Παράσταση Δυνάμεων Πρώτων Αριθμών Μέσω Δυαδικών Τετραγωνικών Μορφών

Διδακτορική Διατριβή

Γιώργος Συλλιγάρδος

Μαθηματικό τμήμα Πανεπιστημίου Κρήτης

e-mail: siligard@poseidon.math.uch.gr

Η παρούσα διατριβή εκπονήθηκε και με οικονομική ενίσχυση

του Ιδρύματος Κρατικών Υποτροφιών (Ι.Κ.Υ.)

Επιβλέπων καθηγητής Γιάννης Α. Αντωνιάδης

Στους γονείς μου

Διασυνιά και Μανώλη

Συμβολισμοί

Σε όλο το παρόν κείμενο, με i θα συμβολίζουμε την φανταστική μονάδα. Με ζ_n θα συμβολίζουμε την πρωταρχική ρίζα της μονάδας $e^{\frac{2\pi i}{n}}$, $n \in \mathbb{N}$ ενώ το ζ_3 συχνά θα συμβολίζεται και ως ω. Αν $\mathbb{Q}(\sqrt{m})$ πραγματικό σώμα αριθμών με ε_m θα συμβολίζουμε την θεμελιώδη μονάδα του. Για ένα δακτύλιο R συμβολίζουμε με $R^\times$ την πολλαπλασιαστική ομάδα των μονάδων του. Αν F ένα αλγεβρικό σώμα αριθμών με R_F θα συμβολίζουμε τον δακτύλιο των ακεραίων αλγεβρικών αυτού και για κάθε ιδεώδες $\mathfrak{a} \lhd F$ του R_F ή $\alpha \in R_F$ με $N_F(\mathfrak{a})$, $N_F(\alpha)$ θα συμβολίζουμε τις αντίστοιχες απόλυτες (δηλαδή ως προς το $\mathbb{Q}$) norms. Αν F'/F είναι Galois επέκταση αλγεβρικών σωμάτων αριθμών,με $G(F'/F)$ θα συμβολίζουμε την αντίστοιχη ομάδα Galois και, αν επιπλέον η F'/F είναι αβελιανή και $\mathfrak{p}$ είναι πρώτο ιδεώδες του F τότε με $[\frac{F'|F}{\mathfrak{p}}]$ θα συμβολίζουμε το σύμβολο του Artin για τον πρώτο $\mathfrak{p}$. Για μια επέκταση του Galois αλγεβρικών σωμάτων αριθμών F'/F και ένα πρώτο $\mathfrak{p}$ του F με $spl_{\mathfrak{p}}(F'/F)$ θα συμβολίζουμε το σώμα ανάλυσης του $\mathfrak{p}$ στην F'/F. Επιπλέον, αν ο $\mathfrak{p}$ δεν διακλαδίζεται στην F'/F με $f_{\mathfrak{p}}(F'/F)$ θα συμβολίζουμε με τον κοινό βαθμό αδρανείας όλων των πρώτων του F' πανω από το $\mathfrak{p}$ στην F'/F και όταν $F = \mathbb{Q}$, χάριν απλότητας, θα συμβολίζουμε το $f_{p\mathbb{Z}}(F'/\mathbb{Q})$ με $f_p(F')$ και το $spl_{p\mathbb{Z}}(F'/\mathbb{Q})$ με $spl_p(F')$. Αν F είναι σώμα αριθμών, $\mathfrak{p}$ ένας πεπερασμένος πρώτος του F, $\alpha \in R_F$ και $n \in \mathbb{N}$ με $\mathfrak{p} \nmid \alpha n$, $\zeta_n \in F$ τότε το $(\frac{\alpha}{\mathfrak{p}})_n$ θα συμβολίζει το n-στού βαθμού σύμβολο του **Legendre** . Δηλαδή το $(\frac{\alpha}{\mathfrak{p}})_n$ ορίζεται σαν η μοναδική n- ρίζα της μονάδας τέτοια ώστε $\alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv (\frac{\alpha}{\mathfrak{p}})_n (\mathrm{mod}\mathfrak{p})$. Είναι γνωστό ότι (βλ. [3] άσκηση 5.13):

$$(\frac{\alpha}{\mathfrak{p}})_n = 1 \quad \text{αν και μόνο αν η} \quad \alpha \equiv x^n (\mathrm{mod}\mathfrak{p}) \quad \text{είναι επιλύσιμη στον} \quad R_F$$

Για την περίπτωση $n = 2$ θα παραλείπουμε τον δείκτη n.

Έστω D ένας, ελεύθερος τετραγώνου, αρνητικός ακέραιος τέτοιος ώστε $D \equiv 0, 1 (\mathrm{mod} 8)$. Γράφουμε $D = f^2 D_0$, όπου D_0 θεμελιώδης διακρίνουσα και $f \in \mathbb{N}$. Με $H(D)$ Θα συμβολίζουμε την ομάδα κλάσεων όλων των θετικά ορισμένων πρωταρχικών δυαδικών τετραγωνικών μορφών διακρίνουσας D και με $\hbar(D)$ (η απλά $\hbar$) την τάξη της $H(D)$. Έστω $k = \mathbb{Q}(\sqrt{D_0})$. Με $k(D)$ θα συμβολίζουμε το ring class field modulo f του k. Από την θεωρία κλάσεων σωμάτων έχουμε, μέσω του συμβόλου του Artin, τους ακόλουθους ισομορφισμούς :

$$H(D) \stackrel{\simeq}{\longleftrightarrow} \frac{I_k(f)}{P_{k,\mathbb{Z}}(f)} \stackrel{\simeq}{\longleftrightarrow} G(k(D)/k).$$

Εδώ $I_k(f)$ είναι η ομάδα όλων των ιδεωδών του k που είναι πρώτα προς το f και $P_{k,\mathbb{Z}}(f)$ είναι η υποομάδα των κυρίων ιδεωδών aR_k της $I_k(f)$ όπου $a \in (\mathbb{Z} + fR_k)$. Μέσω των παραπάνω ισομορφισμών η εικόνα ενός $C \in H(D)$ αντιστοιχεί στο σύμβολο του Artin $[\frac{k(D)|k}{C}]$. Έστω τώρα e ένας θετικός ακέραιος. Με $H_e(D)$ θα συμβολίζουμε το γινόμενο όλων των q-Sylow υποομάδων του $H(D)$ για όλους τους πρώτους διαιρέτες q του e και με $\hbar_e(D)$ (ή απλά $\hbar_e$) την τάξη του. Έστω $H(D) \cong H_e(D) \times H'_e(D)$. Με $\hbar'_e(D)$ (ή απλά $\hbar'_e$) θα συμβολίζουμε την τάξη του $H'_e(D)$ και επομένως $(\hbar'_e, e) = 1$. Με $k_e(D)$ θα συμβολίζουμε το υπόσωμα του σώματος $k(D)$ το οποίο αντιστοιχεί στην ομάδα $H'_e(D)$. Συνεπώς το σώμα $k_e(D)$ είναι επέκταση βαθμού $\hbar_e$ πάνω από το k το οποίο περιέχει όλα τα ενδιάμεσα σώματα της $k(D)/k$ των οποίων ο βαθμός πάνω από το k διαιρεί το $\hbar_e$. Είναι προφανές ότι τα $H_e(D)$, $k_e(D)$ κλπ. εξαρτώνται μόνο από το σύνολο των πρώτων διαιρετών του e και όχι από τους εκθέτες με τους οποίους εμφανίζονται στην ανάλυση πρώτων του e στο $\mathbb{Z}$. Αν H είναι μια υποομάδα της $H_e(D)$, με $L_H^{(e)}$ θα συμβολίζουμε το σώμα που αντιστοιχεί στην H μέσω αντιστοιχίας Galois στην $k_e(D)$ και, αν $H = \langle C_1, C_2, ..., C_r \rangle$, τότε το σώμα $L_H^{(e)}$ θα το συμβολίζουμε με $L^{(e)}_{C_1, C_2, \cdots, C_r}$. Τέλος, για ένα στοιχείο C της $H(D)$ και ένα ακέραιο m, η παράσταση $C \longrightarrow m$ θα δείχνει ότι ο m παρίσταται από την C και όταν γράφουμε για μία ομάδα G ότι: $G = (m_1, m_2, ..., m_l)$ θα εννοούμε ότι η G είναι αβελιανή και παράγεται από l στοιχεία τάξεων m_1, m_2, ..., m_l αντίστοιχα.

Περιεχόμενα

Εισαγωγή

Ιστορικά, η μελέτη παράστασης αριθμών μέσω δυαδικών τετραγωνικών μορφών, δηλαδή μέσω μορφών του τύπου: $ax^2+bxy+cy^2$ όπου $a,b,c \in \mathbb{Z}$, παραπέμπει σε εργασίες και μελέτες του Fermat. O Fermat σε ένα γράμμα του το 1640 στον Mersenne αναφέρεται στην παράσταση πρώτων αριθμών από την μορφή x^2+y^2, και σε κατοπινά γράμματα του προς το Pascal το 1654 αναφέρεται στην παράσταση πρώτων αριθμών από τις μορφές x^2+2y^2, x^2+3y^2. Πάνω στα αποτελέσματα και τις εικασίες του Fermat εργάστηκε αργότερα ο Euler ενώ η συστηματική μελέτη των δυαδικών τετραγωνικών μορφών με ακεραίους συντελεστές ξεκίνησε αργότερα από τον Lagrange (ο οποίος πρώτος εισήγαγε τις ιδέες της διακρίνουσας, της ισοδυναμίας και της ανηγμένης μορφής). Παρόλο που οι έννοιες της σύνθεσης τετραγωνικών μορφών καθώς και της θεωρίας γένους ήταν κατά κάποιο τρόπο "κρυμμένες" στις εργασίες του Lagrange η συστηματική και θεμελιωμένη μελέτη τους βρίσκεται αργότερα στην εργασία του Gauss με τίτλο : "Disquisitiones Arithmiticae". Η παράσταση ακεραίων αριθμών μέσω δυαδικών τετραγωνικών μορφών συνδέθηκε μεταγενέστερα, χρησιμοποιώντας προχωρημένα μαθηματικά εργαλεία, με τον τύπο ανάλυσης των πρώτων διαιρετών τους σε κάποια υποσώματα των αντίστοιχων ring class fields .

Η παρούσα εργασία χωρίζεται σε δύο μέρη.

Στο πρώτο μέρος μελετάται η παράσταση ακεραίων μέσω τετραγωνικών μορφών διακρίνουσας $-256qr$ όπου q,r είναι πρώτοι αριθμοί με $q \equiv 5(\mathrm{mod}\ 8), r \equiv 3(\mathrm{mod} 8)$, υπό την προϋπόθεση $\hbar_2(D_0) \mid 4$. Χρησιμοποιούμε ιδιότητες εμφύτευσης υποσωμάτων του αντίστοιχου ring class field για να βρούμε γεννήτορες των σωμάτων και να εξάγουμε συνθήκες παράστασης συγκεκριμένων δυνάμεων πρώτων αριθμών από ambiguous κλάσεις, δηλαδή από κλάσεις με τάξη 1 ή 2, τετραγωνικών μορφών διακρίνουσας $-256qr$ στην $H(-256qr)$. Στην περίπτωση που $\left(\frac{q}{r}\right) = -1$, τα αποτελέσματα είναι πολύ καλά αφού μπορούμε να βρούμε ικανές και αναγκαίες συνθήκες παράστασης για κάθε μια ambiguous κλάση. Στην περίπτωση που $\left(\frac{q}{r}\right) = 1$, τα αποτελέσματα δεν είναι τόσο καλά αλλα παρ΄ όλα αυτά μπορούμε να πάρουμε ικανές και αναγκαίες συνθήκες παράστασης από κάποιο ζεύγος ambiguous κλάσεων. Το πρώτο μέρος τελειώνει με μια σύντομη μελέτη πάνω στο πως η δυνατότητα παράστασης των δυνάμεων πρώτων που μελετούμε από ambiguous κλάσεις διακρίνουσας $-256qr$ σχετίζεται με την δυνατότητα παράστασης των δυνάμεων αυτών από ambiguous κλάσεις διακρίνουσας $-2^s qr$ με $s \in \mathbb{Z}, s \geq 4$.

Στο δεύτερο μέρος συσχετίζουμε κάποια σώματα κλάσεων με σώματα που παράγονται χρησιμοποιώντας ρίζες θεμελιωδών μονάδων πραγματικών τετραγωνικών σωμάτων αριθμών. Το αποτέλεσμα είναι ότι μπορούμε να πάρουμε ικανές συνθήκες παράστασης συγκεκριμένων δυνάμεων πρώτων αριθμών από κλάσεις μορφών διακρίνουσας D μέσω συμβόλων του Legendre από κλάσεις μορφών διακρίνουσας D στις ακόλουθες περιπτώσεις:

1. $D = -256qr$, q, r πρώτοι με $q \equiv 5(\mathrm{mod} 8)$, $r \equiv 3(\mathrm{mod} 8)$, $\hbar_2(D_0) \mid 4$.
2. $D = -4m$, $m > 1$ ακέραιος, ελεύθερος τετραγώνου με $m \equiv 1(\mathrm{mod} 12)$, $\hbar_3(D_0) \mid 9$.

Ειδικά στην πρώτη περίπτωση η οποία μελετάται και στο πρώτο μέρος της παρούσας εργασίας καταφέρνουμε να πάρουμε ακριβείς συνθήκες παράστασης για κάθε κλάση της ομάδας κλάσεων με τάξη διαιρέτη του 4. Το δεύτερο μέρος τελειώνει με την παρουσίαση ενός τρόπου υπολογισμού των συμβόλων Legendre που εμφανίζονται.

Η εργασία αυτή γίνεται στα πλαίσια των υποχρεώσεων μου για την απόκτηση διδακτορικού διπλώματος στην Θεωρία Αριθμών. Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Ιωάννη Αντωνιάδη για την υποστήριξη και την καθοδήγηση του, καθώς το Ίδρυμα Κρατικών Υποτροφιών (Ι.Κ.Υ.) για την οικονομική ενίσχυση που μου παρείχε κατά την διάρκεια εκπόνησης της διατριβής.

Συλλιγάρδος Γιώργος

Ηράκλειο 12 / 8 / 2000

Προκαταρτικά

Στην παράγραφο αυτή μελετούμε την παράσταση δυνάμεων πρώτων αριθμών μέσω τετραγωνικών μορφών οποιασδήποτε διακρίνουσας D, $D \equiv 0, 1 (\bmod 4)$. Τα αποτελέσματα αυτά θα χρησιμοποιηθούν στις ειδικές περιπτώσεις που θα μελετήσουμε στην συνέχεια.

Πρόταση 0.0.1 *Έστω D αρνητικός ακέραιος, ελεύθερος τετραγώνου, με $D \equiv 0, 1(\mathrm{mod} 4)$. Έστω $e \in \{2, 3, 4, 6\}$, p περιττός πρώτος αριθμός $p > 2$ με $\left(\frac{D}{p}\right) = 1$. Αν $C \in H(D)$ με $C^e = 1$ και $spl_p(k_e(D)) = L_C^{(e)}$ τότε $C \longrightarrow p^{\hbar'_e}$. Αν $e = 4$ τότε επιπλέον οι σχέσεις $spl_p(k_2(D)) = L_C^{(2)}$ και $C \longrightarrow p^{\hbar'_2}$ είναι ισοδύναμες.*

<u>Απόδειξη:</u> Έστω $p = \mathfrak{p}_0\mathfrak{p}_1$ η ανάλυση του p σε πρώτα ιδεώδη του k. Άρα $N(\mathfrak{p}_0) = N(\mathfrak{p}_1) = p$ και $[\mathfrak{p}_1] = [\mathfrak{p}_0]^{-1}$ Έστω επίσης ότι $spl_p(k_e(D)) = L_C^{(e)}$. Αυτό σημαίνει ότι $\left\langle [\frac{k_e(D)|k}{\mathfrak{p}_0}] \right\rangle = \left\langle [\frac{k_e(D)|k}{C}] \right\rangle$. Οι ομάδες $\left\langle [\frac{k_e(D)|k}{\mathfrak{p}_0}] \right\rangle, \left\langle [\frac{k_e(D)|k}{C}] \right\rangle$ έχουν τάξη που διαιρεί το e. Συνεπώς, επειδή $(\hbar'_e, e) = 1$, θα έχουμε $\left\langle [\frac{k_e(D)|k}{C}] \right\rangle = \left\langle [\frac{k_e(D)|k}{\mathfrak{p}_0^{\pm\hbar'_e}}] \right\rangle$ και αφού κάθε κυκλική ομάδα τάξης 2, 3, 4 ή 6 έχει το πολύ δύο γεννήτορες (οι οποίοι είναι αντίστροφοι μεταξύ τους) έχουμε: $[\frac{k_e(D)|k}{C}] = [\frac{k_e(D)|k}{\mathfrak{p}_0^{\pm\hbar'_e}}]$. Η τελευταία σχέση μπορεί να γραφεί ως:

$$[\frac{k(D) \mid k}{C}][\frac{k(D) \mid k}{\mathfrak{p}_0^{\pm\hbar'_e}}] \in G(k(D)/k_e(D)).$$

Η $G(k(D)/k_e(D))$ έχει όμως τάξη πρώτη προς το e και συνεπώς $[\frac{k(D)|k}{C}] = [\frac{k(D)|k}{\mathfrak{p}_0^{\pm\hbar'_e}}]$ το οποίο μας δίνει τελικά ότι $C = [\mathfrak{p}_0^{\pm\hbar'_e}]$ και συνεπώς, αφού $N(\mathfrak{p}_0^{\pm\hbar'_e}) = p^{\hbar'_e}$, θα έχουμε: $C \longrightarrow p^{\hbar'_e}$.

Θεωρούμε τώρα την περίπτωση: $e = 4$ και υποθέτουμε ότι $C \longrightarrow p^{\hbar'_2}$. Θα έχουμε λοιπόν ότι υπάρχει ακέραιο ιδεώδες A του k που να αντιστοιχεί στην κλάση C με norm $N(A) = p^{\hbar'_2}$. Επομένως $A = \mathfrak{p}_0^x \mathfrak{p}_1^y$ για κάποια $x, y \in \mathbb{Z}$ με $x + y = p^{\hbar'_2}$. Έχουμε λοιπόν $[\frac{k(D)|k}{C}] = [\frac{k(D)|k}{A}] = [\frac{k(D)|k}{\mathfrak{p}_0}]^x [\frac{k(D)|k}{\mathfrak{p}_1}]^y = [\frac{k(D)|k}{\mathfrak{p}_0}]^{x-y}$. Στην συνέχεια, παίρνοντας τον περιορισμό του συμβόλου του Artin στό $k_2(D)$ συνάγουμε ότι $[\frac{k_2(D)|k}{C}] = [\frac{k_2(D)|k}{\mathfrak{p}_0}]^{x-y}$. Όμως το $[\frac{k_2(D)|k}{\mathfrak{p}_0}]^{x-y}$, ως στοιχείο της $G(k_2(D)/k)$, έχει τάξη δύναμη του 2. Άρα τα σύμβολα του Artin $[\frac{k_2(D)|k}{\mathfrak{p}_0}]^{x-y}$, $[\frac{k_2(D)|k}{\mathfrak{p}_0}]$ παράγουν την ίδια υποομάδα της $G(k_2(D)/k)$ (αφού $x + y = p^{\hbar'_2}$ έχουμε ότι ο $x + y$ είναι περιττός άρα και ο $x - y$ είναι περιττός). Επομένως $spl_p(k_2(D)) = L_C^{(2)}$. $\square$

Παρατήρηση: Στην απόδειξη του αντιστρόφου της πρότασης 0.0.1 για την περίπτωση $e = 4$ στηριχτήκαμε στο γεγονός ότι για $x, y \in \mathbb{Z}$, αν ο $x + y$ είναι περιττός τότε και ο $x - y$ είναι περιττός. Η απόδειξη δεν μπόρεσε να εφαρμοστεί στις άλλες περιπτώσεις αφου ο μόνος φυσικός $n > 1$ με την ιδιότητα $\forall x, y \in \mathbb{Z}$, αν $(x + y, n) = 1$ τότε $(x - y, n) = 1$ είναι ο 2. Αυτό που ισχύει για όλα τα $e \in \{2, 3, 4, 6\}$ είναι ότι αν $C \longrightarrow p^{\hbar'_e}$, τότε $spl_p(k_e(D)) \subseteq L_C^{(e)}$. Τέλος, η παραπάνω πρόταση αναφέρεται μόνο σε $e \in \{2, 3, 4, 6\}$ αφού αυτοί είναι οι μόνοι φυσικοί για τους οποίους η $\frac{\mathbb{Z}}{eZ}$ έχει το πολύ δύο γεννήτορες.

Έστω D_0 θεμελιώδης διακρίνουσα και $f \in \mathbb{N}$. Έστω επίσης $k = \mathbb{Q}(\sqrt{D_0})$. Θέτουμε $D = f^2 D_0$ οπότε το D είναι διακρίνουσα με οδηγό f. Στην συνέχεια θέτουμε :

$I_k = \{\mathfrak{a} \mid \mathfrak{a} \lhd k\}, \quad P_k = \{\alpha R_k \mid \alpha \in k\}, \quad I_k(f) = \{\mathfrak{a} \mid \mathfrak{a} \lhd k, (N(\mathfrak{a}), f) = 1\}$,

$P_k(f) = \{\alpha R_k \mid \alpha \in R_k, (N(\alpha), f) = 1\}, \quad P_{k,\mathbb{Z}}(f) = \{\alpha R_k \mid \alpha \in (\mathbb{Z} +$

$fR_k), (N(\alpha), f) = 1\}$.

