτερα, για τις κορυφές ισχύουν:

$$\mathcal{J}(\rho) = 0, \quad \mathcal{J}(i) = 1728, \quad \mathcal{J}(i\infty) = \infty,$$

όπου $\rho := e^{2\pi i/3}$. Στο σημείο $i\infty$ έχουμε πόλο τάξης 1, στο ρ σημείο μηδενισμού τάξης 3, και η συνάρτηση $\mathcal{J}(\tau) - 1728$ έχει διπλό σημείο μηδενισμού το $\tau = i$.

Απόδειξη. Αρχικά θα δείξουμε ότι η $\mathcal{J}$ λαμβάνει όλες τις τιμές ακριβώς μία φορά στην κλειστότητα της R_Γ, δηλαδή ότι για κάθε $z \in \mathbb{C}$ υπάρχει $\tau_0 \in R_\Gamma \cup \partial R_\Gamma$ τέτοιο ώστε $\mathcal{J}(\tau_0) = z$. Έστω ότι αυτό δεν ισχύει, δηλαδή υπάρχει κάποιο $z \in \mathbb{C}$ τέτοιο ώστε $\mathcal{J}(\tau) \neq z$ για κάθε $\tau \in R_\Gamma \cup \partial R_\Gamma$.

Θεωρούμε τη συνάρτηση $f(\tau) := \mathcal{J}(\tau) - z$. Εφόσον η $\mathcal{J}$ έχει τουλάχιστον έναν πόλο τάξης 1 στο $\tau = i\infty$, από το Πόρισμα 5.5.10 η f θα έχει και ένα τουλάχιστον σημείο μηδενισμού στην κλειστότητα της R_Γ. Αυτό, όμως, αντίκειται στην υπόθεσή μας, συνεπώς καταλήγουμε σε άτοπο.

Για τη μοναδικότητα, αν υποθέσουμε ότι για κάποιο $z \in \mathbb{C}$ υπάρχουν δύο μιγαδικοί τ_1, τ_2 στην κλειστότητα της R_Γ με την ιδιότητα $\mathcal{J}(\tau_1) = \mathcal{J}(\tau_2) = z$, τότε, θεωρώντας ξανά τη συνάρτηση $\mathcal{J}(\tau) - z$, παρατηρούμε ότι μηδενίζεται στα τ_1 και τ_2. Πάλι από το Πόρισμα 5.5.10, έπεται ότι η f θα έχει είτε δύο απλούς πόλους είτε ένα διπλό στην κλειστότητα της R_Γ. Αυτό, όμως, είναι άτοπο, καθώς η συνάρτηση $\mathcal{J}$ έχει έναν απλό πόλο στο σημείο $\tau = i\infty$. Συνεπώς, η $\mathcal{J}$ λαμβάνει όλες τις τιμές ακριβώς μία φορά στην κλειστότητα της R_Γ.

Θα υπολογίσουμε τώρα τις τιμές $\mathcal{J}(\rho), \mathcal{J}(i)$ και $\mathcal{J}(i\infty)$. Πρώτα επαληθεύουμε ότι $g_2(\rho) = 0 = g_3(i)$. Αφού γνωρίζουμε ότι $\rho^3 = 1$ και $\rho^2 + \rho + 1 = 0$, έχουμε ότι

$$\frac{1}{60} g_2(\rho) = \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\rho)^4} = \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m\rho^3+n\rho)^4} =$$

$$= \frac{1}{\rho^4} \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m\rho^2+n)^4} = \frac{1}{\rho} \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(n-m-m\rho)^4} =$$

$$= \frac{1}{\rho} \sum_{\substack{(N,M)\in\mathbb{Z}\times\mathbb{Z} \\ (N,M)\neq(0,0)}} \frac{1}{(N+M\rho)^4} = \frac{1}{60\rho} g_2(\rho) \Rightarrow g_2(\rho) = 0.$$

Όμοια βρίσκουμε $g_3(i) = 0$. Συνεπώς,

$$\mathcal{J}(\rho) = 12^3 \frac{g_2^3(\rho)}{\Delta(\rho)} = 0 \quad \text{και} \quad \mathcal{J}(i) = 12^3 \frac{g_2^3(i)}{g_2^3(i)} = 1728.$$

Για το σημείο $i\infty$ χρησιμοποιούμε το ανάπτυγμα Laurent της συνάρτησης $\mathcal{J}$. Έχουμε, λοιπόν, ότι

$$\mathcal{J}(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{\infty} c(n) e^{2\pi i n\tau}, \quad c(n) \in \mathbb{Z}.$$

Αν θέσουμε $\tau = i\infty$, παρατηρούμε ότι $e^{-2\pi i(i\infty)} = \infty$, ενώ $e^{2\pi i(i\infty)} = 0$. Συνεπώς, εύκολα βλέπουμε ότι $\mathcal{J}(i\infty) = \infty$. Οι πολλαπλότητες και οι τάξεις υπολογίζονται από το Θεώρημα 5.5.8. □

Θεώρημα 5.5.13 Κάθε ρητή συνάρτηση της $\mathcal{J}-$αναλλοιώτου είναι modular συνάρτηση. Αντίστροφα, 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 $\mathcal{J}(\tau)$. Καθώς το $\mathbb{C}$ είναι αλγεβρικά κλειστό σώμα, μπορούμε να υποθέσουμε ότι

$$P(\mathcal{J}(\tau)) = \prod_{i=1}^{m} (\mathcal{J}(\tau) - a_i) \quad \text{και} \quad Q(\mathcal{J}(\tau)) = \prod_{j=1}^{n} (\mathcal{J}(\tau) - b_j),$$

όπου τα a_i και b_j είναι τα σημεία μηδενισμού των P και Q αντίστοιχα. Έτσι, η συνάρτησή μας παίρνει τη μορφή

$$f(\tau) = \frac{\prod_{i=1}^{m} (\mathcal{J}(\tau) - a_i)}{\prod_{j=1}^{n} (\mathcal{J}(\tau) - b_j)}.$$

Μάλιστα, από το Θεώρημα 5.5.8 έπεται ότι $m = n$, επομένως

$$f(\tau) = \prod_{i=1}^{n} \frac{\mathcal{J}(\tau) - a_i}{\mathcal{J}(\tau) - b_i}. \tag{5.10}$$

Έστω τώρα $z_1, ..., z_n \in \mathbb{C}$ τέτοια ώστε

$$\mathcal{J}(z_i) = a_i, \quad \forall i = 1, 2, ..., n$$

και $p_1, ..., p_n \in \mathbb{C}$ τέτοια ώστε

$$\mathcal{J}(p_i) = b_i, \quad \forall i = 1, 2, ..., n.$$

Τότε τα $p_1, ..., p_n$ αποτελούν πόλους της f και άρα η f είναι μερόμορφη συνάρτηση. Ακόμη, αφού η $\mathcal{J}$ είναι modular συνάρτηση, ισχύει ότι

$$\mathcal{J}(\tau) = \mathcal{J}(A\tau), \quad \forall A \in SL_2(\mathbb{Z}).$$

Κατά συνέπεια, από την (5.10) προκύπτει ότι

$$f(A\tau) = f(\tau), \quad \forall A \in SL_2(\mathbb{Z}).$$

Τέλος, τα σημεία $p_1, ..., p_n$ αποτελούν πόλους πεπερασμένης τάξης, καθώς πρόκειται για απλά σημεία μηδενισμού του πολυωνύμου $Q(\mathcal{J}(\tau))$. Από όλα τα παραπάνω έπεται ότι η f είναι modular συνάρτηση.

Αναφορικά με το δεύτερο σκέλος του θεωρήματος, έστω g μία modular συνάρτηση. Υποθέτουμε ότι τα $z_1, ..., z_n$ είναι σημεία μηδενισμού και τα $p_1, ..., p_n$ πόλοι αυτής. Θεωρούμε τη συνάρτηση

$$h(\tau) := \prod_{k=1}^{n} \frac{\mathcal{J}(\tau) - \mathcal{J}(z_k)}{\mathcal{J}(\tau) - \mathcal{J}(p_k)},$$

όπου αντικαθιστούμε την τιμή της $\mathcal{J}$ με 1, όταν $p_k = \infty$ ή $z_k = \infty$ σύμφωνα με την Πρόταση 5.5.12. Τότε η h, η οποία είναι modular συνάρτηση από το πρώτο σκέλος 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, δηλαδή είναι αναλυτική και συνεπώς σταθερή συνάρτηση από το θεώρημα του Liouville. Επομένως, δείξαμε ότι η g γράφεται ως πολυωνυμική συνάρτηση της $\mathcal{J}-$αναλλοιώτου και άρα η απόδειξη ολοκληρώθηκε. □

Ολοκληρώνοντας τη μελέτη μας πάνω στις modular συναρτήσεις, θα δούμε μία εφαρμογή στο αντίστροφο πρόβλημα για τις σειρές Eisenstein.

Στη θεωρία του Weierstrass για τις ελλειπτικές συναρτήσεις, το θεμελιώδες ζεύγος περιόδων ω_1, ω_2 καθορίζει τις συναρτήσεις g_2 και g_3 σύμφωνα με τις σχέσεις

$$g_2 = g_2(\omega_1, \omega_2) = 60 \sum_{m,n} \frac{1}{(m\omega_1 + n\omega_2)^4}$$

και

$$g_3 = g_3(\omega_1, \omega_2) = 140 \sum_{m,n} \frac{1}{(m\omega_1 + n\omega_2)^6}.$$

Ένα θεμελιώδες ερώτημα είναι να αποφασίσουμε εάν οι g_2 και g_3 μπορούν να πάρουν αυθαίρετα προκαθορισμένες τιμές, με μόνη προϋπόθεση οι τιμές αυτές να ικανοποιούν τη συνθήκη $g_2^3 - 27g_3^2 \neq 0$. Αυτό είναι το αντίστροφο πρόβλημα για τις σειρές Eisenstein, αφού για την απάντηση απαιτείται να λύσουμε τις παραπάνω σχέσεις ως προς ω_1 και ω_2. Το παρακάτω θεώρημα δείχνει ότι το πρόβλημα αυτό έχει λύση.

Θεώρημα 5.5.14 Δεδομένων δύο μιγαδικών αριθμών a_2, a_3 με την ιδιότητα $a_2^3 - 27a_3^2 \neq 0$, υπάρχουν $\omega_1, \omega_2 \in \mathbb{C}$ με μη πραγματικό λόγο, έτσι ώστε να ισχύουν $g_2(\omega_1, \omega_2) = a_2$ και $g_3(\omega_1, \omega_2) = a_3$.

Απόδειξη. Διακρίνουμε τρεις περιπτώσεις:

1. Έστω $a_2 = 0$. Σε αυτή την περίπτωση $a_3 \neq 0$, αφού έχουμε υποθέσει ότι $a_2^3 - 27a_3^2 \neq 0$. Έστω $\omega_1 \in \mathbb{C}$ τέτοιο ώστε

   $$\omega_1^6 = \frac{g_3(1, \rho)}{a_3}$$

   και έστω $\omega_2 = \rho\omega_1$ (όπου $\rho = e^{2\pi i/3}$). Γνωρίζουμε ότι $g_3(1, \rho) \neq 0$ γιατί από την Πρόταση 5.5.12 ισχύει $g_2(1, \rho) = 0$ και $\Delta(1, \rho) = g_2^3 - 27g_3^2 \neq 0$. Τότε έχουμε

   $$g_2(\omega_1, \omega_2) = g_2(\omega_1, \rho\omega_1) = \frac{1}{\omega_1^4} g_2(1, \rho) = 0 = a_2$$

   και

   $$g_3(\omega_1, \omega_2) = g_3(\omega_1, \rho\omega_1) = \frac{1}{\omega_1^6} g_3(1, \rho) = a_3.$$

2. Έστω $a_3 = 0$. Τότε, με το ίδιο επιχείρημα, $a_2 \neq 0$. Έστω $\omega_1 \in \mathbb{C}$ τέτοιο ώστε

   $$\omega_1^4 = \frac{g_2(1, i)}{a_2}$$

   και έστω $\omega_2 = i\omega_1$. Εδώ γνωρίζουμε ότι $g_2(1, i) \neq 0$ γιατί πάλι από την Πρόταση 5.5.12 έχουμε $g_3(1, i) = 0$ και $\Delta(1, i) \neq 0$. Τότε

   $$g_2(\omega_1, \omega_2) = g_2(\omega_1, i\omega_1) = \frac{1}{\omega_1^4} g_2(1, i) = a_2$$

   και

   $$g_3(\omega_1, \omega_2) = g_3(\omega_1, i\omega_1) = \frac{1}{\omega_1^6} g_3(1, i) = 0 = a_3.$$

3. Έστω $a_2 a_3 \neq 0$. Επιλέγουμε $\tau \in \mathcal{H}$ τέτοιο ώστε

$$\mathcal{J}(\tau) = \frac{a_2^3}{a_2^3 - 27a_3^2.}$$

Σημειώνουμε ότι $\mathcal{J}(\tau) \neq 0$ αφού $a_2 \neq 0$ και ότι ισχύει

$$\frac{\mathcal{J}(\tau) - 1}{\mathcal{J}(\tau)} = \frac{27a_3^2}{a_2^3}. \tag{5.11}$$

Για αυτό το τ, επιλέγουμε το ω_1 έτσι ώστε να ικανοποιεί

$$\omega_1^2 = \frac{a_2}{a_3} \cdot \frac{g_3(1,\tau)}{g_2(1,\tau)}$$

και έστω $\omega_2 = \tau\omega_1$. Τότε έχουμε ότι

$$\frac{g_2(\omega_1,\omega_2)}{g_3(\omega_1,\omega_2)} = \frac{\omega_1^{-4} g_2(1,\tau)}{\omega_1^{-6} g_3(1,\tau)} = \omega_1^2 \frac{g_2(1,\tau)}{g_3(1,\tau)} = \frac{a_2}{a_3},$$

δηλαδή

$$g_3(\omega_1,\omega_2) = \frac{a_3}{a_2} g_2(\omega_1,\omega_2). \tag{5.12}$$

Όμως ισχύει επίσης ότι

$$\frac{\mathcal{J}(\tau) - 1}{\mathcal{J}(\tau)} = \frac{27g_3^2(\omega_1,\omega_2)}{g_2^3(\omega_1,\omega_2)} = \frac{27(a_3/a_2)^2 g_2^2(\omega_1,\omega_2)}{g_2^3(\omega_1,\omega_2)} = \frac{27a_3^2}{a_2^2 g_2(\omega_1,\omega_2)}.$$

Συγκρίνοντας την τελευταία σχέση με την (5.11) προκύπτει $g_2(\omega_1,\omega_2) = a_2$ και άρα από την (5.12) έπεται $g_3(\omega_1,\omega_2) = a_3$.

