ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΜΑΘΗΜΑΤΙΚΟ ΤΜΗΜΑ

Γιώργος Ε. Συλλιγάρδος

Πρώτοι Αριθμοί της Μορφής $x^2 + ny^2$

Ηράκλειο 1997

Στην οικογένειά μου

Πρώτοι αριθμοί της μορφης x^2+ny^2

Πολλές φορές σαν εφαρμογή της θεωρίας των δακτυλίων αποδεικνύεται ότι ένας περιττός πρώτος αριθμός p γράφεται στην μορφή $p=x^2+y^2$ για κάποιους ακέραιους αριθμούς x,y αν και μόνο αν $p\equiv 1(\mathrm{mod}4)$. Η εφαρμογή αυτή καθώς και ανάλογες προτάσεις του Fermat για πρώτους αριθμούς που γράφονται στις μορφές x^2+2y^2 , x^2+3y^2 , δίνουν το έναυσμα για την μελέτη των πρώτων αριθμών που παρίστανται από τετραγωνικές μορφές
(δηλαδή των πρώτων αριθμών που γράφονται στην μορφή $ax^2+bxy+cy^2$,$a,b,c\in Z$ για κάποιους ακέραιους αριθμούς x,y).

Σκοπός αυτής της εργασίας είναι να χαρακτηριστούν οι περιττοί πρώτοι αριθμοί που παρίστανται από τις τετραγωνικές μορφές x^2+ny^2 , $n\in N$. Για τον σκοπό αυτό θα "επιστρατευθούν" δύο πολύ σημαντικοί κλάδοι της θεωρίας αριθμών : η class field theory και η θεωρία του μιγαδικού πολλαπλασιασμού. Η κατανομή των κεφαλαίων περιγράφεται αναλυτικά παρακάτω.

Στο πρώτο κεφάλαιο γίνονται στοιχειώδεις προσεγγίσεις του προβλήματος από την μία μέσω της γενικής θεωρίας γένους τετραγωνικών μορφών και από την άλλη μέσω των συμβόλων Legendre. Όπως θα διαπιστώσει ο αναγνώστης , δουλεύοντας με τέτοια στοιχειώδη εργαλεία μπορούμε να χρακτηρίσουμε πρώτους αριθμούς της μορφής x^2+ny^2 για ορισμένα μόνο $n\in N$. Καθίσταται λοιπόν αναγκαία η μελέτη του προβλήματος από μια πιο προχωρημένη σκοπιά , κάτι που πραγματοποιείται στο δεύτερο κεφάλαιο. Πιο συγκεκριμένα , μετά από σύντομη υπενθύμηση ορισμών και θεωρημάτων από την στοιχειώδη αλγεβρική θεωρία αριθμών και την θεωρία των moduli , γίνεται εκτενής παρουσίαση της θεωρίας των τάξεων τετραγωνικών σωμάτων αριθμών καθώς και των ιδιοτήτων τους. (Στο σημείο αυτό θα αποδειχθεί η ισομορφία μεταξύ της ομάδας κλάσεων τετραγωνικών μορφών και της ομάδας κλάσεων τάξης για αρνητική διακρίνουσα , αποτέλεσμα που συνδέει την θεωρία τετραγωνικών μορφών και την θεωρία τάξεων.). Στην συνέχεια , αφού γίνει αναφορά στην class field theory και στο θεώρημα
πυκνότητας του Ceboterev , ορίζεται η έννοια του ring class field τάξης και αποδεικνύεται το ακόλουθο θεώρημα

ΘΕΩΡΗΜΑ : Έστω $n\in N$ και έστω $K=Q(\sqrt{-n})$. Υπάρχει ανάγωγο μονικό πολυώνυμο $f_n(x)$ βαθμού $h(-4n)$ ώστε για κάθε περιττό πρώτο αριθμό p που δεν διαιρεί την διακρίνουσα του f_n να ισχύει η παρακάτω ιδοδυναμία :

" $\exists x,y\in Z : p=x^2+ny^2$ " $\leftrightarrow$ " $\left(\frac{-n}{p}\right)_2=1$ και η $f_n(x)\equiv 0(\mathrm{mod}p)$ έχει λύση στο Z "

Επίσης σαν f_n μπορεί να εκλεγεί οποιοδήποτε ανάγωγο πολυώνυμο πανω από το Q πραγματικού αλγεβρικού ακεραίου α , ώστε το K(α) να είναι το ring class field της τάξης $Z[\sqrt{-n}]$ του τετραγωνικού φανταστικού σώματος K.

Τέλος , αν f(x) είναι μονικό πολυώνυμο βαθμού h(-4n) του Z[x] ώστε η πιο πάνω ισοδυναμία να ικανοποιείται για κάθε p περιττό πρώτο που δεν διαιρεί την διακρίνουσα του f , τότε το f είναι ανάγωγο πολυώνυμο πάνω από το K και είναι το ανάγωγο πολυώνυμο πάνω από το K κάποιου στοιχείου b ώστε το K(b) να είναι το ring class field της τάξης $Z[\sqrt{-n}]$ του K.

Το κεφάλαιο 2 κλείνει εφαρμόζοντας το παραπάνω θεώρημα για τον χαρακτηρισμό πρώτων αριθμών των μορφών x^2+14y^2 , x^2+27y^2 και x^2+64y^2.

Το κεφάλαιο 3 ασχολείται με το υπολογιστικό μέρος του προβλήματος και ο σκοπός του είναι να χαρακτηρίσει όσο το δυνατόν πιο "εύχρηστα" τα ring class fields ώστε να είναι εύκολη υπολογιστικά η εφαρμογή του θεωρήματος που αναφέρθηκε παραπάνω . Συγκεκριμένα , στην §1 χρησιμοποιώντας την $\wp$ - συνάρτηση του Weierstrass ορίζεται η j - αναλλοίωτη ενός lattice. Στην §2 ορίζεται η modular εξίσωση και γίνεται λεπτομερής μελέτη των ιδιοτήτων της. Στην §3 , που είναι και η πιο ουσιαστική παράγραφος του κεφαλαίου 3 , χρησιμοποιώντας την modular εξίσωση , χαρακτηρίζονται τα ring class fields τάξης μέσω της j - αναλλοίωτης. Τέλος στην §4 αποδεικνύεται βελτιωμένη έκδοση του θεωρήματος (θεώρημα 3.4.1.3) στην οποία έχουν επισυναφθεί οι πληροφορίες της §3 που αφορούν τον υπολογισμό των ring class fields.

Το τελικό θεώρημα (θεώρημα 3.4.1.3) από υπολογιστικής άποψης μπορεί να μην είναι ιδανικό , όμως η αξία του βρίσκεται στο γεγονός ότι συνδέει την class field theory και την θεωρία του μιγαδικού πολλαπλασιασμού για να δώσει απάντηση στο στοιχειώδες ερώτημα της παράστασης πρώτων αριθμών από τις μορφές x^2+ny^2 , $n\in\mathbb{N}$.

Ευχαριστώ τον καθηγητή κ. Γιάννη Αντωνιάδη για την πολύτιμη βοήθεια που μου παρείχε στην προσπάθεια μου να γνωρίσω ένα όμορφο κλάδο των μαθηματικών καθώς επίσης και για την καθοδήγηση του σε όλη την διάρκεια συγγραφής αυτής της εργασίας. Ευχαριστώ επίσης τους γονείς μου που με την συμπαράσταση και την υπομονή του δημιούργησαν ευνοϊκές συνθήκες για τις σπουδές μου.

Γιώργος Ε. Συλλιγάρδος
Ηράκλειο 23/ 12/ 1996

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 2

ΚΕΦΑΛΑΙΟ 3

ΚΕΦΑΛΑΙΟ 1

ΤΕΤΡΑΓΩΝΙΚΕΣ ΜΟΡΦΕΣ
&
ΣΥΜΒΟΛΑ LEGENDRE

§1 ΥΠΕΝΘΥΜΙΣΕΙΣ ΑΠΟ ΤΗΝ ΣΤΟΙΧΕΙΩΔΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

1.1.1 ΣΥΜΒΟΛΑ LEGENDRE ΚΑΙ JACOBI

1.1.1.1 ΟΡΙΣΜΟΣ : Έστω p περιττός πρώτος και m ένας ακέραιος. Ορίζουμε το τετραγωνικό σύμβολο

του Legendre $\left(\frac{m}{p}\right)_2$ ως εξής

- **Αν p|m τότε $\left(\frac{m}{p}\right)_2 = 0$**
- **Αν (m,p)=1 και υπάρχει $x\in Z$ με $x^2\equiv 1(\mathrm{mod}p)$, τότε $\left(\frac{m}{p}\right)_2 = 1$**
- **Αν (m,p)=1 και δεν υπάρχει $x\in Z$ με $x^2\equiv 1(\mathrm{mod}p)$ τότε $\left(\frac{m}{p}\right)_2 = -1$**

1.1.1.2 ΠΡΟΤΑΣΗ :

I. $\forall a\in Z$, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)_2 (\mathrm{mod}p)$

II. $\forall p,q\in P^*$ $\left(\frac{p}{q}\right)_2 = \left(\frac{q}{p}\right)_2 (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

III. $\forall p\in P^*$ $\left(\frac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}}$

IV. $\forall p\in P^*$, $\forall m,n\in Z$ $\left(\frac{m}{p}\right)_2\left(\frac{n}{p}\right)_2 = \left(\frac{mn}{p}\right)_2$

V. $\forall p\in P^*$ $\left(\frac{2}{p}\right)_2 = (-1)^{\frac{p^2-1}{8}}$

VI. **Αν** $m\equiv n(\mathrm{mod}p)$ **τότε ,** $\left(\frac{m}{p}\right)_2 = \left(\frac{n}{p}\right)_2$

1.1.1.3 ΟΡΙΣΜΟΣ Έστω $m>0$ περιττός ακέραιος και $M\in Z$ με $(M,m)=1$.Έστω επίσης $m=p_1p_2\ldots p_s$ η ανάλυση του m σε πρώτους αριθμούς.Ορίζουμε το γενικευμένο σύμβολο

του Legendre (σύμβολο Jacobi) ως εξής :

$$\left(\frac{M}{m}\right)_2 := \prod_{i=1}^{s}\left(\frac{M}{p_i}\right)_2$$

1.1.1.4 ΛΗΜΜΑ Αν $\alpha_1,\alpha_2,\ldots,\alpha_v$ είναι ακέραιοι περιττοί αριθμοί , τότε τα ακόλουθα είναι ισοδύναμα :

I. $\alpha_1+\alpha_2+\ldots+\alpha_v\equiv v(\mathrm{mod}4)\leftrightarrow\alpha_1\alpha_2\ldots\alpha_v\equiv 1(\mathrm{mod}4)$

II. $(\alpha_1\alpha_2\ldots\alpha_v)^2\equiv 1(\mathrm{mod}16)\leftrightarrow\alpha_1^2+\alpha_2^2+\ldots+\alpha_v^2\equiv v(\mathrm{mod}16)$

1.1.1.5 ΠΡΟΤΑΣΗ

I. Αν M,N,m ακέραιοι και $M\equiv N(\mathrm{mod}m)$ τότε $\left(\frac{M}{m}\right)_2=\left(\frac{N}{m}\right)_2$

II. Αν M,N,m ακέραιοι τότε $\left(\frac{MN}{m}\right)_2=\left(\frac{M}{m}\right)_2\left(\frac{N}{m}\right)_2$

III. Αν M,N,m,n ακέραιοι $\left(\frac{M}{mn}\right)_2=\left(\frac{M}{m}\right)_2\left(\frac{M}{n}\right)_2$

IV. Αν M,m φυσικοί αριθμοί περιττοί και (M,m)=1 τότε $\left(\frac{M}{m}\right)_2=(-1)^{\frac{M-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{M}\right)_2$

V. (α). Αν m ακέραιος αριθμός , τότε $\left(\frac{-1}{m}\right)_2=(-1)^{\frac{m-1}{2}}$

(β). Αν m ακέραιος αριθμός , τότε $\left(\frac{2}{m}\right)_2=(-1)^{\frac{m^2-1}{2}}$

VI. Αν D,m,n ακέραιοι με $D\equiv 0,1(\mathrm{mod}4)$ και $m\equiv n(\mathrm{mod}D)$ τότε $\left(\frac{D}{m}\right)_2=\left(\frac{D}{n}\right)_2$

VII. Αν M,m ακέραιοι και η ισοτιμία $x^2\equiv M(m)$ έχει λύση , τότε $\left(\frac{M}{m}\right)_2=1$

1.1.1.6 ΠΡΟΤΑΣΗ Αν D ακέραιος διάφορος του μηδενός και $D\equiv 0,1(\mathrm{mod}4)$, τότε υπάρχει μοναδικός

ομομορφισμός $\chi: Z_D^*\to\{\pm1\}$ με την ιδιότητα

$\chi([p]_D)=\left(\frac{D}{p}\right)_2$ για κάθε p περιττό πρώτο αριθμό με $p\nmid D$

Επίσης $\chi([-1]_D)=\begin{cases}+1\,,\ \alpha\nu\ D>0\\-1\,,\ \alpha\nu\ D<0\end{cases}$ και ακόμα $[Z_D^*:\ker\chi]=2$

(Βλ. λήμμα 1.14 σελ.16 [Cox]).

1,1,1,7 ΠΟΡΙΣΜΑ Έστω p περιττός πρώτος και $n\in Z-\{0\}$ με $p\nmid n$. Αν $\chi: Z_{-4n}^*\to\{\pm1\}$

ο ομομορφισμός της πρότασης 1.1.6 , τότε τα ακόλουθα είναι ισοδύναμα

I. $p|x^2+ny^2$ **για κάποιους ακεραίους x,y με (x,y)=1**

II. $\left(\frac{-n}{p}\right)_2 = 1$

III. $[p]_D \in \ker\chi$

<u>1.1.1.8 ΠΡΟΤΑΣΗ</u> **Αν p,q περιττοί πρώτοι , τότε** $\left(\frac{p}{q}\right)_2 = 1 \leftrightarrow p \equiv \pm b^2 (\mathrm{mod} 4q)$ **, για κάποιον b περιττό πρώτο.**

§2 ΤΕΤΡΑΓΩΝΙΚΕΣ ΜΟΡΦΕΣ

1.2.1 ΓΕΝΙΚΑ ΓΙΑ ΤΕΤΡΑΓΩΝΙΚΕΣ ΜΟΡΦΕΣ

1.2.1.1 ΟΡΙΣΜΟΣ : Ένα πολυώνυμο δυο μεταβλητών f(x,y) του Z[x,y] της μορφής $f(x,y)=Ax^2+Bxy+Cy^2$
θα λέγεται τετραγωνική μορφή . Αν επιπλέον ισχύει ΜΚΔ(A,B,C)=1 , τότε η f
λέγεται πρωταρχική (primitive)

1.2.1.2 ΟΡΙΣΜΟΣ : Δύο τετραγωνικές μορφές f,g θα λέγονται ισοδύναμες αν και μόνο αν υπάρχει

πίνακας $M=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2x2}(Z)$ **με** $\det(M)=\pm 1$ **ώστε , για**

$\begin{pmatrix} u \\ v \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ **με u,v,x,y ακεραίους , να ισχύει f(x,y)=g(u,v)**

- **Αν det(M)=1 , οι f,g θα λέγονται κανονικά ισοδύναμες(properly equivalent)**
- **Αν det(M)=-1 , οι f,g θα λέγονται αντικανονικά ισοδύναμες(improperly equivalent)**

1.2.1.3 ΣΗΜΕΙΩΣΗ : Η ισοδυναμία και η κανονική ισοδυναμία ορίζουν σχέσεις ισοδυναμίας στο σύνολο
των τετραγωνικών μορφών . Οι κλάσεις ισοδυνάμων τετραγωνικών μορφών που
ορίζουν η ισοδυναμία και η κανονική ισοδυναμία θα λέγονται Langrangian-κλάσεις
και κλάσεις αντίστοιχα.

1.2.1.4 ΟΡΙΣΜΟΣ : Έστω f μια τετραγωνική μορφή και m ένας ακέραιος. Αν υπάρχουν κ,λ ακέραιοι
ώστε m=f(κ,λ) τότε λέμε ότι ο m παρίσταται (ή αναπαρίσταται) από την μορφή f . Αν επιπλέον (κ,λ)=1 τότε λέμε ότι ο m παρίσταται κανονικά από την f.
Αν υπάρχουν κ,λ,n ακέραιοι ώστε $m \equiv f(κ,λ) (\mathrm{mod} n)$, θα λέμε ότι ο m παρίσταται modulo n από την f. Τέλος , θα λέμε ότι ένα σύνολο παρίσταται (παρίσταται κανονικά, παρίσταται modulo n) από την f αν κάθε στοιχείο του παρίσταται (παρίσταται κανονικά, παρίσταται modulo n) από την f.

<u>1.2.1.5 ΠΑΡΑΤΗΡΗΣΗ</u> : Έστω $f(x,y)=Ax^2+Bxy+Cy^2$ μία τετραγωνική μορφή και $\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ με

a,b,c,d ακεραίους τότε $f(u,v)=f(a,c)x^2+(2Aab+B(ad+cb)+C2cd)xy+f(b,d)y^2$

<u>1.2.1.6 ΠΟΡΙΣΜΑ</u> : Αν f,g είναι μορφές ισοδύναμες και η g είναι πρωταρχική , τότε και η f είναι πρωταρχική.

<u>ΑΠΟΔΕΙΞΗ</u>

Η απόδειξη στηρίζεται σε απλή εφαρμογή της σχέσης της παρατήρησης 1.2.1.5 και αφήνεται ώς άσκηση.

<u>1.2.1.7 ΠΑΡΑΤΗΡΗΣΗ</u> : Αν $M=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2x2}(Z)$ και $\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ με (u,v)=1 , τότε και (χ,y)=1 .

Άρα κάθε αριθμός παρίσταται κανονικά από μιά τετραγωνική μορφή αν και μόνο αν παρίσταται κανονικά από κάθε ισοδύναμη της μορφή .