Είναι γνωστό (βλ. [3] Θεώρημα 7.24, σχέση 7.25) ότι υπάρχει επιμορφισμός $\frac{I_k(f)}{P_{k,\mathbb{Z}}(f)} \longrightarrow \frac{I_k}{P_k}$ του οποίου, είναι εύκολο να δεί κανείς, ότι ο πυρήνας είναι η $\frac{P_k(f)}{P_{k,\mathbb{Z}}(f)}$. Επειδή όμως $\frac{I_k(f)}{P_{k,\mathbb{Z}}(f)} \simeq H(D)$ και $\frac{I_k}{P_k} \simeq H(D_0)$, εχουμε την ακόλουθη ακριβή ακολουθία:

$$1 \longrightarrow \frac{P_k(f)}{P_{k,\mathbb{Z}}(f)} \longrightarrow H(D) \longrightarrow H(D_0) \longrightarrow 1$$

Επίσης, μέσω του ισομορφισμού που επάγει το σύμβολο του Artin μεταξύ των ομάδων κλάσεων και των ομάδων Galois, ο προαναφερθής επιμορφισμός επάγει έναν επιμορφισμό:

$$G(k(D)/k) \longrightarrow G(k(D_0)/k)$$

τον οποίο δίνει ο περιορισμός στο $k(D_0)$.

Στην συνέχεια θα θεωρήσουμε τις ακόλουθες δύο περιπτώσεις:

- 1η Περίπτωση: $D = -256qr$, q, r πρώτοι με $q \equiv 5(\mathrm{mod} 8)$, $r \equiv 3(\mathrm{mod}\ 8)$, $\hbar_2(D_0) \mid 4$.

- 2η Περίπτωση: $D = -4m$, $m > 1$ ακέραιος ελεύθερος τετραγώνου $m \equiv 1(\mathrm{mod} 4)$,
  $\hbar_3(D_0) \mid 9$.

Η θεμελιώδης διακρίνουσα σε κάθε περίπτωση είναι:

$$D_0 = \begin{cases} -qr & , \text{στην 1η Περίπτωση}\cdot \\ -4m & , \text{στην 2η Περίπτωση} \end{cases}$$

Στην διαπραγμάτευση αυτών που θα ακολουθήσουν στην συνέχεια της εργασίας θα χρησιμοποιηθεί ευρέως το παρακάτω λήμμα:

Λήμμα 0.0.2 *Άν M/K επέκταση Galois σωμάτων αριθμών με ομάδα Galois τύπου (2,2) με ενδιάμεσα σώματα $F_1,\ F_2,\ F_3$ και $\mathfrak{p}$ ένα πρώτο ακέραιο ιδεώδες του K που δεν διακλαδίζεται στο M τότε ή ακριβώς ένα από τα $f_{\mathfrak{p}}(F_1/K),\ f_{\mathfrak{p}}(F_2/K),\ f_{\mathfrak{p}}(F_3/K)$ είναι 1 ή όλα είναι ίσα με 1.*

Απόδειξη: Η ομάδα αδρανείας του $\mathfrak{p}$ στην M/K είναι τετριμμένη, συνεπώς η ομάδα ανάλυσης είναι ισόμορφη με την

$$G\left(\frac{R_M}{\mathfrak{q}}/\frac{R_K}{\mathfrak{p}}\right)$$

όπου $\mathfrak{q}$ τυχαίο **πρώτο** ακέραιο ιδεώδες του M πάνω από το $\mathfrak{p}$. Επομένως η ομάδα ανάλυσης είναι κυκλική οπότε αποκλείεται να ισούται με την $G(M/K)$. Το σώμα ανάλυσης κατά συνέπεια του $\mathfrak{p}$ στην M/K είναι:
είτε το F_1 οπότε $f_p(F_1/K) = 1,\ f_p(F_2/K) = 2,\ f_p(F_3/K) = 2$,
είτε το F_2 οπότε $f_p(F_2/K) = 1,\ f_p(F_1/K) = 2,\ f_p(F_3/K) = 2$,
είτε το F_3 οπότε $f_p(F_3/K) = 1,\ f_p(F_1/K) = 2,\ f_p(F_2/K) = 2$,
είτε το M οπότε $f_p(F_1/K) = f_p(F_2/K) = f_p(F_3/K) = 1$. $\square$

Κεφάλαιο 1

Δυνάμεις Πρώτων Αριθμών και Τετραγωνικές Μορφές Διακρίνουσας $-256qr$

Στο κεφάλαιο αυτό θα ασχοληθούμε μόνο με την 1η περίπτωση της προηγούμενης παραγράφου , δηλαδή με τετραγωνικές μορφές διακρίνουσας $D = -256qr$ όπου q, r είναι πρώτοι αριθμοί με $q \equiv 5(\text{mod}8)$ και $r \equiv 3(\text{mod}8)$ και επίσης $\hbar(-qr) \mid 4$. Το σώμα γένους του $k = \mathbb{Q}(\sqrt{-qr})$ είναι το $\Sigma = \mathbb{Q}(\sqrt{q}, \sqrt{r}, \sqrt{2}, i) = k(\zeta_8)(\sqrt{q})$ (βλ. [3] σελ. 121 θεώρημα 6.1 και [11] Θεώρημα 2). Θέτουμε: $D_s = 2^{2s}D_0$, $s \geq 4$ όπου βέβαια $D_0 = -qr$ και έτσι $D = D_4$. Για λόγους απλότητας στον συμβολισμό, αν H είναι υποομάδα της $H_2(D_s)$ θα συμβολίζουμε με L_H το υπόσωμα $L_H^{(2)}$ του $k_2(D)$.

1.1 Αποτελέσματα από θεωρία γένους

Οι ambiguous κλάσεις της $H_2(D_s)$ είναι (βλ. [3] Lemma 3.10 και [9] Table 2):

$I_s = [1, 0, 2^{2s-2}qr], \quad [4, 4, 1+2^{2s-4}qr], \quad [qr, 0, 2^{2s-2}], \quad [4qr, 4qr, qr+2^{2s-4}],$
$[q, 0, 2^{2s-2}r], \quad [4q, 4q, q + 2^{2s-4}r], \quad [r, 0, 2^{2s-2}q], \quad [4r, 4r, r + 2^{2s-4}q].$

Αν περιοριστούμε τώρα σε ακέραιους αριθμούς $m \in \mathbb{Z}$, $m \geq 0$ τέτοιους ώστε $\left(\frac{D}{p}\right) = 1$, γιά κάθε πρώτο p με $p \mid m$, έχουμε το ακόλουθο :

Λήμμα 1.1.1

- *Οι κλάσεις* I_s *και* $[4,4,1+2^{2s-4}qr]$ *παριστούν ακεραίους αριθμούς* m *με* $m \equiv 1(\text{mod} 8)$ *και* $\left(\frac{m}{q}\right)=1$
- *Οι κλάσεις* $[qr,0,2^{2s-2}]$ *και* $[4qr,4qr,qr+2^{2s-4}]$ *παριστούν ακεραίους αριθμούς* m *με* $m \equiv 7(\text{mod} 8)$ *και* $\left(\frac{m}{q}\right)=1$
- *Οι κλάσεις* $[q,0,2^{2s-2}r]$ *και* $[4q,4q,q+2^{2s-4}r]$ *παριστούν ακεραίους αριθμούς* m *με* $m \equiv 5(\text{mod} 8)$ *και* $\left(\frac{m}{q}\right)=\left(\frac{r}{q}\right)$ *και*
- *Οι κλάσεις* $[r,0,2^{2s-2}q]$ *και* $[4r,4r,r+2^{2s-4}q]$ *παριστούν ακεραίους αριθμούς* m *με* $m \equiv 3(\text{mod} 8)$ *και* $\left(\frac{m}{q}\right)=\left(\frac{r}{q}\right)$.

Απόδειξη: Έστω ότι $I_s \longrightarrow m$ με $m \geq 0$ και $\left(\frac{D}{p}\right)=1, \forall p \mid m$. Υπάρχουν $x,y \in \mathbb{Z}$ ώστε $x^2+2^{2s-2}qry^2=m$. Προφανώς ο x είναι περιττός (αφού ο μ είναι περιττός) οπότε $m \equiv x^2 \equiv 1(\text{mod} 8)$. Εξάλλου

$$\left(\frac{m}{q}\right)=\left(\frac{x^2+2^{2s-2}qry^2}{q}\right)=\left(\frac{x^2}{q}\right)=1.$$

Έστω τώρα $[4,4,1+2^{2s-4}qr] \longrightarrow n$ με $n \geq 0$ και $\left(\frac{D}{p}\right)=1, \forall p \mid n$. Αυτό σημαίνει ότι υπάρχουν $x,y \in \mathbb{Z}$ ώστε $4x^2+4xy+(1+2^{2s-4}qr)y^2=n$. Παρατηρούμε όμως ότι ο y είναι αναγκαστικά περιττός (αν ήταν άρτιος θα είχαμε $n \equiv 0(mod 2)$ που είναι άτοπο) και έτσι $x(x+y) \equiv 0(\text{mod} 2)$. Θα έχουμε επομένως ότι

$$n \equiv 4x^2+4xy+y^2 \equiv 4x^2+4xy+1 \equiv 4x(x+y)+1 \equiv 1(\text{mod} 8).$$

Τέλος,

$$\left(\frac{n}{q}\right)=\left(\frac{4x^2+4xy+(1+2^{2s-4}qr)y^2}{q}\right)=\left(\frac{4x^2+4xy+y^2}{q}\right)=\left(\frac{(2x+y)^2}{q}\right)=1.$$

Οι περιπτώσεις με τα άλλα ζεύγη των ambiguous κλάσεων μπορούν να μελετηθούν ανάλογα. $\square$

Συνεπώς οι οκτώ ambiguous κλάσεις διαμοιράζονται σε 4 γένη και κάθε γένος έχει δύο κλάσεις. Στην συνέχεια αποδεικνύουμε την ακόλουθη πρόταση:

Πρόταση 1.1.2 *Κάθε στοιχείο C της $H_2(D_s)$ με $C \longrightarrow m$ για κάποιο $m \in \mathbb{Z}$, $m \geq 0$ με $\left(\frac{D}{p}\right) = 1$,*
για κάθε πρώτο p με $p \mid m$, αντιστοιχεί σε ένα σύμβολο του Artin

$$[\frac{\Sigma \mid k}{C}]$$

έτσι ώστε να επάγεται ο ισομορφισμός:

$$\frac{H_2(D_s)}{H_2(D_s)^2} \xrightarrow{\simeq} (\mathbb{Z}/_{8\mathbb{Z}})^{\times} \times \{\pm 1\}$$

με

$$C \bmod (H_2(D_s)^2) \longrightarrow ([\frac{\mathbb{Q}(\zeta_8) \mid \mathbb{Q}}{m}], [\frac{\mathbb{Q}(\sqrt{q}) \mid \mathbb{Q}}{m}]).$$

<u>Απόδειξη:</u> Έστω $m \in \mathbb{Z}$, $m \geq 0$ με $C \longrightarrow m$ για κάποιο $C \in H_2(D_s)$. Υπάρχει συνεπώς ακέραιο ιδεώδες $A \lhd R_k$ με $N(A) = m$ τέτοιο ώστε $[\frac{k_2(D_s)|k}{C}] = [\frac{k_2(D_s)|k}{A}] = [\frac{k_2(D_s)|k}{\mathfrak{p}_1{}^{\nu_1}\mathfrak{p}_2{}^{\nu_2}...\mathfrak{p}_\kappa{}^{\nu_\kappa}}]$ όπου $A = \mathfrak{p}_1{}^{\nu_1}\mathfrak{p}_2{}^{\nu_2}...\mathfrak{p}_\kappa{}^{\nu_\kappa}$ η ανάλυση του A σε πρώτους παράγοντες με $\mathfrak{p}_\xi$ πρώτο ιδεώδες του k πάνω από το p_ξ, $\xi \in \{1, 2, ..., \kappa\}$ όπου $m = p_1^{\nu_1}p_2^{\nu_2}...p_r^{\nu_r}$ η ανάλυση του m σε πρώτους του $\mathbb{Z}$. Έτσι, παίρνοντας περιορισμό στο Σ έχουμε: $[\frac{\Sigma|k}{C}] = [\frac{\Sigma|k}{\mathfrak{p}_1}]^{\nu_1}[\frac{\Sigma|k}{\mathfrak{p}_2}]^{\nu_2}...[\frac{\Sigma|k}{\mathfrak{p}_\kappa}]^{\nu_\kappa}$. Αλλά επειδή $f_{p_\xi} = 1$ έπεται ότι $[\frac{\Sigma|k}{\mathfrak{p}_\xi}] = [\frac{\Sigma|\mathbb{Q}}{p_\xi}]$ οπότε $[\frac{\Sigma|k}{C}] = [\frac{\Sigma|\mathbb{Q}}{m}]$. Επειδή όμως $H_2(D_s)^2 = H_2(D_s) \cap H(D_s)^2$, από τον ορισμό του σώματος γένους, προκύπτει ότι για $C, C' \in H_2(D_s)$ ισχύει η ισοδυναμία:

$$C \equiv C'(\bmod H_2(D_s)^2) \quad \text{αν και μόνο αν} \quad [\frac{\Sigma \mid k}{C}] = [\frac{\Sigma \mid k}{C'}].$$

Τέλος, αφού $\Sigma = k(\zeta_8)(\sqrt{q})$, το $[\frac{\Sigma|\mathbb{Q}}{m}]$ μπορεί να αντιστοιχισθεί στο ζεύγος: $([\frac{\mathbb{Q}(\zeta_8)|\mathbb{Q}}{m}], [\frac{\mathbb{Q}(\sqrt{q})|\mathbb{Q}}{m}])$ που με την σειρά του αντιστοιχεί στο ζεύγος: $(m(\mathrm{mod}\ 8), \left(\frac{q}{m}\right))$ του $\frac{\mathbb{Z}}{8\mathbb{Z}} \times \{\pm 1\}$. Οι αντιστοιχίες αυτές είναι " ένα προς ένα " και ομομορφισμοί ομάδων οπότε παίρνουμε έναν μονομορφισμό:

$$\frac{H_2(D_s)}{H_2(D_s)^2} \xrightarrow{\simeq} (\mathbb{Z}/_{8\mathbb{Z}})^{\times} \times \{\pm 1\}$$

ο οποίος, σύμφωνα με το προηγούμενο λήμμα 1.1.1, είναι ισομορφισμός. □

Παρατήρηση: Αυτό που έχουμε λοιπόν μέχρι στιγμής από την θεωρία γένους είναι ότι για κάθε ζεύγος $(m(\mathrm{mod}8), \varepsilon) \in ((\mathbb{Z}/_{8\mathbb{Z}})^{\times} \times \{\pm 1\})$ υπάρχει ένα $\nu \in \mathbb{Z}$ ώστε $\nu \equiv m(\mathrm{mod}8)$ με $C \longrightarrow \nu$ για κάποιο $C \in H_2(D_s)$.

Από την παράγραφο 2 του [7] έχουμε ότι $\frac{P_k(s^2)}{p_{k,\mathbb{Z}}(2^s)} = (2^{s-2}, 2)$ και συνεπώς λόγω της ακριβούς ακολουθίας

$$1 \longrightarrow \frac{P_k(f)}{P_{k,\mathbb{Z}}(f)} \longrightarrow H(D) \longrightarrow H(D_0) \longrightarrow 1$$

έχουμε την ακόλουθη ακριβή ακολουθία:

$$1 \longrightarrow (2^{s-2}, 2) \longrightarrow H_2(D_s) \longrightarrow H_2(D_0) \longrightarrow 1 \tag{1.1}$$

για $s \geq 4$.

Αν $\left(\frac{q}{r}\right) = 1$ τότε η διοφαντική εξίσωση $u^2 - 4qv^2 - D_0 w^2 = 0$ έχει λύση (βλ. [2] Θεώρημα 4) και μία λύση της (u, v, w) θα λέγεται πρωταρχική όταν ο μέγιστος κοινός διαιρέτης των u, v, w είναι 1.

Διακρίνουμε τις περιπτώσεις:

- Περίπτωση Ια: $\left(\frac{q}{r}\right) = -1$.

- <u>Περίπτωση Ιβ</u>: $\left(\frac{q}{r}\right) = 1$ και $\left(\frac{q}{v}\right) = -1$, όπου (u, v, w) είναι πρωταρχική λύση της
  $u^2 - 4qv^2 - D_0w^2 = 0$.

- <u>Περίπτωση Ιγ</u>: $\left(\frac{q}{r}\right) = 1$ και $\left(\frac{q}{v}\right) = 1$, όπου (u, v, w) είναι πρωταρχική λύση της
  $u^2 - 4qv^2 - D_0w^2 = 0$.

Από [3] proposition 3.11 έχουμε ότι η $H(D_0)$ έχει ακριβώς 2 ambiguous κλάσεις, οπότε η $H_2(D_0)$ είναι αναγκαστικά κυκλική. Επίσης, η $H(D_s)$ έχει 8 ambiguous κλάσεις οπότε είναι γενικά του τύπου: $(2^\kappa, 2^\lambda, 2^\xi)$ αλλά, όπως είδαμε πριν, υπάρχουν μόνο δύο ambiguous κλάσεις σε κάθε γένος, οπότε η $H(D_s)$ είναι του τύπου: $(2^{s-2+c_{qr}}, 2, 2)$, όπου $2^{c_{qr}+1}$ είναι η τάξη της $H_2(D_0)$. Θέτουμε $c_{qr}(s) = s - 2 + c_{qr}$, $s \geq 4$. Όταν αναφερόμαστε σε συγκεκριμένα q, r θα παραλείπουμε τον δείκτη qr. Από το θεώρημα 4 του [2] προκύπτει ότι στην περίπτωση Ια: $c(s) = s - 2$, και στην περίπτωση Ιβ: $c(s) = s - 1$. Η περίπτωση Ιγ δίνει $c(s) \geq s$ και δεν θα μας απασχολήσει όπως έχουμε πεί στην εισαγωγή (αφού στην περίπτωση αυτή η υποομάδα κλάσεων $H_2(D_0)$ έχει τάξη μεγαλύτερη του 4) αφού εμείς έχουμε υποθέσει ότι $\hbar_2(D_0) \mid 4$. Θέτουμε: $H_2(D_s) = \langle A_s, B_s, C_s \rangle$ όπου $A_s^{2^{c(s)}} = B_s^2 = C_s^2 = I_s$ και έτσι οι ambiguous κλάσεις της $H_2(D_s)$ είναι:

$$I_s,\ A_s^{2^{c(s)-1}},\ B_s,\ C_s,\ A_s^{2^{c(s)-1}} \cdot B_s,\ A_s^{2^{c(s)-1}} \cdot C_s,\ B_s \cdot C_s,\ A_s^{2^{c(s)-1}} \cdot B_s \cdot C_s$$

οι οποίες διαμοιράζονται στα ακόλουθα 4 γένη:

$\mathcal{G}_1$, $\mathcal{G}_2 = B_s\mathcal{G}_1$, $\mathcal{G}_3 = C_s\mathcal{G}_1$ και $\mathcal{G}_4 = B_sC_s\mathcal{G}_1$, όπου $\mathcal{G}_1 = \{I_s, A_s^{2^{c(s)-1}}\}$.

και επομένως, από το λήμμα 1.1.1, έχουμε: $A_s^{2^{c(s)-1}} = [4, 4, 1 + 2^{2s-4}qr]$. Χωρίς περιορισμό της γενικότητας μπορούμε να γράψουμε: $B_s = [qr, 0, 2^{2s-2}]$ και $C_s = [q, 0, 2^{2s-2}r]$ όποτε έχουμε το ακόλουθο λήμμα

Λήμμα 1.1.3 *Τα ακόλουθα ισχύουν:*
$A_s^{2^{c(s)-1}} = [4, 4, 1 + 2^{2s-4}qr], \quad B_s = [qr, 0, 2^{2s-2}], \quad C_s = [q, 0, 2^{2s-2}r],$
$A_s^{2^{c(s)-1}} \cdot B_s = [4qr, 4qr, qr + 2^{2s-4}], \quad A_s^{2^{c(s)-1}} \cdot C_s = [4q, 4q, q + 2^{2s-4}r],$
$A_s^{2^{c(s)-1}} \cdot B_s \cdot C_s = [4r, 4r, r + 2^{2s-4}q], \quad B_s \cdot C_s = [r, 0, 2^{2s-2}q].$

Απόδειξη: Το σύστημα

$$\left\{\begin{array}{rcl} 4x & \equiv & 0(\mathrm{mod}(8rq)) \\ rqx & \equiv & 4rq(\mathrm{mod}8rq)) \\ 2x & \equiv & -2^{2s-1}rq(\mathrm{mod}8rq)) \end{array}\right\}$$

έχει λύση $x = 4rq$ και επομένως $A_s^{2^{c(s)-1}} \cdot B_s = [4qr, 4qr, \frac{16r^2q^2+2^{2s}qr}{16qr}] = [4qr, 4qr, qr + 2^{2s-4}]$ (βλ. [3] λήμμα 3.2).

Το σύστημα

$$\left\{\begin{array}{rcl} 4x & \equiv & 0(\mathrm{mod}(8q)) \\ qx & \equiv & 4q(\mathrm{mod}8q)) \\ 2x & \equiv & -2^{2s-1}q(\mathrm{mod}8q)) \end{array}\right\}$$

έχει λύση $x = 4q$ και επομένως $A_s^{2^{c(s)-1}} \cdot C_s = [4qr, 4qr, \frac{16q^2+2^{2s}qr}{16q}] = [4q, 4q, q + 2^{2s-4}r]$.

Επίσης έχουμε $C_s^{-1} = [q, 0, 2^{2s-2}r]$ και συνεπώς, επειδή το σύστημα

$$\left\{\begin{array}{rcl} qx & \equiv & 0(\mathrm{mod}(2rq)) \\ rx & \equiv & 0(\mathrm{mod}2rq)) \\ 0x & \equiv & -2^{2s-1}qr(\mathrm{mod}2rq)) \end{array}\right\}$$

έχει λύση $x=0$, θα έχουμε: $[r,0,2^{2s-2}q]C_s^{-1}=[r,0,2^{2s-2}q]\cdot[q,0,2^{2s-2}r]^{-1}=[qr,0,2^{2s-2}]=B_s$. Τελικά θα έχουμε $B_s\cdot C_s=[r,0,2^{2s-2}q]$ το οποίο δίνει και $A_s^{2^{c(s)-1}}\cdot B_sC_s=[4r,4r,r+2^{2s-4}q]$.