Η απόδειξη, λοιπόν, ολοκληρώθηκε. □

Κεφάλαιο 6

Το Θεώρημα των Heegner - Stark

6.1 Σχετικές Επεκτάσεις Αλγεβρικών Σωμάτων Αριθμών

Ανάλογα προς τη θεωρία των απόλυτων επεκτάσεων, δηλαδή επεκτάσεων της μορφής $K/\mathbb{Q}$, αναφορικά με το νόμο ανάλυσης, ισχύουν και για τις σχετικές επεκτάσεις αλγεβρικών σωμάτων αριθμών L/K τα ακόλουθα:

Έστω K αλγεβρικό σώμα αριθμών, L πεπερασμένη επέκταση του K. Αν P πρώτο ιδεώδες του K, τότε το PR_L είναι ιδεώδες του L και αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών στο L,

$$PR_L = P_1^{e_1}...P_k^{e_k},$$

όπου τα πρώτα ιδεώδη P_i του L περιέχουν το P.

Ο ακέραιος αριθμός e_i λέγεται *δείκτης διακλαδώσεως* του P στο ιδεώδες P_i. Λέμε ότι το P *διακλαδίζεται* στο L αν για κάποιο από τα e_i ισχύει $e_i > 1$. Αποδεικνύεται ότι το πλήθος των πρώτων ιδεωδών του K που διακλαδίζονται στο L είναι πεπερασμένο.

Κάθε ιδεώδες P_i ορίζει μία επέκταση πεπερασμένων σωμάτων της μορφής

$$R_K/P \subset R_L/P_i,$$

ο βαθμός της οποίας λέγεται *δείκτης αδρανείας* του P στο P_i και συμβολίζεται με f_i.

Θεώρημα 6.1.1 Έστω $K \subset L$ αλγεβρικά σώματα αριθμών, P πρώτο ιδεώδες του K. Αν $e_1, ..., e_k$ οι δείκτες διακλαδώσεως και $f_1, ..., f_k$ οι δείκτες αδρανείας, όπως ορίστηκαν παραπάνω, τότε ισχύει

$$\sum_{i=1}^{k} e_i f_i = [L : K].$$

Απόδειξη. Βλ.[8],σελ.100-101. □

Θεώρημα 6.1.2 Αν η L/K είναι επέκταση Galois, P πρώτο ιδεώδες του K, τότε ισχύουν

$$e_1 = ... = e_k =: e, \quad f_1 = ... = f_k =: f$$

και

$$[L : K] = efk.$$

Απόδειξη. Βλ.[8],σελ.101. □

Αν, λοιπόν, έχουμε L/K μία επέκταση Galois, τότε το πρώτο ιδεώδες P διακλαδίζεται στο L αν $e > 1$, ενώ είναι μη-διακλαδιζόμενο αν $e = 1$. Στην ειδική περίπτωση $e = f = 1$, λέμε ότι το P *αναλύεται πλήρως* στο L. Σε αυτή την περίπτωση το ιδεώδες PR_L είναι το γινόμενο $[L : K]$ πρώτων ιδεωδών, που είναι το μέγιστο δυνατό πλήθος σύμφωνα με το Θεώρημα 6.1.2.

Το παρακάτω θεώρημα είναι το αντίστοιχο του θεωρήματος του Dedekind στις απόλυτες επεκτάσεις.

Θεώρημα 6.1.3 Έστω L/K επέκταση Galois, όπου $L = K(\alpha)$ για κάποιο $\alpha \in R_L$. Έστω $f(x) = Irr(\alpha, K) \in R_K[x]$. Αν P πρώτο ιδεώδες του R_K και το $f(x)$ είναι διαχωρίσιμο $modP$, τότε:

1. Το P δε διακλαδίζεται στο L.
2. Αν ισχύει
$$f(x) \equiv f_1(x) \cdot ... \cdot f_k(x)(modP),$$
όπου τα f_i ανάγωγα πολυώνυμα $modP$, τότε τα $P_i = PR_L + f_i(\alpha)R_L$ είναι πρώτα ιδεώδη του R_L, με $P_i \neq P_j$ για $i \neq j$, και ισχύει
$$PR_L = P_1...P_k.$$
Επιπλέον, όλα τα f_i έχουν τον ίδιο βαθμό, που είναι ο βαθμός αδρανείας f.
3. Το P αναλύεται πλήρως στο L αν και μόνο αν η ισοτιμία $f(x) \equiv 0(modP)$ έχει λύση στον R_K.

Απόδειξη. Βλ.[8],σελ.102-103. □

6.2 Το σώμα κλάσεων του Hilbert

Έστω K αλγεβρικό σώμα αριθμών και R_K ο δακτύλιος των ακεραίων αλγεβρικών αυτού. Τα πρώτα ιδεώδη του R_K θα λέγονται *πεπερασμένοι πρώτοι* του σώματος K. Οι άπειροι πρώτοι ορίζονται μέσω εμφυτεύσεων του σώματος K. Συγκεκριμένα, ένας *πραγματικός άπειρος πρώτος* είναι μία εμφύτευση

$$\sigma : K \hookrightarrow \mathbb{R},$$

ενώ ένας *μιγαδικός άπειρος πρώτος* είναι ένα ζεύγος συζυγών μιγαδικών εμφυτεύσεων

$$\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C},$$

όπου $\sigma \neq \bar{\sigma}$.

Έτσι, αν L/K (πεπερασμένη) επέκταση αλγεβρικών σωμάτων αριθμών, ένας άπειρος πρώτος σ του K *διακλαδίζεται* στο L ακριβώς όταν ο σ είναι πραγματικός στο K και μιγαδικός όταν επεκτείνεται στο L.

Για παράδειγμα, ο άπειρος πρώτος του $\mathbb{Q}$ είναι μη-διακλαδιζόμενος στο σώμα $\mathbb{Q}(\sqrt{d}),\ d > 0$, ενώ είναι διακλαδιζόμενος στο σώμα $\mathbb{Q}(\sqrt{d}),\ d < 0$. Αν, πάλι, το K είναι ένα τετραγωνικό μιγαδικό σώμα αριθμών, τότε ο άπειρος πρώτος του K είναι μιγαδικός και συνεπώς δε διακλαδίζεται σε οποιαδήποτε επέκταση αυτού.

Ορισμός 6.2.1 Μια επέκταση αλγεβρικών σωμάτων αριθμών L/K θα λέγεται *μη-διακλαδιζόμενη* αν δε διακλαδίζεται σε κανένα πρώτο αυτής, πεπερασμένο ή άπειρο.

Η L/K θα λέγεται *αβελιανή* αν είναι επέκταση Galois και επιπλέον η ομάδα Galois, $Gal(L/K)$, είναι αβελιανή.

Άμεση συνέπεια ενός σημαντικότατου και πάρα πολύ δύσκολου κλάδου της Θεωρίας Αριθμών, της Θεωρίας Κλάσεων Σωμάτων, αποτελούν τα ακόλουθα θεωρήματα.

Θεώρημα 6.2.2 Έστω K αλγεβρικό σώμα αριθμών. Υπάρχει πάντα μία πεπερασμένη επέκταση του K, έστω H, που ικανοποιεί τις ακόλουθες ιδιότητες:

- Η επέκταση H/K είναι μη-διακλαδιζόμενη και αβελιανή.
- Κάθε άλλη μη-διακλαδιζόμενη και αβελιανή επέκταση του K, έστω L, περιέχεται στο σώμα H.

Ορισμός 6.2.3 Το σώμα H με τις παραπάνω ιδιότητες λέγεται *σώμα κλάσεων του Hilbert.*

Στην ειδική περίπτωση που το σώμα K είναι τετραγωνικό μιγαδικό σώμα αριθμών, αποδεικνύεται εύκολα ότι η επέκταση $H/\mathbb{Q}$ είναι επέκταση Galois.

Το δεύτερο θεώρημα είναι άμεση συνέπεια του νόμου αντιστροφής του Artin.

Θεώρημα 6.2.4 Έστω K αλγεβρικό σώμα αριθμών, $\mathcal{R}(K)$ η ομάδα κλάσεων ιδεωδών αυτού και H το σώμα κλάσεων του Hilbert. Τότε ισχύει

$$\mathcal{R}(K) \cong Gal(H/K).$$

Από το θεώρημα αυτό συμπεραίνουμε ότι ο βαθμός της επέκτασης H/K ισούται ακριβώς με τον αριθμό κλάσεων h_K του σώματος K.

Ο υπολογισμός του σώματος κλάσεων του Hilbert δεν είναι εύκολη υπόθεση. Για αλγεβρικά σώματα αριθμών με μικρό αριθμό κλάσεων, το πρόβλημα είναι εύκολο στην περίπτωση που το σώμα κλάσεων του Hilbert ταυτίζεται με το σώμα γένους του K και το K είναι τετραγωνικό μιγαδικό σώμα αριθμών.

Παράδειγμα 6.2.5 Θα αποδείξουμε ότι το σώμα κλάσεων του Hilbert του μιγαδικού τετραγωνικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{-14})$ είναι το

$$H = K\Big(\sqrt{2\sqrt{2}-1}\Big).$$

Απόδειξη. Έχουμε ότι $-14 \equiv 2(mod 4)$, συνεπώς η διακρίνουσα του σώματος είναι ίση με $d(K) = 4(-14) = -56$. Για να υπολογίσουμε τον αριθμό κλάσεων του σώματος K, αρκεί να υπολογίσουμε τον αριθμό κλάσεων πρωταρχικών θετικά ορισμένων τετραγωνικών μορφών διακρίνουσας $\Delta = -56$. Ακολουθώντας, λοιπόν, την ίδια διαδικασία όπως στο Παράδειγμα 1.2.16, βρίσκουμε τις ανηγμένες τετραγωνικές μορφές

$$X^2 + 14Y^2, \quad 2X^2 + 7Y^2 \text{ και } 3X^2 \pm 2XY + 5Y^2$$

και άρα προκύπτει ότι $h_K = 4$.

Έστω τώρα $\alpha = \sqrt{2\sqrt{2}-1}$. Για να είναι το $K(\alpha)$ το σώμα κλάσεων Hilbert του σώματος K αρκεί να δείξουμε ότι $[K(\alpha) : K] = 4$ και ότι η $K(\alpha)/K$ είναι μη-διακλαδιζόμενη και αβελιανή επέκταση του K.

Μπορούμε εύκολα να δούμε ότι το α είναι ρίζα του πολυωνύμου $f(x) = x^4 + 2x^2 - 7$ και ότι το πολυώνυμο αυτό είναι ανάγωγο υπέρ το $\mathbb{Q}$. Επομένως, ισχύει ότι $f(x) = Irr(\alpha, \mathbb{Q})$ και $[\mathbb{Q}(\alpha) : \mathbb{Q}] = degf(x) = 4$.

Ισχύει ότι $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, αφού $\alpha \in \mathbb{R}$. Επειδή το K είναι μιγαδικό σώμα αριθμών, προκύπτει ότι

$$\mathbb{Q}(\alpha) \cap K = \mathbb{Q}.$$

Από την παραπάνω σχέση και τις ισότητες

$$[K(\alpha) : \mathbb{Q}(\alpha)] = 2, \quad [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 \quad \text{και} \quad [K : \mathbb{Q}] = 2$$

έπεται ότι $[K(\alpha) : K] = 4$. Αυτό σημαίνει ότι το πολυώνυμο $f(x)$ είναι ανάγωγο και υπέρ το K.

Θα δείξουμε τώρα ότι η επέκταση $K(\alpha)/K$ είναι αβελιανή.