<u>1.2.1.8 ΠΑΡΑΤΗΡΗΣΗ</u> : Αν ο ακέραιος m παρίσταται από την μορφή f , τότε ο m γράφεται $m=d^2m'$,

όπου m' παρίσταται κανονικά από την f.

<u>1.2.1.9 ΠΡΟΤΑΣΗ</u> : Μιά μορφή f αναπαριστά κανονικά ένα ακέραιο m αν και μόνο αν η f είναι

κανονικά ισοδύναμη με μια τετραγωνική μορφή g(x,y) της μορφής : $g(x,y)=mx^2+bxy+cy^2$, για κάποιους ακεραίους b,c.

<u>ΑΠΟΔΕΙΞΗ</u>

$(\rightarrow)$ Έστω k,l ακέραιοι με (k,l)=1 και f(k,l)=m .Αφού (k,-l)=1 , θα υπάρχουν s,r ακέραιοι ώστε

ks-lr=1 .Άρα $\det\begin{pmatrix} k & r \\ l & s \end{pmatrix} = 1$.Θέτουμε $\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} k & r \\ l & s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$, οπότε από την παρατήρηση 2.1.5 έχουμε οτι $f(u,v)=f(k,l)x^2+Txy+Ly^2$,για κάποιους ακεραίους T και L και συνεπώς για $g(x,y)=mx^2+Txy+Ly^2$ έχουμε f(u,v)=g(x,y).

$(\leftarrow)$ Αν η f είναι κανονικά ισοδύναμη με μια τετραγωνική μορφή g της μορφής $g(x,y)=mx^2+bxy+cy^2$, τότε επειδή g(1,0)=m και επειδή ισοδύναμες μορφές παριστούν κανονικά τους ίδιους αριθμούς , θα έχουμε ότι ο m παρίσταται κανονικά από την f.

1.2.1.10 ΟΡΙΣΜΟΣ : Διακρίνουσα μιας τετραγωνικής μορφής $f(x,y)=Ax^2+Bxy+Cy^2$ λέγεται ο αριθμός

B^2-4AC και συμβολίζεται με D_f.

1.2.1.11 ΠΡΟΤΑΣΗ : Για κάθε ακέραιο αριθμό D με $D \equiv 0,1(\mathrm{mod}4)$ υπάρχει πρωταρχική μορφή με διακρίνουσα D.

ΑΠΟΔΕΙΞΗ

Θεωρούμε την μορφή $x^2-\frac{D}{4}y^2$, αν $D\equiv 0(\mathrm{mod}4)$ και την μορφή $x^2+xy+\frac{1-D}{4}y^2$ αν $D\equiv 1(\mathrm{mod}4)$

1.2.1.12 ΟΡΙΣΜΟΣ : Κάθε ακέραιος D με $D\equiv 0,1(\mathrm{mod}4)$ θα λέγεται διακρίνουσα.

1.2.1.13 ΠΡΟΤΑΣΗ : Έστω f,g τετραγωνικές μορφές και $M=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2x2}(Z)$. Αν για

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

ισχύει $f(x,y)=g(u,v)=g(ax+by,cx+dy)$, τότε $D_f=\det(M)^2 \cdot D_g$

ΑΠΟΔΕΙΞΗ

Εύκολες πράξεις

1.2.1.14 ΠΟΡΙΣΜΑ : Ισοδύναμες μορφές έχουν την ίδια διακρίνουσα

1.2.1.15 ΠΡΟΤΑΣΗ : Αν $f(x,y)=Ax^2+Bxy+Cy^2$ μια τετραγωνική μορφή τότε $4Af(x,y)=(2Ax+By)^2-D_fy^2$

ΑΠΟΔΕΙΞΗ

Εύκολες πράξεις

1.2.1.16 ΠΡΟΤΑΣΗ : Αν $f(x,y)=Ax^2+Bxy+Cy^2$ μια τετραγωνική μορφή , τότε :

(i) Αν $D_f>0$ τότε η f παριστά και θετικούς και αρνητικούς ακεραίους

(ii) Αν $D_f<0$ τότε

- **Αν $A>0$, τότε η f παριστά μόνο θετικούς ακέραιους (για $x,y\neq 0$)**
- **Αν $A<0$, τότε η f παριστά μόνο αρνητικούς ακεραίους (για $x,y\neq 0$)**

ΑΠΟΔΕΙΞΗ

Η πρόταση είναι προφανής συνέπεια της πρότασης 1.2.1.15

1.2.1.17 ΟΡΙΣΜΟΣ : (I) Μια τετραγωνική μορφή που παριστά μόνο μη αρνητικούς ακέραιους λέγεται

θετικά ορισμένη (positive definite)

(ii) Μια τετραγωνική μορφή που παριστά μόνο μη θετικούς ακεραίους λέγεται αρνητικά ορισμένη (negative definite)

(iii) Για ακέραιο αριθμό D με $D\equiv 0,1 \pmod 4$ θα συμβολίζουμε με F(D) το σύνολο όλων των τετραγωνικών μορφών διακρίνουσας D και με $F_{pd}(D)$ το σύνολο των πρωταρχικών θετικά ορισμένων μορφών διακρίνουσας D

<u>1.2.1.18 ΠΑΡΑΤΗΡΗΣΕΙΣ</u> : (I) Αν μια τετραγωνική μορφή είναι θετικά (αρνητικά) ορισμένη , τότε και κάθε ισοδύναμη της μορφή θα είναι θετικά (αρνητικά) ορισμένη

(ii) Αν $f(x,y)=Ax^2+Bxy+Cy^2$ μια τετραγωνική μορφή τότε για $M_f=\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}$ ισχύει $f(x,y)=\begin{pmatrix} x & y \end{pmatrix} M_f \begin{pmatrix} x \\ y \end{pmatrix}$, οπότε μια μορφή είναι θετικά (αρνητικά) ορισμένη αν και μόνο αν ο πίνακας M_f είναι θετικα (αρνητικά) ορισμένος.

<u>1.2.1.19 ΠΑΡΑΤΗΡΗΣΗ</u> : Αν $f(x,y)=Ax^2+Bxy+Cy^2$ μια τετραγωνική μορφή τότε $D_f\equiv 0,1 \pmod 4$

<u>1.2.1.20 ΠΡΟΤΑΣΗ</u> : Αν D ακέραιος αριθμός με $D\equiv 0,1 \pmod 4$ και m ακέραιος περιττός με (m,D)=1

τότε τα ακόλουθα είναι ισοδύναμα :

(i). Ο m παρίσταται κανονικά από μια πρωταρχική μορφή διακρίνουσας D.

(ii). Ο m παρίσταται κανονικά από μια μορφή διακρίνουσας D.

(iii). Ο D είναι τετραγωνικό υπόλοιπο modulo m

Στην περίπτωση που ο m δεν είναι απαραίτητα περιττός , ισχύει η συνεπαγωγή (ii) → (iii)

<u>ΑΠΟΔΕΙΞΗ</u>

<u>(i) → (ii)</u> Προφανές

<u>(ii) → (iii)</u> Έστω $f(x,y)=Ax^2+Bxy+Cy^2$ τετραγωνική μορφή με $m=f(k,l)$ για $k,l\in Z$. Από την πρόταση 1.2.1.9 έχουμε ότι υπάρχουν ακέραιοι T,L ώστε η f να είναι κανονικά ισοδύναμη με την μορφή $g(x,y)=mx^2+Txy+Ly^2$. Έπειδή οι f,g είναι ισοδύναμες θα έχουμε $D_f=D_g=T^2-4mL$. Άρα $D_f\equiv T^2 \pmod m$ οπότε $D=D_f\equiv T^2 \pmod m$. Δηλαδή ο D είναι τετραγωνικό υπόλοιπο modulo m

(Όπως είναι φανερό η παραπάνω απόδειξη ισχύει για κάθε ακέραιο m.)

<u>(iii) → (i)</u> Έστω ότι ο D είναι τετραγωνικό υπόλοιπο modulo m . Άρα υπάρχει $B\in Z$ ώστε $D\equiv B^2 \pmod m$. Θα αποδείξουμε ότι μπορούμε , χωρίς περιορισμό της γενικότητας , να υποθέσουμε ότι $D\equiv B^2 \pmod 4$. Πράγματι :

- Αν B=περιττός και $D\equiv 1 \pmod 4$ τότε το ζητούμενο είναι προφανές

- Αν B=περιττός και D≡0(mod4) , τότε B+m=άρτιος και έτσι $(B+m)^2 \equiv 0 \equiv D(mod4)$ Εξάλλου $(B+m)^2 \equiv B^2 \equiv D(modm)$ άρα μπορούμε να βάλλουμε στην θέση

του B το B+m

- Αν B=άρτιος και D≡0(mod4) τότε το ζητούμενο είναι προφανές
- Αν B=άρτιος και D≡1(mod4) τότε B+m=περιττός και $(B+m)^2 \equiv D(mod4)$

Επίσης $(B+m)^2 \equiv B^2 \equiv D(modm)$.

Έτσι αφού m=περιττός θα έχουμε $D \equiv B^2(mod4m)$, άρα υπάρχει $C \in Z$ ώστε $D=B^2-4mC$ Συνεπώς η τετραγωνική μορφή $f(x,y)=mx^2+Bxy+Cy^2$ έχει διακρίνουσα $D_f=D$ και παριστά κανονικά τον m (βλ. Προταση 1.2.1.9) . Επίσης η f είναι πρωταρχική αφού (m,D)=1 άρα (m,B)=1 οπότε και ΜΚΔ(m,B,C)=1

<u>1.2.1.21 ΠΡΟΤΑΣΗ</u> : Αν D ακέραιος με D≡0,1(mod4) , D<0 και p περιττός πρώτος αριθμός με p ∤ D

τότε $\left(\frac{D}{p}\right)_2 = 1$ αν και μόνο αν ο p παρίσταται κανονικά από πρωταρχική θετικά

ορισμένη μορφή διακρίνουσας D

<u>ΑΠΟΔΕΙΞΗ</u>

Εξ' ορισμού έχουμε οτι $\left(\frac{D}{p}\right)_2 = 1$ αν και μόνο αν ο D είναι τετραγωνικό υπόλοιπο modulo p .

Έτσι , η

πρόταση 1.2.1.20 δίνει ότι $\left(\frac{D}{p}\right)_2 = 1$ αν και μόνο αν ο p παρίσταται από πρωταρχική μορφή διακρίνουσας

D. Όμως D<0 και έτσι αφού η εν λόγω μορφή παριστά τουλάχιστον ένα θετικό ακέραιο (τον p),

η πρόταση 1.2.1.16 μας δίνει ότι η μορφή είναι θετικά ορισμένη.

<u>1.2.1.22 ΠΟΡΙΣΜΑ</u> : Αν n είναι ένας φυσικός και p περιττός πρώτος με p ∤ n τότε $\left(\frac{-n}{p}\right)_2 = 1$ αν και

μόνο αν ο p παρίσταται απο μια πρωταρχική θετικά ορισμένη μορφή διακρίνουσας -4n.

<u>ΑΠΟΔΕΙΞΗ</u>

Για D=-4n<0 έχουμε $\left(\frac{-n}{p}\right)_2 = 1 \leftrightarrow \left(\frac{-4n}{p}\right)_2 = 1 \leftrightarrow \left(\frac{D}{p}\right)_2 = 1$. Το ζητούμενο είναι τώρα προφανές από την πρόταση 1.2.1.21

1.2.2 ΘΕΩΡΙΑ ΑΝΗΓΜΕΝΩΝ ΤΕΤΡΑΓΩΝΙΚΩΝ ΜΟΡΦΩΝ

1.2.2.1 ΟΡΙΣΜΟΣ : Έστω f μια πρωταρχική θετικά ορισμένη μορφή με $f(x,y)=Ax^2+Bxy+Cy^2$. Αν η f ικανοποιεί τα ακόλουθα :

(i) $|B|\leq A\leq C$

(ii) (a) Αν $|B|=A$ τότε $B\geq 0$

(b) Αν $C=A$ τότε $B\geq 0$

Τότε η f λέγεται ανηγμένη. Αν η f ικανοποιεί μόνο το (ι) , τότε λέγεται σχεδόν ανηγμένη.

1.2.2.2 ΠΑΡΑΤΗΡΗΣΗ : Αν f μορφή θετικά ορισμένη με $f(x,y)=Ax^2+Bxy+Cy^2$ τότε $A=f(1,0)\geq 0$ και $C=f(0,1)\geq 0$.

1.2.2.3 ΘΕΩΡΗΜΑ : Κάθε πρωταρχική θετικά ορισμένη μορφή είναι κανονικά ισοδύναμη με μια μοναδική ανηγμένη μορφή.

ΑΠΟΔΕΙΞΗ

Η απόδειξη είναι τεχνική και παραλείπεται.(βλ. [Cox] σελ 27 θεώρημα. 2.8)

1.2.2.4 ΟΡΙΣΜΟΣ : Επειδή από την 1.2.1.11 πρόταση και το 1.2.2.3 θεώρημα έχουμε ότι αν $D\equiv 0,1 \pmod 4$ με $D<0$ τότε υπάρχει ανηγμένη μορφή διακρίνουσας D , έχει νόημα για ένα τέτοιο D να ορίσουμε το σύνολο RF(D) των ανηγμένων τετραγωνικών μορφών διακρίνουσας D.

1.2.2.5 ΠΑΡΑΤΗΡΗΣΕΙΣ : (ι) Οι μορφές $3x^2+2xy+5y^2$, $3x^2-2xy+5y^2$ είναι ανηγμένες . Είναι επίσης ισοδύναμες αλλά όχι κανονικά ισοδύναμες.

(ιι) Οι μορφές $2x^2+2xy+3y^2$, $2x^2-2xy+3y^2$ είναι ισοδύναμες και μάλιστα κανονικά ισοδύναμες , όμως μόνο η $2x^2+2xy+3y^2$ είναι ανηγμένη.

1.2.2.6 ΟΡΙΣΜΟΣ : Έστω D ακέραιος αριθμός με $D<0$. Με C(D) θα συμβολίζουμε το σύνολο των κλάσεων (με την κανονική ισοδυναμία) των θετικά ορισμένων πρωταρχικών μορφών διακρίνουσας D . Επίσης θα συμβολίζουμε με h(D) το πλήθος των στοιχείων του C(D).

<u>1.2.2.7 ΘΕΩΡΗΜΑ</u> : Αν D ακέραιος αριθμός με D<0 και D≡0,1(mod4) τότε ο h(D) είναι ο αριθμός των ανηγμένων θετικά ορισμένων πρωταρχικών μορφών διακρίνουσας D , και h(D)<∞.

(Δηλαδή h(D)=#C(D)=#RF(D))

<u>ΑΠΟΔΕΙΞΗ</u>

Επειδή κάθε στοιχείο-κλάση του C(D) αντιπροσωπεύεται πλήρως από μια μοναδική ανηγμένη
τετραγωνική μορφή εχουμε κατ'αρχήν ότι ο h(D) είναι ο αριθμός των ανηγμένων θετικά ορισμένων
πρωταρχικών μορφών διακρίνουσας D . Μένει τώρα να δείξουμε ότι αριθμός των ανηγμένων θετικά
ορισμένων πρωταρχικών μορφών διακρίνουσας D είναι πεπερασμένος . Πράγματι , αν $Ax^2+Bxy+Cy^2$
είναι ανηγμένη μορφή διακρίνουσας D, τότε εξ'ορισμού : $B^2-4AC=D$. Επίσης $|B|\le A$ άρα και

$B^2\le A^2$, $A\le C$ οπότε $-D=4AC-B^2\ge 4A^2-A^2=3A^2$ και έτσι λοιπόν $A\le\sqrt{\frac{-D}{3}}$.

Η τελευταία σχέση δείχνει ότι υπάρχουν πεπερασμένες επιλογές για το A (Μάλιστα ισχύει ότι :
$A\in\left\{0,1,2,\ldots,\left[\sqrt{\frac{-D}{3}}\right]\right\}$). Επίσης το ότι $|B|\le A$ δίνει πεπερασμένες επιλογές για το B .
Τέλος

η σχέση $B^2-4AC=D$ δίνει το C συναρτήσει των A,B και συνεπώς έχουμε πεπερασμένες επιλογές και
για το C άρα και για την τετραγωνική μορφή .

<u>1.2.2.8 Εφαρμογή</u> : Με βάση την μέθοδο που εμφανίζεται στην απόδειξη του Θεωρήματος 1.2.2.7 μπορούμε να υπολογίσουμε :

D	h(D)	C(D)
-4	1	$\{[x^2+y^2]\}$
-8	1	$\{[x^2+2y^2]\}$
-12	1	$\{[x^2+3y^2]\}$
-20	2	$\{[x^2+5y^2],[2x^2+2xy+3y^2]\}$
-28	1	$\{[x^2+7y^2]\}$
-32	2	$\{[x^2+8y^2],[3x^2+2xy+3y^2]\}$
-56	4	$\{[x^2+14y^2],[2x^2+7y^2],[3x^2\pm 2xy+5y^2]\}$
-108	3	$\{[x^2+27y^2],[4x^2\pm 2xy+7y^2]\}$
-124	3	$\{[5x^2\pm 4xy+7y^2],[x^2+31y^2]\}$
-256	4	$\{[x^2+64y^2],[4x^2+4xy+17y^2],[5x^2\pm 2xy+13y^2]\}$

**(Οι μορφές των οποίων οι κλάσεις εμφανίζονται στον παραπάνω πίνακα είναι σε
ανηγμένη μορφή.)**

1.2.3 $p=x^2+ny^2$ ΚΑΙ ΤΕΤΡΑΓΩΝΙΚΕΣ ΜΟΡΦΕΣ ΣΤΟΙΧΕΙΩΔΗΣ ΘΕΩΡΙΑ ΓΕΝΟΥΣ

1.2.3.1 ΠΡΟΤΑΣΗ : (I) Αν D ακέραιος με D<0 , D≡0,1(mod4) και p περιττός πρώτος αριθμός με $p \nmid D$,

τότε $\left(\frac{D}{p}\right)_2 = 1$ αν και μόνο αν ο p παρίσταται από μια εκ των h(D) ανηγμένων μορφών διακρίνουσας D.