Χρησιμοποιώντας τα παραπάνω αποτελέσματα από την θεωρία γένους μπορούμε να αποδείξουμε την επόμενη :

Πρόταση 1.1.4 *Αν p είναι περιττός πρώτος με $(\frac{D}{p})=1$, τότε*

1. *Αν ο $p^{\hbar'}$ παρίσταται από μία εκ των I_s, $A_s^{2^{c(s)-1}}$ τότε παρίσταται από ακριβώς μία και επίσης ισχύει $p\equiv 1(\mathrm{mod}8)$ και $(\frac{q}{p})=1$*
2. *Αν ο $p^{\hbar'}$ παρίσταται από μία εκ των B_s, $A_s^{2^{c(s)-1}}\cdot B_s$ τότε παρίσταται από ακριβώς μία και επίσης ισχύει $p\equiv 7(\mathrm{mod}8)$ και $(\frac{q}{p})=1$*
3. *Αν ο $p^{\hbar'}$ παρίσταται από μία εκ των C_s, $A_s^{2^{c(s)-1}}\cdot C_s$ τότε παρίσταται από ακριβώς μία και επίσης ισχύει $p\equiv 5(\mathrm{mod}8)$ και $(\frac{q}{p})=(\frac{q}{r})$*
4. *Αν ο $p^{\hbar'}$ παρίσταται από μία εκ των B_sC_s, $A_s^{2^{c(s)-1}}\cdot B_s\cdot C_s$, τότε παρίσταται από ακριβώς μία και επίσης ισχύει $p\equiv 3(\mathrm{mod}8)$ και $(\frac{q}{p})=(\frac{q}{r})$.*

Απόδειξη: Θα αναφερθούμε μόνο στην απόδειξη του 1. Ανάλογα αποδεικνύονται και οι υπόλοιπες. Οι κλάσεις I_s και $A_s^{2^{c(s)-1}}$ παράγουν διαφορετικές ομάδες. Συνεπώς

$$L_{I_s}^{(2)}\neq L_{A_s^{2^{c(s)-1}}}^{(2)}$$

πράγμα που σημαίνει, από την πρόταση 0.0.1, ότι αν ο $p^{\hbar'}$ παρίσταται από μία εκ των I_s, $A_s^{2^{c(s)-1}}$ τότε παρίσταται από ακριβώς μία. Από το λήμμα 1.1.1 τώρα έχουμε ότι $(\frac{q}{p^{\hbar_2'}})=1$ και $p^{\hbar_2'}=1(\mathrm{mod}8)$. Όμως ο $\hbar_2'$ είναι περιττός και συνεπώς $1 = (\frac{q}{p^{\hbar'_2}}) = (\frac{q}{p})$. Εξάλλου, επειδή p περιττός και $\hbar'_2 - 1$ άρτιος, έχουμε ότι $p^{\hbar'_2 - 1} \equiv 1(\mathrm{mod} 8)$ άρα $1 \equiv p^{\hbar'_2} \equiv p(\mathrm{mod} 8)$. $\square$

1.2 Μελέτη των υποσωμάτων του $k_2(D_s)$

Θέτουμε $L_0 = L_{A_s^2, B_s, C_s}$. Το L_0 παίζει σημαντικό ρόλο ο οποίος θα φανεί παρακάτω. Η ομάδα Galois $G(L_{A_s^2}/k)$ είναι του τύπου $(2,2,2)$. Επομένως το σώμα $L_{A_s^2}$ ταυτίζεται με το σώμα γένους Σ. Το σώμα $L_{A_s^2}$ έχει 7 υποσώματα τα οποία είναι επεκτάσεις βαθμού 2 πάνω από το k. Συγκεκριμένα, αυτά τα σώματα είναι τα $k(\sqrt{q}),\ k(\sqrt{2}),\ k(i),\ k(\sqrt{2q}),\ k(i\sqrt{q}),\ k(i\sqrt{2})$, και $k(i\sqrt{2q})$. Το L_0 είναι υπόσωμα του $L_{A_s^2}$ το οποίο περιέχεται σε κυκλική επέκταση βαθμού 4 πάνω από το k ($L_0 \subseteq L_{A_s^4, B_s, C_s}$). Το θεώρημα 22 του [10] μας δίνει ότι:

Πρόταση 1.2.1 *Αν $d_1, d_2 \in \mathbb{Z}$ ώστε να ορίζονται οι ακόλουθες τετραγωνικές επεκτάσεις του $\mathbb{Q}$: $k_1 = \mathbb{Q}(\sqrt{d_1})$, $k_2 = \mathbb{Q}(\sqrt{d_2})$ με $k_1 \neq k_2$, τότε το $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ περιέχεται σε κυκλική επέκταση του $\mathbb{Q}(\sqrt{d_1}\sqrt{d_2})$ η οποία είναι διεδρική βαθμού 8 πάνω από το $\mathbb{Q}$ αν και μόνο αν για κάθε πρώτο p του $\mathbb{Z}$ το σύμβολο του Hilbert $\left(\frac{d_1, d_2}{p}\right)$ είναι ίσο με 1.*

Αν προχωρούσαμε σε υπολογισμούς, θα καταλήγαμε στο ότι:

$$L_0 = \begin{cases} k(\sqrt{q}) & , \text{αν } (\frac{q}{r}) = 1 \\ k(\sqrt{2q}) & , \text{αν } (\frac{q}{r}) = -1. \end{cases}$$

Δεν θα το κάνουμε εδώ, διότι το L_0 θα προκύψει παρακάτω καθώς θα υπολογίζουμε όλες τις κυκλικές βαθμού 4 μη διακλαδιζόμενες πέραν του 2 επεκτάσεις του k που δίνουν διεδρική ομάδα Galois πάνω από το $\mathbb{Q}$.

Συνεχίζοντας, παρατηρούμε ότι $D_{s+1} = 4D_s$ και ότι $k_2(D_s) \subseteq k_2(D_{s+1})$. Επίσης, ο γεννήτορας A_s μπορεί να επιλεγεί έτσι ώστε ο επιμορφισμός $G(k_2(D_{s+1})/k) \longrightarrow G(k_2(D_s)/k)$, ο οποίος δίνεται μέσω του περιορισμού στο $k_2(D_s)$, να επάγει επιμορφισμό

$$\Phi_s : H_2(D_{s+1}) \longrightarrow H_2(D_s) : [a, 2b, 4c] \xrightarrow{\Phi_s} [a, b, c]$$

όπου $b^2 - 4ac = D_s$ (βλ. παράγραφο 1 του [7] για ανάλογη περίπτωση) με $\Phi_s(A_{s+1}) = A_s$, $\Phi_s(B_{s+1}) = B_s$ και $\Phi_s(C_{s+1}) = C_s$. Επίσης, για κάθε ζεύγος ακεραίων s, t με $s \geq t \geq 4$, έχουμε $G(k_2(D_s)/k_2(D_t)) = \left\langle A_s^{2^{c(t)}} \right\rangle$.
Προφανώς ισχύει το ακόλουθο λήμμα

Λήμμα 1.2.2 *Αν $H_{s+1} \leq H_2(D_{s+1})$ και $\Phi(H_{s+1}) = H_s$, τότε $L_{H_s} \subseteq L_{H_{s+1}}$.*

Επίσης μπορούμε εύκολα να πιστοποιήσουμε ότι οι μόνες υποομάδες της $H_2(D_s)$ των οποίων η ομάδα πηλίκο ως πος την $H_2(D_s)$ είναι κυκλική τάξης 4 είναι : $\left\langle A_s^2 B_s, C_s \right\rangle$, $\left\langle A_s^2 C_s, B_s \right\rangle$, $\left\langle A_s^2 B_s, B_s C_s \right\rangle$ και $\left\langle A_s^4, B_s, C_s \right\rangle$. Παρακάτω θα υπολογίσουμε τα σώματα που τους αντιστοιχούν.

Στην εισαγωγή της εργασίας [9] αναφέρεται η ακόλουθη πρόταση:

Πρόταση 1.2.3 *Για ένα ελεύθερο τετραγώνου θετικό ακέραιο αριθμό m, από όλες τις αντι-Pell διοφαντικές εξισώσεις: $x^2 - my^2 = dt$, όπου $d \geq 1$ είναι θετικός διαιρέτης του m, $dt \neq 1$ και*

$$t = \begin{cases} 1 & , \textit{αν } m \equiv 1, 2 (\mathrm{mod} 4) \cdot \\ \textit{1 η 2} & , \textit{αν } m \equiv 3 (\mathrm{mod} 4) \cdot \end{cases}$$

ακριβώς μία είναι επιλύσιμη στο $\mathbb{Z}$.

Επομένως στην περίπτωσή μας:

Λήμμα 1.2.4

- $(\frac{q}{r})= 1$ *αν και μόνο αν η* $x^2 - qry^2 = q$ *είναι επιλύσιμη στο* $\mathbb{Z}$.

- $(\frac{q}{r})= -1$ *αν και μόνο αν η* $x^2 - qry^2 = 2q$ *είναι επιλύσιμη στο* $\mathbb{Z}$.

Απόδειξη: Οι πιθανές περιπτώσεις είναι: $d = q, r, qr$ και $t = 1, 2$. Έστω $(\frac{q}{r})= 1$. Θα αποδείξουμε ότι σε όλες τις άλλες περιπτώσεις η Διοφαντική εξίσωση $x^2 - qry^2 = dt$ δεν είναι επιλύσιμη στο $\mathbb{Z}$. Έχουμε

Αν $x^2 - qry^2 = 2q$ τότε $(\frac{2}{r})= 1$. Άτοπο.

Αν $x^2 - qry^2 = r$ τότε $x^2 + y^2 \equiv 3(\mathrm{mod} 8)$. Άτοπο.

Αν $x^2 - qry^2 = 2r$ τότε $(\frac{2}{q})= 1$. Άτοπο.

Αν $x^2 - qry^2 = qr$ τότε $qrx'^2 - y^2 = 1$ για $x' \in \mathbb{Z}$ οπότε $(\frac{-1}{r})= 1$. Άτοπο.

Αν $x^2 - qry^2 = 2qr$ τότε $qrx'^2 - y^2 = 2$ για $x' \in \mathbb{Z}$ οπότε $(\frac{2}{q})= 1$. Άτοπο.

Συνεπώς, λόγω της πρότασης 1.2.3 απεδείχθη το πρώτο μέρος του λήμματος.

Εστω τώρα $(\frac{q}{r})= -1$. Τότε

Αν $x^2 - qry^2 = q$ τότε $(\frac{q}{r})= 1$. Άτοπο.

Αν $x^2 - qry^2 = r$ τότε $(\frac{r}{q})= 1$. Άτοπο.

Αν $x^2 - qry^2 = qr$ τότε $qrx'^2 - y^2 = 1$ για $x' \in \mathbb{Z}$ οπότε $(\frac{-1}{r})= 1$. Άτοπο.

Αν $x^2 - qry^2 = 2qr$ τότε $qrx'^2 - y^2 = 2$ για $x' \in \mathbb{Z}$ οπότε $(\frac{2}{q})= 1$. Άτοπο.

Αν $x^2 - qry^2 = 2r$ τότε $x^2 + y^2 \equiv 6(\mathrm{mod} 8)$. Άτοπο.

Συνεπώς, και πάλι λόγω της πρότασης 1.2.3, απεδείχθη και το δεύτερο μέρος του λήμματος.□

Στην συνέχεια, κάνοντας χρήση του λήμματος 1.2.4, θα αποδείξουμε την ακόλουθη πρόταση :

Πρόταση 1.2.5 *Έστω*

$$t = \begin{cases} 1 & , \alpha\nu\ (\frac{q}{r}) = 1 \cdot \\ 2 & , \alpha\nu\ (\frac{q}{r}) = -1 \cdot \end{cases}$$

Η διοφαντική εξίσωση $qx^2 - ry^2 = t$ *είναι επιλύσιμη στο* $\mathbb{Z}$. *Θέτουμε* $\mu = t - y\sqrt{-tr}$, $v = 2(t - x\sqrt{tq})$, $\bar{\mu} = t + y\sqrt{-tr}$, $\bar{v} = 2(t + x\sqrt{tq})$ *και θεωρούμε τα τέσσερα σώματα:* $k(\sqrt{w\mu})$, $w = \pm1,\pm2$. *Τα σώματα αυτά είναι κυκλικές επεκτάσεις του* k *βαθμού 4 και διεδρικές επεκτάσεις του* $\mathbb{Q}$ *με* $G(k(\sqrt{w\mu})/k) =<\sigma> \rtimes <\tau>$ *όπου* $\sigma^4 = \tau^2 = 1$ *και* $\sigma(\sqrt{-qr}) = \sqrt{-qr}$, $\sigma(\sqrt{w\mu}) = \sqrt{w\bar{\mu}}$, $\tau(\sqrt{-qr}) = -\sqrt{-qr}$, $\tau(\sqrt{w\mu}) = \sqrt{w\mu}$. *Επίσης τα σώματα αυτά είναι δικεκριμμένα και μη διακλαδιζόμενα εκτός του 2 πάνω απο το* k *και το διάγραμμα Galois των σωμάτων φαίνεται ακόλουθα:*

$$\begin{tikzcd}
 & & k(\sqrt{w\mu}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt{wv}) & \mathbb{Q}(\sqrt{w\bar{v}}) & k(\sqrt{tq}) & \mathbb{Q}(\sqrt{w\bar{\mu}}) & \mathbb{Q}(\sqrt{w\mu}) \\
 & \mathbb{Q}(v) \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] & k \arrow[u, dash] & \mathbb{Q}(\mu) \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] & \\
 & & \mathbb{Q} \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] & &
\end{tikzcd}$$

Σχήμα 1

Απόδειξη: Έχουμε ότι η $x^2 - qry^2 = tq$ είναι επιλύσιμη στο $\mathbb{Z}$ οπότε $q \mid x$ και συνεπώς η $qx^2 - ry^2 = t$ είναι επιλύσιμη στο $\mathbb{Z}$. Έστω λοιπόν x, y ακέραια λύση της $qx^2 - ry^2 = t$ και θέτουμε $\mu = t - y\sqrt{-tr}$, $v = 2(t - x\sqrt{tq})$, $\bar{\mu} = t - y\sqrt{-tr}$, $\bar{v} = 2(t + x\sqrt{tq})$ και θεωρούμε τα τέσσερα σώματα: $k(\sqrt{w\mu})$, $w = \pm1,\pm2$. Έχουμε $qx^2 = t + ry^2$ οπότε $tqx^2 = t^2 + try^2$ και συνεπώς

$tqx^2 = (t + y\sqrt{-tr})(t - y\sqrt{-tr})$ που τελικά δίνει $tqx^2 = \bar{\mu}\mu$. Προφανώς ισχύει το ακόλουθο διάγραμμα Galois:

$$\begin{tikzcd}[arrows=dash]
 & k(\sqrt{tq}) = k(\mu) = k(v) \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{Q}(v) \arrow[dr] & k \arrow[d] & \mathbb{Q}(\mu) \arrow[dl] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Σχήμα 2

Παρατηρούμε ότι οι ρίζες του αναγώγου πολυωνύμου του $w\mu$ πάνω από το $\mathbb{Q}$ είναι οι $\pm\sqrt{w\mu}$, $\pm\sqrt{w\bar{\mu}}$ που δεν ανήκουν όλες στο $\mathbb{Q}(\sqrt{w\mu})$ και αυτό σημαίνει ότι η $\mathbb{Q}(\sqrt{w\mu})/\mathbb{Q}$ δεν είναι Galois. Πράγματι, αν είχαμε $\sqrt{w\bar{\mu}} \in \mathbb{Q}(\sqrt{w\mu})$, τότε λόγω $tqx^2 = \bar{\mu}\mu$ θα είχαμε και $\sqrt{tq} \in \mathbb{Q}(\sqrt{w\mu})$ οπότε και $k(\mu) = k(v) \subset \mathbb{Q}(\sqrt{w\mu})$ (βλ. το διάγραμμα Galois πιο πάνω). Αν θεωρήσουμε λοιπόν το ανάγωγο πολυώνυμο του $\sqrt{w\mu}$ πάνω από το $\mathbb{Q}(v)$, αυτό θα έχει την μορφή $x^2 - (a + bv)$ για κάποια $a, b \in \mathbb{Q}$ και συνεπώς $w^2\mu^2 = a + bv$ που δίνει $\mathbb{Q}(\mu) = \mathbb{Q}(\sqrt{a + bv})$ πού είναι άτοπο αφού η $\mathbb{Q}(\mu)$ είναι βαθμού 2 πάνω από το $\mathbb{Q}$ ενώ η $\mathbb{Q}(\sqrt{a + bv})$ βαθμού 4. Δείξαμε λοιπόν ότι η $\mathbb{Q}(\sqrt{w\mu})/\mathbb{Q}$ δεν είναι Galois . Ισχύει επίσης ότι η $\mathbb{Q}(\sqrt{w\mu})/\mathbb{Q}$ έχει ένα μόνο ενδιάμεσο σώμα: το $\mathbb{Q}(\mu)$. Πράγματι, κάθε ενδιάμεση επέκταση της $\mathbb{Q}(\sqrt{w\mu})/\mathbb{Q}$ είναι της μορφής $\mathbb{Q}(\sqrt{\lambda})$ με $\lambda \in \mathbb{Z}$ ελεύθερο τετραγώνου. Αν είχαμε λοιπόν $\mathbb{Q}(\sqrt{\lambda}) \neq \mathbb{Q}(\mu)$ τότε, λόγω του ότι οι βαθμοί επέκτασης των $\mathbb{Q}(\sqrt{\lambda})$ και $\mathbb{Q}(\mu)$ πάνω από το $\mathbb{Q}$ είναι ίδιοι, θα συμπεραίναμε ότι $\mathbb{Q}(\sqrt{w\mu}) = \mathbb{Q}(\sqrt{\lambda}, \mu)$ που δεν μπορεί να ισχύει αφού η $\mathbb{Q}(\sqrt{\lambda}, \mu)/\mathbb{Q}$ είναι Galois. Μπορούμε τώρα εύκολα να δούμε ότι το σώμα $\mathbb{Q}(\sqrt{w\mu})$ δεν περιέχει κανένα από τα $Q(v), k$ και ότι είναι διαφορετικό από τα $\mathbb{Q}(\sqrt{w\bar{\mu}})$, $\mathbb{Q}(\sqrt{wv})$, $\mathbb{Q}(\sqrt{w\bar{v}})$, $\mathbb{Q}(\sqrt{w\bar{v}})$. Παρόμοια μπορούμε να δούμε ότι και η $\mathbb{Q}(\sqrt{w\bar{\mu}})/\mathbb{Q}$ δεν είναι Galois και ότι έχει μόνο ένα ενδιάμεσο σώμα: το $\mathbb{Q}(\bar{\mu})$. Ακόλουθα, θα δείξουμε ότι $\sqrt{w\bar{\mu}},\ \sqrt{wv},\ \sqrt{w\bar{v}}\ \in k(\sqrt{w\mu})$. Έχουμε $\sqrt{w\mu}\sqrt{w\bar{\mu}} = \sqrt{w^2tqx^2} = wx\sqrt{tq}$. Όμως $k(\sqrt{tq}) = k(\frac{q\sqrt{-tr}}{-qr}) = k(\sqrt{-tr}) = k(\mu) \subset k(\sqrt{w\mu})$ οπότε $\sqrt{w\bar{\mu}} \in k(\sqrt{tq}, \sqrt{w\mu}) = k(\sqrt{w\mu})$. Άρα $\sqrt{w\bar{\mu}} \in k(\sqrt{w\mu})$. Επίσης, $(\sqrt{w\mu} \pm \sqrt{w\bar{\mu}})^2 = w\mu + w\bar{\mu} \pm 2w\sqrt{\mu\bar{\mu}} = w(\mu + \bar{\mu}) \pm 2w\sqrt{\mu\bar{\mu}} = 2tw \pm 2xw\sqrt{tq} = 2w(t \pm x\sqrt{tq})$. Συμπεραίνουμε λοιπόν ότι:

$$(\sqrt{w\mu} + \sqrt{w\bar{\mu}})^2 = (\sqrt{w\bar{v}})^2 \quad \text{και} \quad (\sqrt{w\mu} - \sqrt{w\bar{\mu}})^2 = (\sqrt{wv})^2$$

πράγμα που σημαίνει ότι $\sqrt{wv},\ \sqrt{w\bar{v}}\ \in k(\sqrt{w\mu})$. Στην συνέχεια θα δείξουμε ότι η $k(\sqrt{w\mu})/k$ είναι κυκλική βαθμού 4 και η $k(\sqrt{w\mu})/\mathbb{Q}$ Galois με ομάδα Galois την διεδρική ομάδα $\mathcal{D}_4$. Κατ' αρχήν οι ρίζες του αναγώγου πολυωνύμου του $\sqrt{w\mu}$ πάνω από το $\mathbb{Q}$ όπως έχουμε πεί είναι οι $\pm\sqrt{w\mu}$, $\pm\sqrt{w\bar{\mu}}$ οι οποίες δείξαμε ότι ανήκουν στο $k(\sqrt{w\mu})$ και συνεπώς η $k(\sqrt{w\mu})/\mathbb{Q}$ είναι Galois . Άρα και η $k(\sqrt{w\mu})/k$ είναι Galois και έστω $\sigma \in G(k(\sqrt{w\mu})/k)$ με $\sigma(\sqrt{w\mu}) = \sqrt{w\bar{\mu}}$. Τα $\mathbf{1},\ \sigma,\ \sigma^2,\ \sigma^3$ είναι όλα διαφορετικά μεταξύ τους. Προς απόδειξη τούτου θα δείξουμε ότι τα $\mathbf{1},\ \sigma,\ \sigma^2,\ \sigma^3$ παίρνουν διαφορετικές τιμές στο $\sqrt{w\mu}$. Προφανώς: $\mathbf{1}(\sqrt{w\mu}) = \sqrt{w\mu},\ \sigma(\sqrt{w\mu}) = \sqrt{w\bar{\mu}}$. Αφού $\sigma(\sqrt{w\mu}) = \sqrt{w\bar{\mu}}$, θα ισχύει $\sigma(\sqrt{w\mu}^2) = \sqrt{w\bar{\mu}}^2$ και συνεπώς $\sigma(\mu) = \bar{\mu}$. Αλλά $\mu = t - y\sqrt{-tr}$ πράγμα που σημαίνει ότι $\sigma(\sqrt{-tr}) = -\sqrt{-tr}$. Επομένως έχουμε

$$\sigma(\sqrt{tq}) = \sigma\left(\frac{\sqrt{-qrt^2}}{\sqrt{-tr}}\right) = \frac{t\sigma(\sqrt{-qr})}{\sigma(\sqrt{-tr})} = \frac{t\sqrt{-qr}}{-\sqrt{-tr}} = -\sqrt{tq}$$