Μπορούμε εύκολα να δούμε ότι οι ρίζες του πολυωνύμου $f(x)$ είναι οι

$$\alpha, \quad \beta = i\sqrt{2\sqrt{2}+1}, \quad -\alpha \quad \text{και} \quad -\beta.$$

Για το β έχουμε:

$$\beta = i\sqrt{2\sqrt{2}+1} = i\frac{\sqrt{2\sqrt{2}+1}\sqrt{2\sqrt{2}-1}}{\sqrt{2\sqrt{2}-1}} = \frac{\sqrt{-7}}{\alpha} = \frac{\sqrt{-14}}{\alpha\sqrt{2}} \in K(\alpha),$$

αφού προφανώς $\sqrt{-14} \in K(\alpha)$ και επίσης

$$\alpha \in K(\alpha) \Rightarrow \alpha^2 \in K(\alpha) \Rightarrow 2\sqrt{2} - 1 \in K(\alpha) \Rightarrow \sqrt{2} \in K(\alpha).$$

Από τα παραπάνω συμπεραίνουμε ότι το $K(\alpha)$ είναι το σώμα ανάλυσης του πολυωνύμου $f(x)$, δηλαδή η επέκταση $K(\alpha)/K$ είναι κανονική. Καθώς η $K(\alpha)/K$ είναι και διαχωρίσιμη, έπεται ότι είναι επέκταση Galois. Τέλος, αφού ισχύει $[K(\alpha) : K] = 4$, η επέκταση θα είναι κατ'ανάγκη αβελιανή.

Απομένει να δείξουμε ότι η επέκταση $K(\alpha)/K$ είναι μη-διακλαδιζόμενη.

Αφού το σώμα μας είναι μιγαδικό τετραγωνικό και οι δύο εμφυτεύσεις του σώματος K είναι επίσης μιγαδικές, από όσα αναφέραμε παραπάνω προκύπτει ότι οι δύο άπειροι πρώτοι δεν διακλαδίζονται. Θα δείξουμε ότι ισχύει το ίδιο και για τους πεπερασμένους πρώτους, δηλαδή όλα τα πρώτα ιδεώδη του σώματος K στο $K(\alpha) = L$.

Είδαμε ότι $\sqrt{2} \in K(\alpha)$. Έστω $K_1 := K(\sqrt{2}) \leq K(\alpha)$. Έχουμε τότε τη σχέση

$$K \leq K_1 \leq K(\alpha).$$

Λόγω της πολλαπλασιαστικότητας των δεικτών διακλάδωσης, αρκεί, λοιπόν, να δείξουμε ότι οι επεκτάσεις $K(\alpha)/K_1$ και K_1/K είναι μη-διακλαδιζόμενες.

Προς τούτο, δείχνουμε πρώτα το ακόλουθο:

Λήμμα 6.2.6 Έστω $L = K(\sqrt{u})$ τετραγωνική επέκταση του K, όπου $u \in R_K$, και P πρώτο ιδεώδες του R_K. Ισχύουν:

1. Αν $2u \notin P$, τότε το P δεν διακλαδίζεται στο L.

2. Αν $2 \in P$, $u \notin P$ και $u = b^2 - 4c$ για κάποια $b, c \in R_K$, τότε το P δεν διακλαδίζεται στο L.

Για το (1.), παρατηρούμε ότι η διακρίνουσα του πολυωνύμου $x^2 - u \in K[x]$ είναι $4u \notin P$. Αυτό σημαίνει ότι το $x^2 - u$ αναλύεται σε γινόμενο δύο γραμμικών πολυωνύμων διαφορετικών μεταξύ τους, συνεπώς από το Θεώρημα 6.1.3 το ιδεώδες P δεν διακλαδίζεται στο L.

Για το (2.), παρατηρούμε ότι το πολυώνυμο $x^2 + bx + c \in R_K[x]$ έχει διακρίνουσα $b^2 - 4c \notin P$, συνεπώς όπως προηγουμένως το P δεν διακλαδίζεται στο L. Αποδείξαμε, συνεπώς, το λήμμα.

Τώρα θα δείξουμε ότι η επέκταση K_1/K είναι μη-διακλαδιζόμενη.

Έστω P ένα πρώτο ιδεώδες του K. Έχουμε $K_1 = K(\sqrt{2})$, άρα από το (1.) του Λήμματος, αν ισχύει $2 \notin P$, τότε το P δε διακλαδίζεται στο K_1. Έστω ότι $2 \in P$. Τότε επειδή $\sqrt{-14}, \sqrt{2} \in K_1$ έπεται ότι $\sqrt{-7} \in K_1$ και μάλιστα

$$K_1 = K(\sqrt{2}) = K(\sqrt{-7}).$$

Αν $-7 \in P$, τότε επειδή $2 \in P$ θα ισχύει και $1 = -7 + 2 \cdot 3 \in P$, δηλαδή $P = R_K$, το οποίο είναι άτοπο. Συνεπώς, ισχύει $-7 \notin P$. Όμως $-7 = 1^2 - 4 \cdot 2 \notin P$ και άρα από το (2.) του Λήμματος το ιδεώδες P δεν διακλαδίζεται στο K_1. Δείξαμε, έπομένως, ότι η επέκταση K_1/K είναι μη-διακλαδιζόμενη.

Απομένει να δείξουμε ότι η επέκταση $K(\alpha)/K_1$ είναι μη-διακλαδιζόμενη.

Έστω $\mu = \alpha^2 = 2\sqrt{2} - 1$ και $\mu' = -2\sqrt{2} - 1 \in K_1 = K(\sqrt{2}) = K(\sqrt{-7})$. Ισχύει ότι $\sqrt{\mu} \cdot \sqrt{\mu'} = \sqrt{-7} \in K_1$. Όμως $\sqrt{\mu} = \alpha \in K(\alpha)$, οπότε και $\sqrt{\mu'} \in K(\alpha)$ και τελικά

$$K(\alpha) = K(\sqrt{\mu}) = K(\sqrt{\mu'}).$$

Έστω τώρα P πρώτο ιδεώδες του K_1. Αν ισχύει $2 \notin P$, τότε αφού $\mu + \mu' = -2$, αναγκαστικά ένα από τα μ και μ' δεν θα ανήκει στο P. Έστω, χωρίς βλάβη της γενικότητας, ότι $\mu \notin P$. Τότε $2\mu \notin P$ και επειδή $K(\alpha) = K(\sqrt{\mu})$, από το (1.) του Λήμματος το P δε διακλαδίζεται στο $K(\alpha)$. Αν, τώρα, $2 \in P$, τότε και $2\sqrt{2} \in K_1$. Αν ίσχυε $\mu \in P$, τότε προκύπτει $1 \in P$, άτοπο. Επομένως, $\mu \notin P$. Όμως το μ γράφεται $\mu = (1 + \sqrt{2})^2 - 4$, οπότε από το (2.) του Λήμματος το P δεν διακλαδίζεται στο σώμα $K(\alpha)$. Επομένως, η επέκταση $K(\alpha)/K_1$ είναι

μη-διακλαδιζόμενη.

Τελικά έπεται ότι η επέκταση $K(\alpha)/K$ είναι μη-διακλαδιζόμενη αβελιανή βαθμού 4, συνεπώς το σώμα κλάσεων του Hilbert του K είναι το $K(\alpha)$. □

Εδώ πρέπει να κάνουμε την εξής παρατήρηση: η παραπάνω απόδειξη έχει ένα μειονέκτημα, διότι δε μας ζητήθηκε να προσδιορίσουμε το σώμα κλάσεων του Hilbert, αλλά να δείξουμε ότι είναι αυτό! Η πραγματική απόδειξη για μια σειρά ανάλογων παραδειγμάτων βρίσκεται στο άρθρο [14]. Σχετικά με το σώμα κλάσεων του Hilbert του σώματος $K = \mathbb{Q}(\sqrt{-47})$ που έχει αριθμό κλάσεων $h_K = 5$, παραπέμπουμε στο [12].

Έστω τώρα K ένα τετραγωνικό μιγαδικό σώμα αριθμών, R_f μία τάξη του K, με $f \in \mathbb{N}$, και A ένα γνήσιο (proper) κλασματικό R_f-ιδεώδες αυτού.

Το πρώτο θεμελιώδες θεώρημα του μιγαδικού πολλαπλασιασμού είναι το ακόλουθο:

Θεώρημα 6.2.7 Η τιμή της απόλυτης αναλλοίωτης $\mathcal{J}(A)$[1] είναι ένας πραγματικός αριθμός, ο οποίος είναι ακέραιος αλγεβρικός, και το σώμα $K(\mathcal{J}(A))$ είναι το *ring class field* του K *modf*.

Απόδειξη. Βλ.[8], Θεώρημα 11.1, σελ.220. □

Από εδώ προκύπτει το εξής σημαντικό πόρισμα:

Πόρισμα 6.2.8 Αν K μιγαδικό τετραγωνικό σώμα αριθμών, τότε το σώμα κλάσεων του Hilbert H του K είναι το

$$H = K(\mathcal{J}(R_K)).$$

6.3 Modular Συναρτήσεις ως προς την ομάδα $\Gamma_0(N)$

Στην παράγραφο αυτή θα ορίσουμε modular συναρτήσεις ως προς μία κλάση υποομάδων της ομάδας $SL_2(\mathbb{Z})$.

Έστω N ένας θετικός ακέραιος αριθμός. Το σύνολο

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 (mod N) \right\}$$

[1] Ως $\mathcal{J}(A)$ συμβολίζουμε την τιμή του δικτυωτού μίας βάσης αυτού.

αποτελεί (πολλαπλασιαστική) υποομάδα της $SL_2(\mathbb{Z})$ και μάλιστα πεπερασμένου δείκτη, όπως θα δούμε παρακάτω.

Ορισμός 6.3.1 Μία μιγαδική συνάρτηση $f : \mathcal{H} \to \mathbb{C} \cup \{\infty\}$ θα λέγεται modular συνάρτηση ως προς την ομάδα $\Gamma_0(N)$ αν ικανοποιεί τις παρακάτω ιδιότητες:

1. Η $f(z)$ είναι μερόμορφη συνάρτηση στο $\mathcal{H}$.
2. Αν $z \in \mathcal{H}$, ισχύει $f(Az) = f(z), \quad$ για κάθε $A \in \Gamma_0(N)$.
3. Η $f(z)$ είναι μερόμορφη στις κορυφές (cusps).

Η ιδιότητα (3) χρειάζεται περαιτέρω επεξήγηση:

Ας υποθέσουμε ότι για τη συνάρτηση $f(z)$ ισχύουν οι ιδιότητες (1) και (2). Έστω ένας πίνακας $A \in SL_2(\mathbb{Z})$. Τότε η συνάρτηση $f(Az)$ είναι περιοδική με περίοδο N. Πράγματι, αν ορίσουμε τον πίνακα

$$T_N := \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix},$$

τότε έχουμε ότι $T_N(z) = z + N$. Έστω τώρα

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Υπολογίζοντας το γινόμενο AT_NA^{-1}, εύκολα διαπιστώνουμε ότι ο πίνακας $AT_NA^{-1} \in \Gamma_0(N)$. Επομένως,

$$f(A(z+N)) = f(AT_N(z)) = f(AT_NA^{-1}Az) \overset{\iota\delta.(2)}{=} f(Az).$$

Έτσι, αν θέσουμε $q := q(z) = e^{2\pi iz}$, τότε η $f(Az)$ είναι μία ολόμορφη συνάρτηση του $q^{1/N}$, ορισμένη για $0 < |q^{1/N}| < 1$. Αυτό σημαίνει ότι η $f(Az)$ έχει ανάπτυγμα Laurent της μορφής

$$f(Az) = \sum_{n=-\infty}^{+\infty} a(n)q^{n/N},$$

το οποίο λέγεται *q-ανάπτυγμα της* $f(Az)$.

Λέγοντας, τώρα, ότι η συνάρτηση f είναι μερόμορφη στις κορυφές εννοούμε ότι, για όλους τους πίνακες $A \in SL_2(\mathbb{Z})$, το ανάπτυγμα Laurent της συνάρτησης $f(Az)$ έχει πεπερασμένου πλήθους μη-μηδενικούς αρνητικούς συντελεστές.

Παράδειγμα 6.3.2 Η απόλυτη αναλλοίωτη $\mathcal{J}(z)$, όπως είδαμε στην παράγραφο 5.4, είναι μία ολόμορφη συνάρτηση στο άνω μιγαδικό ημιεπίπεδο $\mathcal{H}$, αναλλοίωτη κάτω από τη δράση των στοιχείων της $SL_2(\mathbb{Z})$ και μερόμορφη στις κορυφές, αφού εδώ η μοναδική κορυφή είναι το 0 και, όπως γνωρίζουμε, το ανάπτυγμα Laurent της $\mathcal{J}$ είναι το

$$\mathcal{J}(z) = \frac{1}{q} + \sum_{n=0}^{\infty} a(n)q^n, \quad a(n) \in \mathbb{Z}.$$

Επομένως, η $\mathcal{J}(z)$ είναι modular συνάρτηση ως προς την ομάδα $\Gamma_0(1) = SL_2(\mathbb{Z})$.