(ii) Αν n είναι φυσικός αριθμός και p περιττός πρώτος αριθμός με $p \nmid n$ τότε $\left(\frac{-n}{p}\right)_2 = 1$

αν και μόνο αν ο p αναπαρίσταται από μια από τις h(-4n) ανηγμένες τετραγωνικές μορφές διακρίνουσας -4n.

ΑΠΟΔΕΙΞΗ

Είναι προφανής συνέπεια του της πρότασης 1.2.1.21 , του πορίσματος 1.2.1.22 και του θεωρήματος 1.2.2.3

1.2.3.2 ΘΕΩΡΗΜΑ : Αν D ακέραιος με D<0 και D≡0,1(mod4) , και $\chi: Z_D^* \to \{\pm 1\}$: $\chi([p]_D) = \left(\frac{D}{p}\right)_2$ ο ομομορφισμός της πρότασης 1.1.1.6 , τότε για p περιττό πρώτο ισχύει ότι $[p]_D \in \ker(\chi)$ αν και μόνο αν ο p παρίσταται από μια εκ των h(D) ανηγμένων τετραγωνικών μορφών διακρίνουσας D

ΑΠΟΔΕΙΞΗ

$[p]_D \in \ker\chi \leftrightarrow \left(\frac{D}{p}\right)_2 = 1$, οπότε το ζητούμενο προκύπτει από την πρόταση 1.2.3.1

1.2.3.3 ΘΕΩΡΗΜΑ : Αν n φυσικός αριθμός , τότε h(-4n)=1 ↔ n∈{1,2,3,4,7}

ΑΠΟΔΕΙΞΗ

$(\leftarrow)$ Προφανές από την εφαρμογή 1.2.2.8

$(\rightarrow)$ Θα δείξουμε ότι αν h(-4n)=1 τότε αναγκαστικά. n∈{1,2,3,4,7}. Πράγματι , έστω ότι n∉{1,2,3,4,7}..Επειδή η x^2+ny^2 είναι ανηγμένη μορφή διακρίνουσας -4n , αν δείξουμε ότι υπάρχει ανηγμένη μορφή διακρίνουσας -4n διαφορετική της x^2+ny^2 τότε έχουμε καταλήξει σε άτοπο αφού h(-4n)=1 .

1η Περίπτωση : "Ο n να μην είναι δύναμη πρώτου αριθμού"

Τότε υπάρχουν φυσικοί a,c με 1<a<c και (a,c)=1 ώστε n=ac . Άρα η μορφή ax^2+cy^2 είναι ανηγμένη μορφή διακρίνουσας -4n και είναι διαφορετική της x^2+ny^2 συνεπώς έχουμε άτοπο

2η Περίπτωση : "Ο n να είναι δύναμη πρώτου αριθμού"

(I) Αν $n=2^r$,με $r\in N$ τότε επειδή n≠2,4 θα έχουμε r≥3

(α) Για r=3 έχουμε $h(-4\cdot 2^3)=h(-32)=2$ (βλ. Εφαρμογή 1.2.2.8)

(β) Για r>3 , η μορφή $4x^2+4xy+(2^{r-2}+1)y^2$ είναι ανηγμένη αφού $4\le 2^{r-2}+1$, έχει διακρίνουσα –4n και είναι διαφορετική της x^2+ny^2 και συνεπώς έχουμε άτοπο .

(II) Αν $n=p^r$ όπου p είναι περιττός πρώτος τότε :

(α) Αν ο n+1 δεν είναι δύναμη πρώτου τότε υπάρχουν φυσικοί a,c με 2≤a≤c και (a,c)=1 ώστε n+1=ac, οπότε η μορφή $ax^2+2xy+cy^2$ είναι ανηγμένη διακρίνουσας -4n και διαφορετική της x^2+ny^2 οπότε έχουμε και πάλι άτοπο

(β) Αν ο n+1 είναι δύναμη πρώτου τότε ο p είναι περιττός άρα και ο n είναι περιττός και συνεπώς ο n+1 είναι άρτιος.

Έτσι ∃s∈N ώστε $n+1=2^s$. Επειδή όμως $n\notin\{1,2,3,4,7\}$ θα έχουμε αναγκαστικά s≥4, οπότε :

- Για s=4,5 έχουμε αντίστοιχα n=15,31. Όμως το 15 δεν είναι δύναμη πρώτου και η περίπτωση n=31 δίνει $h(-4\cdot 31)=h(-124)=3>1$ πράγμα άτοπο .
- Για $s\ge 6$ θεωρούμε την μορφή $8x^2+6xy+(2^{s-3}+1)y^2$ η οποία είναι ανηγμένη διακρίνουσας -4n και διαφορετική της x^2+ny^2 οπότε έχουμε άτοπο .

1.2.3.4 ΟΡΙΣΜΟΣ : Γένος μιας θετικά ορισμένης πρωταρχικής μορφής f με $D=D_f<0$ λέγεται το σύνολο όλων των θετικά ορισμένων πρωταρχικών μορφών διακρίνουσας D που αναπαριστούν modulo D τους ίδιους αριθμούς πρώτους προς το D αριθμούς.

1.2.3.5 ΠΑΡΑΤΗΡΗΣΕΙΣ Ισοδύναμες θετικά ορισμένες πρωταρχικές μορφές έχουν το ίδιο γένος και συνεπώς όπως μπορεί κανείς εύκολα να δει η έννοια του γένους ορίζει σχέση ισοδυναμίας στο σύνολο $F_{pd}(D)$ η οποία είναι γενικότερη κατά κάποιο τρόπο από την κανονική ισοδυναμία λόγω του ότι η έννοια του γένους αποτελεί και σχέση ισοδυναμίας στο σύνολο C(D)

1.2.3.6 ΟΡΙΣΜΟΣ : Έστω D ακέραιος αριθμός με $D<0$ και $D\equiv 0,1(\mathrm{mod}4)$. Ορίζουμε την κύρια μορφή (principal form) διακρίνουσας D να είναι :

$$x^2-\frac{D}{4}y^2 \quad \text{αν } D\equiv 0(\mathrm{mod}4) \quad \text{και}$$

$$x^2+xy+\frac{1-D}{4}y^2 \quad \text{αν } D\equiv 1(\mathrm{mod}4).$$

Επίσης η κλάση της C(D) η οποία περιέχει την κύρια μορφή διακρίνουσας D θα λέγεται κύρια κλάση.

1.2.3.7 ΠΡΟΤΑΣΗ : Αν f(x,y) είναι πρωταρχική μορφή και M ακέραιος αριθμός , τότε υπάρχουν x,y ακέραιοι ώστε ΜΚΔ(f(x,y),M)=1 και ΜΚΔ(x,y)=1 . (Δηλαδή , η f παριστά κανονικά και αριθμούς πρώτους προς τον M.)

ΑΠΟΔΕΙΞΗ

Η απόδειξη είναι τεχνική και παραλείπεται (βλ. ασκ.2.18 σελ 45 [Cox])

1.2.3.8 ΘΕΩΡΗΜΑ : Έστω ακέραιος D με $D<0, D\equiv 0,1(\mathrm{mod}4)$, και $\chi : Z_D^{*} \to \{\pm 1\}$: $\chi([m]_D)=\left(\frac{D}{m}\right)_2$

$\forall m \in Z$ με (m,D)=1 , ο γνωστός ομομορφισμός της πρότασης 1.1.1.6 της §1 .

Ισχύουν τα ακόλουθα :

(ι) Κάθε ακέραιος m πρώτος προς το D που αναπαρίσταται από κάποια μορφή διακρίνουσας D , αν παρθεί modulo D , δίνει στοιχείο του Z_D^* το οποίο ανήκει ειδικότερα στο kerχ. Επιπλέον , οι πρώτοι προς το D αριθμοί που παρίστανται από την κύρια μορφή διακρίνουσας D , αν παρθούν modulo D συγκροτούν υποομάδα H του kerχ.

(ιι) Αν f(x,y) τυχαία πρωταρχική μορφή διακρίνουσας D , τότε αν όλοι οι πρώτοι προς το D αριθμοί που παρίστανται από την f παρθούν modulo D , συγκροτούν ένα coset της H στον kerχ

ΑΠΟΔΕΙΞΗ

(ι) Έστω ακέραιος m πρώτος προς τον D και ο οποίος παρίσταται από κάποια μορφή διακρίνουσας D.

Θα δείξουμε ότι $[m]_D \in \ker\chi$. Από παρατήρηση 1.2.1.8 έχουμε ότι υπάρχουν d,m_1 ακέραιοι ώστε

$m=d^2m_1$ και ο m_1 να παρίσταται κανονικά από την f. Έχουμε $\chi([m]_D)=\chi([d^2]_D)\cdot\chi([m_1]_D)=\chi([m_1]_D)$

Τώρα από πρόταση 1.2.1.20 έχουμε ότι $\chi([m_1]_D)=1$ άρα και $\chi([m]_D)=1$ δηλαδή $[m]_D \in \ker\chi$.

Έστω τώρα f(x,y) η κύρια μορφή διακρίνουσας D και έστω H:={f(x,y)mod(D) | $x,y \in Z$}. Θα ισχύει

προφανώς από τα παραπάνω ότι $H \subseteq \ker\chi$. Διακρίνουμε τις περιπτώσεις :

$1^η$ Περίπτωση : D≡0(mod4)

Έστω D=-4n για n φυσικό. Η κύρια μορφή για την D είναι η $f(x,y)=x^2+ny^2$. Αλλά $(x^2+ny^2)(z^2+nw^2)=(xz\pm nyw)^2+n(xw\mp yz)^2, \forall x,y,z,w \in Z$, οπότε αν $[a]_D,[b]_D \in H$, τότε εξ' ορισμού της H υπάρχουν $a' \in [a]_D, b' \in [b]_D$ ώστε να υπάρχουν x,y,z,w ακέραιοι με $a'=x^2+ny^2, b'=z^2+nw^2$ οπότε από την παραπάνω ταυτότητα προκύπτει ότι ο $a'b'$ παρίσταται από την κύρια μορφή διακρίνουσας D.

Άρα $[a'b']_D \in H \to [a']_D[b']_D \in H \to [a]_D[b]_D \in H$ και συνεπώς $H \subseteq \ker\chi$.

$2^η$ Περίπτωση : D≡1(mod4)

Στην περίπτωση αυτή η κύρια μορφή διακρίνουσας D είναι η $f(x,y)=x^2+xy+\frac{1-D}{4}y^2$.

Εύκολα βλέπουμε ότι ισχύει : $\forall x,y \in Z \quad 4(x^2+xy+\frac{1-D}{4}y^2) \equiv (2x+y)^2 (\mathrm{mod} D)$

Χρησιμοποιώντας αυτήν την σχέση θα δείξουμε ότι το σύνολο H είναι ακριβώς η υποομάδα

των τετραγώνων του Z_D^*. Πράγματι :

- Αν y=άρτιος τότε αφού D≡1(mod4) θα έχουμε

$$4(x^2+xy+\frac{1-D}{4}y^2) \equiv (x+\frac{y}{2})^2 (\mathrm{mod} D)$$

- Αν y=περιττός τότε y+D=άρτιος και θα έχουμε

$$(x^2+xy+\frac{1-D}{4}y^2)\equiv 4(x^2+x(y+D)+\frac{1-D}{4}(y+D)^2)\equiv(x+\frac{y+D}{2})^2(\mathrm{mod}D)$$

Σε κάθε λοιπόν περίπτωση τα στοιχεία f(x,y)modD για τα διάφορα x,y∈Z ανήκουν στην υποομάδα των τετραγώνων του Z_D^*.

Αντίστροφα , αν α∈Z με [α]∈ Z_D^* τότε $[\alpha]^2\in(Z_D^*)^2$ οπότε γράφοντας α=2x+y για x,y∈Z, θα έχουμε $(2x+y)^2\equiv 4(x^2+xy+\frac{1-D}{4}y^2)\equiv(2x)^2+(2x)(2y)+\frac{1-D}{4}(2y)^2(\mathrm{mod}\ D)$

Άρα $[a^2]\in H\rightarrow[a]^2\in H$ και συνεπώς το H είναι ακριβώς η υποομάδα των τετραγώνων του Z_D^* οπότε και στην περίπτωση αυτή H⊆kerχ (αφού Z_D^*⊆kerχ).

(ii) 1η Περίπτωση : <u>D≡0(mod4)</u>

Έστω π.χ. D=-4n με n φυσικό αριθμό. Από την πρόταση 1.2.3.7 έχουμε ότι η f παριστά κανονικά και αριθμούς πρώτους προς το D. Έστω m ένας τέτοιος ακέραιος αριθμός. Σύμφωνα λοιπόν με την πρόταση 1.2.1.9 η f είναι κανονικά ισοδύναμη με μια μορφή $g(x, y)=mx^2+Bxy+Cy^2$, B,C∈Z . Τώρα $D_g=D_f=-4n$ άρα $B^2-4mC=-4n$ και συνεπώς ο B είναι άρτιος. Έστω λοιπόν $B=2B_1$, $B_1\in Z$ Από την ταυτότητα της πρότασης 1.2.1.15 έχουμε : $mg(x,y)=(mx+B_1y)^2+ny^2$ (T). Επίσης από το πόρισμα 1.2.1.6 και επειδή η f είναι πρωταρχική, έχουμε ότι και η g είναι πρωταρχική. Θα δείξουμε τώρα ότι οι ακέραιοι αριθμοί που παρίστανται από την g και είναι πρώτοι προς το D , αν παρθούν modulo D συγκροτούν ένα το coset $[m]_D^{-1}H$ της H στον kerχ οπότε και θα έχουμε τελειώσει αφού οι f και g παριστούν τους ίδιους ακεραίους. (Στο εξής μέχρι το τέλος της απόδειξης , τις κλάσεις modulo D θα τις συμβολίζουμε για απλότητα χωρίς τον δείκτη D.) Η προς απόδειξη σχέση είναι η εξης : $[m]^{-1}H=\{g(x,y)(\mathrm{mod}D)|x,y\in Z,(g(x,y),D)=1\}$. Κατ΄ αρχήν ο εγκλεισμός ⊇ είναι προφανής γιατί αν x,y ακέραιοι και (g(x,y),D)=1 τότε η σχέση (T) μας δίνει $mg(x,y)\equiv(mx+B_1y)^2+ny^2(\mathrm{mod}D)$, οπότε επειδή η κύρια μορφή της D=-4n είναι η x^2+ny^2 , θα έχουμε ότι το mg(x,y) παρίσταται modulo D από την κύρια μορφή διακρίνουσας D και συνεπώς το [mg(x,y)] ανήκει στην H. Άρα $[m][g(x,y)]\in H$ και έτσι

$[g(x,y)] \in [m]^{-1}H$. Μένει λοιπόν ο εγκλεισμός $\subseteq$: Έστω $[u] \in [m]^{-1}H$, οπότε $[mu] \in H$

και έτσι $mu \equiv z^2 + nw^2 (modD)$ για κάποιους z,w ακέραιους αριθμούς με $(z^2+nw^2,D)=1$.

Επειδή (m,D)=1 έχουμε ότι η εξίσωση $mz^*+B_1 w \equiv z(modD)$ έχει λύση ως προς τον z*,

οπότε αν για ευκολία στους συμβολισμούς θέσουμε w*:=w θα έχουμε : $z^2 + nw^2 \equiv (mz^*+B_1w^*)^2 + nw^{*2} \ (modD) \rightarrow mu \equiv (mz^*+B_1w^*)^2 + nw^{*2} \ (modD)$ και έτσι από την πρόταση 1.2.1.15 έχουμε $mu \equiv g(z^*, w^*)(modD)$, οπότε επειδή (m,D)=1 , θα ισχύει :

$u \equiv g(z^*, w^*)(modD)$. Συνεπώς , $[u] = [g(z^*, w^*)]$ και έτσι , αφού $[u] \in [m]^{-1}H \subseteq$ kerχ θα έχουμε

$(u, D) = 1 \rightarrow (g(z^*, w^*), D) = 1 \rightarrow [g(z^*, w^*)] \in \{g(x,y)(modD) | x, y \in Z, (g(x,y), D) = 1\}$

και έτσι $[u] \in \{g(x,y)(modD) | x, y \in Z, (g(x,y), D) = 1\}$.

2η Περίπτωση : <u>D≡1(mod4)</u>

Η περίπτωση αυτή αποδεικνύεται όμοια με την πρώτη και έτσι παραλείπεται.

<u>ΠΑΡΑΤΗΡΗΣΕΙΣ:</u> **(ι) Αν D ακέραιος με D<0,D≡0,1(mod4) , H* coset της ομάδος H στον kerχ του θεωρήματος 1.2.3.8 και μια πρωταρχική τετραγωνική μορφή f παριστά modulo D ένα στοιχείο της H* , τότε παριστά modulo D και κάθε στοιχείο της H*. Μάλιστα ισχύει ότι H*={ f(x,y)modD|f(x,y)modD∈Z_D^* , x,y∈Z}.**

(Πράγματι , το σύνολο S={f(x,y)(modD)| f(x,y)(modD)∈Z_D^*, x,y∈Z} είναι -λόγω θεωρήματος 1.2.3.8 ένα coset της H στον kerχ και S∩H, οπότε θα έχουμε H*=S={f(x,y)(modD)| f(x,y)(modD)∈Z_D^*, x,y∈Z} .)