πράγμα που σημαίνει ότι

$$\sigma^2(\sqrt{w\mu}) = \sigma(\sqrt{w\bar{\mu}}) = \sigma\left(\sqrt{\frac{w^2tqx^2}{w\mu}}\right) = \frac{xw\sigma(\sqrt{tq})}{\sigma(w\bar{\mu})} = \frac{-xw\sqrt{tq}}{w\bar{\mu}} = \frac{-xw\sqrt{tq}}{\sqrt{\frac{wtqx^2}{\mu}}} = -\sqrt{w\mu}.$$

Επίσης είναι εύκολο να δούμε ότι $\sigma^3(\sqrt{w\mu}) = \sigma(-\sqrt{w\mu}) = -\sqrt{w\bar{\mu}}$ και $\sigma(\sqrt{w\bar{\mu}}) = -\sqrt{w\bar{\mu}}$, $\sigma(\mu) = \bar{\mu}$, $\sigma(v) = \sigma(\bar{v})$. Σύμφωνα με τα παραπάνω: $G(k(\sqrt{w\mu})/k) = \langle\sigma\rangle$. Έστω τώρα $\tau \in G(k/\mathbb{Q})$ με $\sqrt{-qr} = -\sqrt{-qr}$. Επεκτείνουμε το τ στην $G(k(\sqrt{w\mu})/\mathbb{Q})$ με $\tau(\sqrt{w\mu}) = \sqrt{w\mu}$ και έχουμε τα ακόλουθα:

$$(\tau\sigma)(\sqrt{-qr}) = \tau(\sqrt{-qr}) = -\sqrt{-qr}$$
$$(\sigma^3\tau)(-qr) = -\sigma^3(\sqrt{-qr}) = -\sqrt{-qr}$$

Εξάλλου, $\tau(\sqrt{w\mu}) = \sqrt{w\mu} \Rightarrow \tau(\mu) = \mu \Rightarrow \tau(\sqrt{-tr}) = \sqrt{-tr}$. Συνεπώς

$$\tau(\sqrt{tq}) = \tau\left(\frac{\sqrt{-qrt^2}}{\sqrt{-tr}}\right) = \frac{t\tau(\sqrt{-qr})}{\tau(\sqrt{-tr})} = \frac{-t\sqrt{-qr}}{\sqrt{-tr}} = -\sqrt{tq}$$

που σημαίνει ότι:

$$\tau(\sqrt{w\bar{\mu}}) = \tau\left(\sqrt{\frac{w^2tqx^2}{w\mu}}\right) = \frac{xw\tau(\sqrt{tq})}{\tau(w\mu)} = \frac{-xw\sqrt{tq}}{w\mu} = \frac{-xw\sqrt{tq}}{\sqrt{\frac{wtqx^2}{\bar{\mu}}}} = -\sqrt{w\bar{\mu}}.$$

και τελικά έχουμε:

$$(\tau\sigma)(\sqrt{w\mu}) = \tau(\sqrt{w\bar{\mu}}) = -\sqrt{w\bar{\mu}}$$
$$(\sigma^3\tau)(\sqrt{w\mu}) = \sigma^3(\sqrt{w\mu}) = -\sqrt{w\bar{\mu}}$$

που αποδεικνύει ότι: $G(k(\sqrt{w\mu})/\mathbb{Q}) = \langle\sigma\rangle \rtimes \langle\tau\rangle$. Θα δείξουμε τώρα ότι η επέκταση $k(\sqrt{w\mu})/k$ είναι μη διακλαδιζομένη εκτός του 2. Έχουμε $k(\sqrt{tq}) = k(\sqrt{-tr})$ και από θεωρία επεκτάσεων του Kummer (βλ. [6] chapter V §39) έχουμε ότι η επέκταση $k(\sqrt{tq})/k$ είναι μη διακλαδιζομένη εκτός του 2 οπότε αρκεί να δείξουμε ότι η $G(k(\sqrt{w\mu})/k(\sqrt{tq}))$ είναι μη διακλαδιζομένη εκτός του 2. Πράγματι, έστω $\mathfrak{p}$ πρώτο ιδεώδες του $R_{k(\sqrt{tq})}$ με $\mathfrak{p} \nmid 2$. Θα δείξουμε ότι ένα εκ των $x^2 - wv,\ x^2 - w\mu$ είναι διαχωρίσιμο modulo $\mathfrak{p}$, πράγμα που, λόγω της ισότητας $k(\sqrt{wv}) = k(\sqrt{w\mu})$, θα μας δώσει ότι το $\mathfrak{p}$ δεν διακλαδίζεται στο $k(\sqrt{w\mu})$. Έστω ότι κανένα από τα $x^2 - wv,\ x^2 - w\mu$ δεν είναι διαχωρίσιμο modulo $\mathfrak{p}$. Αυτό σημαίνει ότι για κάθε πρώτο ιδεώδες $\mathfrak{q}$ του $R_{k(\sqrt{w\mu})}$ με $\mathfrak{q} \mid \mathfrak{p}$ θα είχαμε αφ' ενός $\mathfrak{q} \nmid 2$ και αφ' ετέρου

$$\sqrt{wv} \equiv -\sqrt{wv} (\mathrm{mod} \mathfrak{q}) \ \text{ και } \ \sqrt{w\mu} \equiv -\sqrt{w\mu} (\mathrm{mod} \mathfrak{q}).$$

Συνεπώς $2\sqrt{wv}, 2\sqrt{w\mu} \in \mathfrak{q} \ \Rightarrow 4wv, 4w\mu \in \mathfrak{q}$. Αφού όμως $\mathfrak{q} \nmid 2$ θα έχουμε $\mathfrak{q} \mid v, \mu$ και συνεπώς $\mathfrak{q} \mid v\bar{v} - 4\mu\bar{\mu}$. Αφού $v\bar{v} - 4\mu\bar{\mu} = -4t^2$ προκύπτει ότι $\mathfrak{q} \mid -4t^2 \Rightarrow \mathfrak{q} \mid 2$. Άτοπο.$\square$

Η σύνδεση της προηγούμενης πρότασης με το πρόβλημα που μελετούμε θα φανεί μετά από το ακόλουθο λήμμα:

Λήμμα 1.2.6 *Κάθε κυκλική επέκταση L πάνω από το $k = \mathbb{Q}(\sqrt{-qr})$ βαθμού 4 μή διακλαδιζόμενη εκτός του 2 η οποία είναι και διεδρική επέκταση του $\mathbb{Q}$ περιέχεται σε κάθε $k(D_s)$ για κάθε $s \geq 4$ και συνεπώς περιέχεται και στο $k(D_4) = k(D)$.*

Απόδειξη: Σύμφωνα με το θεώρημα 11 του [10] , το L περιέχεται σε ένα ring class field πάνω από το k και αφού η L είναι μη διακλαδιζόμενη εκτός του 2 επέκταση του k, έπεται ότι το L θα περιέχεται σε κάποιο $k_2(D_{s_0})$ για κάποιο $s_0 \geq 2$. Όμως η ομάδα πηλίκο της $H_2(D_{s_0})$ modulo $G(k_2(D_{s_0})/L)$ είναι $G(L/k) = (2^2)$ και έτσι $s_0 \geq 4$. Επίσης, αφού η ομάδα πηλίκο της $H_2(D_{s_0})$ modulo $G(k_2(D_{s_0})/L)$ είναι κυκλική βαθμού 4, θα έχουμε ότι η $G(k_2(D_{s_0})/L)$ είναι μία εκ' των $\left\langle A_{s_0}^2 B_{s_0}, C_{s_0}\right\rangle$, $\left\langle A_{s_0}^2 C_{s_0}, B_{s_0}\right\rangle$, $\left\langle A_{s_0}^2 B_{s_0}, B_{s_0} C_{s_0}\right\rangle$ και $\left\langle A_{s_0}^4, B_{s_0}, C_{s_0}\right\rangle$. Αλλά $G(k_2(D_{s_0})/k_2(D_4)) = \left\langle A_{s_0}^{2^{c(4)}}\right\rangle$ οπότε $G(k_2(D_{s_0})/k_2(D_4)) \subseteq G(k_2(D_{s_0})/L)$ που σημαίνει $L \subseteq k_2(D_4) \subseteq k_2(D_s)$, για κάθε $s \geq 4$. $\square$

Σύμφωνα λοιπον με το παραπάνω λήμμα τα σώματα $k(\sqrt{w\mu})$, $w = \pm 1, \pm 2$ που είχαμε βρεί περιέχονται στο $k(D)$ το οποίο περιέχει ακριβώς 4 υποσώματα βαθμού 4 κυκλικά πάνω από το k. Συνεπώς:

$$\{L_{A_s^2 B_s, C_s}, L_{A_s^2 C_s, B_s}, L_{A_s^2 B_s, B_s C_s}, L_{A_s^4, B_s, C_s}\} = \{k(\sqrt{\mu}), k(\sqrt{-\mu}), k(\sqrt{2\mu}), k(\sqrt{-2\mu})\}.$$

Τώρα είναι προφανές ότι το σώμα $L_0 = L_{A_s^2, B_s, C_s}$ που είχαμε θεωρήσει αρχικά είναι το $k(\sqrt{tq})$ αφού είναι η τομή των $L_{A_s^2 B_s, C_s}$, $L_{A_s^2 C_s, B_s}$, $L_{A_s^2 B_s, B_s C_s}$, $L_{A_s^4, B_s, C_s}$.

Πριν συνεχίσουμε παρατηρούμε τα ακόλουθα:

Λήμμα 1.2.7 *Για όλα τα* $\iota \in \{0, 1, ...c(s)\}, j \in \{0, 1\}$ *και* $\ell \in \{0, 1\}$ *έχουμε:*

$$L_{A_{s+1}^{2^\iota}, B_{s+1}^j, C_{s+1}^\ell} = L_{A_s^{2^\iota}, B_s^j, C_s^\ell}$$

<u>Απόδειξη:</u> Από λήμμα 1.2.2 έχουμε

$$L_{A_{s+1}^{2^\iota}, B_{s+1}^j, C_{s+1}^\ell} \supseteq L_{A_s^{2^\iota}, B_s^j, C_s^\ell}.$$

Αυτά τα δύο σώματα είναι ίδιου βαθμού $2^{\iota+2-j-\ell}$ πάνω από το k και συνεπώς πρέπει να ταυτίζονται.$\square$

Πόρισμα 1.2.8

$$L_{A_{s+1}^{2^{c(s)}}, B_{s+1}, C_{s+1}} = L_{B_s, C_s}, \quad L_{A_{s+1}^{2^{c(s)}}} = L_{I_s} = k_2(D_s).$$

Το $L_{A_s^4,B_s,C_s}$ εμφυτεύεται σε μια κυκλική επέκταση βαθμου 8 πάνω απο το k (την $L_{A_{s+1}^8,B_{s+1},C_{s+1}}/k$). Από [12] και το local global principle, έχουμε το ακόλουθο αποτέλεσμα:

Πρόταση 1.2.9 *Άν $M/\mathbb{Q}$ επέκταση αλγεβρικών σωμάτων αριθμών όπου $M = \mathbb{Q}(\sqrt{z(A+B\sqrt{a})},\sqrt{b})$ με $A^2 - aB^2 = ab$, $a, b \in \mathbb{Q}$ όχι τετραγωνικώς ισοδύναμα, $A, B \in \mathbb{Q}$ και $z \in \mathbb{Q}$, τότε το M είναι διεδρική επέκταση του $\mathbb{Q}$ βαθμού 8 κυκλική πάνω από το $\mathbb{Q}(\sqrt{b})$. Επιπλέον το M μπορεί να εμφυτευθεί σε μια διεδρική επέκταση βαθμού 16 πάνω από το $\mathbb{Q}$ αν και μόνο αν:*

$$\left(\frac{-b,-zA}{p}\right) = \left(\frac{-ab,-2a}{p}\right)$$

για κάθε πρώτο αριθμό p, όπου $(\frac{\cdot,\cdot}{p})$ είναι το σύμβολο του Hilbert .

Στην συνέχεια θα υπολογίσουμε το σώμα $L_{A_s^4,B_s,C_s}$:

Πρόταση 1.2.10

$$L_{A_s^4,B_s,C_s} = \begin{cases} k(\sqrt{-2\mu}) & , \text{αν } (\frac{q}{r}) = 1 \cdot \\ k(\sqrt{-\mu}) & , \text{αν } (\frac{q}{r}) = -1 \cdot \end{cases}$$

και από όλα τα $L_{A_s^2B_s,C_s}$, $L_{A_s^2C_s,B_s}$, $L_{A_s^2B_s,B_sC_s}$, $L_{A_s^4,B_s,C_s}$ μόνο το $L_{A_s^4,B_s,C_s}$ εμφυτεύεται σε κυκλική επέκταση βαθμου 8 πάνω από το k που είναι διεδρική βαθμού 16 πάνω από το $\mathbb{Q}$.

Απόδειξη: Για τον ορισμό και τις ιδιότητες του συμβόλου του Hilbert παραπέμπουμε τον αναγνώστη στο [1].

- Αν $(\frac{q}{p}) = 1$, τότε γράφουμε

$$k(\sqrt{w\mu}) = \mathbb{Q}\left(\sqrt{w\frac{x}{r}\left(\frac{r}{x} - \frac{r}{x}y\sqrt{-r}\right)}, \sqrt{-qr}\right)$$

και επομένως από την πρόταση 1.2.9 έχουμε ότι αν $L_{A_s^4,B_s,C_s} = k(\sqrt{w\mu})$ τότε για κάθε πρώτο p με
$(\frac{qr,-w}{p})= (\frac{-qr^2,2r}{p})$ θα έχουμε ότι:

- Η περίπτωση $w = -1$ οδηγεί σε άτοπο αφού $(\frac{qr,1}{q})= 1$ και $(\frac{-qr^2,2r}{q})= -1$.
- Η περίπτωση $w = 2$ οδηγεί σε άτοπο αφού $(\frac{qr,-2}{r})= 1$ και $(\frac{-qr^2,2r}{r})= -1$.
- Η περίπτωση $w = 1$ οδηγεί σε άτοπο αφού $(\frac{qr,-1}{q})= 1$ και $(\frac{-qr^2,2r}{q})= -1$.

Άρα κατ' ανάγκη $w = -2$.

- Αν $(\frac{q}{p})= -1$, τότε γράφουμε

$$k(\sqrt{w\mu}) = \mathbb{Q}\left(\sqrt{w\frac{x}{r}\left(\frac{2r}{x} - \frac{r}{x}y\sqrt{-2r}\right)}, \sqrt{-qr}\right)$$

και, πάλι από την πρόταση 1.2.9, έχουμε ότι αν $L_{A_s^4,B_s,C_s} = L(\sqrt{w\mu})$ τότε για κάθε πρώτο p με
$(\frac{qr,-2w}{p})= (\frac{-2qr^2,4r}{p})$ ή ισοδύναμα $(\frac{qr,-2w}{p})= (\frac{-2q,r}{p})$ θα έχουμε ότι:

- Η περίπτωση $w = 1$ οδηγεί σε άτοπο αφού $(\frac{qr,-2}{r})= 1$ και $(\frac{-2q,r}{r})= -1$.
- Η περίπτωση $w = -2$ οδηγεί σε άτοπο αφού $(\frac{qr,4}{r})= 1$ και $(\frac{-2q,r}{r})= -1$.
- Η περίπτωση $w = 2$ οδηγεί σε άτοπο αφού $(\frac{qr,-4}{q})= 1$ και $(\frac{-2q,r}{q})= -1$.

Άρα κατ' ανάγκη $w = -1$. $\square$

1.3 Κύρια αποτελέσματα

Περιοριζόμαστε τώρα στην περίπτωση $s = 4$ και για απλότητα στον συμβολισμό θα παραλείπουμε τον δείκτη s υποθέτοντας πάντοτε ότι βρισκόμαστε στην περίπτωση $s = 4$.

Θεώρημα 1.3.1 *Έστω*

$$t = \begin{cases} 1 & ,\ \text{αν}\ (\frac{q}{r}) = 1, \\ 2 & ,\ \text{αν}\ (\frac{q}{r}) = -1 \end{cases}$$

και έστω $x, y \in \mathbb{Z}$ με $qx^2 - ry^2 = t$. Έστω επίσης p περιττός πρώτος με

$$(\frac{D}{p}) = 1 \quad \text{και} \quad (\frac{tq}{p}) = 1$$

Θέτουμε $\mu = t - y\sqrt{-tr}$ και ορίζουμε το σύμβολο u_p ως εξής:

$$u_p = \begin{cases} (-1)^{\frac{p-1}{2}}, & \text{αν}\ p \mid x, \\ (\frac{-\mu}{p}), & \text{αν}\ p \nmid x\ \text{και}\ (\frac{q}{r}) = -1, \\ (\frac{-2\mu}{p}), & \text{αν}\ p \nmid x\ \text{και}\ (\frac{q}{r}) = 1, \end{cases}$$

όπου στα σύμβολα Legendre, που εμφανίζονται, σαν $\sqrt{-tr}$ θεωρούμε τυχαία ακέραια λύση της επιλύσιμης ισοδυναμίας $x^2 \equiv -tr(\mathrm{mod} p)$. (Ο αναγνώστης μπορεί να παρατηρήσει ότι το σύμβολο u_p είναι έτσι ορισμένο ωστε $u_p = 1$ αν και μόνο αν $f_p(L_{A^4,B,C}) = 1$). Κάτω από αυτές τις υποθέσεις και με αυτόν το συμβολισμό, ισχύουν τα ακόλουθα:

- *Στην περίπτωση Ια όπου $\left(\frac{q}{r}\right) = -1$ έχουμε ότι ο $p^{\hbar'}$ παρίσταται από ακριβώς μία ambiguous κλάση και ακριβέστερα:*
  - *Αν $p \equiv 1(\mathrm{mod} 8)$ τότε: $I \longrightarrow p^{\hbar'} \Leftrightarrow u_p = 1$ και $A^2 \longrightarrow p^{\hbar'} \Leftrightarrow u_p = -1 \cdot$*

– *Αν* $p \equiv 7(\bmod 8)$ *τότε:* $B \longrightarrow p^{\hbar'} \Leftrightarrow u_p = 1$ *και* $A^2B \longrightarrow p^{\hbar'} \Leftrightarrow u_p = -1\cdot$

– *Αν* $p \equiv 5(\bmod 8)$ *τότε:* $C \longrightarrow p^{\hbar'} \Leftrightarrow u_p = 1$ *και* $A^2C \longrightarrow p^{\hbar'} \Leftrightarrow u_p = -1\cdot$

– *Αν* $p \equiv 3(\mathrm{mod}8)$ *τότε:* $BC \longrightarrow p^{\hbar'} \Leftrightarrow u_p = 1$ *και* $A^2BC \longrightarrow p^{\hbar'} \Leftrightarrow u_p = -1$.