Είδαμε στο προηγούμενο κεφάλαιο ότι το σώμα των modular συναρτήσεων ως προς την $SL_2(\mathbb{Z})$ είναι το $\mathbb{C}(\mathcal{J}(z))$. Ανάλογα αποδεικνύεται:

Πρόταση 6.3.3 Οι συναρτήσεις $\mathcal{J}(z)$ και $\mathcal{J}(Nz)$ είναι modular συναρτήσεις ως προς την ομάδα $\Gamma_0(N)$ και το σώμα όλων των modular συναρτήσεων ως προς την ομάδα $\Gamma_0(N)$ είναι το σώμα των ρητών συναρτήσεων

$$\mathbb{C}(\mathcal{J}(z), \mathcal{J}(Nz)).$$

Παρατήρηση 6.3.4 Σύμφωνα με τον ορισμό, για να ελέγξουμε ότι η συνάρτηση $f(z)$ είναι μερόμορφη στις κορυφές, θα πρέπει να εξετάσουμε το q-ανάπτυγμα της $f(Az)$ για κάθε πίνακα $A \in SL_2(\mathbb{Z})$. Κάτι τέτοιο, όμως, δεν είναι απαραίτητο, καθώς λόγω της ιδιότητας (2) του ορισμού η συνάρτηση παραμένει αναλλοίωτη κάτω από τη δράση της ομάδας $\Gamma_0(N)$. Επομένως, αρκεί να ελέγξουμε το q-ανάπτυγμα των $f(A_i z)$, $i \in I$, όπου το σύνολο $\{A_i \mid i \in I\}$ ορίζει ένα πλήρες σύνολο αντιπροσώπων των (δεξιών) συμπλόκων της $SL_2(\mathbb{Z})$ ως προς την υποομάδα της, $\Gamma_0(N)$. Το σύνολο αυτό, όπως θα δούμε παρακάτω, είναι πεπερασμένο.

Πράγματι, θεωρούμε το σύνολο

$$R(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad = N,\ a > 0,\ 0 \le b < d,\ (a, b, d) = 1 \right\}.$$

Ο πίνακας

$$S_N := \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \in R(N)$$

και έχουμε ότι $S_N(z) = Nz$.

Επιπλέον, για την ομάδα $\Gamma_0(N)$ ισχύει

$$\Gamma_0(N) = (S_N^{-1} SL_2(\mathbb{Z}) S_N) \cap SL_2(\mathbb{Z}),$$

και μάλιστα, για κάθε πίνακα $A \in R(N)$ το σύνολο

$$(S_N^{-1} SL_2(\mathbb{Z}) A) \cap SL_2(\mathbb{Z})$$

αποτελεί ένα πλήρες σύνολο (δεξιών) συμπλόκων της $\Gamma_0(N)$ στην $SL_2(\mathbb{Z})$, το οποίο επάγει μια αμφιμονοσήμαντη απεικόνιση μεταξύ των στοιχείων του $R(N)$ και του συνόλου των (δεξιών) συμπλόκων της $\Gamma_0(N)$ στην $SL_2(\mathbb{Z})$.

Συνεπώς, έπεται ότι $[SL_2(\mathbb{Z}) : \Gamma_0(N)] = |R(N)|$. Αποδεικνύεται (βλ.[8], Ασκ.11.9) ότι

$$|R(N)| = N \cdot \prod_{p|N} \Big(1 + \frac{1}{p}\Big).$$

Με βάση τα παραπάνω, μπορούμε τώρα να υπολογίσουμε το q-ανάπτυγμα της συνάρτησης $\mathcal{J}(Nz)$ και να δείξουμε ότι είναι μερόμορφη στις κορυφές.

Έστω τώρα το σύνολο

$$\{\Gamma_0(N) A_i, \quad i = 1, 2, ..., |R(N)|\},$$

που αποτελεί ένα πλήρες σύστημα (δεξιών) συμπλόκων της ομάδας $\Gamma_0(N)$ στην $SL_2(\mathbb{Z})$. Θεωρούμε το πολυώνυμο του X,

$$\Phi_N(X, z) = \prod_{i=1}^{|R(N)|} \Big(X - \mathcal{J}(NA_i z)\Big).$$

Αποδεικνύεται ότι οι συντελεστές $\mathcal{J}(NA_i z)$ του Φ_N είναι ολόμορφες modular συναρτήσεις (ως προς την ομάδα $SL_2(\mathbb{Z})$) (Βλ.[8], σελ.229-231). Συνεπώς, οι συντελεστές είναι πολυώνυμα της $\mathcal{J}-$αναλλοιώτου, $\mathcal{J}(z)$. Με άλλα λόγια, υπάρχει πολυώνυμο $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$ με

$$\Phi_N(X, \mathcal{J}(z)) = \prod_{i=1}^{|R(N)|} \Big(X - \mathcal{J}(NA_i z)\Big).$$

Ορισμός 6.3.5 Η εξίσωση $\Phi_N(X, Y) = 0$ λέγεται *modular εξίσωση*.

Η εξίσωση αυτή είναι ιδιαίτερα χρήσιμη για την απόδειξη της Πρότασης 6.3.3. Δίνουμε επίσης κάποιες σημαντικές ιδιότητές της, οι οποίες παίζουν σημαντικό ρόλο στις αποδείξεις των προτάσεων που θα ακολουθήσουν.

Θεώρημα 6.3.6 Έστω N ένας θετικός ακέραιος. Ισχύουν:

1. $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$.

2. $\Phi_N(X,Y) = \Phi_N(Y,X)$.

3. Αν το N δεν είναι τέλειο τετράγωνο, τότε το πολυώνυμο $\Phi_N(X,Y)$ είναι πολυώνυμο του X βαθμού μεγαλύτερου του 1 με οδηγό συντελεστή ± 1.

4. Αν $N = p$ πρώτος αριθμός, τότε

$$\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p)(mod p\mathbb{Z}[X,Y])^2.$$

Απόδειξη. Βλ.[8], σελ.231-235. □

6.4 Modular Συναρτήσεις και Singular Moduli

Μία ιδιαίτερα χρήσιμη συνάρτηση, εκτός από την απόλυτη αναλλοίωτη, είναι η συνάρτηση $\gamma_2(z)$, η οποία ορίζεται ως

$$\gamma_2(z) = \sqrt[3]{\mathcal{J}(z)}.$$

Αποδεικνύεται ότι η $\gamma_2(3z)$ είναι modular συνάρτηση ως προς την ομάδα $\Gamma_0(9)$ (βλ.[8], σελ.250-251). Θα χρησιμοποιήσουμε το αποτέλεσμα αυτό στη συνέχεια για να δείξουμε ότι η συνάρτηση $\gamma_2(z)$ παράγει τα ring class fields για τάξεις των οποίων η διακρίνουσα δε διαιρείται από το 3.

Υπενθυμίζουμε ότι

$$\mathcal{J}(z) = 12^3 \frac{g_2^3(z)}{\Delta(z)}.$$

Η διακρίνουσα $\Delta(z)$ δεν μηδενίζεται πουθενά στο απλά συνεκτικό χωρίο $\mathcal{H}$. Συνεπώς, έχει μία ολόμορφη κυβική ρίζα, $\sqrt[3]{\Delta(z)}$. Επιπλέον, η $\Delta(z)$ παίρνει πραγματικές τιμές στο μιγαδικό άξονα, καθώς ισχύουν $g_2(\overline{L}) = \overline{g_2(L)}$, $g_3(\overline{L}) = \overline{g_3(L)}$ και $\mathcal{J}(\overline{L}) = \overline{\mathcal{J}(L)}$ για κάποιο δικτυωτό L. Μπορούμε, λοιπόν, να διαλέξουμε την $\sqrt[3]{\Delta(z)}$ έτσι ώστε να έχει την ίδια ιδιότητα.

Με αυτόν τον τρόπο, η $\gamma_2(z)$ ορίζεται ως

$$\gamma_2(z) = 12 \frac{g_2(z)}{\sqrt[3]{\Delta(z)}}$$

[2] Η ισοτιμία αυτή είναι γνωστή ως *ισοτιμία του Kronecker*.

και μάλιστα είναι η μοναδική κυβική ρίζα της $\mathcal{J}(z)$ η οποία παίρνει τιμές πραγματικούς αριθμούς στο μιγαδικό άξονα.

Παρατήρηση 6.4.1 Εδώ χρειάζεται λίγη προσοχή, γιατί παρόλο που η συνάρτηση $\mathcal{J}(z)$ παραμένει αναλλοίωτη όταν αντικαταστήσουμε το z με το $z+1$, για τη συνάρτηση $\gamma_2(z)$ ισχύει

$$\gamma_2(z+1) = \zeta_3^{-1}\gamma_2(z), \quad \text{όπου } \zeta_3 = e^{2\pi i/3}.$$

Αυτό σημαίνει ότι η $\gamma_2(z)$ δεν είναι modular συνάρτηση ως προς την ομάδα $SL_2(\mathbb{Z})$.

Διατυπώνουμε, τώρα, το ακόλουθο σημαντικότατο θεώρημα, από το οποίο συμπεραίνουμε ότι η συνάρτηση $\gamma_2(z)$ παράγει τα ring class fields για τάξεις των οποίων η διακρίνουσα δε διαιρείται από το 3.

Θεώρημα 6.4.2 Έστω $\alpha \in \mathcal{H}$ μία ρίζα της πρωταρχικής τετραγωνικής εξίσωσης $Ax^2 + Bx + C = 0$, με $3 \nmid A$ και $B \equiv 0(mod 3)$, διακρίνουσας $d(\alpha) = B^2 - 4AC = f^2 d$. Τότε ο αριθμός $\gamma_2(\alpha)$ είναι ακέραιος αλγεβρικός και, αν $3 \nmid d(\alpha)$, ισχύει

$$\mathbb{Q}(\gamma_2(\alpha)) = \mathbb{Q}(\mathcal{J}(\alpha)).$$

Απόδειξη. Θα δώσουμε μία περίληψη των βημάτων της απόδειξης. Ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στα [8] (Θεώρημα 12.2, σελ.249) και [24] (σελ.145) για μια πλήρη απόδειξη.

Καταρχάς χρησιμοποιούμε το γεγονός ότι η $\gamma_2(3z)$ είναι modular συνάρτηση ως προς την ομάδα $\Gamma_0(9)$. Στην πορεία της απόδειξης αυτού προκύπτουν και τα ακόλουθα ενδιάμεσα, χρήσιμα στοιχεία:

1. $\gamma_2(z) = q^{-1/3}\Big(1 + \sum_{n=1}^{\infty} b_n q^n\Big), \quad b_n \in \mathbb{Q},\ q = e^{2\pi i z}$,
2. $\gamma_2(z+1) = \zeta_3^{-1}\gamma_2(z)$ και
3. αν
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$
τότε
$$\gamma_2\left(\frac{az+b}{cz+d}\right) = \zeta_3^{ac-ab+a^2cd-cd}\gamma_2(z).$$

Από την Πρόταση 6.3.3 έχουμε ότι η $\gamma_2(3z)$ είναι ρητή συνάρτηση των $\mathcal{J}(z)$ και $\mathcal{J}(9z)$.

Στο επόμενο βήμα χρησιμοποιούμε το αποτέλεσμα (1) και συγκεκριμένα το γεγονός ότι το q-ανάπτυγμα της $\gamma_2(3z)$ έχει ρητούς συντελεστές. Ισχύει η ακόλουθη πρόταση:

Πρόταση 6.4.3 Έστω $f(z)$ μια modular συνάρτηση ως προς την ομάδα $\Gamma_0(N)$. Τότε:

1. Αν το q-ανάπτυγμα της $f(z)$ έχει ρητούς συντελεστές, τότε
$$f(z) \in \mathbb{Q}\Big(\mathcal{J}(z), \mathcal{J}(Nz)\Big).$$
2. Επίσης, αν η $f(z)$ είναι ολόμορφη στο $\mathcal{H}$, $z_0 \in \mathcal{H}$ και ισχύει
$$\frac{\partial \Phi_N}{\partial X}\Big(\mathcal{J}(Nz_0), \mathcal{J}(z_0)\Big) \neq 0,$$
τότε $f(z_0) \in \mathbb{Q}(\mathcal{J}(z_0), \mathcal{J}(Nz_0))$.

Απόδειξη. Βλ. [8], Θεώρημα 12.7, σελ.252-253. □

Επομένως, από το (1) της παραπάνω πρότασης προκύπτει ότι
$$\gamma_2(3z) \in \mathbb{Q}\Big(\mathcal{J}(z), \mathcal{J}(9z)\Big).$$
Εμείς θέλουμε την τιμή $\gamma_2(z_0)$ για $z_0 = \alpha$ του θεωρήματος. Συνεπώς θα πρέπει να υπολογίσουμε την $\gamma_2(3z)$ για $z := \alpha/3$.