<u>1.2.3.10 ΟΡΙΣΜΟΣ</u> **Έστω D ακέραιος αριθμός με D<0,D≡0,1(mod4) και χ:Z_D^* →{±1} : χ($[p]_D$)= $\left(\frac{D}{p}\right)_2$ ο γνωστός ομομορφισμός. Έστω επίσης H≤kerχ , η υποομάδα των αναπαριστάμενων modulo D αριθμών της κύριας μορφής διακρίνουσας D. Γένος ενός τυχαίου coset H* της H στον kerχ θα ονομάζεται το σύνολο των θετικά ορισμένων πρωταρχικών μορφών διακρίνουσας D που παριστούν modulo D κάποιο και συνεπώς κάθε στοιχείο της H* (λόγω του θεωρήματος 1.2.3.8 (ιι)) , και θα συμβολίζεται gen(H*). Το γένος της H θα ονομάζεται κύριο γένος.**

1.2.3.11 ΠΑΡΑΤΗΡΗΣΕΙΣ : (ι) Ο ορισμός 1.2.3.10 δεν είναι κενός περιεχομένου. Πράγματι, αν H* είναι coset της H στον kerχ (με τους γνωστούς συμβολισμούς) τότε gen(H*)≠Ψ. Η τελευταία σχέση ισχύει γιατί αν [m] ανήκει στην H*, τότε επειδή $H^* \subseteq ker\chi \subseteq Z_D^*$, θα έχουμε κατ' αρχήν ότι (m,D)=1. Επίσης μπορούμε χωρίς περιορισμό της γενικότητας να υποθέσουμε ότι ο m είναι περιττός αριθμός. (Αν ο m είναι άρτιος τότε αναγκαστικά ο D είναι περιττός αφού (m,D)=1 και έτσι εργαζόμαστε παίρνοντας τον περιττό m+D ο οποίος ανήκει στην κλάση του m modulo D.)

Τώρα , επειδή [m]∈kerχ , θα έχουμε ότι $\left(\frac{D}{m}\right)_2 = 1$, και επομένως η πρόταση 1.2.1.20 μας δίνει ότι υπάρχει πρωταρχική θετικά ορισμένη μορφή f διακρίνουσας D , που να παριστά κανονικά τον m (Η πρόταση που χρησιμοποιούμε δίνει ύπαρξη πρωταρχικής μορφής διακρίνουσας D. Το γεγονός ότι αυτή είναι θετικά ορισμένη προκύπτει από το ότι D<0 , το ότι η μορφή παριστά τουλάχιστον ένα θετικό ακέραιο : τον m και την πρόταση 1.2.1.16 .) . Έτσι f∈gen(H*)

(ii) Αν (με τους γνωστούς συμβολισμούς) g∈gen(H*) τότε : gen(g)=gen(H*)

1.2.3.12 ΘΕΩΡΗΜΑ : Έστω D ακέραιος αριθμός με D<0 , D≡0,1(mod4) και χ,H ο ομομορφισμός και η ομάδα αντίστοιχα οπως και στον ορισμό 1.2.3.10 . Αν H* είναι ένα coset της H στον kerχ και p ένας περιττός πρώτος αριθμός με p∤D , τότε :

$[p]_D \in H^* \leftrightarrow$ " ο p παρίσταται modulo D από μια ανηγμένη μορφή διακρίνουσας D η οποία ανήκει στο γένος της H* "

ΑΠΟΔΕΙΞΗ

$(\rightarrow)$ Έστω $[p]_D \in H^*$ άρα αν $f \in gen(H^*)$ έχουμε ότι ο p παρίσταται κανονικά από την f και $H^*=\{f(x,y)(modD) \mid f(x,y)(modD) \in Z_D^*, x,y \in Z\}$. Τώρα η f είναι θετικά ορισμένη , πρωταρχική και κανονικά ισοδύναμη με ανηγμένη μορφή g διακρίνουσας D. Όπότε οι f,g παριστούν τους ίδιους ακεραίους άρα παριστούν και τους ακεραίους modulo D και συνεπώς ανήκουν στο ίδιο γένος. Άρα gen(g)=gen(f)=gen(H*) άρα η g ανήκει στο γένος της H* και προφανώς παριστά τον p.

(←) Έστω g ανηγμένη μορφή που παριστά modulo D τον p και ανήκει στο γένος της H*. Ισχύει τότε

$H^*=\{g(x,y)(modD)|\ g(x,y)(modD)\in Z_D^*\ x,y\in Z\}$ οπότε $[p]_D \in \{g(x,y)(modD)|\ g(x,y)(modD)\in Z_D^*,\ x,y\in Z\}=H^*$

1.2.3.13 ΠΟΡΙΣΜΑ : Αν n φυσικός αριθμός και p περιττός πρώτος με $p|n$, τότε τα ακόλουθα είναι ισοδύναμα

(I) Ο p παρίσταται από μορφή διακρίνουσας -4n που ανήκει στο κύριο γένος διακρίνουσας -4n

(ii) Υπάρχει ακέραιος α ώστε να συμβαίνει ένα εκ' των ακόλουθων δύο

- **$p\equiv\alpha^2(mod4n)$**
- **$p\equiv\alpha^2+n(mod4n)$**

ΑΠΟΔΕΙΞΗ

Η κύρια μορφή διακρίνουσας -4n είναι η x^2+ny^2 . Ανάλογα με το αν ο y είναι άρτιος η περιττός έχουμε
$x^2+ny^2\equiv x^2(mod4n)$ ή $x^2+ny^2\equiv x^2+n(mod4n)$. Τώρα , ο p παρίσταται από μορφή διακρίνουσας -4n που
ανήκει στο κύριο γένος διακρίνουσας -4n αν και μόνο αν ο p παρίσταται modulo 4n από την κύρια μορφή
διακρίνουσας -4n και συνεπώς αν και μόνο αν υπάρχουν α,β ακέραιοι αριθμοί με
$p\equiv\alpha^2+n\beta^2(mod4n)$, δηλαδή αν και μόνο αν $p\equiv\alpha^2$ ή $\alpha^2+n(mod4n)$

1.2.3.14 ΠΑΡΑΔΕΙΓΜΑ-ΕΦΑΡΜΟΓΗ : Χαρακτηρισμός των περιτών πρώτων αριθμών της μορφής x^2+5y^2

Είναι γνωστό ότι $p\equiv 1,3,7,9(\mathrm{mod}\,20)\leftrightarrow\left(\frac{-5}{p}\right)_2=1$. Όμως $\left(\frac{-5}{p}\right)_2=1$ αν και μόνο αν ο p παρίσταται από πρωταρχική μορφή διακρίνουσας -4 - 5<0 . Όμως επειδή αυτή η μορφή θα παριστά τον p>0 και θα έχει διακρίνουσα αρνητική θα είναι θετικά ορισμένη, οπότε κατά τα γνωστά ο p θα παρίσταται από μια εκ των h(-20) ανηγμένων θετικά ορισμένων τετραγωνικών μορφών . Έτσι σύμφωνα με τον πίνακα της εφαρμογής 1.2.2.8 έχουμε ότι $\left(\frac{-5}{p}\right)_2=1$ αν και μόνο αν υπάρχουν $x,y\in Z$ ώστε $p=x^2+5y^2$ ή $p=2x^2+2xy+3y^2$.

Όμως $\forall x,y\in Z$ ισχύει $x^2+5y^2\equiv 1,9(mod20)$ και $2x^2+2xy+3y^2\equiv 3,7(mod20)$. (Εδώ $\ker\chi=\{[1],[3],[7],[9]\}$ και
σύμφωνα με τους συμβολισμούς του 1.2.3.8 θεωρήματος $H=\{[1],[9]\}<\ker\chi$, και το $\{[3],[7]\}$ είναι ένα coset της H στον $\ker\chi$.) Άρα

$p\equiv 1,9(mod20)\leftrightarrow$ " υπάρχουν $x,y\in Z$ ώστε $p=x^2+5y^2$ "

και $p\equiv 3,7(mod20)\leftrightarrow$ " υπάρχουν $x,y\in Z$ ώστε $p=2x^2+2xy+3y^2$ ".

1.2.3.15 ΣΧΟΛΙΑ : Στην περίπτωση αυτή είχαμε δύο γένη , τα οποία αποτελούνταν από μία κλάση το καθένα.

Γενικά , αν για τον ακέραιο D με $D<0, D\equiv 0,1 \pmod 4$ έχουμε γένη στην C(D) αποτελούμενα από μία κλάση (κάτι που δεν ισχύει πάντα), τότε μπορούμε με την παραπάνω μεθοδολογία να χαρακτηρίσουμε τους πρώτους αριθμούς που παρίστανται από την κύρια μορφή διακρίνουσας D. Στον παρακάτω πίνακα αναφέρουμε μερικά $n\in N$ (ομαδοποιημένα σύμφωνα με τον αριθμό κλάσεων h(-4n)) για τα οποία η ομάδα C(D) έχει μια κλάση ανά γένος.

$h(-4n)$	n με μία κλάση ανά γένος
1	1,2,3,4,7
2	5,6,8,9,10,12,13,15,16,18,22,25,28,37,38
4	21,24,30,33,40,42,45,48,57,60,70,72,78,85,88,93,102,112,130,133,177,190,232,253
8	105,120,165,168,210,240,273,280,312,330,345,357,385,408,462,520,760
16	840,1320,1365,1848

1.2.4 ΣΥΝΘΕΣΗ ΚΛΑΣΕΩΝ ΚΑΙ ΟΜΑΔΑ ΚΛΑΣΕΩΝ - ΑΠΟΤΕΛΕΣΜΑΤΑ

ΑΠΟ ΘΕΩΡΙΑ ΓΕΝΟΥΣ-

1.2.4.1 ΟΡΙΣΜΟΣ : Σύνθεση (composition) δύο πρωταρχικών θετικά ορισμένων μορφών διακρίνουσας D θα λέγεται κάθε πρωταρχική θετικά ορισμένη μορφή F με την ιδιότητα : $F(B_1(x,y;z,w),B_2(x,y;z,w)) = f(x,y)\cdot g(z,w)$ για $B_i(x,y;z,w)=a_ixz+b_ixw+c_iyz+d_iyw$ όπου $i=0,1$ και $a_i,b_i,c_i,d_i \in Z$.

1.2.4.2 ΟΡΙΣΜΟΣ : Επειδή για $D\neq 0$ με τους συμβολισμούς του προηγούμενου ορισμού έχουμε ότι $a_1b_2-a_2b_1=\pm f(1,0)$ και ότι $a_1c_2-a_2c_1=\pm g(1,0)$ (βλ. [Gauss] §235) μια σύνθεση θα λέγεται ευθεία σύνθεση (direct composition) των f,g αν $a_1b_2-a_2b_1=f(1,0)$ και $a_1c_2-a_2c_1=g(1,0)$

1.2.4.3 ΠΡΟΤΑΣΗ : Αν οι μορφές f,g είναι κανονικά ισοδύναμες με τις f_1,g_1 αντίστοιχα , τότε κάθε σύνθεση (ευθεία σύνθεση) των f,g είναι κανονικά ισοδύναμη με οποιαδήποτε σύνθεση (ευθεία σύνθεση) των f_1,g_1. Επίσης για $D<0, D\equiv 0,1 \pmod 4$ ισχύει ότι το σύνολο των κλάσεων (σύμφωνα με την κανονική ισοδυναμία) των θετικά ορισμένων πρωταρχικών μορφών διακρίνουσας D γίνεται αβελιανή ομάδα με πράξη την σύνθεση.

ΑΠΟΔΕΙΞΗ

Η πρόταση μπορεί να ακοδειχτεί με απευθείας υπολογισμό. Για λεπτομέρειες παραπέμπουμε στο βιβλίο του Gauss : [Gauss] §236,245,249.

1.2.4.4 ΠΡΟΤΑΣΗ : (1) Αν $\alpha_1,\alpha_2,\ldots,\alpha_n,\beta_1,\beta_2,\ldots,\beta_v,m$ ακέραιοι αριθμοί με $ΜΚΔ(\alpha_1,\alpha_2,\ldots,\alpha_n,m)=1$ τότε το σύστημα $\{\alpha_i x\equiv\beta_i \pmod m\}_{i=1,2\ldots,n}$ έχει λύση αν και μόνο αν $\forall i,j$ $\alpha_i\beta_j\equiv\alpha_j\beta_i \pmod m$.

Μάλιστα , άν υπάρχει λύση για το σύστημα τότε είναι μοναδική mod m.

(2) Αν $f(x,y)=ax^2+bxy+cy^2$, $g(x,y)=a_1x^2+b_1xy+c_1y^2$ είναι τετραγωνικές μορφές διακρίνουσας D , τότε

a) $\frac{b+b_1}{2}\in Z$

b) Αν $ΜΚΔ(a,a_1,\frac{b+b_1}{2})=1$, τότε υπάρχει ακέραιος B μοναδικός $\bmod 2aa_1$

$$\textbf{ώστε}\ \begin{cases} \mathbf{B \equiv b(mod 2a)} \\ \mathbf{B \equiv b_1(mod 2a_1)} \\ \mathbf{B^2 \equiv D(mod 4aa_1)} \end{cases} \qquad \textbf{(Σ 1.2.4.4)}$$

ΑΠΟΔΕΙΞΗ

(1) ($\rightarrow$) Αν χ_o λύση του $\{\alpha_i x \equiv \beta_i (mod m)\}_{i=1,2,\ldots,n}$ τότε $\forall$ i $\alpha_i\chi_o \equiv \beta_i (mod m)$ οπότε $\forall i,j$ ισχύει

$\alpha_i\beta_j \equiv \alpha_i\alpha_j\chi_o (mod m) \rightarrow \alpha_i\beta_j \equiv \beta_i\alpha_j (mod m)$

($\leftarrow$) ¨Εστω ότι $\alpha_i\beta_j \equiv \beta_i\alpha_j (mod m)$ $\forall i,j$. Επειδή ΜΚΔ$(\alpha_1,\alpha_2,\ldots,\alpha_n,m)=1$, θα υπάρχουν k_i,k $i=1,2,\ldots,n$ ώστε $km+k_1\alpha_1+\ldots+k_n\alpha_n=1$ και συνεπώς

$$(\sum_{j=1}^{n} k_j\beta_j)\alpha_i \equiv (\sum_{j=1}^{n} k_j\beta_j\alpha_i) \equiv (\sum_{j=1}^{n} k_j\beta_i\alpha_j) \equiv (\sum_{j=1}^{n} k_j\alpha_j)\beta_i \equiv \beta_i (mod m)\ \forall i\ ,$$

οπότε λύση του

συστήματος $\{\alpha_i x \equiv \beta_i (mod m)\}_{i=1,2,\ldots,n}$ είναι η $\sum_{j=1}^{n} k_j\beta_j$.Τώρα αν x,y λύσεις του συστήματος

$$\text{τότε } (\sum_{j=1}^{n} k_j\alpha_j) \equiv 1 (mod m) \rightarrow [\sum_{j=1}^{n} k_j(\alpha_j x)] \equiv x (mod m) \rightarrow$$

$$[\sum_{j=1}^{n} (k_j\beta_j)] \equiv x (mod m)\ .\ \text{¨Ομοια}$$

$$(\sum_{j=1}^{n} k_j\beta_j) \equiv y (mod m) \text{ οπότε και } x \equiv y (mod m).$$

(2) a) $D = b^2-4ac = b_1^2-4a_1c_1 \rightarrow b^2 \equiv b_1^2 (mod 4) \rightarrow b \equiv b_1 (mod 2)$.

b) Προκύπει εύκολα χρησιμοποιώντας το (1) και το γεγονός ότι ισχύουν οι ακόλουθες ισοδυναμίες :

$$\left\{\begin{matrix} B \equiv b(mod 2a) \\ B \equiv b_1(mod 2a_1) \\ B^2 \equiv D(mod 4aa_1) \end{matrix}\right\} \leftrightarrow \left\{\begin{matrix} Ba_1 \equiv ba_1(mod 2aa_1) \\ Ba \equiv b_1a(mod 2aa_1) \\ (b+b_1)B \equiv bb_1+D(mod 4aa_1) \end{matrix}\right\} \leftrightarrow \left\{\begin{matrix} Ba_1 \equiv ba_1(mod 2aa_1) \\ Ba \equiv b_1a(mod 2aa_1) \\ (\frac{b+b_1}{2})B \equiv \frac{bb_1+D}{2}(mod 2aa_1) \end{matrix}\right\}$$

<u>1.2.4.5 ΟΡΙΣΜΟΣ</u> : Αν $f(x,y)=ax^2+bxy+cy^2$, $g(x,y)=a_1x^2+b_1xy+c_1y^2$ τετραγωνικές μορφές πρωταρχικές και θετικά ορισμένες διακρίνουσας $D<0$ ώστε ΜΚΔ$(a,a_1,\frac{b+b_1}{2})=1$, τότε κάθε τετραγωνική μορφή $F(x,y)$ με $F(x,y)=aa_1x^2+Bxy+(\frac{B^2-D}{4aa_1})y^2$, όπου B είναι μια λύση του συστήματος Σ 1.2.4.4 της προηγούμενης πρότασης λέγεται Dirichlet σύνθεση των μορφών f και g και συμβολίζουμε F=fog.

<u>1.2.4.6 ΠΡΟΤΑΣΗ</u> : Αν f και g είναι πρωταρχικές θετικά ορισμένες μορφές διακρίνουσας D<0 και F μια

Dirichlet σύνθεση τους τότε η F είναι πρωταρχική θετικά ορισμένη μορφή διακρίνουσας

D και επίσης η F είναι ευθεία σύνθεση των f,g.

<u>ΑΠΟΔΕΙΞΗ</u>

.

Θα δείξουμε κατ' αρχήν ότι η F είναι ευθεία σύνθεση των f,g .Πράγματι, ακολουθώντας τους συμβολισμούς

του προηγούμενου ορισμού , θέτουμε $C=\frac{B^2-D}{4aa_1}$, οπότε $F=aa_1x^2+Bxy+C^2$. Τώρα , η μορφή $f^*(x,y)=$

$ax^2+Bxy+Ca_1y^2$ είναι κανονικά ισοδύναμη με την f και η μορφή $g^*(x,y)=a_1x^2+Bxy+Cay^2$ είναι κανονικα

ισοδύναμη με την g. Πράγματι :

Το σύστημα Σ 1.2.3.5 δίνει ότι $B\equiv b(\mathrm{mod}2a)$. Έτσι γράφοντας $B=2ak+b$,$k\in Z$

παίρνουμε $f^*(x,y)=ax^2+(2ak+b)xy+(ak^2+kb+c)y^2$ και συνεπώς για $\begin{pmatrix}u\\v\end{pmatrix}=\begin{pmatrix}1&k\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$

θα πάρουμε $f(u,v)=f^*(x,y)$. Οι f,f^* λοιπόν είναι κανονικά ισοδύναμες. Εντελώς

όμοια , γράφοντας $B=2a_1\lambda+b_1$,$\lambda\in Z$ και θεωρώντας τον μετασχηματισμό

$\begin{pmatrix}u\\v\end{pmatrix}=\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$, έχουμε $g(u,v)=g^*(x,y)$, οπότε οι g,g^* είναι ισοδύναμες.