- *Στην περίπτωση Ιβ όπου* $\left(\frac{q}{r}\right) = 1$ *έχουμε:*

  – *Αν* $u_p = -1$ *τότε* $A^4 \longrightarrow p^{2\hbar'}$ *αλλά καμία ambiguous κλάση δεν παριστά τον* $p^{\hbar'}\cdot$

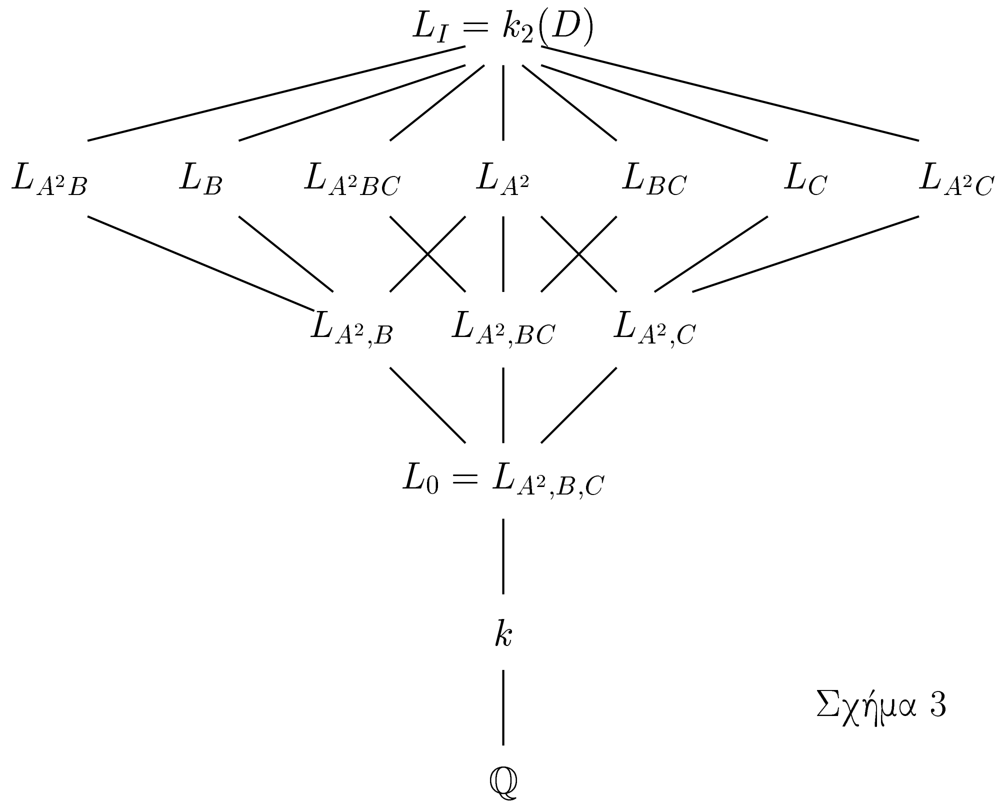
  – *Αν* $u_p = 1$ *τότε ο* $p^{\hbar'}$ *παρίσταται απο ακριβώς μία ambiguous κλάση.*

Απόδειξη: Η πρόταση 1.2.10 μας δίνει ότι $L_{A^4,B,C} = k(\sqrt{-2t\mu})$. Κατ΄ αρχή θα δείξουμε ότι το σύμβολο u_p έχει οριστεί κατά τέτοιο τρόπο για τα p που αναφέρονται στην εκφώνηση ώστε να ισχύει $u_p = 1$ αν και μόνο αν $f_p(L_{A^4,B,C}) = 1)$. Πράγματι, παρατηρούμε αρχικά ότι η συνθήκη

$$(\frac{tq}{p})= 1$$

που θέλουμε να ικανοποιεί το p είναι ισοδύναμη (βλ. σχήμα στην πρόταση 1.2.5) λόγω $(\frac{D}{p})= 1$ με το ότι $f_p(L_0) = 1$ και συνεπώς ο p αναλύεται πλήρως στο $L_{A^4,B,C}$ αν και μόνο αν $f_p(L_{A^4,B,C}/L_0) = 1$ ή ισοδύναμα αν και μόνο αν $(\frac{-2t\mu}{p})= 1$. Επειδή το u_p έχει οριστεί έτσι ώστε για κάθε $p \nmid x$ να ισχύει $u_p = (\frac{-2t\mu}{p})$ η ισοδυναμία που ζητάμε ισχύει προφανώς για όλα τα $p \nmid x$, ενώ για τα p με $p \mid x$ μπορούμε να δούμε ότι αφού $k(\sqrt{w\mu}) = k(\sqrt{wv})$ θα ισχύει και $L_{A^4,B,C} = k(\sqrt{-2tv})$ οπότε αφού $v \equiv 2t (mod p)$, έχουμε τελικά ότι

$$f_p(L_{A^4,B,C}/L_0) = 1 \Leftrightarrow (\frac{-2tv}{p}) = 1 \Leftrightarrow (\frac{-4t^2}{p}) = 1 \Leftrightarrow (\frac{-1}{p}) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}}.$$



Σχήμα 3

Στην συνέχεια μελετούμε την περίπτωση Ια όπου $\left(\frac{q}{r}\right) = -1$. Στην περίπτωση αυτή η ομάδα κλάσεων είναι η $H(D) = \langle A, B, C \rangle$ με $A^4 = B^2 = C^2 = I$ και οι ambiguous κλάσεις είναι οι I, A^2, B,C, A^2B, A^2C, BC και A^2BC. Έχουμε $f_p(L_0) = 1$ και αφού $L_{A^2}/L_{A^2,B,C}$ είναι τύπου $(2, 2)$, ακριβώς ένα από τα $f_p(L_{A^2,B})$, $f_p(L_{A^2,BC})$, $f_p(L_{A^2,C})$ ισούται με 1 ή όλα είναι ίσα με 1 (βλ. σχήμα 3).

- Αν $f_p(L_{A^2,B}) = f_p(L_{A^2,BC}) = f_p(L_{A^2,C}) = 1$ τότε $f_p(L_{A^2}) = 1$ και επομένως, το σώμα ανάλυσης του p στην $k_2(D)$ είναι είτε το L_I είτε το

L_{A^2} , οπότε $I \longrightarrow p^{\hbar'}$ ή $A^2 \longrightarrow p^{\hbar'}$.

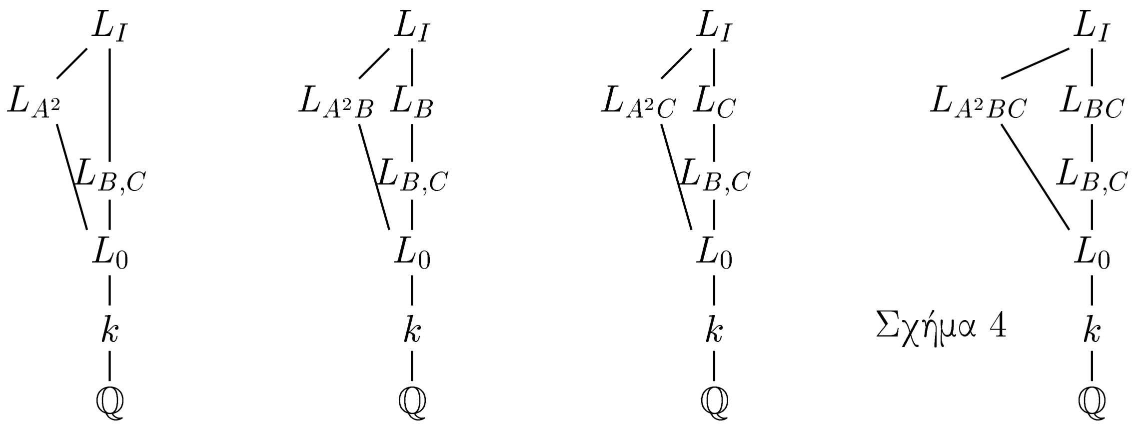
- Αν ακριβώς ένα από τα $f_p(L_{A^2,B})$, $f_p(L_{A^2,BC})$, $f_p(L_{A^2,C})$ ισούται με 1 τότε $f_p(L_{A^2}) \neq 1$ και

  - Αν $f_p(L_{A^2,B}) = 1$ τότε, αφού $L_I/L_{A^2,B}$ είναι τύπου $(2,2)$, θα έχουμε $f_p(L_{A^2B}) = 1$ ή $f_p(L_B) = 1$ και επομένως το σώμα ανάλυσης του p στο $k_2(D)$ θα είναι ή το L_{A^2B} ή το L_B, οπότε $A^2B \longrightarrow p^{\hbar'}$ ή $B \longrightarrow p^{\hbar'}$.

  - Αν $f_p(L_{A^2,BC}) = 1$ τότε, εργαζόμενοι όπως παραπάνω, έχουμε ότι $A^2BC \longrightarrow p^{\hbar'}$, ή $BC \longrightarrow p^{\hbar'}$..

  - Αν $f_p(L_{A^2,C}) = 1$ τότε, και πάλι εργαζόμενοι όπως παραπάνω, έχουμε ότι $A^2C \longrightarrow p^{\hbar'}$ ή $C \longrightarrow p^{\hbar'}$.

Αυτό που μέχρι τώρα έχουμε δείξει είναι το αντίστροφο της πρότασης 1.1.4. Στην συνέχεια θα διαχωρίσουμε τις ambiguous κλάσεις. Έχουμε υποθέσει ότι $(\frac{D}{p})= 1$ και $(\frac{tq}{p})= 1$, συνεπώς $f_p(L_0) = 1$. Επίσης $u_p = 1$ ακριβώς τότε όταν $f_p(L_{B,C} = 1$. Αν $p \equiv 7(\mathrm{mod}8)$ δείξαμε πριν ότι μία εκ των B, A^2B παριστά τον $p^{\hbar'}$, οπότε το σώμα ανάλυσης του p στο $k_2(D)$ είναι ή το L_B ή το L_{A^2B}. Αφού το σώμα L_{A^2B} είναι γνήσιο υποσύνολο του $L_{B,C}L_{A^2B}$, έχουμε ότι το σώμα ανάλυσης του p στην $k_2(D)$ είναι το L_B αν και μόνο αν $u_p = 1$ και έτσι $B \longrightarrow p^{\hbar'}$ αν και μόνο αν $u_p = 1$. Οι άλλες περιπτώσεις στις οποίες $p \equiv 1, 3, 5(\mathrm{mod}8)$ μπορούν να αποδειχθούν εντελώς ανάλογα (βλ. σχήμα 4).



Σχήμα 4

Συνεχίζουμε με την περίπτωση Ιβ στην οποία $\left(\frac{q}{r}\right) = 1$. Εδώ η ομάδα κλάσεων είναι η $H(D) = \langle A, B, C\rangle$ με $A^8 = B^2 = C^2 = I$ και οι ambiguous κλασεις είναι I, A^4, B, C, A^4B, A^4C, BC και A^4BC. Υπενθυμίζουμε ότι $u_p = 1$ αν και μόνο αν $f_p(L_{A^4,B,C}) = 1$. Έχουμε $f_p(L_0) = 1$ και επειδή η επέκταση $L_{A^2}/L_{A^2,B,C}$ είναι του τύπου $(2,2)$, ακριβώς ένας εκ των βαθμών αδρανείας $f_p(L_{A^2,B})$, $f_p(L_{A^2,BC})$, $f_p(L_{A^2,C})$ είναι ίσος με 1, ή όλοι είναι ίσα με 1 (βλ. σχήμα 5).

- Αν $f_p(L_{A^2,B}) = f_p(L_{A^2,BC}) = f_p(L_{A^2,C}) = 1$ τότε $f_p(L_{A^2}) = 1$. Επιπλέον:
  - Αν $f_p(L_{A^4,B,C}) = 1$ τότε και $f_p(L_{A^2}L_{A^4,B,C}) = 1$. Η σύνθεση όμως των σωμάτων L_{A^2} και $L_{A^4,B,C}$ είναι το σώμα L_{A^4}. Επομένως θα είχαμε $f_p(L_{A^4}) = 1$ πράγμα που σημαίνει ότι $A^4 \longrightarrow p^{h'}$ ή $I \longrightarrow p^{h'}$.(Σημείωση Το σώμα $L_{A^4,B,C}$ δεν παρίσταται στο διάγραμμα του σχήματος 5.)
  - Αν $f_p(L_{A^4,B,C}) = -1$ τότε $f_p(L_{A^4}) = -1$ και έτσι $A^2 \longrightarrow p^{h'}$ που σημαίνει ότι $A^4 \longrightarrow p^{2h'}$ αλλα ο $p^{h'}$ δεν παρίσταται από καμία am-

biguous κλάση.

- Αν ακριβώς ένα εκ των $f_p(L_{A^2,B})$, $f_p(L_{A^2,BC})$, $f_p(L_{A^2,C})$ ισούται με 1 τότε $f_p(L_{A^2}) \neq 1$. Συνεπώς:

  - Αν $f_p(L_{A^2,B}) = 1$ τότε

    * Αν $f_p(L_{A^4,B,C}) = 1$ τότε, αφού $L_{A^2B}L_{A^4,B,C} = L_{A^4}$, θα είχαμε $f_p(L_{A^2B}) = -1$ και έτσι $f_p(L_{A^4,B}) = 1$ που δίνει $f_p(L_{A^4B}) = 1$ ή $f_p(L_B) = 1$ οπότε $A^4B \longrightarrow p^{\hbar'}$ ή $B \longrightarrow p^{\hbar'}$.

    * Αν $f_p(L_{A^4,B,C}) = -1$ τότε $f_p(L_{A^4,B}) = -1$ επομένως $f_p(L_{A^2B}) = 1$ έτσι $A^2B \longrightarrow p^{\hbar'}$ που δίνει $A^4 \longrightarrow p^{2\hbar'}$ και ο $p^{\hbar'}$ δεν παρίσταται από καμία ambiguous κλάση.

  - Αν $f_p(L_{A^2,C}) = 1$ τότε ομοίως

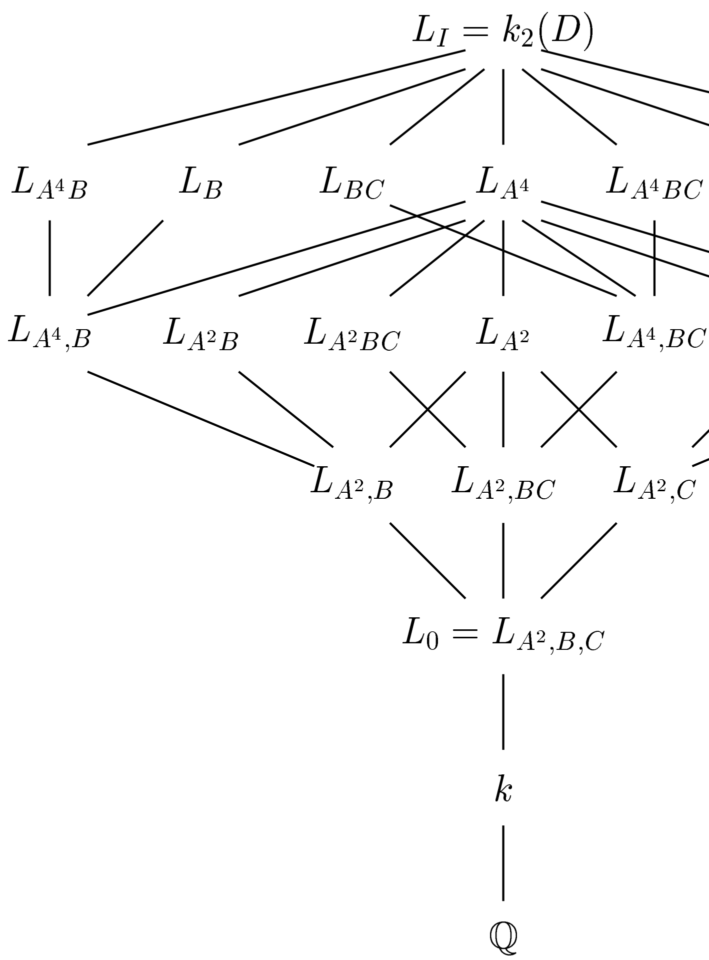
    * Αν $f_p(L_{A^4,B,C}) = 1$ τότε $A^4C \longrightarrow p^{\hbar'}$ ή $C \longrightarrow p^{\hbar'}$.

    * Αν $f_p(L_{A^4,B,C}) = -1$ τότε $A^4 \longrightarrow p^{2\hbar'}$ και ο $p^{\hbar'}$ δεν παρίσταται από καμία ambiguous κλάση.

  - Αν $f_p(L_{A^2,BC}) = 1$ τότε

    * Αν $f_p(L_{A^4,B,C}) = 1$ έχουμε ότι $A^4BC \longrightarrow p^{\hbar'}$ ή $BC \longrightarrow p^{\hbar'}$.

    * Αν $f_p(L_{A^4,B,C}) = -1$ τότε $A^4 \longrightarrow p^{2\hbar'}$ και ο $p^{\hbar'}$ δεν παρίσταται από καμία ambiguous κλάση, δηλαδή αποδείξαμε πλήρως το θεώρημα. $\square$



Σχήμα 5

Κλείνουμε την παράγραφο προσδιορίζοντας τα σώματα $L_{A^2B,C}$, $L_{A^2C,B}$, $L_{A^2B,BC}$ και $L_{A^4,B,C}$. Τα αποτελέσματα παρουσιάζονται στον ακόλουθο πίνακα:

Περίπτωση	$\left(\frac{q}{r}\right)$	$L_{A^4,B,C}$	$L_{A^2C,B}$	$L_{A^2B,C}$	$L_{A^2B,BC}$
Ια	-1	$k(\sqrt{-2\mu})$	$k(\sqrt{-\mu})$	$k(\sqrt{2\mu})$	$k(\sqrt{\mu})$
Ιβ	1	$k(\sqrt{-\mu})$	$k(\sqrt{-2\mu})$	$k(\sqrt{\mu})$	$k(\sqrt{2\mu})$

Απόδειξη: Έστω $\left(\frac{q}{r}\right) = -1$. Από το θεώρημα πυκνότητας του Cebotareb (βλ. [3] θεώρημα 8.17) προκύπτει ότι τα σύνολα $spl(k_2(D))$, $spl(L_{B,C})$, έχουν πυκνότητες

$$\frac{1}{[k_2(D):\mathbb{Q}]} \quad \text{και} \quad \frac{1}{[L_{B,C}:\mathbb{Q}]}$$

αντίστοιχα. Συνεπώς μπορούμε να πάρουμε περιττό πρώτο αριθμό p έτσι ώστε το σώμα ανάλυσης του στο $k_2(D)$ να είναι το L_{BC}, οπότε $BC \longrightarrow p^{2\hbar'}$, και επομένως, λόγω της πρότασης 1.1.4, θα έχουμε $p \equiv 3(\mathrm{mod} 8)$. Έτσι $f_p(L_{A^2B,BC}) = f_p(L_{A^4,B,C}) = 1$ (αφού $L_{A^2B,BC}, L_{A^4,B,C} \subseteq L_{BC}$). Ο βαθμός αδρανείας $f_p(L_{A^4,B,C})$ είναι 1, συνεπάγεται ότι $\left(\frac{-\mu}{p}\right) = 1$ και συνεπώς $\left(\frac{\mu}{p}\right) = -1$. Άρα $L_{A^2B,BC} \neq k(\sqrt{-2\mu})$ και $L_{A^2B,BC} \neq k(\sqrt{\mu})$, συνεπώς $L_{A^2B,BC} = k(\sqrt{2\mu})$. Μπορούμε επίσης να πάρουμε p_1 έτσι ώστε το σώμα ανάλυσης του στο $k_2(D)$ να είναι το L_C το οποίο δίνει $p_1 \equiv 5(\mathrm{mod} 8)$. Ομοίως, όπως προηγουμένως, θα έχουμε $f_{p_1}(L_{A^2B,C}) = f_{p_1}(L_{A^4,B,C}) = 1$ και συνάγουμε ότι θα πρέπει και πάλι $\left(\frac{-\mu}{p_1}\right) = 1$ το οποίο συνεπάγεται ότι $\left(\frac{\mu}{p_1}\right) = 1$. Άρα $L_{A^2B,C} \neq k(\sqrt{-2\mu})$ που δίνει $L_{A^2B,C} = k(\sqrt{\mu})$ και επομένως $L_{A^2C,B} = k(\sqrt{-2\mu})$. Η περίπτωση Ιβ στην οποία $\left(\frac{q}{r}\right) = 1$ μπορεί να μελετηθεί εντελώς όμοια παίρνοντας πρώτους αριθμούς p, p_1 ώστε τα σώματα ανάλυσης τους σο $k_2(D)$ να είναι L_{BC} και L_C αντίστοιχα (κάτι το οποίο θα δώσει $p \equiv 3(\mathrm{mod} 8)$ και $p_1 \equiv 5(\mathrm{mod} 8)$). $\square$

1.4 Το πρόβλημα παράστασης για αυθαίρετο D_s

Στην παράγραφο αυτή προσπαθούμε να δούμε κατά πόσο η παράσταση του $p^{\hbar'_{s_0}}$ από μία ambiguous κλάση διακρίνουσας D_{s_0} επιδρά στην ικανότητα παράστασης του $p^{\hbar'_s}$ από ambiguous κλάση διακρίνουσας D_s , $s \geq s_0 \geq 4$.

Πρόταση 1.4.1 *Αν s ακέραιος αριθμός με $s \geq 4$, p ένας περιττός πρώτος με $(\frac{D_0}{p})$= 1 και X_{s+1} μία ambiguous κλάση διακρίνουσας D_{s+1}, τότε ισχύει η* *ακόλουθη συνεπαγωγή:*

$$X_{s+1} \longrightarrow p^{\hbar'_{s+1}} \Rightarrow \Phi_s(X_{s+1}) \longrightarrow p^{\hbar'_s}.$$

Απόδειξη: Αφού $X_{s+1} \longrightarrow p^{\hbar'_{s+1}}$ θα έχουμε ότι το σώμα ανάλυσης του p στο $k_2(D_{s+1})$ είναι το $L_{X_{s+1}}$ που δίνει $f_p(L_{X_{s+1}}) = 1$ και επομένως λόγω του λήμματος 1.2.2, έχουμε ότι $f_p(L_{\Phi_s(X_{s+1})}) = 1$. Η περίπτωση $X_{s+1} = I_{s+1}$ είναι τετριμμένη. Αν $X_{s+1} \neq I_{s+1}$ τότε το $f_p(L_{\Phi_s(X_{s+1})}) = 1$ συνεπάγεται (λόγω του ότι η $L_{I_s}/L_{\Phi_s(X_{s+1})}$ είναι επέκταση βαθμού 2) ότι το σώμα ανάλυσης του p στην $k_2(D_s)$ είναι ή το $L_{\Phi_s(X_{s+1})}$ ή το L_{I_s}. Αν ήταν το L_{I_s} τότε αφού $L_{I_s} = L_{A_{s+1}^{2^{c(s)}}}$ θα είχαμε $f_p(L_{X_{s+1}} L_{A_{s+1}^{2^{c(s)}}}) = 1$ και συνεπώς $f_p(L_{I_{s+1}}) = 1$ που είναι άτοπο διότι $X_{s+1} \neq I_{s+1}$. $\square$

Πόρισμα 1.4.2 *Έστω $s \in \mathbb{Z}, s \geq 4$ και p περιττός πρώτος με $(\frac{D_0}{p}) = 1$. Αν $X_s \in \{I_s, B_s, C_s, B_sC_s\}$ τότε*

- *Αν $A_s^{2^{c(s)-1}} X_s \longrightarrow p^{\hbar'_s}$ ή $X_s \longrightarrow p^{\hbar'_s}$ τότε $X_\iota \longrightarrow p^{\hbar'_\iota}, \forall \iota \in \{4, ..., s-1\}$,*
- *Αν $A_s^{2^{c(s)-1}} X_s \longrightarrow p^{\hbar'_s}$ τότε καμία ambiguous κλάση διακρίνουσας D_ι δεν παριστά τον $p^{\hbar'_\iota}$,$\forall \iota \geq s+1$.*

Απόδειξη: Υπενθυμίζουμε ότι $\Phi(A_s) = A_{s-1}$, $\Phi(B_s) = B_{s-1}$, $\Phi(C_s) = C_{s-1}$. Παρατηρούμε στην συνέχεια ότι $\Phi(A_s^{2^{c(s)-1}}) = A_{s-1}^{2^{c(s)-1}} = I$ (αφού $\Phi(A_s) = A_{s-1}$ και το A_{s-1} έχει τάξη $2^{c(s-1)} = 2^{c(s)-1}$). Έστω λοιπόν ότι $A_s^{2^{c(s)-1}} X_s \longrightarrow p^{\hbar'_s}$. Τότε $\Phi(A_s^{2^{c(s)-1}} X_s) \longrightarrow p^{\hbar'_{s-1}}$, δηλαδή $X_{s-1} \longrightarrow p^{\hbar'_{s-1}}$. Αν πάλι $X_s \longrightarrow p^{\hbar'_s}$ τότε $\Phi(X_s) \longrightarrow p^{\hbar'_{s-1}}$ οπότε $X_{s-1} \longrightarrow p^{\hbar'_{s-1}}$. Σε κάθε περίπτωση λοιπόν έχουμε ότι $X_{s-1} \longrightarrow p^{\hbar'_{s-1}}$ και συνεχίζοντας ομοίως έχουμε $X_\iota \longrightarrow p^{\hbar'_\iota}, \forall \iota \in \{4, ..., s-1\}$, δηλαδή την απόδειξη του πρώτου μέρους του πορίσματος. Είναι φανερό από τα παραπάνω, ότι οι εικόνες των ambiguous κλάσεων μεσω της Φ_s ανήκουν στο σύνολο $\{I_s, B_s, C_s, B_sC_s\}$, $s \geq 4$ και συνεπώς, αν $A_s^{2^{c(s)-1}} X_s \longrightarrow p^{\hbar'_s}$, τότε δεν είναι δυνατόν μια ambiguous κλάση διακρίνουσας D_ι να παριστά τον $p^{\hbar'_\iota}$ για κάποιο $\iota \geq s+1$, δηλαδή έχουμε την απόδειξη του δεύτερου μέρους του πορίσματος. $\square$

Αντίστροφα έχουμε το ακόλουθο Θεώρημα:

Θεώρημα 1.4.3 *Αν p είναι περιττός πρώτος με $(\frac{D_0}{p}) = 1$ και $X_s \in \{I_s, B_s, C_s, B_sC_s\}$ για $s \in \mathbb{Z}, s \geq 4$ με $X_s \longrightarrow p^{\hbar'_s}$, τότε ισχύει ακριβώς μία από τις ακόλουθες παραστάσεις:*

- $X_{s+1} \longrightarrow p^{\hbar'_{s+1}}$
- $A_{s+1}^{2^{c(s)}} X_{s+1} \longrightarrow p^{\hbar'_{s+1}}$.