Αποδεικνύεται ότι
$$\frac{\partial \Phi_9}{\partial X}\Big(\mathcal{J}(3\alpha), \mathcal{J}\Big(\frac{\alpha}{3}\Big)\Big) \neq 0.$$
Αφού η $\gamma_2(3z)$ είναι ολόμορφη στο $\mathcal{H}$, από το (2) της Πρότασης 6.4.3 συνεπάγεται ότι
$$\gamma_2(\alpha) \in \mathbb{Q}(\mathcal{J}([1, \alpha/3]), \mathcal{J}([1, 3\alpha])).$$

Θεωρούμε τώρα την τάξη $\mathcal{O} := [1, \alpha]$. Τότε βρίσκουμε ότι η τάξη $\mathcal{O}' = [1, 3\alpha]$ έχει δείκτη 3 στην $\mathcal{O}$ και η τάξη $[1, \alpha/3]$ είναι ένα γνήσιο κλασματικό ιδεώδες της $\mathcal{O}'$, έστω A.

Θα χρησιμοποιήσουμε το εξής: Αν $\mathcal{O}$ είναι μία τάξη του μιγαδικού τετραγωνικού σώματος αριθμών K και A είναι ένα γνήσιο (proper) κλασματικό ιδεώδες αυτής, τότε η τιμή της συνάρτησης $\mathcal{J}$, $\mathcal{J}(A)$, είναι ακέραιος αλγεβρικός και το σώμα $K(\mathcal{J}(A))$ είναι το ring class field της τάξης $\mathcal{O}$, δηλαδή
$$K(\mathcal{J}(A)) = K(\mathcal{J}(\mathcal{O})).$$

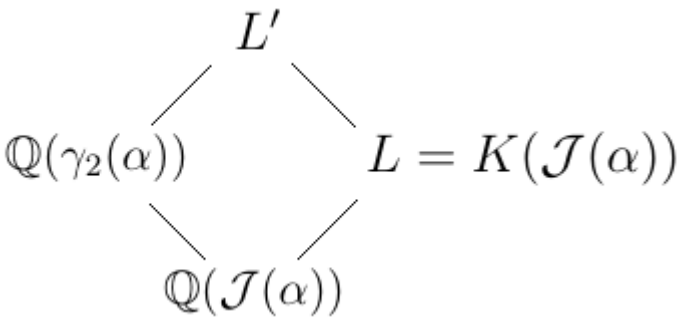
Από το παραπάνω, η τάξη $\mathcal{O}' = [1, 3\alpha]$ και το γνήσιο ιδεώδες αυτής, $A = [1, \alpha/3]$, είναι γεννήτορες του ίδιου ring class field υπέρ του τετραγωνικού μιγαδικού σώματος αριθμών K, δηλαδή του ring class field της τάξης $\mathcal{O}'$, έστω L'. Επομένως, έχουμε ότι $\gamma_2(\alpha) \in L'$.

Αν, τώρα, L είναι το ring class field της τάξης $\mathcal{O}$, ισχύει $L \leq L'$. Η $\mathcal{O}$ έχει διακρίνουσα $d(\mathcal{O}) := d(\alpha)$ και, αφού η τάξη $\mathcal{O}'$ έχει οδηγό 3 στην $\mathcal{O}$, η διακρίνουσά της είναι $d(\mathcal{O}') = 3^2 d(\alpha)$. Υπολογίζουμε τον αριθμό κλάσεων της τάξης $\mathcal{O}'$ από τον γνωστό τύπο (3.4). Έχουμε

$$h(9d(\alpha)) = \frac{3h(d(\alpha))}{[E(\mathcal{O}) : E(\mathcal{O}')]}\Big(1 - \Big(\frac{d(\alpha)}{3}\Big)\frac{1}{3}\Big).$$

Ο δείκτης $[E(\mathcal{O}) : E(\mathcal{O}')]$ ισούται με 1. Επιπλέον, αφού έχουμε υποθέσει ότι $3 \nmid d(\alpha)$, έπεται ότι $(\frac{d(\alpha)}{3}) = \pm 1$. Αυτό σημαίνει ότι είτε θα έχουμε $h(9d(\alpha)) = 2h(d(\alpha))$ ή $h(9d(\alpha)) = 4h(d(\alpha))$, δηλαδή ο βαθμός της επέκτασης $[L' : L]$ θα ισούται είτε με 2 ή με 4.

Προκύπτει, λοιπόν, το διάγραμμα Hasse του Σχήματος 6.1.



Σχήμα 6.1

Προφανώς, $[L : \mathbb{Q}(\mathcal{J}(\alpha))] = 2$. Από αυτή την παρατήρηση και το γεγονός ότι $[L' : L] = 2$ ή 4, έπεται αναγκαστικά ότι ο βαθμός $[\mathbb{Q}(\gamma_2(\alpha)) : \mathbb{Q}(\mathcal{J}(\alpha))]$ είναι δύναμη του 2. Γνωρίζουμε, όμως, ότι η $\gamma_2(\alpha)$ είναι η πραγματική κυβική ρίζα του $\mathcal{J}(\alpha)$, συνεπώς θα πρέπει να ισχύει $[\mathbb{Q}(\gamma_2(\alpha)) : \mathbb{Q}(\mathcal{J}(\alpha))] = 1$ ή 3.

Συνδυάζοντας τα προηγούμενα, έχουμε ότι $[\mathbb{Q}(\gamma_2(\alpha)) : \mathbb{Q}(\mathcal{J}(\alpha))] = 1$, δηλαδή $\mathbb{Q}(\gamma_2(\alpha)) = \mathbb{Q}(\mathcal{J}(\alpha))$, όπως θέλαμε. □

6.5 Η η-συνάρτηση του Dedekind. Οι συναρτήσεις των Weber-Schläfli

Για να είμαστε σε θέση να μελετήσουμε τις τιμές της $\mathcal{J}$ συνάρτησης, θα πρέπει να τις συσχετίσουμε με άλλες σχετικές συναρτήσεις. Μία από αυτές είναι η η-συνάρτηση του Dedekind.

Ορισμός 6.5.1 Η η-συνάρτηση του Dedekind ορίζεται από το ανάπτυγμα

$$\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n), \quad q = e^{2\pi iz},$$

για $z \in \mathcal{H}$. Το παραπάνω απειρογινόμενο συγκλίνει και δεν μηδενίζεται, καθώς $0 < |q| < 1$.

Πρόταση 6.5.2 Ισχύουν τα εξής:

1. Αν $\zeta_n = e^{2\pi i/n}$, τότε $\eta(z+1) = \zeta_{24}\eta(z)$.
2. $\eta(-\frac{1}{z}) = \sqrt{-iz}\cdot\eta(z)$.

Απόδειξη. Βλ. [8], σελ.259. □

Ορισμός 6.5.3 Οι συναρτήσεις των Weber-Schläfli ορίζονται μέσω της η-συνάρτησης του Dedekind ως εξής:

$$f(z) := \zeta_{48}^{-1}\cdot\frac{\eta(\frac{z+1}{2})}{\eta(z)}, \quad f_1(z) := \frac{\eta(\frac{z}{2})}{\eta(z)}, \quad f_2(z) := \sqrt{2}\cdot\frac{\eta(2z)}{\eta(z)}.$$

Από τον ορισμό προκύπτουν τα απειρογινόμενα

$$f(z) = q^{-1/48}\prod_{n=1}^{\infty}(1+q^{(n-1)/2}), \quad f_1(z) = q^{-1/48}\prod_{n=1}^{\infty}(1-q^{(n-1)/2})$$

και

$$f_2(z) = \sqrt{2}\cdot q^{1/24}\prod_{n=1}^{\infty}(1+q^n)$$

και αποδεικνύεται (βλ.[8], σελ.260) ότι ισχύουν οι ταυτότητες

$$f(z)f_1(z)f_2(z) = \sqrt{2} \quad \text{και} \quad f_1(2z)f_2(z) = \sqrt{2}.$$

Επίσης, ισχύουν οι σχέσεις

$$f(z+1) = \zeta_{48}^{-1}f_1(z), \quad f_1(z+1) = \zeta_{48}^{-1}f(z), \quad f_2(1+z) = \zeta_{24}f_2(z)$$

και

$$f(-1/z) = f(z), \quad f_1(-1/z) = f_2(z), \quad f_2(-1/z) = f_1(z).$$

Τέλος, αποδεικνύεται ότι

$$\Delta(z) = (2\pi)^{12}\eta(z)^{24}$$

και

$$\gamma_2(z) = \frac{f(z)^{24} - 16}{f(z)^8} = \frac{f_1(z)^{24} + 16}{f_1(z)^8} = \frac{f_2(z)^{24} + 16}{f_2(z)^8}.$$

Για την απόδειξη βλ.[8] (Θεώρημα 12.17, σελ.257).

6.6 Η απόδειξη των Heegner-Stark

Έστω K μιγαδικό τετραγωνικό σώμα αριθμών με αριθμό κλάσεων $h_K = 1$. Έχουμε δει, από το θεώρημα 4.4.1 του Landau ότι

$$h(-4n) = 1 \Leftrightarrow -4n = -4, -8, -12, -16, -28 \Leftrightarrow n = 1, 2, 3, 4, 7.$$

Στην περίπτωσή μας, η διακρίνουσα του K είναι θεμελιώδης ως διακρίνουσα σώματος. Συνεπώς, αν $d(K) \equiv 0(mod 4)$, θα έχουμε $d(K) = -4$ ή $d(K) = -8$.

Στην περίπτωση $d(K) \equiv 1(mod 4)$, έχουμε δει ότι $d(K) = -p$, όπου p πρώτος αριθμός, $p \equiv 3(mod 4)$.

Αν $p \equiv 7(mod 8)$, τότε το 2 αναλύεται στο σώμα K, αφού για το σύμβολο του Kronecker έχουμε

$$\left(\frac{-p}{2}\right) = 1.$$

Από το Θεώρημα 4.2.4 γνωρίζουμε ότι όλοι οι πρώτοι $q < \frac{p}{4}$ αδρανούν στο σώμα K. Συνεπώς, αναγκαστικά πρέπει να ισχύει

$$\frac{p}{4} \leq 2 \Rightarrow p \leq 8.$$

Από την τελευταία σχέση και το γεγονός ότι $p \equiv 7(mod 8)$ έπεται ότι

$$d(K) = -p = -7.$$

Επομένως, $K = \mathbb{Q}(\sqrt{-7})$, το οποίο πράγματι έχει αριθμό κλάσεων 1.

Θα πρέπει, λοιπόν, να υποθέσουμε τώρα ότι $p \equiv 3(mod 8)$ και να αποδείξουμε ότι, αν $h_K = 1$, τότε $p = 3, 11, 19, 43, 67, 163$. Επειδή για $p = 3$ γνωρίζουμε ότι $h_{\mathbb{Q}(\sqrt{-3})} = 1$, θα θεωρήσουμε τις διακρίνουσες με $p \equiv 3(mod 8)$ και $p \neq 3$, και θα αποδείξουμε ότι τότε

$$p = 11, 19, 43, 67, 163.$$

Πάλι από τον τύπο (3.4) προκύπτει

$$h(-4p) = 2h(-p)\left(1 - \left(\frac{-p}{2}\right)\frac{1}{2}\right) = 3.$$

Αυτό σημαίνει ότι το σώμα $\mathbb{Q}(\mathcal{J}(\sqrt{-p}))$ είναι μία κυβική επέκταση του $\mathbb{Q}$.

Θεώρημα 6.6.1 Η τιμή $f(\sqrt{-p})^2$ είναι πραγματικός αριθμός και ακέραιος αλγεβρικός, ο οποίος ανήκει στο σώμα $\mathbb{Q}(\mathcal{J}(\sqrt{-p}))$ (όπου f η συνάρτηση των Weber-Schläfli).

Απόδειξη. Βλ.[8],Θεώρημα 12.24(ii), σελ.264-268. □

Από το παραπάνω θεώρημα προκύπτει ότι

$$\mathbb{Q}(f(\sqrt{-p})^2) \leq \mathbb{Q}(\mathcal{J}(\sqrt{-p})),$$

ενώ από τη σχέση

$$\mathcal{J}(\sqrt{-p}) = \left(\frac{f(\sqrt{-p})^{24} - 16}{f(\sqrt{-p})^8}\right)^3 \tag{6.1}$$

έχουμε τελικά την ισότητα, δηλαδή

$$\mathbb{Q}(f(\sqrt{-p})^2) = \mathbb{Q}(\mathcal{J}(\sqrt{-p})).$$

Με άλλα λόγια, το $\mathbb{Q}(f(\sqrt{-p})^2)$ είναι το μέγιστο πραγματικό υπόσωμα του ring class field modulo 2.