Αρκεί λοιπόν να δειχτεί (λόγω πρότασης 1.2.4.3) ότι οι f*,g* έχουν ευθεία σύνθεση την F. Πράγματι, αν

θέσουμε $B_1(x,y;z,w)=xz-Czw$, $B_2(x,y;z,w)=axw+a_1yz+Byw$, τότε $f^*(x,y)-g^*(z,w)=F(B_1(x,y;z,w),B_2(x,y;z,w))$.

Συνεπώς η F είναι σύνθεση των f*,g*.Το ότι η σύνθεση είναι ευθεία προκύπτει με απ'ευθειας υπολογισμό.

Μένει τώρα να δείξουμε ότι η F είναι πρωταρχική θετικά ορισμένη μορφή διακρίνουσας D.

Επειδή οι f,g είναι θετικά ορισμένες με αρνητική διακρίνουσα , θα έχουμε $a,a_1>0\rightarrow a-a_1>0$. Επίσης ,

με απευθείας υπολογισμό μπορεί να δειχτεί ότι $D_f=D<0$ και συνεπώς η F είναι θετικά ορισμένη.

Αν τώρα p πρώτος αριθμός που διαιρεί τους συντελεστές της F τότε επειδή $f^*(x,y)-g^*(z,w)=$

$= F(B_1(x,y;z,w),B_2(x,y;z,w))$.και οι f,g κανονικά ισοδύναμες με τις f*,g* αντίστοιχα, θα έχουμε ότι

ο p διαιρεί κάθε αριθμό της μορφής $f(x,y)-g(z,w)$, $x,y,z,w\in Z$ επειδή όμως $c=f(0,1)$, $a=f(1,0)$,

$a+b+c=f(1,1)$, $c_1=g(0,1)$, $a_1=g(1,0)$, $a_1+b_1+c_1=g(1,1)$, θα έχουμε ότι ο p διαιρεί κάθε γινόμενο κ-λ όπου

κ∈ {a,c,a+b+c} και λ∈ $\{a_1,c_1,a_1+b_1+c_1\}$. Εξάλλου ΜΚΔ(a,b,c)=1 (διότι η f είναι πρωταρχική) οπότε

ΜΚΔ(a,c,a+b+c)=1. Όμοια ΜΚΔ($a_1,c_1,a_1+b_1+c_1$)=1. Άρα υπάρχει στοιχείο του {a,c,a+b+c} που δεν

διαιρείται από το p και στοιχείο του $\{a_1,c_1,a_1+b_1+c_1\}$ που δεν διαιρείται από το p , πράγμα άτοπο από

τα παραπάνω.

<u>1.2.4.7 ΠΟΡΙΣΜΑ</u> : Η σύνθεση Dirichlet είναι ειδική περίπτωση της ευθείας σύνθεσης

<u>1.2.4.8 ΘΕΩΡΗΜΑ</u> : Έστω D ακέραιος αριθμός με D≡0,1(modm) και D<0. Το σύνολο των κλάσεων C(D)

εφοδιασμένο με την σύνθεση Dirichlet γίνεται αβελιανή ομάδα με μοναδιαίο στοιχείο

την κλάση που περιέχει την κύρια μορφή διακρίνουσας D. Επίσης , για κάθε κλάση

$[ax^2+bxy+cy^2]\in C(D)$ ισχύει $[ax^2+bxy+cy^2]^{-1}=[ax^2-bxy+cy^2]$.

<u>ΑΠΟΔΕΙΞΗ</u>

Έστω $f(x,y)=ax^2+bxy+cy^2$, $g(x,y)=a_1x^2+b_1xy+c_1y^2$ δύο θετικά ορισμένες πρωταρχικές μορφές διακρίνουσας

D. Επειδή η g παριστά αριθμούς πρώτους προς το a (βλ. Πρόταση 1.2.3.7), μπορούμε λόγω της

πρότασης 1.2.1.9 να υποθέσουμε ότι ΜΚΔ(a,a_1)=1 και συνεπώς

ΜΚΔ($a,a_1,\frac{b+b_1}{2}$)=1. Ορίζεται λοιπόν

η Dirichlet σύνθεση F των f,g .Ορίζουμε τώρα την πράξη [f(x,y)]o[g{x,y)]=[F(x,y)] μεταξύ των κλάσεων

[f(x,y)] και [g(x,y)] .Η πράξη αυτή είναι καλά ορισμένη (Πράγματι, από την πρόταση 1.2.4.6 η F είναι

πρωταρχική θετικά ορισμένη διακρίνουσας D και το ότι για διαφορετικές συνθέσεις Dirichlet F,F'

των f,g ισχύει [F]=[F'] , καθώς και το ότι [f_1(x,y)]o[g_1(x,y)]=[f(x,y)]o[g(x,y)] όταν [f(x,y)]=[f_1(x,y)] ,[g(x,y)]=[g_1(x,y)] προκύπτουν με απ'ευθείας υπολογισμό.).Έστω τώρα f_o η κύρια

μορφή διακρίνουσας D. Από τον ορισμο της f_o μπορεί κανείς αμέσως να δει ότι η συνθήκη του

ΜΚΔ που χρειάζεται για να υπάρχει η σύνθεση Dirichlet της f_o με οποιαδήποτε μορφή της F_{pd}(D) ,

ικανοποιείται αυτόματα. Τώρα αν f∈F_{pd}(D) με $f(x,y)= ax^2+bxy+cy^2$, τότε το B=b ικανοποιεί το σύστημα

Σ 1.2.4.4 της πρότασης 1.2.4.4 για την περίπτωση των f και f_o

Πράγματι , στην περίπτωση των f , f_o το σύστημα Σ 1.2.4.4

γίνεται $\left\{\begin{array}{c} B\equiv b(\mathrm{mod}2a) \\ B\equiv(\mathrm{mod}2) \\ B^2\equiv D(\mathrm{mod}4a)\end{array}\right\}$, αν $D\equiv 0(\mathrm{mod}4)$ και γίνεται

$\left\{\begin{array}{c} B\equiv b(\mathrm{mod}2a) \\ B\equiv 1(\mathrm{mod}2) \\ B^2\equiv D(\mathrm{mod}4a)\end{array}\right\}$

αν $D\equiv 1(\mathrm{mod}4)$, οπότε γράφοντας $D=b^2-4ac$ και παρατηρώντας ότι

"$b\equiv 1(\mathrm{mod}2)\leftrightarrow D\equiv 1(\mathrm{mod}4)$" , είναι εύκολο να δούμε ότι η $B=b$ είναι λύση

του συστήματος σε κάθε περίπτωση.

Η σύνθεση Dirichlet F των f,f_o είναι λοιπόν σύμφωνα με τον ορισμό 1.2.4.5 η $F(x,y)=f(x,y)$ και συνεπώς

το $[f_o]$ είναι το ουδέτερο στοιχείο του C(D) με πράξη την Dirichlet σύνθεση.Τέλος για $f\in F_{pd}(D)$ με

$f(x,y)=ax^2+bxy+cy^2$ θέτουμε $f^*(x,y)=ax^2-bxy+cy^2$ και θεωρούμε την μορφή $g(x,y)=cx^2+bxy+ay^2$

η οποία μέσω του πίνακα $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\in sl(2,Z)$ είναι κανονικά ισοδύναμη με την f^*.Έχουμε

$ΜΚΔ(a,c,\frac{b+b}{2}) = MKD(a,c,b)=1$, οπότε η σύνθεση Dirichlet F των f,g ορίζεται και το σύστημα

Σ 1.2.4.4 για τις f,g γίνεται $\left\{\begin{array}{c} B\equiv b(\mathrm{mod}2a) \\ B\equiv b(\mathrm{mod}2c) \\ B^2\equiv D(\mathrm{mod}4ac)\end{array}\right\}$. Το σύστημα αυτό έχει προφανώς λύση το b και έτσι

θα έχουμε $F(x,y)=acx^2+bxy+y^2$ Θα δείξουμε ότι η F είναι κανονικά ισοδύναμη με την κύρια μορφή

διακρίνουσας D.

Πράγματι , όπως είπαμε και πιό πάνω , επειδή $D=b^2-4ac$ θα ισχύει ότι

"$b\equiv 1(\mathrm{mod}2)\leftrightarrow D\equiv 1(\mathrm{mod}4)$" έτσι θεωρώντας τον πίνακα A της sl(2,Z)

ο οποίος ορίζεται να είναι

$\begin{pmatrix}-k & -1\\ 1 & 0\end{pmatrix}$, αν $D\equiv 0(\mathrm{mod}4)$ με $b=2k$, $k\in Z$

$\begin{pmatrix}k & -1\\ 1 & 0\end{pmatrix}$, αν $D\equiv 1(\mathrm{mod}4)$ με $b=2k+1$, $k\in Z$

και θέτοντας $\begin{pmatrix}u\\ v\end{pmatrix}=A\begin{pmatrix}x\\ y\end{pmatrix}$, θα πάρουμε $f_o(u,v)=F(x,y)$ (όπου f_o είναι

η κύρια μορφή διακρίνουσας D).

Συνεπώς $[f_o]=[F]=[f]o[g]=[f]o[f^*]$, δηλαδή $[f]^{-1}=[f^*]$.

<u>1.2.4.9 ΟΡΙΣΜΟΣ</u> : (I) Για κάθε μορφή $(ax^2+bxy+cy^2)\in F_{pd}(D)$ η μορφή $(ax^2-bxy+cy^2)\in F_{pd}(D)$ θα λέγεται

αντίθετη (opposite) της $ax^2+bxy+cy^2$ και συμβολίζεται f— (Από τα προηγούμενα

έχουμε ότι $[f—(x,y)]=[f(x,y)]^{-1}$)

(ii) Αν $f(x,y)\in F_{pd}(D)$ τότε η Langranzian-κλάση (Langranzian-class) της f ορίζεται να είναι

το σύνολο $[f(x,y)]U[f—(x,y)]$

<u>1.2.4.10 ΠΡΟΤΑΣΗ</u> : Αν D είναι ακέραιος με $D<0$, $D\equiv 0,1(mod4)$ και $f(x,y)= ax^2+bxy+cy^2$ είναι ανηγμένη μορφή

διακρίνουσας D (οπότε εξ'ορισμού έχουμε $|b|\le a\le c$). Ισχύει ότι η $[f(x,y)]$ έχει τάξη 2 στην

C(D) για $a=|b|$ ή $a=c$, ενώ για $|b|<a<c$ η $[f(x,y)]$ έχει τάξη 2 αν και μόνο αν $b=0$.

<u>ΑΠΟΔΕΙΞΗ</u>

Επειδή $[f]^{-1}=[f—]$, θα έχουμε ότι η $[f]$ έχει τάξη 2 στην C(D) αν και μόνο αν $f = f—$. Αν $|b|<a<c$, τότε η f—

είναι επίσης ανηγμένη (βλ. ορισμό 1.2.2.1) , οπότε " $f = f— \leftrightarrow b=0$ "(λόγω θεωρήματος 1.2.2.3). Άν τώρα $a=|b|$

τότε εξ' ορισμού των ανηγμένων μορφών θα έχουμε $b>0$ και έτσι $a=b$ οπότε θέτοντας $\begin{pmatrix}u\\v\end{pmatrix}=\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$, έχουμε $f(x,y)=f—(u,v)$. Αν πάλι $a=c$, τότε θέτοντας $\begin{pmatrix}u\\v\end{pmatrix}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$, έχουμε $f(x,y)=f—(u,v)$.

Έτσι λοιπόν για $a=|b|$ ή $a=c$ έχουμε πάντα $[f] = [f—]$.

<u>1.2.4.11 ΕΦΑΡΜΟΓΗ</u> : 'Εστω D=-164. Χρησιμοποιώντας τον πίνακα της εφαρμογής 1.2.2.8 βλέπουμε ότι

$h(D)=h(-164)=8$, και μόνο μια κλάση έχει τάξη ≤ 2 , οπότε η C(-164) είναι αβελιανή

τάξεως 8 με μόνο ένα στοιχείο τάξεως 2 και συνεπώς $C(-164)\cong Z_8$

Για λόγους πληρότητας αναφέρουμε και τα ακόλουθα από την θεωρία γένους:

<u>1.2.4.12 ΟΡΙΣΜΟΣ</u> : Έστω $D\in Z$ με $D<0, D\equiv 0,1(mod4)$. Έστω επίσης r το πλήθος των διαφορετικών περιττών

πρώτων διαιρετών του D. Ορίζουμε τον αριθμό μ_D ως εξής :

- **Για $D\equiv 1(mod4)$ ορίζουμε $\mu_D=r$**
- **Για $D\equiv 0(mod4)$ με $D=-4n$, ορίζουμε**
  - **$\mu_D=r$ αν $n\equiv 3,7(mod8)$**
  - **$\mu_D=r+1$ αν $n\equiv 1,2,4,5,6(mod8)$**
  - **$\mu_D=r+2$ αν $n\equiv 0(mod8)$**

<u>1.2.4.13 ΠΡΟΤΑΣΗ</u>: Έστω $D \in Z$ με $D<0, D \equiv 0,1 \pmod 4$. Ισχύουν τα ακόλουθα :

- **Το πλήθος των στοιχείων με τάξη≤2 στην ομάδα κλάσεων C(D) είναι $2^{\mu_D - 1}$**
  (όπου μ_D είναι ο αριθμός που ορίστηκε πιο πάνω)
- **Υπάρχουν ακριβώς $2^{\mu_D - 1}$ γένη μορφών διακρίνουσας D και το κύριο**
  γένος είναι ακριβώς το $C(D)^2$

(Λεπτομέρειες για την απόδειξη μπορούν να βρεθούν στο βιβλίο του Cox :

[COX] θεωρ. 3.15 σελ. 54)

§ 3 ΚΥΒΙΚΟ ΚΑΙ ΔΙΤΕΤΡΑΓΩΝΙΚΟ ΣΥΜΒΟΛΟ ΤΟΥ LEGENDRE ΚΑΙ ΕΦΑΡΜΟΓΕΣ

1.3.1 ΓΕΝΙΚΑ ΓΙΑ ΤΟ Z[ω]

1.3.1.1 ΟΡΙΣΜΟΙ-ΥΠΕΝΘΥΜΙΣΕΙΣ : Σε όλη την § 3 το ω θα συμβολίζει την 3η ρίζα της μονάδος : $e^{\frac{2\pi i}{3}}$ (όπου $i^2=1$). Επίσης θα συμβολίζουμε με R το Z[ω] , και με σ(-) την μιγαδική συζυγία.. Όπως είναι γνωστό ο R είναι ευκλείδιος δακτύλιος και συνεπώς δακτύλιος κυρίων ιδεωδών. Τα ανάγωγα στοιχεία του R είναι και πρώτα.Για κάθε a του R ισχύει Ass(a)= $\{\pm a,\pm\omega a,\pm\omega^2 a\}$ και επίσης για (x+yω) στοιχείο του R με $x,y\in Z$, η νόρμα του (x+yω) είναι $N(x+y\omega)=x^2-xy+y^2$.(Προφανώς αν N(x+yω) είναι πρώτος αριθμός τότε το (x+yω) είναι πρώτο στοιχείο του R.). Αναφέρουμε τώρα κάποια αποτελέσματα από την θεωρία αριθμών και τον νόμο ανάλυσης στο Q(ω)

- **Αν p πρώτος αριθμός του Z τότε**
  - **Αν p=3 , τότε $p=-\omega^2(1-\omega)^2$ και (1-ω) είναι πρώτος του R**
  - **Αν $p\equiv 1(\mathrm{mod}3)$, τότε υπάρχει πρώτος π του R ώστε και ο σ(π) να είναι πρώτος του R μη συνεταιρικός του π και $p=\pi\cdot\sigma(\pi)$.**
  - **Αν $p\equiv 2(\mathrm{mod}3)$, τότε ο p είναι πρώτο στοιχείο του R.**
- **Το σύνολο των πρώτων στοιχείων του R είναι η ξένη ένωση των συνόλων : Ass($\{\pi\in R \mid N(\pi)\in P$ και $N(\pi)\equiv 1(\mathrm{mod}3)\}$, Ass(1-ω) , Ass($\{p\in P \mid p\equiv 2(\mathrm{mod}3)\}$).**
- **Για κάθε πρώτο στοιχείο του R : π ισχύουν τα ακόλουθα :**
  - **(1) Το $\frac{R}{\pi R}$ είναι σώμα με πλήθος στοιχείων N(π). Επίσης $N(\pi)\in\{p,p^2\}$ για κάποιο $p\in P$ και μάλιστα**
    - **αν $N(\pi)=p^2$ τότε $\pi=p\equiv 2(\mathrm{mod}3$ και η προβολή $Z_p\to\frac{R}{\pi R}$ είναι μονομορφισμός**
    - **αν N(π)=p , τότε $p\equiv 1(\mathrm{mod}3)$ ή p=3 και η προβολή $Z_p\to\frac{R}{\pi R}$ είναι ισομορφισμός.**
  - **(2) Αν $a\in R-\{0\}$ με $\pi\nmid a$, τότε $a^{N(\pi)-1}\equiv 1(\mathrm{mod}\pi)$ στο R**
  - **(3) $\pi\nmid 3\leftrightarrow\pi\notin Ass(1-\omega)\leftrightarrow N(\pi)\neq 3$**
  - **(4) Αν $\pi\nmid 3$ τότε :**
    - **$3|_{N(\pi)-1}$**
    - **τα $1(\mathrm{mod}\pi)$, $\omega(\mathrm{mod}\pi)$, $\omega^2(\mathrm{mod}\pi)$, είναι διαφορετικά στοιχεία του δακτυλίου $\frac{R}{\pi R}$.**

Για λεπτομέρειες παραπέμπουμε στο βιβλίο του Cox : [Cox] §4 σελ. 75

1.3.2 ΚΥΒΙΚΟ ΣΥΜΒΟΛΟ ΤΟΥ LEGENDRE ΚΑΙ ΒΑΣΙΚΕΣ ΙΔΙΟΤΗΤΕΣ ΤΟΥ

1.3.2.1 ΣΧΟΛΙΑ : **Αν $a\in R$ και π πρώτο στοιχείο του R με $\pi \nmid a$, $\pi \nmid 3$, τότε $\frac{N(\pi)-1}{3}\in Z$ και το $a^{\frac{N(\pi)-1}{3}}$ είναι λύση της εξίσωσης $x^3\equiv 1(\mathrm{mod}\pi)$. Επειδή τώρα τα $1(\mathrm{mod}\pi)$, $\omega(\mathrm{mod}\pi)$, $\omega^2(\mathrm{mod}\pi)$ είναι λύσεις της $x^3\equiv 1(\mathrm{mod}\pi)$ και διαφορετικές $\mathrm{mod}\pi$, θα έχουμε ότι το $a^{\frac{N(\pi)-1}{3}}$ είναι ισότιμο $\mathrm{mod}\pi$ με ένα μοναδικό από τα $1(\mathrm{mod}\pi)$, $\omega(\mathrm{mod}\pi)$, $\omega^2(\mathrm{mod}\pi)$**

1.3.2.2 ΟΡΙΣΜΟΣ : **Έστω π πρώτο στοιχείο του R με $\pi \nmid 3$. Ορίζουμε την συνάρτηση $\left(\frac{\cdot}{\pi}\right)_3 : Z[\omega] \to \{1,\omega,\omega^2\}\cup\{0\}$ ως εξής : Για $a\in Z[\omega]$ το $\left(\frac{a}{\pi}\right)_3$ είναι**

- **αν $\pi \mid a$, το 0**
- **αν $\pi \nmid a$,το μοναδικό στοιχείο του $\{1,\omega,\omega^2\}$ που είναι ισότιμο με $a^{\frac{N(\pi)-1}{3}}$ modulo π.**

Το $\left(\frac{\cdot}{\pi}\right)_3$ ονομάζεται κυβικός χαρακτήρας υπολοίπων ή κυβικό σύμβολο του Legendre.