Επιπλέον, $X_{s+1} \longrightarrow p^{\hbar'_{s+1}} \Leftrightarrow f_p(L_{B_{s+1}, C_{s+1}}) = 1$.

Απόδειξη: Η απόδειξη είναι σχεδόν προφανής αν μελετήσει κανείς τα ακόλουθα διαγράμματα Galois

$$
\begin{tikzcd}[column sep=small]
 & L_{I_{s+1}} = k_2(D_{s+1}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
L_{A_{s+1}^{2^{c(s)}} X_{s+1}} \arrow[dr, dash] & L_{X_{s+1}} \arrow[d, dash] & L_{A_{s+1}^{2^{c(s)}}} = L_{I_s} = k_2(D_s) \arrow[dl, dash] \\
 & L_{A_{s+1}^{2^{c(s)}}, X_{s+1}} = L_{X_s} &
\end{tikzcd}
\qquad
\begin{tikzcd}
L_{I_{s+1}} = k_s(D_{s+1}) \arrow[d, dash] \\
L_{A_{s+1}^{2^{c(s)}}} = k_2(D_s) = L_{I_s} \arrow[d, dash] \\
L_{A_{s+1}^{2^{c(s)-1}}}
\end{tikzcd}
$$

Σχήμα 6

Αν $X_s \neq I_s$ τότε $f(L_{X_s}) = 1$ και $f(k_2(D_s)) \neq 1$ οπότε το σώμα ανάλυσης του p στην $k_2(D_{s+1})$ είναι ακριβώς ένα από τα $L_{A_{s+1}^{2^{c(s)}} X_{s+1}}$, $L_{X_{s+1}}$ και αυτό γιατί η σύνθεση αυτών των δύο σωμάτων είναι το $L_{I_{s+1}}$ (βλ. σχήμα 6), πράγμα που σημαίνει ότι κάποια από τις κλάσεις $A_{s+1}^{2^{c(s)}}X_{s+1}$, X_{s+1} παριστά τον $p^{\hbar'_{s+1}}$ (και σύμφωνα με την πρόταση 0.0.1 ακριβώς μία). Αν $X_s = I_s$ τότε αφού $L_{X_s} = L_{A_{s+1}^{2^{c(s)}}}$, έχουμε ότι το σώμα ανάλυσης του p στην $k_2(D_{s+1})$ είναι ακριβώς ένα εκ των $L_{I_{s+1}}$, $L_{A_{s+1}^{2^{c(s)}}}$. Τέλος παρατηρούμε ότι $L_{I_{s+1}} = L_{A_{s+1}^{2c(s)}X_{s+1}} L_{B_{s+1},C_{s+1}}$ που σημαίνει ότι $X_{s+1} \longrightarrow p^{\hbar'_{s+1}}$ αν και μόνο αν $f_p(L_{B_{s+1},C_{s+1}}) = 1$.□

Από τα Θεωρήματα 1.3.1 και1.4.3 προκύπτει το ακόλουθο πόρισμα:

Πόρισμα 1.4.4 *Έστω* $\left(\frac{q}{r}\right) = -1$. *Για ένα πρώτο περιττό* p *με* $(\frac{D_0}{p})= 1$ *και*

$$(\frac{q}{p})= \begin{cases} 1, & \text{αν } p \equiv 1, 7(\text{mod} 8) \cdot \\ (\frac{q}{r}), & \text{αν } p \equiv 3, 5(\text{mod} 8). \end{cases}$$

Το σύμβολο u_p *του Θεωρήματος 1.3.1 είναι καλά ορισμένο. Ισχύει ότι* $u_p = 1$ *αν και μόνο αν ακριβώς μία εκ των* $A_5^4B_5$, B_5 *παριστά τον* $p^{\hbar'_5}$. *Επιπλέον,* $B_5 \longrightarrow p^{\hbar'_5}$ *αν και μόνο αν* $f(L_{B_5,C_5}) = 1$. *Επίσης αν η* $A_5^4B_5$ *παριστά τον* $p^{\hbar'_5}$, *τότε δεν υπάρχει ambiguous κλάση διακρίνουσας* D_s *που να παριστά τον* $p^{\hbar'_s}$, *για κάθε* $s \geq 5$.

Κεφάλαιο 2

Παράσταση Δυνάμεων Πρώτων Αριθμών και Σύμβολα του Legendre

Σε αυτό το μέρος θα εξετάσουμε την σχέση μεταξύ της παράστασης δυνάμεων πρώτων από κλάσεις τετραγωνικών μορφών και του χαρακτήρα Legendre της θεμελιώδους μονάδας του εμπλεκομένου πραγματικού τετραγωνικού σώματος αριθμών. Οι περιπτώσεις 1, 2 που αναφέρονται στην εισαγωγή θα μελετηθούν ξεχωριστά. Υπενθυμίζουμε ότι αυτές είναι:

- 1η Περίπτωση $D = -256qr$, q, r πρώτοι με $q \equiv 5(\text{mod} 8)$, $r \equiv 3(\text{mod } 8)$, $\hbar_2(D_0) \mid 4$.
- 2η Περίπτωση $D = -4m$, $m > 1$ ακέραιος, ελεύθερος τετραγώνου με $m \equiv 1(\text{mod} 12)$, $\hbar_3(D_0) \mid 9$.

Η 1η περίπτωση υποδιαιρείται στις περιπτώσεις Ια και Ιβ όπως και στο προηγούμενο κεφάλαιο.

2.1 Προκαταρτικές προτάσεις

Λήμμα 2.1.1 *Για κάθε* $s \in \mathbb{Z}$, $s \geq 2$, *ισχύουν τα ακόλουθα:*

- (i) $H_2(-2^{2s}qr) = (2^{s-2+c_{qr}}, 2, 2)$, όπου $H_2(-qr) = (2^{c_{qr}+1})$ στην πρώτη περίπτωση,

- (ii) $H_3(D) \in \{(3), (3,3), (3^2)\}$ στην δεύτερη περίπτωση.

Απόδειξη: Η (i) έχει μελετηθεί στο πρώτο μέρος της εργασίας (βλ. 1.1) Για την (ii) τα αναφερόμενα στην εκφώνηση είναι προφανή από τις υποθέσεις. $\square$

Το ακόλουθο λήμμα θα φανεί πολύ χρήσιμο στην συνέχεια αφού θα μας δώσει την δυνατότητα να συνδέσουμε σώματα αριθμών που θα έχουμε κατασκευάσει με υποσώματα των εμπλεκομένων ring class fields.

Λήμμα 2.1.2

- (i) Κάθε κυκλική επέκταση L του k βαθμού 4 μη διακλαδιζομένη εκτός του 2 και διεδρική υπέρ του $\mathbb{Q}$ περιέχεται στο $k_2(-256qr)$.

- (ii) Κάθε μη διακλαδιζομένη επέκταση L του k τάξης 3 (αντίστοιχα τάξης 2) περιέχεται στο $k_3(-4m)$ (αντίστοιχα στο $k_2(-4m)$).

Απόδειξη: Η (i) έχει μελετηθεί στο πρώτο μέρος της εργασίας και είναι το λήμμα 1.2.6. Για την (ii) έχουμε ότι κάθε μη διακλαδιζόμενη επέκταση του k βρίσκεται στο Hilbet class field του k που είναι το $k(-4m)$. $\square$

2.2 Επεκτάσεις του k παραγόμενες με την βοήθεια ριζικών της θεμελιώδους μονάδας

Πρόταση 2.2.1 *Έστω q, r πρώτοι αριθμοί με $q \equiv 5(\mathrm{mod}8)$, $r \equiv 3(\mathrm{mod}8)$. Έστω επίσης $\mathsf{w} \in \{1,2\}$ και*

$$t = \begin{cases} 1 & , \text{αν } (\frac{q}{r}) = 1 \cdot \\ 2 & , \text{αν } (\frac{q}{r}) = -1. \end{cases}$$

Θέτουμε: $k = \mathbb{Q}(\sqrt{-qr})$, $k_0 = \mathbb{Q}(\sqrt{qr})$, $K = kk_0$, $\alpha = \sqrt[4]{\mathsf{w}^2\varepsilon_{qr}}$ $M = K(\alpha)$. Τα ακόλουθα ισχύουν: Υπάρχει $\mathsf{v} \in K$ τέτοιο ώστε $\mathsf{w}^2\varepsilon_{qr} = tq\mathsf{v}^2$. Η επέκταση M/K είναι κυκλική Kummerian επέκταση βαθμού 4, $M/\mathbb{Q}$ είναι διεδρική με $G(M/\mathbb{Q}) = \langle\sigma,\tau\rangle \rtimes \langle\varrho\rangle$ και $\sigma(\sqrt{qr}) = \sqrt{qr}$, $\tau(\sqrt{qr}) = -\sqrt{qr}$, $\varrho(\sqrt{qr}) = \sqrt{qr}$, $\sigma(i) = i$, $\tau(i) = -i$, $\varrho(i) = -i$, $\sigma(\alpha) = i\alpha$, $\tau(\alpha) = \frac{\mathsf{w}}{\alpha}$, $\varrho(\alpha) = \alpha$. Επίσης η M/K είναι μή διακλαδιζόμενη εκτός του 2 και τα σώματα L, L' που αντιστοιχούν στις ομάδες $\langle\tau\rangle$, $\langle\sigma\tau\rangle$ μέσω της αντιστοιχίας Galois είναι κυκλικές επεκτάσεις του k βαθμού 4 μη διακλαδιζόμενες εκτός του 2 και διεδρικές πάνω από το $\mathbb{Q}$. Τέλος $K(\sqrt{\varepsilon_{qr}}) = k(i,\sqrt{tq})$. Ακολουθεί το διάγραμμα των προαναφερομένων υποσωμάτων της επέκτασης $M/\mathbb{Q}$.

$$
\begin{tikzcd}
 & & M \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] & \\
L \arrow[dr, dash] & L' \arrow[d, dash] & K(\sqrt{\varepsilon_{qr}}) \arrow[dl, dash] \arrow[d, dash] & \\
 & k(\sqrt{tq}) \arrow[d, dash] & K=k(i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
 & k \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & k_0 \arrow[dl, dash] \\
 & & \mathbb{Q} &
\end{tikzcd}
$$

Σχήμα 7

Απόδειξη: Λόγω των ισχυουσών ισοδυναμιών για τα q, r, η θεμελιώδης μονάδα του τετραγωνικού πραγματικού σώματος αριθμών $k = \mathbb{Q}(\sqrt{-qr})$ έχει norm ίση με 1. Η ιδιότητα αυτή θα χρησιμοποιηθεί στα παρακάτω χωρίς ιδιαίτερη αναφορά. Παρατηρούμε ότι $R_{k_0} = \mathbb{Z}[\sqrt{qr}]$. Έχουμε ότι η διοφαντική εξίσωση $x^2 - qry^2 = tq$ είναι επιλύσιμη στους ακεραίους (βλ. λήμμα 1.2.4). Θέτουμε

$$b = x + y\sqrt{qr},\ \bar{b} = x - y\sqrt{qr} \tag{2.1}$$

και έχουμε $b\bar{b} = tq$. Τα $2, q$ διακλαδίζονται στο k_0. Γράφουμε $(t) = \mathfrak{q}_t^2$, $(q) = \mathfrak{q}^2$ όπου το $\mathfrak{q}$ είναι ένα πρώτο ιδεώδες του R_{k_0} και το $\mathfrak{q}_t$ είναι ένα πρώτο ιδεώδες του R_{k_0} ή όλος ο δακτύλιος R_{k_0}. Προφανώς το ιδεώδες (b) διαιρεί το $(\mathfrak{q}\mathfrak{q}_t)^2$. Λόγω του ότι $N(b) = b\bar{b} = tq$, αποκλείονται οι περιπτώσεις

$$(b) = \mathfrak{q}_t,\ (b) = \mathfrak{q}_t^2,\ (b) = \mathfrak{q}^2,\ (b) = (\mathfrak{q}_t\mathfrak{q})^2$$

και συνεπώς $(b) = \mathfrak{q}_t\mathfrak{q} \Rightarrow (b)^2 = (\mathfrak{q}_t\mathfrak{q})^2 = (tq)$ οπότε υπάρχει μονάδα ε του $\mathbb{Z}[\sqrt{qr}]$ έτσι ώστε $b^2 = tq\varepsilon$. Έστω $\varepsilon = \varepsilon_{qr}^{\lambda}$, $\lambda \in \mathbb{Z}$ όπου όπως έχουμε ήδη αναφέρει ε_{qr} είναι η θεμελιώδης μονάδα του $R_{k_0} = \mathbb{Z}[\sqrt{qr}]$. Ο λ πρέπει αναγκαστικά να είναι περιττός. Πράγματι, αν ο λ ήταν άρτιος τότε

$$(b\varepsilon_{qr}^{\frac{-\lambda}{2}})^2 = tq$$

οπότε $\exists u \in \mathbb{Z}[\sqrt{qr}] : u^2 = tq$ και αν $u = x + y\sqrt{qr}$ τότε θα έπρεπε $tq = u^2 = x^2 + qry^2 + 2xy\sqrt{qr}$ που συνεπάγεται $xy = 0$ και άρα $tq = x^2 + qry^2$. Άτοπο. Αφού λοιπόν ο λ είναι περιττός μπορούμε να θέσουμε

$$\mathsf{v} = \frac{\mathsf{w}(b\varepsilon_{qr}^{\frac{-\lambda+1}{2}})}{tq}$$

και θα έχουμε $\alpha^4 = \mathsf{w}^2\varepsilon_{qr} = tq\mathsf{v}^2$. Έστω τώρα $G(K/\mathbb{Q}) = \langle \tau, \varrho \rangle$ με $\tau(\sqrt{qr}) = -\sqrt{qr}$, $\varrho(\sqrt{qr}) = \sqrt{qr}$, $\tau(i) = -i$, $\varrho(i) = -i$. Μπορούμε εύκολα να δούμε ότι $\tau(\mathsf{v}) = \frac{\mathsf{w}^2}{tq\mathsf{v}}$, $\varrho(\mathsf{v}) = \mathsf{v}$ και $\tau(\alpha^4) = \left(\frac{\mathsf{w}}{\alpha}\right)^4$, $\varrho(\alpha^4) = \alpha^4$ και έτσι μπορούμε να επεκτείνουμε τα τ, ϱ στο M κατά τέτοιο τρόπο ώστε $\tau(\alpha) = \left(\frac{\mathsf{w}}{\alpha}\right)$, $\varrho(\alpha) = \alpha$. Εξάλλου η M/K είναι επέκταση κυκλική του Kummer και μπορούμε επομένως να θέσουμε $G(M/K) = \langle \sigma \rangle$ με $\sigma(\alpha) = i\alpha$. Παρατηρούμε στην συνέχεια ότι $M = \mathbb{Q}(\alpha, i)$ και επομένως ένα στοιχείο της $G(M/\mathbb{Q})$ καθορίζεται πλήρως από τις τιμές του στα α και i. Επειδή:

$$(\tau\sigma)(\alpha) = \tfrac{-i\mathsf{w}}{\alpha} = (\sigma\tau)(\alpha)$$
$$(\varrho\sigma)(\alpha) = -i\alpha = (\sigma^3\varrho)(\alpha)$$
$$(\tau\sigma)(i) = -i = (\sigma\tau)(i)$$
$$(\varrho\sigma)(i) = -i = (\sigma^3\varrho)(i)$$

έχουμε ότι $G(M/\mathbb{Q}) = \langle \sigma, \tau \rangle \rtimes \langle \varrho \rangle$ με $G(M/k) = \langle \sigma, \tau \rangle$, $G(M/k_0) = \langle \sigma, \varrho \rangle$, $G(M/K) = \langle \sigma, \tau, \varrho \rangle$ Επίσης από νόμο ανάλυσης σε επεκτάσεις του Kummer (βλ. [6] chapter V §39) μπορούμε εύκολα να δούμε ότι οι M/K και K/k είναι μη διακλαδιζόμενες εκτός του 2 και συνεπώς και η M/k είναι μή διακλαδιζόμενη εκτός του 2. Τώρα, τα υποσώματα του M που αντιστοιχούν μέσω της αντιστοιχίας Galois στις ομάδες $\langle\tau\rangle$ και $\langle\sigma\tau\rangle$ είναι κυκλικές του k βαθμού 4 μη διακλαδιζόμενες εκτός του 2 και μάλιστα είναι και διεδρικές επεκτάσεις του $\mathbb{Q}$. Τέλος, η σχέση $\mathsf{w}^2\varepsilon_{qr} = tq\mathsf{v}^2$ δίνει $k(\sqrt{\varepsilon_{qr}}) = k(i, \sqrt{tq})$ (που βέβαια σημαίνει ότι για p περιττό πρώτο με $p \equiv (1 \bmod 4)$ και $(\frac{D}{p})= 1$ ισχύει $(\frac{\varepsilon_{qr}}{p})= (\frac{tq}{p})$).$\square$

Στην συνέχεια θα μελετήσουμε την περίπτωση του τετραγωνικού μιγαδικού σώματος $\mathbb{Q}(\sqrt{-m})$ όπου ο m είναι φυσικός αριθμός ελεύθερος τετραγώνου με $m \equiv 1(\mathrm{mod}4)$.