Έστω τώρα

$$\omega = \frac{3 + \sqrt{-p}}{2}.$$

Το σύνολο $\{1, \omega\}$ αποτελεί βάση ακεραιότητας του σώματος $K = \mathbb{Q}(\sqrt{-p})$. Θέτουμε $\alpha := \zeta_8^{-1} f_2(\omega)^2$. Από τις ταυτότητες των συναρτήσεων των Weber-Schläfli ισχύουν οι σχέσεις

$$f_1(2\omega) f_2(\omega) = \sqrt{2}$$

και

$$f_1(3 + z) = \zeta_{48}^{-1} f(2 + z) = \zeta_{48}^{-2} f_1(1 + z) = \zeta_{48}^{-3} f(z),$$

όπου

$$\zeta_{48}^{-3} = (e^{\frac{2\pi i \cdot 3}{48}})^{-1} = \zeta_{16}^{-1}.$$

Επομένως,

$$f_1(2\omega) = f_1(3 + \sqrt{-p}) = \zeta_{16}^{-1} f(\sqrt{-p})$$

και άρα

$$f_2(\omega)^2 = \left(\frac{\sqrt{2}}{f_1(2\omega)}\right)^2 = \frac{2}{f_1(2\omega)^2} = \frac{2}{\zeta_{16}^{-2} f(\sqrt{-p})^2}$$

με

$$\zeta_{16}^{-2} = (e^{\frac{2\pi i \cdot 2}{16}})^{-1} = \zeta_8^{-1}.$$

Οπότε τελικά

$$\alpha = \zeta_8^{-1} \frac{2}{\zeta_8^{-1} f(\sqrt{-p})^2} = \frac{2}{f(\sqrt{-p})^2}.$$

Αυτό σημαίνει ότι το α είναι γεννήτορας της κυβικής επέκτασης $\mathbb{Q}(f(\sqrt{-p})^2)$. Συμπεραίνουμε, δηλαδή, ότι

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(f(\sqrt{-p})^2) : \mathbb{Q}] = 3.$$

Το ίδιο ισχύει και για τα στοιχεία α^2 και α^4, λόγω της σχέσης (6.1).

Τώρα, ο δακτύλιος των ακεραίων αλγεβρικών του σώματος K είναι ο $R_K = [1, \omega]$. Γνωρίζουμε ότι το σώμα κλάσεων του Hilbert του K είναι το $H = K(\mathcal{J}(\omega))$. Επειδή $h_K = 1$, προκύπτει ότι $\mathbb{Q}(\mathcal{J}(\omega)) = \mathbb{Q} \Rightarrow \mathcal{J}(\omega) \in \mathbb{Q}$ και, αφού ο $\mathcal{J}(\omega)$ είναι ακέραιος αλγεβρικός, συμπεραίνουμε ότι $\mathcal{J}(\omega) \in \mathbb{Z}$. Παρατηρούμε, επίσης, ότι το ω είναι ρίζα του πολυωνύμου

$$x^2 - 3x + \frac{p+9}{4} \in \mathbb{Z}[x],$$

το οποίο ικανοποιεί τις προϋποθέσεις του Θεωρήματος 6.4.2. Συνεπώς,

$$\mathbb{Q}(\gamma_2(\omega)) = \mathbb{Q}(\mathcal{J}(\omega)) = \mathbb{Q} \Rightarrow \gamma_2(\omega) \in \mathbb{Q}$$

και, πάλι επειδή ο $\gamma_2(\omega)$ είναι ακέραιος αλγεβρικός, έχουμε τελικά $\gamma_2(\omega) \in \mathbb{Z}$.

Τώρα,

$$\alpha^4 = (\zeta_8^{-1} f_2(\omega)^2)^4 = \zeta_8^{-4} f_2(\omega)^8 = -f_2(\omega)^8,$$

αφού

$$\zeta_8^{-4} = (e^{\frac{2\pi i}{8} \cdot 4})^{-1} = (e^{\pi i})^{-1} = -1.$$

Όμως γνωρίζουμε από την προηγούμενη παράγραφο ότι ισχύει η σχέση

$$\gamma_2(\omega) = \frac{f_2(\omega)^{24} + 16}{f_2(\omega)^8}.$$

Από τα παραπάνω προκύπτει ότι ο α^4 είναι ρίζα του μονικού πολυωνύμου

$$x^3 - \gamma_2(\omega)x - 16 \in \mathbb{Z}[x]. \tag{6.2}$$

Αυτό το αποτέλεσμα σε συνδυασμό με το γεγονός ότι ο βαθμός της επέκτασης $\mathbb{Q}(\alpha^4)/\mathbb{Q}$ ισούται με 3, μας οδηγεί στο συμπέρασμα ότι το παραπάνω πολυώνυμο είναι το ανάγωγο πολυώνυμο του α^4 υπέρ του $\mathbb{Q}$. Η διαίσθηση του Heegner ήταν ότι αυτή η παρατήρηση περιορίζει αρκετά τη μορφή των ανάγωγων (κυβικών) πολυωνύμων των α και α^2. Θα δούμε με ποιο τρόπο αμέσως παρακάτω.

Το $\alpha = \frac{2}{f(\sqrt{-p})^2}$ είναι ρίζα ενός μονικού τριτοβάθμιου πολυωνύμου με ακέραιους συντελεστές, δηλαδή είναι λύση της εξίσωσης

$$x^3 + ax^2 + bx + c = 0,\ a, b, c \in \mathbb{Z}. \tag{6.3}$$

Από την (6.3) έχουμε ότι

$$(x^3 + bx)^2 = (-ax^2 - c)^2.$$

Από εδώ συνεπάγεται ότι ο α είναι ρίζα του πολυωνύμου

$$x^6 + (2b - a^2)x^4 + (b^2 - 2ac)x^2 - c^2.$$

Επομένως, ο αριθμός α^2 επαληθεύει την εξίσωση

$$x^3 + ex^2 + fx + g = 0,$$

όπου

$$e = 2b - a^2, \quad f = b^2 - 2ac \quad \text{και} \quad g = -c^2.$$

Επαναλαμβάνοντας τη διαδικασία, καταλήγουμε στο συμπέρασμα ότι το α^4 είναι ρίζα του πολυωνύμου

$$x^3 + (2f - e^2)x^2 + (f^2 - 2eg)x - g^2.$$

Καθώς, όμως, το ανάγωγο πολυώνυμο είναι μοναδικό, κατ'ανάγκη από την (6.1) προκύπτουν οι ισότητες

$$2f = e^2, \quad f^2 - 2eg = -\gamma_2(\omega) \quad \text{και} \quad g^2 = 16.$$

Η τελευταία σχέση μας δίνει $g = \pm 4$ και, καθώς $g = -c^2$, βρίσκουμε τελικά $g = -4$ και $c = \pm 2$.

Παρατηρούμε, τώρα, ότι αν αντικαταστήσουμε το α με το $-\alpha$, τότε το α^4 παραμένει σταθερό, αλλά οι συντελεστές του πολυωνύμου a, b, c γίνονται $-a, b, -c$. Επομένως, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $c = 2$. Έτσι έχουμε

$$\gamma_2(\omega) = -f^2 - 8e = -(b^2 - 4a)^2 - 8(2b - a^2). \tag{6.4}$$

Θα καθορίσουμε πλήρως και τα a, b. Η σχέση $2f = e^2$ γράφεται

$$2(b^2 - 4a) = (2b - a^2)^2, \tag{6.5}$$

από όπου συμπεραίνουμε ότι οι αριθμοί a και b είναι άρτιοι. Αν θέσουμε

$$X = -\frac{a}{2}, \qquad Y = \frac{b - a^2}{2},$$

τότε λύνοντας ως προς a και b και αντικαθιστώντας στην (6.5) παίρνουμε τη διοφαντική εξίσωση

$$Y^2 = 2X(X^3 + 1). \tag{6.6}$$

Θα βρούμε τις ακέραιες λύσεις αυτής.

6.7 Η λύση της διοφαντικής εξίσωσης $Y^2 = 2X(X^3 + 1)$

Ισχύει ότι $(X, X^3 + 1) = 1$. Επομένως, $(2X, X^3 + 1) \mid 2 \Rightarrow (2X, X^3 + 1) = 1$ ή $(2X, X^3 + 1) = 2$.

1. Αν $(2X, X^3 + 1) = 1$, χρησιμοποιούμε την ακόλουθη πρόταση, που αποτελεί εφαρμογή του θεμελιώδους θεωρήματος της αριθμητικής:

   Πρόταση 6.7.1 Αν a, b, c ακέραιοι με $(b, c) = 1$ και υπάρχει $n \in \mathbb{N},\ n > 1$, τέτοιο ώστε $a^n = bc$, τότε υπάρχουν θετικοί ακέραιοι s, t πρώτοι μεταξύ τους τέτοιοι ώστε να ισχύει μία από τις περιπτώσεις:

   - $b = s^n,\ c = t^n$ και $a = st$,
   - $b = -s^n,\ c = -t^n$ και $a = st$.

   Απόδειξη. Βλ.[1], σελ.51. □

   Εφαρμόζοντας την παραπάνω πρόταση για την (6.6), προκύπτουν οι ακόλουθες δύο περιπτώσεις:

   (α′) $2X = Z^2,\ X^3 + 1 = W^2$ και $(Z, W) = 1$.

   (β′) $2X = -Z^2,\ X^3 + 1 = -W^2$ και $(Z, W) = 1$.

2. Αν $(2X, X^3 + 1) = 2$, παίρνουμε τις περιπτώσεις:

   (α′) $2X = 2S^2,\ X^3 + 1 = 2T^2$ και $(S, T) = 1$.

(β') $2X = -2S^2,\ X^3+1 = -2T^2$ και $(S,T) = 1$.

Θα επιλύσουμε κάθε μία από αυτές τις εξισώσεις.

Παραλείπουμε προς το παρόν την περίπτωση $1.(\alpha')$, που παρουσιάζει τη μεγαλύτερη δυσκολία, και ξεκινάμε με την περίπτωση $1.(\beta')$. Από τη σχέση $2X = -Z^2$ έπεται ότι $2 \mid X$, δηλαδή $8 \mid X^3$. Συνεπώς,

$$X^3 + 1 \equiv 1(mod 8) \Rightarrow W^2 \equiv -1 \equiv 7(mod 8).$$

Η τελευταία, όμως, ισοτιμία, δεν έχει λύση, επομένως η περίπτωση αυτή δεν μας δίνει ακέραιες λύσεις.

Παρατήρηση 6.7.2 Μία εναλλακτική μέθοδος που θα μπορούσαμε να ακολουθήσουμε είναι η εξής:

Η δεύτερη εξίσωση γράφεται: $X^3 + 1 = -W^2 \Rightarrow (-X)^3 = W^2 + 1$. Προκύπτει, δηλαδή, η διοφαντική εξίσωση

$$Y^3 = X^2 + 1$$

για $Y = -X$ και $X = W$. Θα βρούμε τις ακέραιες λύσεις της.

Έστω λοιπόν $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ μία λύση της εξίσωσης. Τότε παραγοντοποιούμε την εξίσωση στο δακτύλιο $\mathbb{Z}[i]$ ως εξής:

$$y^3 = x^2 + 1 = (x - i)(x + i),$$

όπου $x - i,\ x + i \in \mathbb{Z}[i] = \{a + bi,\ a, b, \in \mathbb{Z}\}$. Με άλλα λόγια, εργαζόμαστε στο δακτύλιο των ακεραίων αλγεβρικών του σώματος του Gauss, $\mathbb{Q}(i)$.

Η norm του τυχαίου στοιχείου $a + bi \in \mathbb{Z}[i]$ ορίζεται ως

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

Η ομάδα των μονάδων του $\mathbb{Z}[i]$ είναι η $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\} =< i >$. Ο δακτύλιος $\mathbb{Z}[i]$ με την παραπάνω norm είναι ευκλείδειος δακτύλιος, δηλαδή ΠΜΑ.

Παρατηρούμε, τώρα, ότι $2 = (-i)(1+i)^2$, όπου το στοιχείο $-i$ είναι μονάδα του δακτυλίου $\mathbb{Z}[i]$ και το $1 + i$ είναι ανάγωγο στοιχείο αυτού.

Αν $d := (x + i, x - i)$, τότε εύκολα βλέπουμε ότι $d \mid 2$. Ισχυριζόμαστε ότι $d \cong 1$ (κατά προσέγγιση μονάδας). Πράγματι, αν $d \ncong 1$, τότε $1 + i \mid d$, επομένως $1 + i \mid x + i$. Η ίδια σχέση ισχύει και για τις norm των στοιχείων αυτών:

$$N(1 + i) \mid N(x + i) \Rightarrow 2 \mid x^2 + 1 = y^3 \Rightarrow 2 \mid y \Rightarrow 8 \mid y^3 = x^2 + 1,$$

δηλαδή προκύπτει η ισοτιμία $x^2 \equiv -1(mod 8)$, η οποία όμως δεν έχει λύση, άτοπο.

Συνεπώς, $d \cong 1$. Αφού $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, η απεικόνιση

$$\varphi : E(\mathbb{Z}[i]) \to E(\mathbb{Z}[i])$$

με $\varphi(\varepsilon) = \varepsilon^3$ είναι αυτομορφισμός ομάδων. Τελικά, έχουμε ότι

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

με $a + bi \in \mathbb{Z}[i]$, οπότε βρίσκουμε $1 = b(3a^2 - b^2) \Rightarrow b = \pm 1$ και $3a^2 - 1 = \pm 1 \Rightarrow a = 0$. Τέλος, από την $x = a(a^2 - 3b^2)$ έπεται ότι $x = 0$ και άρα $y = 1$.