1.3.2.3 ΠΡΟΤΑΣΗ : **(Ιδιότητες κυβικού συμβόλου Legendre) Έστω π πρώτο στοιχείο του R με $\pi \nmid 3$ και έστω $a,b\in R$ και $\varepsilon\in E(R)$. Ισχύουν τα παρακάτω :**

1. $\left(\frac{ab}{\pi}\right)_3=\left(\frac{a}{\pi}\right)_3\left(\frac{b}{\pi}\right)_3$
2. $\left(\frac{a}{\varepsilon\pi}\right)_3=\left(\frac{a}{\pi}\right)_3$
3. Αν $a\equiv b(\mathrm{mod}\pi)$ τότε $\left(\frac{a}{\pi}\right)_3=\left(\frac{b}{\pi}\right)_3$
4. $\left(\frac{a}{\pi}\right)_3^4=\left(\frac{a}{\pi}\right)_3$
5. Αν $\pi \nmid a$ τότε $\left(\frac{a}{\pi}\right)_3^3=1$
6. $\left(\frac{-1}{\pi}\right)_3=1$
7. $\overline{\left(\frac{a}{\pi}\right)_3}=\left(\frac{a}{\pi}\right)_3^2=\left(\frac{a^2}{\pi}\right)_3=\left(\frac{\bar{a}}{\bar{\pi}}\right)_3$
8. Αν $\pi=p$ με $p\in P$ και $p \nmid a$ τότε $\left(\frac{a}{\pi}\right)_3=\left(\frac{a}{p}\right)_3=1$
9. $\left(\frac{\omega}{\pi}\right)_3=\omega^{\left(\frac{N(\pi)-1}{3}\right)}$

(Για λεπτομέρειες παραπέμπουμε στο βιβλίο των Ireland και Rosen : [Ir.Ro] πρότ. 9.33 σελ. 112)

<u>1.3.2.4 ΠΑΡΑΤΗΡΗΣΕΙΣ</u> : Αν π πρώτο στοιχείο του R με π ∤ 3 , τότε το σύμβολο του Legendre $\left(\frac{\cdot}{\pi}\right)_3$ περιορισμένο στο $\left(\frac{R}{\pi R}\right)^*$ επάγει ομομορφισμό ομάδων $\left(\frac{R}{\pi R}\right)^* \to \{1,\omega,\omega^2\}$.

Επίσης η ($\left(\frac{R}{\pi R}\right)^*$, -) είναι κυκλική ομάδα ως πολλαπλασιαστική ομάδα σώματος.

<u>1.3.2.5 ΠΡΟΤΑΣΗ</u> : Αν π πρώτο στοιχείο του R με π ∤ 3 και a∈R με π ∤ a , τότε τα ακόλουθα είναι ισοδύναμα :

I. $\left(\frac{a}{\pi}\right)_3 = 1$

II. $a^{\frac{N(\pi)-1}{3}} \equiv 1 (\mathrm{mod}\pi)$

III. $x^3 \equiv a (\mathrm{mod}\pi)$ **είναι επιλύσιμη στο R**

<u>ΑΠΟΔΕΙΞΗ</u>

(<u>I ↔ II</u>) Προφανές από τους ορισμούς και την μοναδικότητα του κυβικού συμβόλου του Legendre

(<u>II → III</u>) Παίρνουμε u+πR γεννήτορα της κυκλικής ομάδος ($\left(\frac{R}{\pi R}\right)^*$, ·) και γράφουμε $a \equiv u^A (\mathrm{mod}\pi R)$, οπότε επειδή $a^{\frac{N(\pi)-1}{3}} \equiv 1 (\mathrm{mod}\pi)$ μπορούμε εύκολα να δούμε ότι 3 | A και ότι το $u^{A/3}$ είναι λύση της $x^3 \equiv a (\mathrm{mod}\pi)$.

(<u>III → II</u>) Αν x_o είναι λύση της $x^3 \equiv a (\mathrm{mod}\pi)$ τότε αφού π ∤ a θα έχουμε και π ∤ x_o οπότε $1 \equiv (x_o^3)^{\frac{N(\pi)-1}{3}} \equiv a^{\frac{N(\pi)-1}{3}} (\mathrm{mod}\pi)$.

<u>1.3.2.6 ΠΡΟΤΑΣΗ</u> : Αν p∈P* και a∈Z , τότε :

- **Αν p=3 ή p≡2(mod3) , τότε $x^3 \equiv a (\mathrm{mod}p)$ επιλύσιμη στο Z και μάλιστα η λύση είναι μονοσήμαντη modulo p.**
- **Αν p≡1(mod3) , τότε :**
  - **Για p|a , η $x^3 \equiv a (\mathrm{mod}p)$ είναι επιλύσιμη στο Z**

- **Για $p \nmid a$, η $x^3 \equiv a(\mathrm{mod}p)$ είναι επιλύσιμη στο Z αν και μόνο αν $\left(\frac{a}{\pi}\right)_3 = 1$ (όπου $p=\pi \cdot \bar{\pi}$ η ανάλυση του p σε πρώτα στοιχεία του R).**

ΑΠΟΔΕΙΞΗ

Στην περίπτωση που $p \not\equiv 1(\mathrm{mod}3)$ είναι απλή άσκηση άλγεβρας να δειχτεί ότι η απεικόνιση $Z_p^* \to Z_p^*$ με $u \to u^3$ για κάθε $u \in Z_p^*$ είναι ισομορφισμός. Μένει λοιπόν η περίπτωση $p \equiv 1(\mathrm{mod}3)$ στην οποία αν $p=\pi \cdot \bar{\pi}$ είναι η ανάλυση του p σε πρώτα στοιχεία του R, τότε η προβολή $Z_p \to \left(\frac{R}{\pi R}\right)$ είναι ισομορφισμός (βλ. 1.3.1.1 ορισμούς και υπενθυμίσεις στη σελίδα 21). Έτσι λοιπόν αν $p|a$, τότε η $x^3 \equiv a(\mathrm{mod}p)$ έχει λύση την $x=0$. Για $p \nmid a$, τώρα , λόγω του πιο πάνω ισομορφισμού η $x^3 \equiv a(\mathrm{mod}p)$ είναι επιλύσιμη στο Z αν και μόνο αν η $x^3 \equiv a(\mathrm{mod}\pi)$ επιλύσιμη στο R. Όμως το ότι $p \nmid a$ στο Z συνεπάγεται ότι $\pi \nmid a$ στο R(Αν $\pi \mid a$ τότε $N(\pi) \mid N(a) \to p \mid a^2 \to p \mid a$ πράγμα άτοπο.). Επίσης $p \equiv 1(\mathrm{mod}3) \to N(\pi) \equiv 1(\mathrm{mod}3)$ και συνεπώς έχουμε $\pi \nmid 3$ (βλ. 1.3.1.1 ορισμούς και υπενθυμίσεις στη σελίδα 21) και έτσι εφαρμόζοντας την ισοδυναμία $I \leftrightarrow II$ της πρότασης 1.3.2.5 και τα παραπάνω έχουμε το ζητούμενο.

1.3.2.7 ΠΟΡΙΣΜΑ : Για $p \in P$ με $p \equiv 1(\mathrm{mod}3)$ και $p=\pi \cdot \bar{\pi}$ η ανάλυση του p σε πρώτα του R ισχύει $\forall a \in Z$ ότι

$x^3 \equiv a(\mathrm{mod}p)$ επιλύσιμη στο Z αν και μόνο αν $x^3 \equiv a(\mathrm{mod}\pi)$ επιλύσιμη στο R.

1.3.2.8 ΟΡΙΣΜΟΣ : Έστω π πρώτο στοιχείο του R. Το π θα λέγεται πρωτεύον (primary) αν $\pi \equiv -1(\mathrm{mod}3)$ στο R.

1.3.2.9 ΣΧΟΛΙΑ : Ο ορισμός του πρωτεύοντος πρώτου δίνεται για να εξαλειφθεί η ασάφεια που που προκύπτει από το γεγονός ότι κάθε στοιχείο του R έχει 6 συνεταιρικά σε κάποιες περιπτώσεις και είναι ανάλογο με το ότι στο Z θεωρούμε πρώτους μόνο θετικούς αριθμούς και όχι τους αντίθετούς τους. Ο ορισμός θα γίνει κατανοητός στην συνέχεια που θα αποδείξουμε ότι για καθε πρώτο στοιχείο π του R εκτός από το 1-ω , το σύνολο Ass(π) έχει ακριβώς ένα πρωτεύον στοιχείο.

1.3.2.10 ΣΧΟΛΙΑ : 1. Αν $\pi \in R$ και $\pi=a+b\omega$ με $a,b \in Z$, τότε από τον ορισμό 1.3.2.8 προκύπτει εύκολα ότι

το π είναι πρωτεύον αν και μόνο αν $a \equiv -1(\mathrm{mod}3)$ και $b \equiv 0(\mathrm{mod}3)$

2. Από τον όρισμό του πρωτεύοντος πρώτου προκύπτει αμέσως ότι όλοι οι πρώτοι ακέραιοι αριθμοί που είναι και πρώτοι στο R είναι πρωτεύοντες πρώτοι του R. (Θυμίζουμε ότι $P \cap P(R) = \{p \in P : p \equiv 2(\mathrm{mod}3)\}$.)

3. **Με άμεση επαλήθευση μπορούμε να αποδείξουμε ότι κανένα στοιχείο του Ass(1-ω) δεν είναι πρωτεύον.**
4. **Για κάθε πρωτεύοντα πρώτο π του R ορίζεται το κυβικό σύμβολο του Legendre**

<u>1.3.2.11 ΠΡΟΤΑΣΗ</u> : Για κάθε πρωτεύοντα πρώτο π του R με π∉Ass(1-ω) , υπάρχει ακριβώς ένας πρωτεύοντας πρώτος στο σύνολο Ass(π)

<u>ΑΠΟΔΕΙΞΗ</u>

Κατ' αρχήν επειδή π∉Ass(1-ω) έχουμε ότι $\pi\in P$ ή ότι $\pi\in\{u\in P(R) : \bar{u}\in P(R),\ u\bar{u}\in P,\ u\bar{u}\equiv 1(\mathrm{mod}3)\}$
Επίσης επειδή το π είναι πρώτος του S, έχουμε ότι και το Ass(π) είναι σύνολο πρώτων του S.

<u>1η Περιπτωση</u> : " $\pi\in P$ "

Τότε το π είναι εξ'ορισμού πρωτεύον και επειδή $Ass(\pi)=\{\pm\pi,\pm\omega\pi,\pm\omega^2\pi\}$ εύκολα βλέπουμε ότι είναι το μοναδικό πρωτεύον πρώτο στοιχείο του Ass(π).

<u>2η Περίπτωση</u> : " $\pi\in\{u\in P(R) : \bar{u}\in P(R),\ u\bar{u}\in P,\ u\bar{u}\equiv 1(\mathrm{mod}3)\}$ "

Τότε αρκεί να δείξουμε ότι υπάρχει μοναδικό στοιχείο $x+y\omega$ ($x,y\in Z$) του Ass(π) με $x\equiv -1(\mathrm{mod}3)$ και $y\equiv 0(\mathrm{mod}3)$ (βλ. 1.2.3.10 σχόλια).Αν $\pi=a+b\omega$ ($a,b\in Z$) τότε $Ass(\pi)=\{\pm(a+b\omega),\pm(b+(a-b)\omega),\pm((a-b)+a\omega)\}$. Έστω $p=\pi\cdot\bar{\pi}=a^2-ab+b^2\in P$. Έχουμε $p\equiv 1(\mathrm{mod}3)$ και ισχύουν οι παρακάτω ισότητες

$\pi = a+b\omega$ (Σ 1.3.2.11.1)
$\omega\pi = -b+(a-b)\omega$ (Σ 1.3.2.11.2)
$\omega^2\pi = (b-a)-a\omega$ (Σ 1.3.2.11.3)
$-\pi = -a-b\omega$ (Σ 1.3.2.11.4)
$-\omega\pi = b+(b-a)\omega$ (Σ 1.3.2.11.5)
$-\omega^2\pi = (a-b)+a\omega$ (Σ 1.3.2.11.6)

Θα δείξουμε τώρα ότι υπάρχει στοιχείο του Ass(π) το οποίο είναι πρωτεύον.Πράγματι, επειδή $p=\pi\cdot\bar{\pi}=a^2-ab+b^2$ θα έχουμε ότι τα a,b δεν μπορεί να είναι ταυτόχρονα διαιρούμενα με το 3 (αλλιώς 9|p που είναι άτοπο). Διακρίνουμε τις περιπτώσεις :

(A) <u>3 ∤ a</u> . Τότε :

- για $a\equiv 2(\mathrm{mod}3)$ έχουμε $p=a^2-ab+b^2\equiv 1-2b+b^2(\mathrm{mod}3)\rightarrow 1\equiv 1-2b+b^2(\mathrm{mod}3)\rightarrow b(b-2)\equiv 0(\mathrm{mod}3)$ οπότε για 3|b έχουμε $\pi\equiv -1(\mathrm{mod}3)$ (βλ. Σ 1.3.2.11.1) , δηλαδή το π είναι πρωτεύον , ενώ για 3|(b-2) έχουμε $-\omega\pi\equiv -1(\mathrm{mod}3)$ (βλ. Σ 1.3.2.11.5) και συνεπώς το -ωπ είναι πρωτεύον.
- για $a\equiv 1(\mathrm{mod}3)$ έχουμε $(-a)\equiv 2(\mathrm{mod}3)$ και από τα παραπάνω έχουμε ότι για τον $-\pi=(-a)+(-b)\omega$ στο Ass(-π) υπάρχει στοιχείο πρωτεύον και έτσι έχουμε το ζητούμενο αφού Ass(π)=Ass(-π).

(B) 3 | a . Τότε :
3 ∤ b (αφού 3 ∤ π) , οπότε για τον πρώτο $-\omega\pi=b+(b-a)\omega$ έχουμε το ζητούμενο από την περίπτωση (A) λόγω του ότι Ass(π)=Ass(-ωπ).

Μένει τώρα να δείξουμε την μοναδικότητα.

(1) <u>Έστω ότι ο π είναι πρωτεύων πρώτος</u>.

- Αν $-\pi\equiv -1(\mathrm{mod}3)$ τότε $\pi\equiv 1(\mathrm{mod}3)$ πράγμα άτοπο.
- Αν $\pm\omega\pi\equiv -1(\mathrm{mod}3)$ τότε $\omega\equiv\pm 1(\mathrm{mod}3)$ πράγμα άτοπο.
- Αν $\pm\omega^2\pi\equiv -1(\mathrm{mod}3)$ τότε $\omega^2\equiv\pm 1(\mathrm{mod}3)$ που μας δίνει πάλι άτοπο.

Στην περίπτωση αυτή λοιπόν έχουμε την μοναδικότητα.

(2) Έστω ότι ο π δεν είναι πρωτεύων πρώτος.

Στην περίπτωση αυτή έχουμε την ύπαρξη (όπως δείξαμε προηγουμένως) ενος πρωτεύοντος πρώτου u στο Ass(π). Από το (1) όμως έχουμε ότι το u είναι ο μοναδικός πρωτεύων πρώτος του Ass(u) και επειδή Ass(u)=Ass(π), έχουμε τελειώσει.

1.3.2.12 ΠΡΟΤΑΣΗ : Αν π πρώτο στοιχείο του R με $\pi \notin Ass(1-\omega)$ τότε υπάρχει ακριβώς ένα στοιχείο u του Ass(π) με την ιδιότητα $u \equiv 1 \pmod 3$

ΑΠΟΔΕΙΞΗ

Από την 1.3.2.11 πρόταση έχουμε ότι υπάρχει μοναδικό $v \in Ass(\pi)$ με την ιδιότητα $v \equiv -1 \pmod 3$, οπότε

$(-v) \equiv 1 \pmod 3$. Αν πάλι $v' \in Ass(\pi)$ με $v' \equiv 1 \pmod 3$, τότε $(-v') \equiv -1 \pmod 3$, και από την μοναδικότητα του v

έχουμε $v' = -v \rightarrow v' = -v$.