Πρόταση 2.2.2 *Έστω m ελεύθερος τετραγώνου φυσικός αριθμός με $m \equiv 1(\mathrm{mod}4)$. Έστω $k = \mathbb{Q}(\sqrt{-m})$, $k_0 = \mathbb{Q}(\sqrt{3m})$, $K = kk_0 = k(\omega)$, $\alpha = \sqrt[3]{\varepsilon_{3m}}$, $M = K(\alpha)$. Ισχύει ότι η M/K είναι Kummerian επέκταση βαθμού 3 και η $M/\mathbb{Q}$ είναι διεδρική τάξης 12. Επιπλέον, $G(M/\mathbb{Q}) = \langle\sigma, \tau\rangle \rtimes \langle\varrho\rangle$ με $\sigma(\sqrt{-m}) = \sqrt{-m}$, $\tau(\sqrt{-m}) = \sqrt{-m}$, $\varrho(\sqrt{-m}) = \sqrt{-m}$, $\sigma(\sqrt{-3}) = \sqrt{-3}$, $\tau(\sqrt{-3}) = -\sqrt{-3}$, $\varrho(\sqrt{-3}) = -\sqrt{-3}$, $\sigma(\alpha) = \omega\alpha$, $\tau(\alpha) = \frac{1}{\alpha}$, $\varrho(\alpha) = \alpha$. Η M/K είναι αβελιανή μη διακλαδιζόμενη εκτός του 3 επέκταση βαθμού 6 και το υπόσωμα L του M που αντιστοιχεί στην $\langle\tau\rangle$ είναι βαθμού 3 επέκταση του k μη διακλαδιζόμενη εκτός του 3 και η δε $L/\mathbb{Q}$ είναι διεδρική τάξης 6. Το διάγραμμα των υποσωμάτων που αναφέρονται δίνεται ακόλουθα:*

$$\begin{tikzcd}
 & M \arrow[dl, dash] \arrow[dd, dash] & \\
L \arrow[dr, dash] \arrow[dd, dash] & & \\
 & K \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
k \arrow[dr, dash] & \mathbb{Q}(\sqrt{-3}) \arrow[d, dash] & k_0 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Σχήμα 8

<u>Απόδειξη:</u> Παρατηρούμε κατ΄ αρχήν ότι

$$M = k(\alpha, \sqrt{-3}), \quad \omega = \frac{-1+\sqrt{-3}}{2} \quad \text{και ότι} \quad R_{k_0} = \begin{cases} \mathbb{Z}[\sqrt{3m}] & , \text{αν } m \not\equiv 0(\mathrm{mod}3) \\ \mathbb{Z}[\sqrt{\frac{m}{3}}] & , \text{αν } m \equiv 0(\mathrm{mod}3). \end{cases}$$

Η θεμελιώδης μονάδα ε_{3m} του τετραγωνικού πραγματικού σώματος $\mathbb{Q}(\sqrt{3m})$ έχει norm ίση με 1. Πράγματι, αν $m \not\equiv 0(\mathrm{mod}3)$ τότε η διοφαντική εξίσωση $x^2 - 3my^2 = -1$ δεν έχει λύση (αφού η σχέση $x^2 - 3my^2 = -1$ δίνει $x^2 + y^2 = 3(\mathrm{mod}4)$ που είναι άτοπο), ενώ αν $m \equiv 0(\mathrm{mod}3)$ τότε η διοφαντική εξίσωση $x^2 - \frac{m}{3}y^2 = -1$ δεν έχει λύση (γιατί $m \equiv 1(\mathrm{mod}4)$ που σημαίνει ότι $\frac{m}{3} \equiv 3(\mathrm{mod}4)$ και συνεπώς μία σχέση της μορφής $x^2 - \frac{m}{3}y^2 = -1$ θα έδινε $x^2 + y^2 = 3(\mathrm{mod}4)$ που είναι άτοπο). Η ομάδα Galois $G(K/\mathbb{Q})$ είναι τύπου $(2,2)$ οπότε μπορούμε να πάρουμε $G(K/\mathbb{Q}) = \langle \tau, \varrho \rangle$ με $\tau(\sqrt{-m}) = \sqrt{-m}$, $\varrho(\sqrt{-m}) = \sqrt{-m}$, $\tau(\sqrt{-3}) = -\sqrt{-3}$, $\varrho(\sqrt{-3}) = -\sqrt{-3}$. Επίσης η M/K είναι Kummerian επέκταση βαθμού 3 οπότε μπορούμε να θεωρήσουμε $G(M/K) = \langle \sigma \rangle$ με $\sigma(\alpha) = \omega\alpha$. Τώρα, επειδή

$$\tau(\alpha^3) = \varepsilon_{3m}^{-1} = (\frac{1}{\alpha})^3, \quad \varrho(\alpha^3) = \alpha^3$$

τα τ, ϱ είναι δυνατόν να επεκταθούν σε όλο το M όπου $\tau(\alpha) = \frac{1}{\alpha}$, $\varrho(\alpha) = \alpha$. Εύκολα διαπιστώνουμε ότι:

$$(\tau\sigma)(\alpha) = \tfrac{1}{\omega\alpha} = (\sigma\tau)(\alpha)$$
$$(\varrho\sigma)(\alpha) = \omega^2\alpha = (\sigma^2\varrho)(\alpha)$$
$$(\tau\sigma)(\sqrt{-3}) = -\sqrt{-3} = (\sigma\tau)(i)$$
$$(\varrho\sigma)(\sqrt{-3}) = -\sqrt{-3} = (\sigma^2\varrho)(\sqrt{-3})$$

από το οποίο συνεπάγεται ότι $G(M/\mathbb{Q}) = \langle\sigma,\tau\rangle \rtimes \langle\varrho\rangle$. Από θεωρία ανάλυσης στις Kummerian επεκτάσεις M/K και K/k μπορούμε να δούμε ότι δεν διακλαδίζονται πέραν του 3 (βλ. [6] chapter V §39). Το σώμα L που ορίζεται στην εκφώνηση να αντιστοιχεί στην $\langle\tau\rangle$, επειδή

$$\frac{\langle\sigma,\tau\rangle \rtimes \langle\varrho\rangle}{\langle\tau\rangle} \simeq \langle\sigma\rangle \rtimes \langle\varrho\rangle\,,$$

είναι όντως διεδρική επέκταση του $\mathbb{Q}$ και βαθμού 3 πάνω από το k.□

2.3 Κύρια αποτελέσματα για την περίπτωση $D = -256qr$

Περιοριζόμαστε τώρα στην 1η περίπτωση όπου $D = -256qr$ με $q \equiv 5(\bmod 8)$, $r \equiv 3(\bmod 8)$, $\hbar_2(D_0) \mid 4$. Για απλότητα όπως και στο προηγούμενο κεφάλαιο θα παραλείπεται ο δείκτης $s = 4$. Θέτουμε $k_0 = \mathbb{Q}(\sqrt{qr})$, $K = kk_0$, $M = K(\sqrt[4]{\varepsilon_{qr}})$, $M' = K(\sqrt[4]{4\varepsilon_{qr}})$. Από την πρόταση 2.2.1 προκύπτει ότι στο M περιέχονται 2 υποσώματα: L_1, L_2 τα οποία αποτελούν μη διακλαδιζόμενες εκτός του 2 κυκλικές επεκτάσεις του k βαθμού 4 και είναι διεδρικές πάνω από το $\mathbb{Q}$. Επίσης και στο M' περιέχονται 2 υποσώματα: L_1', L_2' που είναι μη διακλαδιζόμενες εκτός του 2 κυκλικές επεκτάσεις του k βαθμού 4 και διεδρικές πάνω από το $\mathbb{Q}$. Από το λήμμα 2.1.2 τα L_1, L_2, L_1', L_2' περιέχονται στο

$k_2(-256qr)$ και αφού η $k_2(-256qr)/k$ περιέχει ακριβώς 4 ενδιάμεσα σώματα που να είναι κυκλικά βαθμού 4 και διεδρικά πάνω απο το $\mathbb{Q}$ (βλ. σχόλια μετά το λήμμα 1.2.6) θα έχουμε

$$\{L_1,\ L_2,\ L_1',\ L_2'\} = \{L^{(2)}_{A^4,B,C},\ L^{(2)}_{A^2B,C},\ L^{(2)}_{A^2C,B},\ L^{(2)}_{A^2B,BC}\} = \{k(\sqrt{w\mu}) \mid w = \pm 1, \pm 2\}$$

όπου $\mu = t - y\sqrt{-tr}$ για x, y τυχαίες ακέραιες λύσεις της διοφαντικής $qx^2 - ry^2 = t$ και

$$t = \begin{cases} 1 & , \text{αν } (\frac{q}{r}) = 1, \\ 2 & , \text{αν } (\frac{q}{r}) = -1. \end{cases}$$

Παρατηρούμε ότι $\sqrt{2} \notin M, M'$ ενώ $i \in M, M'$. (Αν π.χ.$\sqrt{2} \in M$ τότε η $K(\sqrt{2})$ θα ήταν υπόσωμα του M. Όμως η $G(K(\sqrt{2})/\mathbb{Q})$ είναι τύπου $(2,2,2)$ και αυτό απαγορεύεται από την δομή της ομάδας $G(M/\mathbb{Q})$.) Είναι εύκολο τώρα να δεί κανείς ότι $\{\ k(i, \sqrt{\mu}),\ k(i, \sqrt{2\mu})\ \} = \{M,\ M'\}$. Στην συνέχεια θα προσδιορίσουμε πότε $M = k(i, \sqrt{\mu})$ και πότε $M = k(i, \sqrt{2\mu})$. Προς τούτο, θα χρειαστούμε το ακόλουθο λήμμα:

Λήμμα 2.3.1 *Αν q, r είναι πρώτοι αριθμοί με $q \equiv 5(\mathrm{mod}8)$, $r \equiv 3(\mathrm{mod}8)$ και $\varepsilon_{qr} = u + v\sqrt{qr}$ η θεμελιώδης μονάδα της $\mathbb{Q}(\sqrt{qr})$, τότε $\varepsilon_{qr} = u \equiv -1(\mathrm{mod}q)$.*

Απόδειξη: Η ε_{qr}, ως μονάδα του σώματος $\mathbb{Q}(\sqrt{qr})$, έχει norm 1 και συνεπώς $u^2 - qrv^2 = 1$ πράγμα που σημαίνει $u \equiv \pm 1(\mathrm{mod}q)$. Υποθέτουμε ότι $u \equiv 1(\mathrm{mod}q)$. Μπορούμε επομένως να γράψουμε $u = 1 + \kappa q$ για κάποιο $\kappa \in \mathbb{Z}$ οπότε, παίρνοντας τετράγωνα, θα έχουμε $u^2 = 1 + 2\kappa q + \kappa^2 q^2$ και έτσι $qrv^2 = 2\kappa q + \kappa^2 q^2 \ \Rightarrow \kappa(q\kappa + 2) = rv^2$. Έστω ότι ο κ είναι περιττός. Τότε $(\kappa, q\kappa + 2) = 1$ οπότε:

- Αν μεν $r \mid \kappa$ θα είχαμε $qrv_1^2 + 2 = v_2^2$ όπου $v = v_1 v_2$ και συνεπώς $\left(\frac{2}{q}\right) = \left(\frac{v_2^2}{q}\right) = 1$ που είναι άτοπο.

- Αν $r \nmid \kappa$ θα είχαμε $v_1^2 q + 2 = rv_2^2$ με $v = v_1 v_2$ οπότε $-1 = \left(\frac{2}{q}\right) = \left(\frac{r}{q}\right)$. Ομως μπορούμε να γράψουμε και $v_1^2 q = -2 + rv_2^2$ οπότε $\left(\frac{q}{r}\right) = \left(\frac{-2}{r}\right) = 1$. Όμως $\left(\frac{r}{q}\right) = \left(\frac{q}{r}\right)$ και έχουμε πάλι άτοπο.

Έστω τώρα ότι ο κ είναι άρτιος. Γράφουμε $\kappa = 2\kappa'$ και έτσι $\kappa'(q\kappa' + 1) = rv'^2$ για $v = 2v'$.

- Αν μεν $r \mid \kappa'$ τότε γράφοντας $\kappa' = r\lambda$ με $\lambda \in \mathbb{Z}$ θα έχουμε $\lambda(qr\lambda + 1) = v'^2$. Επειδή οι λ, $qr\lambda + 1$ είναι πρώτοι μεταξύ τους, θα υπάρχουν ακέραιοι αριθμοί v_1 και v_2 ώστε $v' = v_1 v_2$ και $\lambda = v_2^2, \quad qr\lambda + 1 = v_1^2$. Συνεπώς θα έχουμε τις ακόλουθες σχέσεις:

  $$v_1^2 - qrv_2^2 = 1, \quad v = 2v' = 2v_1 v_2, \quad u + 1 = 2 + \kappa q = 2(qr\lambda + 1) = 2v_1^2.$$

  Οι τελευτέες σχέσεις δίνουν ακέραια λύση (v_1, v_2) της διοφαντικής εξίσωσης: $x^2 - qry^2 = 1$ με $0 < v_1 < u$ και $0 < v_2 < v$, κάτι το οποίο είναι άτοπο αφού $u + v\sqrt{qr}$ είναι θεμελιώδης μονάδα.

- Αν δε $r \nmid \kappa'$ τότε $v_1^2 q + 1 = rv_2^2$ όπου $v = v_1 v_2$ οπότε $1 = \left(\frac{r}{q}\right)$ και γράφοντας $v_1^2 q = -1 + rv_2^2$ μπορούμε να πάρουμε $\left(\frac{q}{r}\right) = -1$ που είναι και πάλι άτοπο, αφού $\left(\frac{r}{q}\right) = \left(\frac{q}{r}\right)$.

Συνεπώς $\varepsilon_{qr} = u + v\sqrt{qr} \equiv u \equiv -1 (\mathrm{mod} q)$.□

Λήμμα 2.3.2 *Ισχύει η ακόλουθη σχέση*

$$f_q(k(\sqrt{\mu}, i)) = \left\{ \begin{array}{lll} 1 & , \alpha\nu & \left(\frac{q}{r}\right) = -1 \\ 2 & , \alpha\nu & \left(\frac{q}{r}\right) = 1 \end{array} \right\} = \frac{2}{t}$$

Απόδειξη: Ισχύει $k(\sqrt{\mu}, i) = k(\sqrt{v}, i)$, όπου μ, v, όπως ορίστηκαν στην πρόταση 1.2.5, και παρατηρούμε ότι

$$(\frac{v}{q}) = (\frac{2(t + x\sqrt{tq})}{q}) = (\frac{2t}{q}).$$

Αν $t = 1$, τότε $(\frac{v}{q}) = 1$ οπότε $f_q(k(\sqrt{\mu}, i)) = 2$. Αν πάλι $t = 2$, τότε $(\frac{v}{q}) = -1$ οπότε $f_q(k(\sqrt{\mu}, i)) = 1$.□

Λήμμα 2.3.3 *Έστω p περιττός πρώτος με*

$$(\frac{-256qr}{p}) = 1.$$

Ισχύει ότι:

1. *Αν $p \equiv 1(\mathrm{mod}4)$ τότε*

$$(\frac{tq}{p}) = (\frac{\varepsilon_{qr}}{\mathfrak{p}}) \quad \text{και αν επιπλέον} \quad (\frac{\varepsilon_{qr}}{\mathfrak{p}}) = 1 \quad \text{τότε} \quad u_p = (\frac{\varepsilon_{qr}}{\mathfrak{p}})_4 (\frac{2}{p})$$

2. *Αν $p \equiv 3(\mathrm{mod}4)$ τότε*

$$(\frac{tq}{p}) = (\frac{\varepsilon_{qr}}{\mathfrak{p}})_4$$

όπου $\mathfrak{p}$ είναι πρώτο ιδεώδες του R_{k_0} πάνω από το $p\mathbb{Z}$.

Απόδειξη: Έχουμε $f_q(K) = 1$ (γιατί $f_q(k) = f_q(\mathbb{Q}(i)) = 1$) και $K(\sqrt[4]{\mathsf{w}\varepsilon_{qr}}) = k(i, \sqrt{tq}) = k(i, \sqrt{-tr})$ οπότε αφού $(\frac{-tr}{q}) = 1$ θα έχουμε σίγουρα ότι $f_q(K(\sqrt{\mathsf{w}\varepsilon_{qr}})) = 1$. Εστω $qR_{k_0} = \mathfrak{q}^2$ η ανάλυση σε πρώτα ιδεώδη στο k_0. Το $\mathfrak{q}R_K$ είναι πρώτο ιδεώδες του R_K και μάλιστα

$$\frac{R_K}{\mathfrak{q}R_K} \simeq \frac{\mathbb{Z}}{q\mathbb{Z}}.$$

Αφού όμως

$$(\frac{-1}{\mathfrak{q}})_4 = (-1)^{\frac{N_{\mathbb{Q}(i)}(\mathfrak{q})-1}{4}} = (-1)^{\frac{q-1}{4}} = -1,$$

από τον νόμο ανάλυσης στην επέκταση $K(\sqrt[4]{\mathsf{w}\varepsilon_{qr}})/K$ θα έχουμε

$$f_{\mathfrak{q}}(K(\sqrt[4]{\mathsf{w}^2\varepsilon_{qr}})/K)=1 \ \Leftrightarrow (\frac{\mathsf{w}^2\varepsilon_{qr}}{\mathfrak{q}})_4 = 1,$$

το οποίο, λόγω του λήμματος 2.3.1, είναι ισοδύναμο με

$$(\frac{-\mathsf{w}^2}{\mathfrak{q}})_4 = 1 \ \Leftrightarrow (\frac{\mathsf{w}^2}{q})_4 = -1 \ \Leftrightarrow (\frac{\mathsf{w}}{q}) = -1 \ \Leftrightarrow \ \mathsf{w}=2.$$

Συνεπώς $f_q(M')=1,\ f_q(M)=2$ και, σύμφωνα με το λήμμα 2.3.2, έχουμε

$$(M,M')=\left\{\begin{array}{ll} (k(i,\sqrt{\mu}),\ k(i,\sqrt{2\mu})) & ,\text{αν } (\frac{q}{r})=1, \\ (k(i,\sqrt{2\mu}),\ k(i,\sqrt{\mu})) & ,\text{αν } (\frac{q}{r})=-1. \end{array}\right\} = (k(i,\sqrt{t\mu}),k(i,\sqrt{2t\mu})) = (k(i,\sqrt{tv}),k(i,\sqrt{2tv}))$$

Θυμόμαστε όμως ότι $L_{A^4,B,C}=k(\sqrt{-2t\mu})=k(\sqrt{-2tv})$ (βλ. πρόταση 1.2.10) οπότε $M'=L^{(2)}_{A^4,B,C}(i)$. Στην συνέχεια παρατηρούμε ότι $f_p(k)=1$. Τώρα, όταν $p\equiv 1(\mathrm{mod}4)$, έχουμε ότι $f_p(K)=1$ που δίνει

$$f_p(K(\sqrt{\varepsilon_{qr}}))=2 \iff f_p(k(\sqrt{tq}))=2 \quad \text{και επομένως} \quad (\frac{tq}{p}) = (\frac{\varepsilon_{qr}}{\mathfrak{p}}).$$

Επίσης, όταν $(\frac{\varepsilon_{qr}}{\mathfrak{p}})=1$, έχουμε $(\frac{4\varepsilon_{qr}}{\mathfrak{p}})_4=\pm 1$ και

$$(\frac{4\varepsilon_{qr}}{\mathfrak{p}})_4 = 1 \iff f_p(M')=1 \iff f_p(L^{(2)}_{A^4,B,C})=1 \iff u_p=1.$$

Αν πάλι $p\equiv 3(\mathrm{mod}4)$ τότε $f_p(K)=2$ και, αφού η $K(\sqrt{\varepsilon_{qr}})/K$ είναι επέκταση του τύπου $(2,2)$, θα έχουμε $f_p(K(\sqrt{\varepsilon_{qr}}))=2$. Έτσι, όταν $f_p(k(\sqrt{tq}))=2$ θα ισχύει $f_p(L^{(2)}_{A^4,B,C})=4$ (Αφού η $L^{(2)}_{A^4,B,C}/k$ είναι κυκλική με ενδιάμεσο σώμα το $k(\sqrt{tq})$) πράγμα που σημαίνει $f_p(M')=4$ και άρα $(\frac{4\varepsilon_{qr}}{\mathfrak{p}})_4=-1$). Όταν $f_p(k(\sqrt{tq}))=1$ θα ισχύει ότι ο p αδρανεί στην $K(\sqrt{\varepsilon_{qr}})/k(\sqrt{tq})$ οπότε, αφού η $M'/k(\sqrt{tq})$ είναι τύπου (2,2), θα έχουμε $f_p(M')=2$ που σημαίνει $(\frac{4\varepsilon_{qr}}{\mathfrak{p}})_4=1$.

$$\begin{tikzcd}
& M' \arrow[dl, dash] \arrow[d, dash] & \\
L^{(2)}_{A^4,B,C} \arrow[d, dash] & K(\sqrt{\varepsilon_{qr}}) \arrow[dl, dash] \arrow[d, dash] & \\
k(\sqrt{tq}) \arrow[d, dash] & K=k(i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
k \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & k_0 \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Σχήμα 9

Εξάλλου ισχύει το ακόλουθο:

$$(\frac{4}{\mathfrak{p}})_4 = (\frac{2}{\mathfrak{p}}) = \left\{ \begin{array}{ll} (\frac{2}{p}) & , \text{αν } p \equiv 1(\bmod 4) \\ 1 & , \text{αν } p \equiv 3(\bmod 4). \end{array} \right\} \tag{2.2}$$

Πράγματι, αν $p \equiv 1(\bmod 4)$ τότε ο p αναλύεται στο $\mathbb{Q}(i)$ οπότε αφού αναλύεται και στο k θα αναλύεται και στο K. Κατά συνέπεια $(\frac{2}{\mathfrak{p}}) = (\frac{2}{p})$ λόγω του ότι τα σώματα $\frac{R_K}{\mathfrak{p}R_K}$ και $\frac{\mathbb{Z}}{p\mathbb{Z}}$ είναι ισόμορφα. Αν πάλι $p \equiv 3(\bmod 4)$ τότε ο p θα αδρανεί στο $\mathbb{Q}(i)$ οπότε ο βαθμός αδράνειας του στο K θα είναι 2 και έτσι $N_K(\mathfrak{p}) = p^2$. Όμως $2^{p-1} \equiv 1(\bmod p)$ και συνεπώς $2^{\frac{(p-1)(p+1)}{2}} \equiv 1(\bmod p) \Rightarrow 2^{\frac{N(p)-1}{2}} \equiv 1(\bmod p) \Rightarrow 2^{\frac{N(p)-1}{2}} \equiv 1(\bmod \mathfrak{p})$ και, από τον ορισμό του συμβόλου Legendre, έχουμε $(\frac{2}{\mathfrak{p}}) = 1$, δηλαδή την απόδειξη της σχέσης (2.2).$\square$

Μπορούμε τώρα να αποδείξουμε το ακόλουθο Θεώρημα

Θεώρημα 2.3.4 *Στην περίπτωση 1 (βλ. σελ. 33), έστω ότι* $(\frac{q}{r}) = -1$. *Επομένως,* $H_2(-256qr) = \langle A, B, C \rangle$ *με* $A^4 = B^2 = C^2 = 1$. *Έστω επίσης* p

περιττός πρώτος με $(\frac{-256qr}{p}) = 1$. *Τα ακόλουθα ισχύουν:*

(1) Ο $p^{\hbar_2'}$ *παρίσταται πάντα από κάποια κλάση* X *της* $H(-256qr)$ *με* $X^4 = I$.

(2) Ο $p^{\hbar_2'}$ *παρίσταται από μια ambiguous κλάση του* $H(-256qr)$ *αν και μόνο αν* $(\frac{tq}{p}) = 1$.