Βρήκαμε έτσι τη μοναδική ακέραια λύση της διοφαντικής εξίσωσης, $(X, Y) = (0, 1)$. Αυτό σημαίνει ότι η $X^3 + 1 = -W^2$ έχει μοναδική λύση την $(X, W) = (-1, 0)$, που όμως δεν επαληθεύει την $2X = -Z^2$.

Συνεχίζουμε με την περίπτωση $2.(\alpha')$. Έχουμε ότι $X = S^2$ και $X^3 + 1 = 2T^2$. Η δεύτερη εξίσωση, συνεπώς, γίνεται

$$S^6 + 1 = 2T^2 \Rightarrow (S^2 + 1)(S^4 - S^2 + 1) = 2T^2.$$

Παρατηρούμε εδώ ότι ο πρώτος παράγοντας θα πρέπει αναγκαστικά να είναι άρτιος και ο δεύτερος περιττός. Επίσης,

$$S^4 - S^2 + 1 = (S^2 + 1)^2 - 3(S^2 + 1) + 3,$$

άρα αν d είναι ο μέγιστος κοινός διαιρέτης των $S^2 + 1$ και $S^4 - S^2 + 1$, τότε κατ'ανάγκη θα ισχύει $d \mid 3$. Όμως εύκολα βλέπουμε ότι $S^2 + 1 \not\equiv 0(mod 3)$, συνεπώς ο d θα ισούται με 1. Πάλι από την Πρόταση 6.7.1 και το γεγονός ότι ο $S^4 - S^2 + 1$ είναι πάντα θετικός αριθμός, έπεται ότι $S^4 - S^2 + 1 = B^2$.

Παρατηρούμε, όμως, ότι για $S^2 > 1$ ισχύει

$$(S^2 - 1)^2 < S^4 - S^2 + 1 < (S^2)^2.$$

Συνεπώς, ο $S^4 - S^2 + 1$ δεν μπορεί να είναι τέλειο τετράγωνο για αυτές τις τιμές του S. Απομένει, συνεπώς, να ελέγξουμε τις τιμές $S = 0, \pm 1$. Από αυτές δίνουν λύση της αρχικής εξίσωσης $S^6 + 1 = 2T^2$ μόνο οι $S = \pm 1$. Συγκεκριμένα, προκύπτουν οι ακέραιες λύσεις

$$(S, T) = (\pm 1, \pm 1).$$

Στην περίπτωση, τώρα, $2.(\beta')$, προκύπτει η εξίσωση

$$S^6 = 1 + 2T^2.$$

Εδώ θα εργαστούμε στο σώμα $K = \mathbb{Q}(\sqrt{-2})$. Γνωρίζουμε ότι $h_K = 1$ και ότι ο δακτύλιος των ακεραίων αλγεβρικών του σώματος είναι ο

$$R_K = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2}, \quad a, b \in \mathbb{Z}\}.$$

Ο R_K είναι ΠΚΙ, συνεπώς και ΠΜΑ. Έχουμε, έτσι, την παραγοντοποίηση

$$(S^2)^3 = (1 + T\sqrt{-2})(1 - T\sqrt{-2}).$$

Έστω $d := (1 + T\sqrt{-2}, 1 - T\sqrt{-2})$. Παρατηρούμε ότι, αφού $d|_{R_K} 1 + T\sqrt{-2}$ και $d|_{R_K} 1 - T\sqrt{-2}$, τότε κατ'ανάγκη ισχύει ότι $d \mid 2$.

Ισχυριζόμαστε τώρα ότι $d \cong 1$ (κατά προσέγγιση μονάδας). Πράγματι, αν $d \ncong 1$, τότε αφού το 2 γράφεται ως $-(\sqrt{-2})^2$ στον R_K και το $\sqrt{-2}$ είναι ανάγωγο στοιχείο αυτού, προκύπτει ότι $\sqrt{-2} \mid d$. Αυτό, όμως, είναι άτοπο, αφού εύκολα βλέπουμε ότι το στοιχείο $\sqrt{-2}$ δεν διαιρεί τα $1 + T\sqrt{-2}$ και $1 - T\sqrt{-2}$. Επομένως, $d \cong 1$.

Η ομάδα των μονάδων του R_K είναι η $E(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$. Επομένως, η απεικόνιση $\varphi : E(\mathbb{Z}[\sqrt{-2}]) \to E(\mathbb{Z}[\sqrt{-2}])$ με $\varphi(\varepsilon) = \varepsilon^3$ είναι ένας αυτομορφισμός ομάδων. Τελικά, έχουμε ότι

$$1 + T\sqrt{-2} = (a + b\sqrt{-2})^3 = a(a^2 - 6b^2) + \sqrt{-2} \cdot b(3a^2 - 2b^2).$$

Επομένως, προκύπτουν οι σχέσεις

$$1 = a(a^2 - 6b^2) \quad \text{και} \quad T = b(3a^2 - 2b^2),$$

από όπου έπεται ότι $a = \pm 1$. Για $a = -1$ έχουμε ότι $1 - 6b^2 = -1$, δηλαδή $3b^2 = 1$, το οποίο είναι αδύνατο, καθώς $b \in \mathbb{Z}$. Επομένως, $a = 1$ και άρα $b = 0$. Για αυτές τις τιμές των a και b βρίσκουμε τις ακέραιες λύσεις

$$(S, T) = (\pm 1, 0).$$

Πάμε τώρα στην περίπτωση $1.(\alpha')$. Η εξίσωση

$$W^2 = X^3 + 1 \tag{6.7}$$

λύθηκε από τον Euler το 1738. Συγκεκριμένα, ο Euler, χρησιμοποιώντας τη μέθοδο της καθόδου του Fermat, απέδειξε ότι οι μοναδικές *ρητές* (όχι απλά ακέραιες) λύσεις της εξίσωσης είναι οι

$$(X, W) = (-1, 0), (0, \pm 1), (2, \pm 3).$$

Εμείς στα πλαίσια αυτής της εργασίας θα αποδείξουμε ότι αυτές είναι οι μοναδικές ακέραιες λύσεις της εξίσωσης (6.7).

Η (6.7) γράφεται

$$X^3 = W^2 - 1 = (W-1)(W+1).$$

Ισχύει ότι $d = (W-1, W+1) \mid 2$, επομένως $d = 1$ ή $d = 2$. Ξεχωρίζουμε δύο περιπτώσεις:

1. Υποθέτουμε ότι ο W είναι άρτιος. Σε αυτή την περίπτωση έχουμε ότι $d = 1$, επομένως από την Πρόταση 6.7.1 προκύπτουν $W + 1 = A^3$ και $W - 1 = B^3$, δηλαδή παίρνουμε την εξίσωση

   $$A^3 - B^3 = 2.^3$$

   Οι μοναδικές τρίτες δυνάμεις που διαφέρουν κατά δύο είναι το 1 και το -1, συνεπώς βρίσκουμε $A = 1$ και $B = -1$. Από την περίπτωση αυτή βρίσκουμε, λοιπόν, την ακέραια λύση

   $$(X, W) = (-1, 0).$$

2. Υποθέτουμε τώρα ότι ο W είναι περιττός, οπότε $d = 2$ και αναγκαστικά ο X είναι άρτιος. Αφού ο W είναι περιττός, θα ισχύει $W \equiv 1$ ή $3(mod 4)$. Καθώς, όμως, η (x, w) είναι λύση της εξίσωσης (6.7) ακριβώς όταν και η $(x, -w)$ είναι λύση, χωρίς βλάβη της γενικότητας αρκεί να υποθέσουμε ότι $W \equiv 1(mod 4)$. Σε αυτή την περίπτωση έπεται ότι $W + 1 \equiv 2(mod 4)$ και $W - 1 \equiv 0(mod 4)$.

   Γράφουμε την εξίσωση στη μορφή

   $$\left(\frac{X}{2}\right)^3 = \frac{W+1}{2} \cdot \frac{W-1}{4}.$$

   Αφού $(W + 1, W - 1) = 2$, προκύπτει

   $$\left(\frac{W+1}{2}, \frac{W-1}{2}\right) = 1 \Rightarrow \left(\frac{W+1}{2}, \frac{W-1}{4}\right) = 1.$$

   Επομένως, πάλι από την Πρόταση 6.7.1, έχουμε ότι

   $$\frac{W+1}{2} = A^3, \quad \frac{W-1}{4} = B^3, \quad A, B \in \mathbb{Z}.$$

[3] Φυσικά θα έπρεπε να θεωρήσουμε και την περίπτωση $W + 1 = -A^3$, $W - 1 = -B^3$. Καθώς, όμως, ισχύουν $-A^3 = (-A)^3$ και $-B^3 = (-B)^3$, τελικά προκύπτει η ίδια μορφή εξίσωσης, επομένως δεν χρειάζεται να λάβουμε αυτή την περίπτωση υπόψην.

Από τις παραπάνω σχέσεις παίρνουμε την εξίσωση

$$A^3 - 2B^3 = 1.$$

Αυτή έχει προφανείς λύσεις τις

$$(A, B) = (1, 0) \quad \text{και} \quad (-1, -1),$$

από τις οποίες βρίσκουμε τις

$$(X, W) = (0, 1) \quad \text{και} \quad (2, -3).$$

Παίρνοντας και τις αρνητικές τιμές του W για $W \equiv 3(mod 4)$ έχουμε και τις λύσεις

$$(X, W) = (0, -1) \quad \text{και} \quad (2, 3).$$

Συμπεραίνουμε, λοιπόν, ότι αν η εξίσωση $A^3 - 2B^3 = 1$ έχει μόνο τις λύσεις $(A, B) = (1, 0)$ και $(-1, -1)$, τότε η εξίσωση (6.7) έχει μόνο τις τέσσερις λύσεις που υπολογίσαμε παραπάνω.

Θα χρησιμοποιήσουμε εδώ το ακόλουθο θεώρημα των Delaunay-Nagell.

Θεώρημα 6.7.3 Η εξίσωση

$$X^3 + dY^3 = 1,$$

όπου $d > 0$ και ελεύθερο κύβων, έχει, εκτός από την προφανή λύση $(X, Y) = (1, 0)$, το πολύ μία ακόμα ακέραια λύση.

Προφανώς, το θεώρημα ισχύει και για $d < 0$, αφού σε κάθε λύση (x, y) της $X^3 + dY^3 = 1$ αντιστοιχεί ακριβώς μία λύση $(x, -y)$ της $X^3 - dY^3 = 1$.

Με βάση τα παραπάνω, η εξίσωση $A^3 - 2B^3 = 1$ έχει το πολύ δύο ακέραιες λύσεις. Καθώς εμείς έχουμε ήδη βρει δύο, δεν υπάρχουν άλλες. Συνεπώς, οι λύσεις της εξίσωσης (6.7) είναι οι τέσσερις λύσεις που βρήκαμε παραπάνω.

Παρατήρηση 6.7.4 Αντί να χρησιμοποιήσουμε το θεώρημα των Delaunay - Nagell, μπορούμε να αποδείξουμε απευθείας ότι η διοφαντική εξίσωση $A^3 - 2B^3 = \pm 1$ έχει ακριβώς τις ακέραιες λύσεις

$$(A, B) = (1, 0), (-1, 0), (1, 1) \quad \text{και} \quad (-1, -1).$$

Εργαζόμαστε στο καθαρά κυβικό αλγεβρικό σώμα αριθμών $K = \mathbb{Q}(\sqrt[3]{2})$. Μία βάση ακεραιότητας του σώματος είναι το σύνολο $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, επομένως ο δακτύλιος των ακέραιων αλγεβρικών είναι ο $R_K = \mathbb{Z}[\sqrt[3]{2}]$ (βλ.[18], σελ.206). Το ανάγωγο πολυώνυμο

$$Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$$

έχει μία πραγματική και δύο μιγαδικές ρίζες. Συνεπώς, η ταυτότητά του είναι ίση με $[r_1, r_2] = [1, 1]$. Από το θεώρημα μονάδων του Dirichlet (Θεώρημα 2.4.4) προκύπτει ότι η ομάδα των μονάδων του δακτυλίου έχει rank $r_1 + r_2 - 1 = 1$. Συμπεραίνουμε ότι

$$E(R_K) = \{\pm 1\} \times < \varepsilon_0 >,$$

όπου ε_0 μία θεμελιώδης μονάδα. Αποδεικνύεται (βλ.[18], σελ.206) ότι $\varepsilon_0 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$, αλλά εμείς προτιμούμε να εργαστούμε με την $\eta := \varepsilon_0^{-1} = \sqrt[3]{2} - 1$. Τα παραπάνω θα αποβούν χρήσιμα στην πορεία, αφού ισχύει

$$N_K(A - B\sqrt[3]{2}) = A^3 - 2B^3.$$

Συνεπώς, αν $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ είναι μία λύση της $A^3 - 2B^3 = 1$, τότε $N_K(x - y\sqrt[3]{2}) = 1$, δηλαδή ο $x - y\sqrt[3]{2}$ είναι μονάδα του δακτυλίου R_K. Αυτό σημαίνει ότι

$$x - y\sqrt[3]{2} = \pm(\sqrt[3]{2} - 1)^k, \quad k \in \mathbb{Z}.$$

Επομένως, θα πρέπει να ελέγξουμε για ποιους ακεραίους k η δύναμη του δεξιού μέλους μας δίνει μονάδα της οποίας ο συντελεστής του $\sqrt[3]{4}$ είναι 0. Αποδεικνύεται (βλ.[18], σελ.209-210) ότι αυτό ισχύει μόνο για $k = 0$ και $k = 1$. Από την πρώτη περίπτωση έχουμε $(x, y) = (1, 0)$ ή $(-1, 0)$, ενώ η δεύτερη περίπτωση μας δίνει $(x, y) = (-1, -1)$ ή $(1, 1)$.