1.3.2.13 ΠΟΡΙΣΜΑ : Αν $p \in P$ με $p \equiv 1 \pmod 3$, τότε ο p γράφεται $p = \pi \cdot \bar{\pi}$, όπου $\pi, \bar{\pi} \in P(R)$ και ο π είναι πρωεύων.

ΑΠΟΔΕΙΞΗ

Από υπενθυμίσεις 1.3.1.1 έχουμε ότι ο p γράφεται $p = \pi \cdot \bar{\pi}$ όπου $\pi, \bar{\pi} \in P(R)$. Από την πρόταση 1.3.2.11

όμως υπάρχει $\varepsilon \in E(R)$ ώστε ο επ να είναι πρωτεύων. Το ζητούμενο είναι τώρα προφανής συνέπεια της σχέσης $p = (\varepsilon\pi)\overline{(\varepsilon\pi)}$. (Σημειώνουμε ότι $E(R) = \{\pm 1, \pm\omega, \pm\omega^2\}$ και έτσι $\forall \varepsilon \in E(R)$ $\sigma(\varepsilon) = \varepsilon^2$ όπου σ είναι η μιγαδική

συζυγία.)

Για λόγους πληρότητας δίνουμε την επέκταση του όρου "πρωτεύων" σε κάθε στοιχείο του R (όχι εννάδα), καθώς και την επέκταση του κυβικού συμβόλου του Legendre σε όλο το R με μερικές βασικές ιδιότητες του. Σημειώνουμε ότι η επέκταση του κυβικού συμβόλου είναι χρήσιμη για την απόδειξη του συμπληρωματικού νόμου της κυβικής αντιστροφής (βλ. [Ir.Ro] ασκ 17,18,19 σελ 135)

1.3.2.14 ΟΡΙΣΜΟΣ : Ένα στοιχείο u του R θα λέγεται πρωτεύον αν δεν είναι εννάδα και επίσης $u \equiv -1 \pmod 3$ στο R.

(Σημείωση : Όπως και στην περίπτωση των πρώτων πρωτεύοντων, ένα στοιχείο $x+y\omega$ του R είναι πρωτεύον αν και μόνο αν $\chi \equiv -1 \pmod 3$ και $y \equiv 0 \pmod 3$)

1.3.2.15 ΠΡΟΤΑΣΗ : Αν $u \in R$ πρωτεύον στοιχείο του R τότε υπάρχουν μονοσήμαντα ορισμένα $s \in N$ και $\pi_1, \pi_2, \ldots, \pi_s$ πρωτεύοντες πρώτοι του R ώστε $u = \pi_1\pi_2 \cdot \ldots \cdot \pi_s$ ή $u = -\pi_1\pi_2 \cdot \ldots \cdot \pi_s$

<u>1.3.2.16 ΟΡΙΣΜΟΣ</u> : Αν $u\in R$ πρωτεύον στοιχείο, τότε ορίζουμε την συνάρτηση $\left(\frac{\cdot}{u}\right)_3 : R \to \{0\} \cup \{1,\omega,\omega^2\}$

ώς εξής : Για $v\in R$ ορίζουμε

$$\left(\frac{v}{u}\right)_3 = \begin{cases} 0 & ,\text{αν } u|v \\ 1 & ,\text{αν } v\in E(R) \\ \left(\frac{v}{\pi_1}\right)_3\left(\frac{v}{\pi_2}\right)_3\cdots\left(\frac{v}{\pi_s}\right) & ,\text{αν } u=\pm\pi_1\pi_2\ldots\pi_s \text{ η ανάλυση του } \pi \text{ σε πρώτα του } R \end{cases}$$

<u>1.3.2.17 ΠΡΟΤΑΣΗ</u> : (ΙΔΙΟΤΗΤΕΣ) Αν $u,u'\in R$ πρωτεύοντα στοιχεία τότε

1. $\left(\frac{ab}{u}\right)_3 = \left(\frac{a}{u}\right)_3 \cdot \left(\frac{b}{u}\right)_3$, $\forall\ a,b\in R$
2. $\left(\frac{a}{u}\right)_3 \in \{1,\omega,\omega^2\}$, $\forall\ a\in R$
3. Αν $a,b\in R$ με $a\equiv b(\text{mod}u)$, τότε $\left(\frac{a}{u}\right)_3 = \left(\frac{b}{u}\right)_3$
4. Αν $a\in Z$ και $u\in Z$ και $u\nmid a$ τότε $\left(\frac{a}{u}\right)_3 = 1$
5. $\left(\frac{w}{u}\right)_3 = \omega^{m+n}$, όπου ως συνήθως $\omega = e^{2\pi i/3}$ και $u=(3m-1)+3n\omega$ (βλ. σημείωση στον ορισμό 1.3.2.14)
6. Το σ(u) είναι πρωτεύον στοιχείο του R .(σ = μιγαδική συζυγία.)

1.3.3 ΝΟΜΟΣ ΚΥΒΙΚΗΣ ΑΝΤΙΣΤΡΟΦΗΣ

Στην παράγραφο αυτή αναφέρουμε τον νόμο κυβικής αντιστροφής καθώς και τον συμπληρωματικό του. Οι αποδείξεις έχουν παραλειφθεί λόγω του ότι είναι αρκετά τεχνικές και μακροσκελείς. (Γίνεται χρήση πολλαπλασιαστικών χαρακτήρων καθώς και αθροισμάτων Gauss και Jacobi.) Γιά λεπτομέρειες βλ. [Ir.Ro] σελ 114-118 .

<u>1.3.3.1 ΘΕΩΡΗΜΑ</u> : (Νόμος κυβικής αντιστροφής) Αν π_1,π_2 είναι πρωταρχικοί πρώτοι του R και

$N(\pi_1)\neq N(\pi_2)$, τότε $\left(\frac{\pi_2}{\pi_1}\right)_3=\left(\frac{\pi_1}{\pi_2}\right)_3$.

<u>1.3.3.2 ΠΟΡΙΣΜΑ</u> : Αν π_1,π_2 είναι πρώτοι του R με $N(\pi_1)\neq N(\pi_2)$ και $\pi_1,\pi_2\equiv\pm1(\mathrm{mod}3)$ τότε

$\left(\frac{\pi_2}{\pi_1}\right)_3=\left(\frac{\pi_1}{\pi_2}\right)_3$.

<u>1.3.3.3 ΘΕΩΡΗΜΑ</u> : (Συμπληρωματικό του νόμου αντιστροφής) Αν π είναι πρωταρχικός πρώτος του R

τότε $\left(\frac{1-\omega}{\pi}\right)_3=\grave{u}^{2m}$, όπου ως συνήθως $\grave{u}=e^{2\pi i/3}$

και $\pi=(3m-1)+3n\grave{u}$ $m,n\in Z$ (βλ. 1.3.2.10 σχόλια)

1.3.4 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ ΤΗΣ ΜΟΡΦΗΣ A^2+27B^2

1.3.4.1 ΛΗΜΜΑ : Άν π=a+bω a,b∈Z ένας πρωτεύων πρώτος του R με π ∤ 2 τότε τα ακόλουθα είναι ισοδύναμα :

1. **Η εξίσωση $x^3\equiv 2(\mathrm{mod}\pi)$ είναι επιλύσιμη στο R**
2. **π≡1(mod2) στο R**
3. **a≡1(mod2) και b≡0(mod2)**

ΑΠΟΔΕΙΞΗ

(2↔3) Προφανές.

(1↔2) Διακρίνουμε τις περιπτώσεις :

1η Περίπτωση : " π∈P "

Στην περίπτωση αυτή επειδή π ∤ 2 θα έχουμε π≠2. Τα π,2 είναι πρώτα στοιχεία του R και μάλιστα πρωτεύοντα και επειδή το π≡1(mod2) στην περίπτωση αυτή πάντα ικανοποιείται (αφού π,2∈P και π≠2) για να δείξουμε την ισοδυναμία 1↔2

θα πρέπει να δείξουμε ότι στην περίπτωση αυτή η εξίσωση $x^3\equiv 2(\mathrm{mod}\pi)$ έχει πάντα λύση στο R. Πράγματι, το π είναι πρωτεύον και συνεπώς π∉Ass(1-ω). (βλ. σχόλια 1.3.2.10) οπότε π ∤ 3 (βλ. ιδιότητες 1.3.1.1). Επίσης $N(\pi)=\pi^2$ και $\frac{N(\pi)-1}{3}=(\pi-1)\frac{\pi+1}{3}$ όπου π πρωτεύον , δηλαδή π≡-1(mod3) → $\frac{\pi+1}{3}\in Z$.

Τώρα, θέτοντας $\kappa=\frac{N(\pi)-1}{3}$ και $\lambda=\frac{\pi+1}{3}$, έχουμε $2^{\kappa}\equiv(2^{\lambda})^{(\pi-1)}\equiv 1(\mathrm{mod}\pi)$ (αφού π≠2 και π,2∈P) και συνεπώς η πρόταση 1.3.2.5 μας δίνει ότι η εξίσωση $x^3\equiv 2(\mathrm{mod}\pi)$ έχει πάντα λύση στο R.

2η Περίπτωση : " π∉P "

Επειδή ο 2 είναι πρωτεύων πρώτος του R , από κυβική αντιστροφή έχουμε $\left(\frac{2}{\pi}\right)_3=\left(\frac{\pi}{2}\right)_3$ (Αφού π|N(π) και π ∤ 2 θα έχουμε και $N(\pi)\neq 2^2=N(2)$.) .Τώρα επειδή το π είναι πρωτεύον έχουμε π∉Ass(1-ω) (βλ. σχόλια 1.3.2.10) και συνεπώς π ∤ 3 (βλ. υπενθυμίσεις 1.3.1.1) , έτσι η πρόταση 1.3.2.5 δίνει ότι $\left(\frac{2}{\pi}\right)_3=1$ αν και μόνο αν η $x^3\equiv 2(\mathrm{mod}\pi)$ είναι επιλύσιμη στο R , οπότε τελικά λόγω των παραπάνω , συνάγουμε ότι $\left(\frac{\pi}{2}\right)_3=1$ αν και μόνο αν η $x^3\equiv 2(\mathrm{mod}\pi)$ είναι

επιλύσιμη στο R. Επίσης $N(2)=4$ και αφού π ∤ 2 θα έχουμε 2 ∤ π (2,π∈P) . Εξάλλου εξ'ορισμού του κυβικού συμβόλου ισχύει $\left(\frac{\pi}{2}\right)_3=\pi^{\frac{4-1}{3}}(\mathrm{mod}2)$ οπότε $\left(\frac{\pi}{2}\right)_3\equiv\pi(\mathrm{mod}2)$ και συνεπώς " $\left(\frac{\pi}{2}\right)_3=1\ \leftrightarrow\ \pi\equiv 1(\mathrm{mod}2)$ ". Χρησιμοποιώντας τώρα και τα προηγούμενα έχουμε τελικά ότι η $x^3\equiv 2(\mathrm{mod}\pi)$ είναι επιλύσιμη στο

R αν και μόνο αν π≡1(mod2).

<u>1.3.4.2 ΠΑΡΑΤΗΡΗΣΗ</u> : Αν $p\in P$ με $p\equiv 1(mod3)$ τότε από το πόρισμα 1.3.2.13 έχουμε ότι $p=\pi\cdot\bar{\pi}$ όπου π είναι

πρωτεύων πρώτος του R και έτσι γράφοντας $\pi=(3m-1)+3n\omega$ με $m,n\in Z$ ($\omega=e^{2\pi\iota/3}$)

θα έχουμε $p=\pi\cdot\bar{\pi}=[(3m-1)+3n\omega]\cdot[(3m-1)+3n\omega^2]$ οπότε $4p=(2a-b)^2+27\left(\frac{b}{3}\right)^2$

όπου $a=3m-1$ και $b=3n$.

<u>1.3.4.3 ΠΡΟΤΑΣΗ</u> : Αν $p\in P$ με $p\equiv 1(mod3)$ τότε υπάρχουν $c,d\in Z$ ώστε $4p=c^2+27d^2$. Τα c,d είναι μοναδικά

ορισμένα μέχρι προσήμου από τις σχέσεις $c=2a-b$ και $d=\frac{b}{3}$ όπου $p=(a+b\omega)\overline{(a+b\omega)}$

με $a,b\in Z$ και το $(a+b\omega)$ να είναι πρωτεύον στοιχείο του R.(βλ. πόρισμα 1.3.2.13)

<u>ΑΠΟΔΕΙΞΗ</u>

Κατ' αρχήν από την παρατήρηση 1.3.4.2 παραπάνω έχουμε ότι τα c,d που αναφέρονται στην προς απόδειξη πρόταση υπάρχουν. Μένει να αποδείξουμε ότι είναι μονοσήμαντα ορισμένα μέχρι προσήμου από τις σχέσεις $c=2a-b$ και $d=\frac{b}{3}$. Έστω λοιπόν ότι $4p=x^2+27y^2$ (Σ 1.3.4.3.1) με $x,y\in Z$. Η σχέση Σ 1.3.4.3.1 μας δίνει $x^2\equiv y^2(mod2)$ και συνεπώς $x\equiv y(mod2)$ άρα $x+3y\equiv 0(mod2)$. Αν τώρα θέσουμε $C=\frac{x+3y}{2}$ και $D=3y$ τότε θα έχουμε $y=\frac{D}{3}$ και $x=2C-D$ και αντικαθιστώντας στην Σ 1.3.4.3.1 θα πάρουμε

$p=(C+D\omega)\overline{(C+D\omega)}$. Αφού όμως τότε $N(C+D\omega)=N(\overline{C+D\omega})=p\in P$, θα έχουμε ότι τα $C+D\omega$, $\overline{C+D\omega}$ είναι πρώτα στοιχεία του R , και έτσι από μονοσήμαντη ανάλυση του p σε πρώτους στο R θα έχουμε ότι

$(C+D\omega)\in Ass(a+b\omega)\cup Ass(\overline{a+b\omega})$. Τώρα :

$$Ass(a+b\omega)\in\begin{Bmatrix} a+b\omega \\ -b+(a-b)\omega \\ (b-a)-a\omega \\ -a-b\omega \\ b+(b-a)\omega \\ (a-b)+a\omega \end{Bmatrix},\quad Ass(\overline{a+b\omega})\in\begin{Bmatrix} (a-b)-b\omega \\ b+a\omega \\ -a-(a-b)\omega \\ -(a-b)+b\omega \\ -b-a\omega \\ a+(a-b)\omega \end{Bmatrix}.$$

Επίσης το $(a+b\omega)$ είναι πρωταρχικό και συνεπώς $a\equiv 1(mod3)$ και $b\equiv 0(mod3)$ οπότε

$\begin{Bmatrix} (a-b)\equiv 1(mod3) \\ a\equiv 1(mod3) \\ (b-a)\equiv 2(mod3) \end{Bmatrix}$ και

έτσι αφού $D\equiv 0(mod3)$ θα έχουμε $(C+D\omega)\in\begin{Bmatrix} a+b\omega \\ -a-b\omega \\ (a-b)-b\omega \\ -(a-b)+b\omega \end{Bmatrix}$ και συνεπώς αντικαθιστώντας τα C,D με τα $\frac{x+3y}{2}$, 3y αντίστοιχα και τα a,b με τα $\frac{c+3d}{2}$, 3d από τα προηγούμενα θα ισχύει $(x,y)\in\{(c,d),(-c,d),(c,-d),(-c,-d)\}$.

1.3.4.4 ΠΡΟΤΑΣΗ : Αν $p\in P$, τότε τα ακόλουθα είναι ισοδύναμα :

- **$p\equiv 1(\mathrm{mod}3)$ και η $x^3\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη στο Z**
- **υπάρχουν ακέραιοι αριθμοί A,B ώστε $p=A^2+27B^2$**

ΑΠΟΔΕΙΞΗ

Κατ'αρχήν αν p=2 η αποδεικτέα ισοδυναμία των προτάσεων ισχύει τετριμμένα.
Μένει λοιπόν η περίπτωση $p\in P^*$. Πρώτα θα κάνουμε ορισμένες παρατηρήσεις πριν προχωρήσουμε στο κυρίως μέρος της απόδειξης.Αν $p\in P^*$ με $p\equiv 1(\mathrm{mod}3)$, τότε ο p σύμφωνα με το πόρισμα 1.3.2.13 γράφεται στην μορφή $p=(a+b\omega)\overline{(a+b\omega)}$ όπου το στοιχείο $a+b\omega$ είναι πρωτεύων πρώτος του R. Επίσης από παρατήρηση 1.3.4.2 έχουμε ότι $4p=(2a-b)^2+27\left(\frac{b}{3}\right)^2$, όπου $a=3m-1$ και $b=3n$. Συνεπώς $4p=c^2+27d^2$ για $c=2a-b$ και $d=\frac{b}{3}$. Θέτουμε $\pi=a+b\omega$ και έτσι ισχύει ότι $\pi\nmid 2$. (Πράγματι, αν $\pi|2$ τότε αφού ο 2 είναι πρώτος του R θα είχαμε $\pi\in Ass(2)$ επομένως $p=N(\pi)=N(2)=4$ πράγμα άτοπο.) Επίσης ισχύει $\pi\nmid 3$. (Πράγματι, αν $\pi|3$ τότε $\pi\in Ass(1-\omega)$ - βλ.1.3.3.11 υπενθυμίσεις - πράγμα άτοπο αφού το $Ass(1-\omega)$ δεν έχει πρωτεύοντα στοιχεία.) Στην συνέχεια προχωράμε στο κυρίως μέρος της απόδειξης.