(3) Όταν $p \equiv 1 (\bmod 4)$, *τότε ο* $p^{\hbar_2'}$ *παρίσταται από μία ambiguous κλάση του* $H(-256qr)$ *αν και μόνο αν*

$$(\frac{\varepsilon_{qr}}{\mathfrak{p}}) = 1$$

και επιπλέον ο $p^{\hbar_2'}$ *παρίσταται από μια εκ των* I, C *αν και μόνο αν*

$$(\frac{\varepsilon_{qr}}{\mathfrak{p}})_4 = (\frac{2}{p})$$

(4) Όταν $p \equiv 3 (\bmod 4)$, *τότε ο* $p^{\hbar_2'}$ *παρίσταται από μία ambiguous κλάση του* $H(-256qr)$ *αν και μόνο αν*

$$(\frac{\varepsilon_{qr}}{\mathfrak{p}})_4 = 1.$$

<u>Απόδειξη:</u> Η ομάδα

$$\frac{H_2(D)}{H_2(D)^2}$$

έχει τα ακόλουθα στοιχεία: $\{I,\ A^2\}$, $\{B,\ A^2B\}$, $\{C,\ A^2C\}$, $\{BC,\ A^2BC\}$, $\{A,\ A^3\}$, $\{AB,\ A^3B\}$, $\{AC,\ A^3C\}$, $\{ABC,\ A^3BC\}$. Υπενθυμίζουμε ότι το σώμα γένους modulo D είναι το $k(\sqrt{q}, \zeta_8)$ και ο ισομορφισμός του Artin επάγει ισομορφισμό

$$\frac{H_2(D)}{H_2(D)^2} \xrightarrow{\simeq} (\mathbb{Z}/_{8\mathbb{Z}})^{\times} \times \{\pm 1\}$$

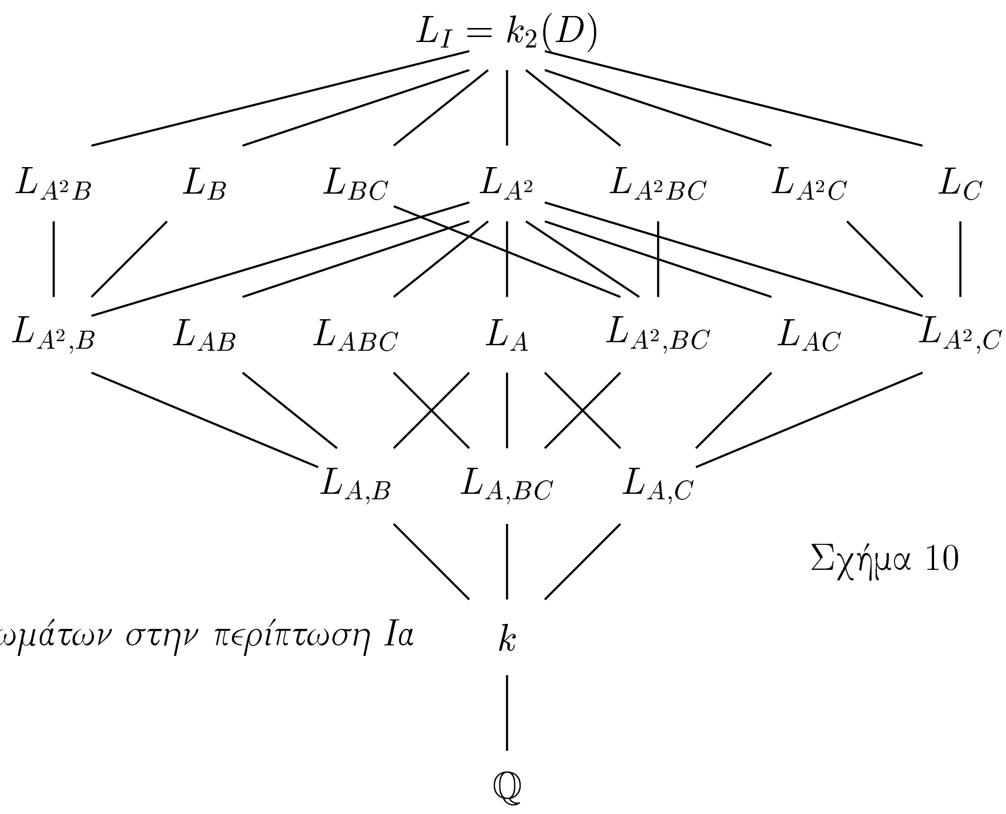
$$\text{με} \quad C \bmod (H_2(D_s)^2) \longrightarrow ([\frac{\mathbb{Q}(\zeta_8) \mid \mathbb{Q}}{m}], [\frac{\mathbb{Q}(\sqrt{q}) \mid \mathbb{Q}}{m}]) \text{ για } C \longrightarrow m.$$

Στο Θεώρημα 1.3.1 είδαμε ότι για ένα περιττό πρώτο p με $\left(\frac{-256qr}{p}\right) = 1$ ισχύει ότι :

(A). Ο $p^{\hbar'_2}$ παρίσταται από ambiguous κλάση διακρίνουσας D τότε $(\frac{q}{p})= \begin{cases} 1, & \text{αν } p \equiv 1,7 (\bmod 8)\cdot \\ -1, & \text{αν } p \equiv 3,5 (\bmod 8). \end{cases}$

Οι άλλες περιπτώσεις του $(\frac{q}{p})$ πρέπει να διαμοιραστούν στα υπόλοιπα γένη του $H_2(-256qr)$ και έτσι έχουμε το ακόλουθο:

(B). Αν $X \longrightarrow p^{\hbar'_2}$ με $X \in \{A, AB, AC, ABC\}$ τότε $(\frac{q}{p})= \begin{cases} -1, & \text{αν } p \equiv 1,7 (\bmod 8)\cdot \\ 1, & \text{αν } p \equiv 3,5 (\bmod 8). \end{cases}$



Σχήμα 10

Πύργος σωμάτων στην περίπτωση Ια

Από το σχήμα 10 παραπάνω και με απλά επιχειρήματα ανάλυσης πρώτων όπως ακριβώς και στην απόδειξη του Θεωρήματος 1.3.1 μπορούμε να δούμε ότι ισχύει και το αντίστροφο του (B) και έτσι έχουμε αποδείξει το (1). (Σημειώνουμε ότι για κάθε $X \in \{A, AB, AC, ABC\}$ ισχύει $L_X = L_{A^2X}$ που σημαίνει: $X \longrightarrow p^{\hbar'_2}$ αν και μόνο αν $A^2X \longrightarrow p^{\hbar'_2}$). Τώρα, $f_p(L_0) = 1$ αν και μόνο αν $(\frac{tq}{p}) = 1$ αν και μόνο αν ο $p^{\hbar'_2}$ παρίσταται από κάποια ambiguous κλάση (βλ. σχήμα 3) και έτσι το (2) του Θεωρήματος προκύπτει άμεσα. Το ίδιο εύκολα προκύπτουν και τα (3), (4) του Θεωρήματος χρησιμοποιώντας το Θεώρημα 1.3.1 και τό λήμμα 2.3.3 □

Τα πράγματα στην περίπτωση $(\frac{q}{r})= 1$ δεν είναι τόσο 'όμορφα' όσο όταν $(\frac{q}{r})= -1$. Παρόλα αυτά μπορούμε να πάρουμε το ακόλουθο, ενδιαφέρον κατά την γνώμη μας, Θεώρημα:

Θεώρημα 2.3.5 *Στην Περίπτωση 1 (βλ. σελ 33), έστω ότι* $(\frac{q}{r}) = 1$. *Αν* p *είναι περιττός πρώτος με* $(\frac{-256qr}{p}) = 1$ *και* $\mathfrak{p}$ *είναι πρώτο ιδεώδες του* R_{k_0} *πάνω από το* p *τότε τα ακόλουθα ισχύουν:*

(1) Ο $p^{\hbar'_2}$ *παρίσταται από κλάση* X *της* $H(-256qr)$ *με* $X^4 = I$ *αν και μόνο αν* $(\frac{tq}{p}) = 1$.

(2) Άν $p \equiv 1(\mathrm{mod} 4)$, *τότε ο* $p^{\hbar'_2}$ *παρίσταται από κλάση* X *της* $H(-256qr)$ *με* $X^4 = I$ *αν και μόνο αν*

$$(\frac{\varepsilon_{qr}}{\mathfrak{p}}) = 1$$

και επιπλέον ο $p^{\hbar'_2}$ *παρίσταται από κάποια ambiguous κλάση της* $H(D)$ *αν και μόνο αν*

$$(\frac{\varepsilon_{qr}}{\mathfrak{p}})_4 = (\frac{2}{p})$$

(3) Άν $p \equiv 3(\mathrm{mod} 4)$, *τότϵ ο* $p^{\hbar'_2}$ *παρίσταται από κλάση* X *της* $H(-256qr)$ *μϵ* $X^4 = I$ *αν και μόνο αν*

$$(\frac{\varepsilon_{qr}}{\mathfrak{p}})_4 = 1.$$

<u>Απόδειξη:</u> Από το σχήμα 5 είναι εύκολο να δεί κανείς ότι για τους p που αναφέρονται στην εκφώνηση του Θεωρήματος, μία κλάση X της $H(-256qr)$ με $X^4 = I$ παριστά τον $p^{\hbar'_2}$ αν και μόνο αν (βλ. και πρόταση 0.0.1) $f_p(L_0) = 1$. Όμως $L_0 = k(\sqrt{tq})$ και έτσι το (1) προκύπτει άμεσα. Τα (2) και (3) είναι συνέπειες του λήμματος 2.3.3 και του Θεωρήματος 1.3.1.□

2.4 Κύρια αποτελέσματα στην περίπτωση $D = -4m$

Για την περίπτωση 2 (βλ. σελ. 33) θέτουμε $k = \mathbb{Q}(\sqrt{-m})$, $k_0 = \mathbb{Q}(\sqrt{3m})$, $K = kk_0$, $M = K(\sqrt[3]{\varepsilon_{3m}})$ και εφαρμόζουμε την πρόταση 2.2.2. Έστω L το σώμα που αντιστοιχεί στην υποομάδα $\langle\tau\rangle$ μέσω της αντιστοιχίας Galois . Το 3 αναλύεται ως $3 = (1-\omega)^2$ στο $\mathbb{Q}(\sqrt{-3})$ και αδρανεί στο k (αφού $m \equiv 1(\mathrm{mod} 12) \Rightarrow m \equiv 1(\mathrm{mod} 3)$). Αυτό σημαίνει ότι η ανάλυση του (3) σε πρώτα ιδεώδη του K είναι $(3) = (1-\omega)^2$. Από νόμο ανάλυσης σε επεκτάσεις του Kummer έχουμε ότι το 3 διακλαδίζεται στο M αν και μόνο αν η ισοδυναμία

$$\varepsilon_{3m} \equiv x^3(\mathrm{mod}(1-\omega)^3)$$

είναι επιλύσιμη στο K. Επομένως έχουμε το ακόλουθο Θεώρημα:

Θεώρημα 2.4.1 *Στην περίπτωση 2 (βλ. σϵλ. 33), αν p ϵίναι πϵριττός πρώτος μϵ* $(\frac{-4m}{p}) = 1$ *και η ισοδυναμία* $\varepsilon_{3m} \equiv x^3(\mathrm{mod}(1-\omega)^3)$ *δϵν ϵίναι ϵπιλύσιμη στο* K *τότϵ:*

(1) Αν $H_3(D) = (3)$ *η* $(3,3)$ *τότε υπάρχει πάντοτε μία κλάση* $X \in H(D)$ *με* $X^3 = 1$ *έτσι ώστε* $X \longrightarrow p^{\hbar'_3}$.

(2) Αν $H_3(D) = (3^2)$ *τότε αν '*$p \equiv 2(\mathrm{mod}3)$*' ή '*$p \equiv 1(\mathrm{mod}3)$, $(\frac{\varepsilon_{3m}}{p})_3 = 1$*' τότε υπάρχει πάντοτε μία κλάση* $X \in H(D)$ *με* $X^3 = 1$ *έτσι ώστε* $X \longrightarrow p^{\hbar'_3}$.

(3) Αν υπάρχει μία κλάση $X \in H(D)$ *με* $X^3 = 1$ *ώστε* $X \longrightarrow p^{\hbar'_3}$ *και επιπλέον υπάρχει μία κλάση* $X' \in H(D)$ *με* ${X'}^2 = 1$ *ώστε* $X' \longrightarrow p^{\hbar'_2}$, *τότε θα υπάρχει και* $E \in H(D)$ *με* $E^6 = 1$ *έτσι ώστε* $E \longrightarrow p^{\hbar'_6}$.

Απόδειξη: Είναι εύκολο να δει κανείς ότι ισχύει η (1). Από την δομή της ομάδας κλάσεων έπεται ότι το σώμα ανάλυσης του p στην $k_3(D)$ θα είναι ή το k ή κάποια επέκταση του k βαθμού 3. Η (1) προκύπτει άμεσα λόγω πρότασης 0.0.1. Για την (2) μεταφερόμαστε στο σχήμα 8 και υποθέτουμε κατ' αρχήν ότι $p \equiv 2(\bmod 3)$. Στην περίπτωση αυτή $f_p(\mathbb{Q}(\sqrt{-3})) = 2$ και συνεπώς αφού, λόγω της υπόθεσης, ισχύει $f_p(k) = 1$ θα έχουμε τελικά $f_p(K/k) = 2$. Η επέκταση M/k όμως είναι τύπου $(3,3)$ και συνεπώς αποκλείεται στην M/K να έχουμε πλήρη αδράνεια για τον πρώτο p πράγμα που σημαίνει ότι $f_p(M) = 2$ και συνεπώς $f_p(L) = 1$. Το σώμα L όμως αντιστοιχεί σε κάποια κλάση Q της ομάδας κλάσεων με τάξη 3 και έτσι, λόγω της πρότασης 0.0.1, έχουμε το ζητούμενο. Έστω τώρα ότι $p \equiv 1(\mathrm{mod}3)$. Στην περίπτωση αυτή $f_p(\mathbb{Q}(\sqrt{-3}) = 1$ οπότε τελικά $f_p(K) = 1$ πράγμα που σημαίνει ότι

$$f_p(L) = 1 \text{ αν και μόνο αν } f_p(M/K) = 1 \text{ αν και μόνο αν } (\frac{\varepsilon_{3m}}{p})_3 = 1.$$

Για την απόδειξη της (3), αν $C_1 \in H(D)$ με $C_1^3 = 1$ ώστε $L_{C_1}^{(3)} = spl_p(k_3(D))$ και $C_2 \in H(D)$ με $C_2^2 = 1$ ώστε $L_{C_2}^{(2)} = spl_p(k_2(D))$, τότε μπορούμε να θεωρήσουμε την $E = C_1C_2$ για την οποία προφανώς ισχύει $E^6 = 1$ και επιπλέον

$$L_E^{(6)} = L_{C_1}^{(3)} L_{C_2}^{(2)} = spl_p(k_2(D))spl_p(k_3(D)).$$

Όμως ως γνωστόν (βλ. [3] λήμμα 6.7 και άσκηση 6.6(d)) ισχύει

$$spl_p(k_2(D))spl_p(k_3(D)) = spl(k_2(D)k_3(D)) = spl_p(k_6(D))$$

και συνεπώς $E \longrightarrow p^{h'_6}$. $\square$

2.5 Υπολογισμός των συμβόλων Legendre

Στην παράγραφο αυτή δίνουμε έναν κομψό τρόπο υπολογισμού των συμβόλων Legendre που εμφανίζονται στην παρούσα εργασία. Η ιδέα προέρχεται απο την εργασία [7] στην οποία ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει για παρόμοιους υπολογισμούς.

Πρόταση 2.5.1 *Έστω $m \in \mathbb{N}$, $m \equiv 3(\mathrm{mod} 4)$ ελεύθερος τετραγώνου και $n \in \mathbb{N}$. Έστω επίσης p περιττός πρώτος με $p \nmid n$. Θέτουμε $F := \mathbb{Q}(\sqrt{m}, \zeta_n)$ και έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες του R_F πάνω από το p. Αν $\varepsilon = u + v\sqrt{m}$ είναι μία μονάδα του $\mathbb{Q}(\sqrt{m})$ τότε $u^2 - mv^2 = 1$. Ορίζουμε την αναδρομική ακολουθία ακεραίων $(\mathsf{A}_j)_{j\in\mathbb{N}}$ ως εξής: $\mathsf{A}_0 = 2$, $\mathsf{A}_1 = 2u$, $\mathsf{A}_{j+2} = 2u\mathsf{A}_{j+1} - \mathsf{A}_j$. Ισχύει ότι $\mathsf{A}_j = \varepsilon^j + \varepsilon^{-j}$, $\forall j \in \mathbb{N}_0$ και:*

$$(\frac{\varepsilon}{\mathfrak{p}})_n = 1 \quad \textit{αν και μόνο αν} \quad \mathsf{A}_{\frac{N_F(\mathfrak{p})-1}{n}} \equiv 2(\mathrm{mod} p)$$

Απόδειξη: Θα αποδείξουμε την σχέση $\mathsf{A}_j = \varepsilon^j + \varepsilon^{-j}$ επαγωγικά. Για $j = 0,\ 1$ είναι προφανής. Υποθέτουμε ότι ισχύει για j και $j+1$, δηλαδή ότι $\mathsf{A}_j = \varepsilon^j + \varepsilon^{-j}$ και $\mathsf{A}_{j+1} = \varepsilon^{j+1} + \varepsilon^{-(j+1)}$. Έχουμε

$$\begin{aligned}
\varepsilon^{j+2} + \varepsilon^{-(j+2)} &= (u+v\sqrt{m})^{j+2} + (u-v\sqrt{m})^{j+2} \\
&= (u+v\sqrt{m})^{j+1}(u+v\sqrt{m}) + (u-v\sqrt{m})^{j+1}(u-v\sqrt{m}) \\
&= -(u+v\sqrt{m})^{j+1}(u-v\sqrt{m}-2u) - (u-v\sqrt{m})^{j+1}(u+v\sqrt{m}-2u) \\
&= -[(u+v\sqrt{m})^{j} + (u-v\sqrt{m})^{j}] + 2u[(u+v\sqrt{m})^{j+1} + (u-v\sqrt{m})^{j+1}] \\
&= -\mathsf{A}_j + 2u\mathsf{A}_{j+1} \\
&= 2u\mathsf{A}_{j+1} - \mathsf{A}_j \\
&= \mathsf{A}_{j+2},
\end{aligned}$$

οπότε από την υπόθεση της μαθηματικής επαγωγής έπεται ότι θα ισχύει $\mathsf{A}_j = \varepsilon^j + \varepsilon^{-j},\ \forall j \in \mathbb{N}_0$. Παρατηρούμε ότι

$$\mathsf{A}_j \equiv 2(\bmod \mathfrak{p}) \quad \Leftrightarrow \quad \varepsilon^j + \varepsilon^{-j} - 2 \equiv 0(\bmod \mathfrak{p}) \quad \Leftrightarrow \quad (\varepsilon^j - 1)^2 \equiv 0(\bmod \mathfrak{p}) \quad \Leftrightarrow \quad \varepsilon^j \equiv 1(\bmod \mathfrak{p}).$$

οπότε

$$(\frac{\varepsilon}{\mathfrak{p}})_n = 1 \quad \Leftrightarrow \quad \varepsilon^{\frac{N_F(\mathfrak{p})-1}{n}} \equiv 1(\mathrm{mod}\mathfrak{p}) \quad \Leftrightarrow \quad \mathsf{A}_{\frac{N_F(\mathfrak{p})-1}{n}} \equiv 2(\mathrm{mod}\mathfrak{p}).$$

Επειδή

$$\mathsf{A}_{\frac{N_F(\mathfrak{p})-1}{n}} \in \mathbb{Z},$$

η τελευταία σχέση είναι ισοδύναμη με

$$\mathsf{A}_{\frac{N_F(\mathfrak{p})-1}{n}} \equiv 2(\mathrm{mod}p). \ \square$$

Βιβλιογραφία

[1] Αντωνιάδη, Γιάννη, *Ο Γενικός Νόμος Αντιστροφής*, Σημειώσεις, Θεσσαλονίκη 1984.

[2] Brown, Ezra, *The Power of 2 Dividing the Class Number of a Binary Quadratic Discriminant*, Journal of Number Theory **5** (1973), 413-419.

[3] Cox, A. David, *Prime Numbers of The Form* $x^2 + ny^2$, J. Wiley, New York, 1989.

[4] Cohn, Harvey, *Introduction to the Construction of Class Fields*, Cambridge University Press, Cambridge (1985).

[5] Cohn, Harvey and Cooke, George *Parametric Form of an Eight Class Field*, Acta Arithmetica XXX (1976), 367-377.

[6] Hecke, Erich *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag, New York, c1981.

[7] Halter Koch, Franz, *Representation of Primes by Binary Quadratic Forms of Discriminant* $-256q$ *and* $-128q$, Glasgow Math. J. **35** (1993), 261-268.

[8] Halter Koch, Franz, *Einseinheitengruppen und prim Restklassengruppen in quadratischen Zahlkoerpen*, Journal of Number Theory **4** (1972), 70-77.

[9] Halter Koch, Franz, *An Artin Character and Representations of Primes by Binary Quadratic Forms II*, Manuscripta Math. **37** (1982), 357-381.

[10] Halter Koch, Franz, *Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe*, Journal of Number Theory **33** (1971), 412-443.

[11] Halter Koch, Franz, *Geschlechtertheorie der Ringklassenkörper*, J. Reine Angew. Math. 250 (1971), 107-108

[12] Ledet, Arne, *Embedding Problems and Equivalence of Quadratic Forms*,
υπό δημοσίευση (βλ. http://www.cs.bgu.ac.il/research/Fields paper No 16).

[13] Siligardos, Giorgos, *The Embedding Problem and Representation of Prime Powers by Ambiguous Classes of Quadratic Forms*, υπό δημοσίευση στο Journal of Number Theory.

[14] Siligardos, Giorgos, *On Power Residue Characters of Units and the Representation of Numbers by Quadratic Forms*, υπό δημοσίευση στο Acta Arithmetica.