Συγκεντρώνοντας όλα τα παραπάνω, έχουμε αποδείξει ότι όλες οι ακέραιες λύσεις της διοφαντικής εξίσωσης

$$Y^2 = 2X(X^3 + 1)$$

είναι οι

$$(X, Y) = (0, 0), (-1, 0), (1, \pm 2) \quad \text{και} \quad (2, \pm 6).$$

Παρατήρηση 6.7.5 Εναλλακτικά, μπορούμε επίσης να γράψουμε την εξίσωση στη μορφή

$$Y^2 = 2X(X^3 + 1) = 2X(X + 1)(X + \omega)(X + \omega^2),$$

όπου ω πρωταρχική 3η ρίζα της μονάδας, και στη συνέχεια να χρησιμοποιήσουμε την αριθμητική του αλγεβρικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{-3})$.

Επιστρέφουμε τώρα στη σχέση

$$\gamma_2(\omega) = -(b^2 - 4a)^2 - 8(2b - a^2).$$

X	Y	$a=-2X$	$b=4X^2+2Y$	$\gamma_2(\omega)$
0	0	0	0	0
-1	0	2	4	-96
1	2	-2	8	-5280
1	-2	-2	0	-32
2	6	-4	28	-640320
2	-6	-4	4	-960

Πίνακας 6.1: Οι τιμές της $\gamma_2(\omega)=-(b^2-4a)^2-8(2b-a^2)$.

Ο Πίνακας 6.1 μας δίνει τις τιμές της $\gamma_2(\omega)$ με βάση όλους τους προηγούμενους υπολογισμούς μας.

Αναφέρουμε, επίσης, ενδεικτικά, ότι οι τιμές της $\gamma_2(\omega)$ για $p=4,7,8$ είναι αντίστοιχα $12,-15$ και 20.

Έχουμε, τελικά, 6 τιμές για τη $\gamma_2(\omega)$ και συνεπώς 6 τιμές για την $\mathcal{J}(\omega)$. Αυτό σημαίνει ότι, επιπλέον των τριών που είχαμε ήδη βρει, δηλαδή των $\mathbb{Q}(\sqrt{-p})$ για $p=4,7,8$, υπάρχουν το πολύ άλλα 6 τετραγωνικά σώματα αριθμών με διακρίνουσα $p\equiv 3(mod 8)$ και αριθμό κλάσεων ίσο με 1. Εμείς, όμως, γνωρίζουμε ακριβώς 6, τα $\mathbb{Q}(\sqrt{-p})$ με $p=3,11,19,43,67,163$. Συνεπώς, *αυτά είναι όλα*!

Αξίζει, τέλος, να προσθέσουμε ότι, με βάση τους υπολογισμούς του, ο Gauss διατύπωσε επίσης την ακόλουθη **εικασία**:

Υπάρχουν άπειρα πραγματικά τετραγωνικά σώματα αριθμών $K=\mathbb{Q}(\sqrt{d})$, με αριθμό κλάσεων ιδεωδών $h_K=1$.

Η εικασία αυτή είναι μέχρι σήμερα *ανοικτή*.

6.8 Σημειώσεις

Για το θεώρημα των Heegner - Stark:

Η πρώτη απόδειξη του προβλήματος του Gauss για τον αριθμό κλάσεων δόθηκε από τον Heegner το 1952 στο άρθρο του (βλ.[13]). Η απόδειξη, όμως, αυτή δεν έγινε αποδεκτή ως σωστή από τη Μαθηματική κοινότητα. Αυτό οφείλεται σε δύο λόγους. Ο πρώτος αφορά στο στυλ του συγγραφέα. Είναι χαρακτηριστικά τα λόγια του Bruno Schoeneberg στο review του για το άρθρο του Heegner στο περιοδικό Zentralblatt:

"*Es sei jedoch bemerkt, daß die Beweise dem Ref. an mehreren Stellen unverständlich sind.*"(Πρέπει, όμως, να παρατηρήσουμε ότι οι αποδείξεις του

άρθρου σε αρκετά σημεία είναι ακατανόητες.)

Ο δεύτερος λόγος είναι το γεγονός ότι στην εργασία του ο Heegner αναφέρεται και παραπέμπει στο βιβλίου του Weber, Lehrbuch der Algebra (βλ.[29]). Το πρόβλημα έπεται από τα λεγόμενα του Weber στην παράγραφο 127, σελ.472 του βιβλίου:

"*Wenn wir einer durch alle Beispiele bestätigten Induktion vertrauen dürfen, so besteht noch das folgende Theorem:*

8) Ist $m \equiv 3(mod 8)$, *so ist* $f(\omega)^3$ *Klassen-invariante.*

Indessen fehlt hier für noch der allgemeine Beweis."

(Σε περίπτωση που μπορούμε να θεωρήσουμε δεδομένη την επαγωγή μέσω των παραδειγμάτων, ισχύει το παρακάτω θεώρημα:

8) Αν $m \equiv 3(mod 8)$, τότε η $f(\omega)^3$ είναι αναλλοίωτη.

Παρόλα αυτά, εδώ εκρεμμεί η γενική απόδειξη.)

Ο Heegner, όμως, όπως αποδείχθηκε αργότερα, αν και αναφέρεται στην εργασία του στην παραπάνω πρόταση, δεν την χρησιμοποιεί για την απόδειξη του θεωρήματος.

Η απόδειξη του Stark (βλ.[27]) είναι η πρώτη αναγνωρισμένη σωστή απόδειξη. Παρόλο που είναι αρκετά υπολογιστικής μορφής ("Stark's proof involved rather messy computations", βλ.[16], σελ.275), ο Stark καταλήγει τελικά στην ίδια διοφαντική εξίσωση που είχε καταλήξει και ο Heegner.

Υπάρχει πολύ ενδιαφέρουσα εξέλιξη του προβλήματος, τόσο πριν την τελική απόδειξη του θεωρήματος των Heegner - Stark όσο και στη συνέχεια, μέχρι σήμερα. Παρόλα αυτά, στο πλαίσιο της παρούσης εργασίας δεν θα επεκταθούμε περισσότερο.

Για τη διοφαντική εξίσωση $Y^2 = X^3 + 1$*:*

Η διοφαντική εξίσωση $Y^2 = X^3 + 1$ έχει, όπως είδαμε, τις προφανείς ακέραιες λύσεις $(X, Y) = (-1, 0), (0, \pm 1)$ και την $(2, \pm 3)$. Ο Euler απέδειξε το 1738 ότι αυτές είναι οι *μοναδικές ρητές* λύσεις της εξίσωσης, συνεπώς και οι μόνες ακέραιες. Προς τούτο, χρησιμοποιεί τη μέθοδο της καθόδου του Fermat. Εικάζεται ότι αν ο Fermat είχε ήδη λύσει την εξίσωση αυτή, σίγουρα θα το είχε κάνει όπως ο Euler.

Η απόδειξη του Euler περιέχεται στις ασκήσεις 12.28 και 12.29 του βιβλίου του Cox (βλ.[8]). Περιλαμβάνεται, επίσης, στη μεταπτυχιακή εργασία της Yukako Kezuka (βλ.[30]).

Ο R. Fueter στο άρθρο του (βλ.[10] ,σελ.80) αποδεικνύει ότι η διοφαντική εξίσωση $X^3 - Y^2 = D$ έχει είτε άπειρες ή καμία ρητή λύση, εκτός από τις περιπτώσεις $D = -1$ και $D = 432$, οπότε υπάρχει ακριβώς μία ακόμα λύση, αν δεν λογαριάσουμε το πρόσημο του Y. Για $D = -1$, αυτή είναι η $(2, \pm 3)$. Κατά τον M. Deuring (βλ.[9], σελ.178), φαίνεται ότι η εργασία του Fueter αποτέλεσε αφετηρία της εργασίας του Heegner.

Φυσικά, σήμερα μπορεί κανείς να χρησιμοποιήσει διάφορα υπολογιστικά προγράμματα για τον υπολογισμό των λύσεων. Ένα παράδειγμα αποτελεί το πρόγραμμα SAGE (https://sagecell.sagemath.org/), με τη χρήση του οποίου έχουμε την απάντηση σε λιγότερο από *ένα* δευτερόλεπτο!

```
In [1]:  1  E=EllipticCurve([0,1])

In [2]:  1  E

Out[2]: Elliptic Curve defined by y^2 = x^3 + 1 over Rational Field

In [3]:  1  E.integral_points()

Out[3]: [(-1 : 0 : 1), (0 : 1 : 1), (2 : 3 : 1)]
```

Σχήμα 6.2: Η λύση της εξίσωσης $Y^2 = X^3 + 1$ με το πρόγραμμα SAGE.

Βιβλιογραφία

[1] Αντωνιάδης Ι. Α. και Κοντογεώργης Α. *Θεωρία Αριθμών και Εφαρμογές*. Αποθετήριο Κάλλιπος, 2015.

[2] Αντωνιάδης Ι. Α. *Αλγεβρική Θεωρία Αριθμών*. Σημειώσεις, Ηράκλειο, 1984.

[3] Λάκκης Κ. *Θεωρία Αριθμών*. Εκδόσεις Ζήτη, Θεσσαλονίκη, 1988.

[4] Apostol T. M. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag, Berlin, 1976.

[5] Ayoub R. G. and Chowla S. On Euler's Polynomial. *Journal of Number Theory*, 13:443–445, 1981.

[6] Borevich Z. I. and Shafarevich I. R. *Number Theory*. Academic Press, New York, 1966.

[7] Connell I. G. On algebraic number fields with unique factorization. *Canadian Mathematical Bulletin*, 5:151–166, 1962.

[8] Cox D.A. *Primes of the Form $x^2 + ny^2$*. Wiley-Interscience, New York, 1989.

[9] Deuring M. Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins. *Inventiones Math.*, 5:169–179, 1968.

[10] Fueter R. *Über kubische diophantische Gleichungen*. *Comment. Math. Helvet.*, 2:69–89, 1930.

[11] Gauss C. F. *Disquisitiones Arithmeticae*. Springer, New York, 1986.

[12] Hasse H. *Über den Klassenkörper zum quadratischen Zahlkörper mit der Discriminante -47*. *Acta Arithmetica*, 9:419–434, 1964.

[13] Heegner K. Diophantische Analysis und Modulfunktionen. *Math. Zeit*, 56:227–253, 1952.

[14] Herz C. S. Construction of Class Fields. *LNM*, 21, 1966.

[15] Hunter J. *Number Theory.* Μετάφραση στα Ελληνικά Ν. Κρητικού, Αθήνα, 1981.

[16] Narkiewicz W. *Classical Problems in Number Theory.* PWN, Warszawa, 1986.

[17] Narkiewicz W. *Elementary and Analytic Theory of Algebraic Numbers.* Springer-Verlag, Berlin, 1990.

[18] Pollak P. *A Conversational Introduction to Algebraic Number Theory, Arithmetic beyond* $\mathbb{Z}$. AMS (Student Mathematical Library Vol.84), Providence, USA, 2017.

[19] Rabinowitsch G. Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. *Journal für die reine und angewandte Mathematik*, 142:153–164, 1913.

[20] Ribenboim P. *Algebraic Numbers.* Wiley-Interscience, New York, 1972.

[21] Ribenboim P. Euler's famous prime generating polynomial and the class number of imaginary quadratic fields. *L' Enseignement Mathematique*, 34:23–42, 1988.

[22] Ribenboim P. *Die Welt der Primzahlen, Geheimnisse und Recorde.* Springer-Verlag, Berlin, 2006.

[23] Scharlau W. and Opolka H. *From Fermat to Minkowski.* Springer-Verlag, New York, 1925.

[24] Schertz R. *Complex Multiplication.* CUP, Cambridge, 2010.

[25] Serre J-P. *Lectures on the Mordell - Weil Theorem.* Vieweg, Braunschweig, 1990.

[26] Siegel C. L. *Über die Classenzahl quadratischer Zahlkörper*. *Acta Arithmetica*, 1:83–86, 1935.

[27] Stark H. M. A complete determination of the complex quadratic fields of class number one. *Michigan Math. J.*, 14:1–27, 1967.

[28] Szekerers G. On the number of divisors of x^2+x+A. *Journal of Number Theory*, 6:434–442, 1974.

[29] Weber H. *Lehrbuch der Algebra, Vol.3.* 2^{nd} edition, Braunschweig, 1908. (Reprint by Chelsea, New York, 1961).

[30] Yukako Kezuka. The Class Number Problem, London, 2012.

[31] Zagier D. B. *Zetafunktionen und quadratische Körper, eine Einführung in die höhere Zahlentheorie.* Springer-Verlag, Berlin, 1981.