$\underline{\underline{(\rightarrow)}}$ Έστω $p\in P^*$ με $p\equiv 1(\mathrm{mod}3)$ και) $x^3\equiv 2(\mathrm{mod}p)$ επιλύσιμη στο Z. Ισχύουν λοιπόν όλα τα παραπάνω για τον p. Επειδή $x^3\equiv 2(\mathrm{mod}p)$ επιλύσιμη στο Z θα έχουμε ειδικότερα ότι η $x^3\equiv 2(\mathrm{mod}\pi)$ επιλύσιμη στο R.
(Πράγματι, κάθε Z-λύση της $x^3\equiv 2(\mathrm{mod}p)$ είναι και λύση της $x^3\equiv 2(\mathrm{mod}\pi)$ αφού $p=\pi\cdot\bar{\pi}$.) Σύμφωνα όμως με αυτά που είπαμε στην εισαγωγή της απόδειξης θα έχουμε $\pi\nmid 2$ και έτσι το λήμμα 1.3.4.1 μας δίνει ότι $\pi\equiv 1(\mathrm{mod}2)$ πράγμα που σημαίνει $a\equiv 1(\mathrm{mod}2)$ και $b\equiv 0(\mathrm{mod}2)$. (βλ. λήμμα 1.3.4.1) Επειδή όμως $c=2a-b$ και $d=\frac{b}{3}$, θα έχουμε ότι $2|c$ και $2|d$. Θέτοντας λοιπόν $A=\frac{c}{2}$ και $B=\frac{d}{2}$ και αντικαθιστώντας στην $4p=c^2+27d^2$, θα πάρουμε $p=A^2+27B^2$.

$\underline{\underline{(\leftarrow)}}$ Έστω $p\in P^*$ και έστω ότι $p=A^2+27B^2$ για κάποια $A,B\in Z$. Έχουμε λοιπόν $4p=(2A)^2+27(2B)^2$. Εξάλλου $p=A^2+27B^2\equiv A^2(\mathrm{mod}3)\rightarrow p\equiv A^2(\mathrm{mod}3)$. Επειδή τώρα $\forall k\in Z\ \ k^2\equiv 0,1(\mathrm{mod}3)$ θα έχουμε και ότι $p\equiv 0,1(\mathrm{mod}3)$. Αν $3|p$ τότε $3=p$ πράγμα άτοπο αφού ο 3 δεν μπορεί να γραφεί στην μορφή $\kappa^2+27\lambda$ με $\kappa,\lambda\in Z$ οπότε $p\equiv 1(\mathrm{mod}3)$. Μένει λοιπόν να δείξουμε τώρα ότι η $x^3\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη στο Z.
Έχουμε $p\equiv 1(\mathrm{mod}3)$ και έτσι η πρόταση 1.3.4.3 δίνει (λόγω μοναδικότητας) ότι $2A=\pm(2a-b)$ και $2B=\pm\left(\frac{b}{3}\right)$. Όμως $2A=\pm(2a-b)\rightarrow b\equiv 0(\mathrm{mod}2)$ και επίσης $a\equiv 1(\mathrm{mod}2)$. (Πράγματι στην εισαγωγή της απόδειξης είχαμε δείξει ότι για $p=(a+b\omega)\overline{(a+b\omega)}$ με το $\pi=a+b\omega$ να είναι πρωτεύων πρώτος του R, ισχύει $\pi\nmid 2$. Αυτό σημαίνει ότι $2\notin Ass(\pi)$ και επειδή ο π είναι πρώτος θα έχουμε $2\nmid\pi$. Όμως $\pi=a+b\omega$ με $b\equiv 0(\mathrm{mod}2)$ και έτσι $2\nmid\pi\rightarrow 2\nmid a\rightarrow a\equiv 1(\mathrm{mod}2)$.) Οι σχέσεις $b\equiv 0(\mathrm{mod}2)$ και

$a \equiv 1 (\mathrm{mod} 2)$ σε συνδυασμό με το λήμμα 1.3.4.1 μας δίνουν ότι η $x^3 \equiv 2 (\mathrm{mod} \pi)$ είναι επιλύσιμη στο R.

Η πρόταση 1.3.2.5 τώρα μας δίνει (αφού $\pi \nmid 2$ και $\pi \nmid 3$) ότι $\left(\frac{2}{\pi}\right)_3 = 1$ και έτσι

τελικά από την πρόταση 1.3.2.6 συμπεραίνουμε ότι $x^3 \equiv 2 (\mathrm{mod} p)$ είναι επιλύσιμη στο Z.

1.3.5 ΔΙΤΕΤΡΑΓΩΝΙΚΟ ΣΥΜΒΟΛΟ LEGENDRE ΚΑΙ ΝΟΜΟΣ ΔΙΤΕΤΡΑΓΩΝΙΚΗΣ ΑΝΤΙΣΤΡΟΦΗΣ

<u>1.3.5.1 ΟΡΙΣΜΟΙ ΣΧΟΛΙΑ</u> : Στις παραγράφους 1.3.5 και 1.3.6 , με S θα συμβολίζουμε τον δακτύλιο Z[i] όπου

$i^2=1$. Ο δακτύλιος S είναι ευκλείδιος και $E(S)=\{\pm1,\pm i\}$. Η ύλη , τα θεωρήματα και οι προτάσεις της παραγράφου αυτής είναι εντελώς ανάλογα με την κυβική περίπτωση και οι αποδείξεις είναι όμοιες και παραλείπονται. Για λεπτομέρειες παραπέμπουμε στα : [Cox] σελ. 81-83 και [Ir.Ro] §8,§9, σελ. 121-127.

<u>1.3.5.2 ΠΡΟΤΑΣΗ</u> : Αν $p\in P$ τότε ισχύουν τα ακόλουθα από τον νόμο ανάλυσης στο S :

- **Αν $p=2$ τότε ο $1+i$ είναι πρώτος του S και $2=i^3(1+i)^2$.**
- **Αν $p\equiv1(\mathrm{mod}4)$ τότε υπάρχει πρώτος π του S ώστε και το $\bar{\pi}$ να είναι πρώτος του S όχι συνεταιρικό του π και να ισχύει $p=\pi\cdot\bar{\pi}$.**
- **Αν $p\equiv3(\mathrm{mod}4)$ τότε ο p είναι πρώτο στοιχείο του S.**

<u>1.3.5.3 ΠΡΟΤΑΣΗ</u> : Για κάθε πρώτο στοιχείο π του S ισχύουν τα ακόλουθα

- **Αν $a\in S$ και $a\notin\pi S$ τότε $a^{N(\pi)-1}\equiv1(\mathrm{mod}\pi)$**
- **Τα $\pm1,\pm i$ είναι διακεκριμμένα modulo π**
- **$4 \mid N(\pi)-1$**
- **Για κάθε στοιχείο a του S , το $a^{\frac{N(\pi)-1}{4}}$ είναι λύση της $x^4\equiv1(\mathrm{mod}\pi)$ και συνεπώς ταυτίζεται με ακριβώς ένα από τα $1(\mathrm{mod}\pi),-1(\mathrm{mod}\pi),i(\mathrm{mod}\pi),-i(\mathrm{mod}\pi)$**

<u>1.3.5.4 ΟΡΙΣΜΟΣ</u> : Αν π είναι πρώτο στοιχείο του S όχι συνεταιρικό του $1+i$, ορίζουμε την συνάρτηση $\left(\frac{\cdot}{\pi}\right)_4 : Z[i]\to\{\pm1,\pm i\}\cup\{0\}$ ως εξής : Για $a\in Z[i]$ το $\left(\frac{a}{\pi}\right)_4$ είναι :

- **Αν $\pi \mid a$, το 0**
- **Αν $\pi \nmid a$, το μοναδικό στοιχειο του $\{\pm1,\pm i\}$ που είναι ισότιμο με $a^{\frac{N(\pi)-1}{4}}$ modulo π**

Το $\left(\frac{\cdot}{\pi}\right)_4$ ονομάζεται διτετραγωνικός χαρακτήρας υπολοίπων ή διτετραγωνικό σύμβολο του Legendre.

<u>1.3.5.5 ΠΡΟΤΑΣΗ</u> : Για κάθε πρώτο π του S ισχύουν τα ακόλουθα :

1. **Αν $\pi \notin Ass(1+i)$ και $a \in S$ με $\pi \nmid a$, τότε ισχύει η παρακάτω ισοδυναμία :**

"$\left(\frac{a}{\pi}\right)_4 = 1$ "$\leftrightarrow$ " $x^4 \equiv a(mod\pi)$ είναι επιλύσιμη στο S".

2. **Αν $\pi \notin Ass(1+i)$ τότε το διτετραγωνικό σύμβολο του Legendre ορίζει ομομορφισμό**

$\left(\frac{\cdot}{\pi}\right)_4 : \left(\frac{S}{\pi S}\right)^* \rightarrow \{\pm 1, \pm i\}$

3. **(α) " $N(\pi) \in P$ " $\leftrightarrow$ " $N(\pi) \in Ass(1+i)$ ή $N(\pi) \equiv 1(mod4)$" .**

Αν $N(\pi)=p \in P$ τότε $Z_p \xrightarrow{\cong} \frac{S}{\pi S}$ (μέσω της απεικόνισης $k+pZ \rightarrow k+\pi S$ για $k \in Z$)

(β) " $N(\pi)=p^2$ με $p \in P$ " $\leftrightarrow$ " $\pi \in P$ ".

Αν $\pi \in P$ τότε το Z_p είναι υπόσωμα του $\frac{S}{\pi S}$ (μέσω της αντιστοιχίας $k+pZ \rightarrow k+\pi S$,$k \in Z$)

<u>1.3.5.6 ΟΡΙΣΜΟΣ</u> : Ένα πρώτο στοιχείο π του S θα λέγεται πρωτεύον αν $\pi \equiv 1(mod(2+2i))$

<u>1.3.5.7 ΠΡΟΤΑΣΗ</u> : Για κάθε πρώτο στοιχείο π του S με $\pi \notin Ass(1+i)$ υπάρχει ακριβώς ένας πρωτεύοντας πρώτος στο σύνολο Ass(π).

<u>1.3.5.8 ΘΕΩΡΗΜΑ</u> : (Νόμος διτετραγωνικής αντιστροφής) Αν π,π* είναι διακεκριμένοι πρωτεύοντες πρώτοι του S και $\pi=a+bi$ με $a,b \in Z$ τότε ισχύουν τα ακόλουθα :

- $\left(\frac{\pi_2}{\pi_1}\right)_4 = \left(\frac{\pi_1}{\pi_2}\right)_4 \cdot (-1)^{\frac{N(\pi_2)-1}{4} \cdot \frac{N(\pi_1)-1}{4}}$
- $\left(\frac{i}{\pi}\right)_4 = i^{\frac{1-a}{2}}$
- $\left(\frac{1+i}{\pi}\right)_4 = i^{\frac{a-b-1-b^2}{4}}$
- $\left(\frac{2}{\pi}\right)_4 = i^{\frac{ab}{2}}$

1.3.6 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ ΤΗΣ ΜΟΡΦΗΣ A^2+64B^2

<u>1.3.6.1 ΠΡΟΤΑΣΗ</u> : Αν $p\in P$ τότε τα ακόλουθα είναι ισοδύναμα :

- **Υπάρχουν ακέραιοι αριθμοί A,B ώστε $p=A^2+64B^2$**
- **$p\equiv 1(\mathrm{mod}4)$ και η εξίσωση $x^4\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη στο Z**

<u>ΑΠΟΔΕΙΞΗ</u>

Κατ' αρχήν για p=2 η ισοδυναμία των προτάσεων της εκφώνησης είναι προφανής.Θα δείξουμε τώρα την ζητούμενη ισοδυναμία για $p\neq 2$.

($\rightarrow$) Έστω ότι για τον $p\in P^*$ ισχύει ότι υπάρχουν ακέραιοι αριθμοί A,B ώστε $p=A^2+64B^2$. Έχουμε λοιπόν $p\equiv A^2(\mathrm{mod}4)$ οπότε αφού $\forall k\in Z$ ισχύει $\kappa^2\equiv 0,1(\mathrm{mod}4)$ και αφού p περιττός πρώτος θα έχουμε $p\equiv 1(\mathrm{mod}4)$. Μένει να δείξω την επιλυσιμότητα της $x^4\equiv 2(\mathrm{mod}p)$ στο Z. Έχουμε ότι για x=A, y=8B ισχύει $p=x^2+y^2=\pi\cdot\overline{\pi}$ όπου $\pi=x+yi$. Τώρα $N(\pi)=p$ οπότε ο π είναι πρώτοστου S. Μπορούμε να υποθέσουμε ότι ο π είναι πρωτεύοντας πρώτος. (Πράγματι :Αν $\pi\in Ass(1+i)$ τότε $p=N(\pi)=2$ πράγμα άτοπο αφού έχουμε $p\neq 2$. Άρα $\pi\notin Ass(1+i)$, οπότε από την πρόταση 1.3.5.7 έχουμε ότι υπάρχει ε μονάδα του S ώστε το $\varepsilon\cdot\pi$ να είναι πρωτεύον πρώτος του S. Επίσης $p=\varepsilon\pi\cdot\overline{\varepsilon\pi}$ αφού $\overline{\varepsilon}=\varepsilon^{-1}$ και έτσι μπορούμε να αντικαταστήσουμε το π με το πρωτεύον $\pi\cdot\varepsilon$.) Έχουμε τώρα ότι το π είναι πρωτεύον πρώτο στοιχείο του S και έτσι $\pi\equiv 1(\mathrm{mod}(2+2i))\rightarrow\pi\equiv 1(\mathrm{mod}2)$, αλλά $\pi=x+yi$ οπότε ο x είναι περιττός και ο y είναι άρτιος (απλή άσκηση). Εξάλλου ο ισομορφισμός $Z_p\cong\frac{S}{\pi S}$ του 3(β) της πρότασης 1.3.5.5 θα μας δώσει ότι η $x^4\equiv 2(\mathrm{mod}\pi)$ είναι επιλύσιμη στο S αν και μόνο αν η $x^4\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη στο Z. Επειδή όμως $\pi\nmid 2$ (Αν $\pi|2$ τότε επειδή το 2 είναι πρώτος του S θα είχαμε $\pi\in Ass(2)$ και συνεπώς $p=N(\pi)=N(2)=4$ άτοπο.) το 4 της πρότασης 1.3.5.5 θα δώσει ότι η $x^4\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη στο Z αν και μόνο αν $\left(\frac{2}{\pi}\right)_4=1$. Για το ζητούμενο λοιπόν αρκεί $\left(\frac{2}{\pi}\right)_4=1$. Αυτό όμως ισχύει λόγω του τύπου $\left(\frac{2}{\pi}\right)_4=i^{\frac{xy}{2}}$ και του ότι y=8B.

($\leftarrow$) Έστω ότι η $x^4\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη στο Z και $p\equiv 1(\mathrm{mod}4)$. Από την πρόταση 1.3.5.2 έχουμε ότι ο p γράφεται $p=\pi\cdot\overline{\pi}$, όπου τα $\pi,\overline{\pi}$ είναι πρωτεύοντες πρώτοι του S. Γράφοντας $\pi=a+bi$ με $a,b\in Z$ θα έχουμε $p=a^2+b^2$ οπότε για το ζητούμενο αρκεί να δείξουμε ότι 8|b. Έχουμε ότι ο π είναι πρωτεύων πρώτος οπότε ο a είναι περιττός και ο b είναι άρτιος και έτσι $8|b\leftrightarrow i^{\frac{ab}{2}}=1$. Για το ζητούμενο αρκεί λοιπόν $i^{\frac{ab}{2}}=1$ δηλαδή ότι $\left(\frac{2}{\pi}\right)_4=1$. Η τελευταία ισότητα ισχύει γιατι αφού $\pi\nmid 2$ (Αν $\pi|2$ τότε $\pi\in Ass(2)\rightarrow p=N(\pi)=4$ άτοπο.) το 4 της πρότασης 1.3.5.5 θα μας δώσει ότι $\left(\frac{2}{\pi}\right)_4=1$ αν και μόνο αν η $x^4\equiv 2(\mathrm{mod}\pi)$ επιλύσιμη στο S και έτσι λόγω του ισομορφισμού $Z_p\cong\frac{S}{\pi S}$ του 3(β) της πρότασης 1.3.5.5 θα πάρουμε ότι $\left(\frac{2}{\pi}\right)_4=1$ αν και μόνο αν η $x^4\equiv 2(\mathrm{mod}p)$ επιλύσιμη στο Z Όμως η $x^4\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη εξ' υποθέσεως και έτσι έχουμε το ζητούμενο.

§1 ΥΠΕΝΘΥΜΙΣΕΙΣ ΚΑΙ ΟΡΙΣΜΟΙ ΑΠΟ ΣΤΟΙΧΕΙΩΔΗ ΑΛΓΕΒΡΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

2.1.1 ΑΛΓΕΒΡΙΚΑ ΣΩΜΑΤΑ ΑΡΙΘΜΩΝ ΚΑΙ ΝΟΜΟΣ ΑΝΑΛΥΣΗΣ

Στην 2.1.1 δεν θα δωθούν αποδείξεις μιά και οι προτάσεις που θα αναφερθούν θεωρούνται γνωστές ή είναι απλές ασκήσεις. Αποδείξεις μπορούν να βρεθούν στα [COX] σελ. 98-105 και [Αντων].

<u>2.1.1.1 ΣΧΟΛΙΑ</u> : Αλγεβρικό σώμα αριθμών (ή απλά σώμα αριθμών)ονομάζεται κάθε πεπερασμένη επέκταση του $\mathbf{Q}$, που είναι υπόσωμα του $\mathbf{C}$. Αν K είναι ένα σώμα αριθμών τότε με R_K θα συμβολίζουμε τον δακτύλιο των ακεραίων αλγεβρικών του K (Δηλαδή το R_K αποτελείται από τα στοιχεία του K των οποίων το ελάχιστο πολυώνυμο πάνω από το $\mathbf{Q}$ έχει ακεραίους συντελεστές και ο μεγιστοβάθμιος συντελεστής του είναι 1.) και με D_K ή d_K την διακρίνουσα του K. Υπενθυμίζουμε ότι αν L/K επέκταση οποιονδήποτε σωμάτων και u αλγεβρικό στοιχείο του L πάνω από το K τότε με $Irr(u/K)(x)\in K[x]$ θα συμβολίζουμε το ανάγωγο πολυώνυμο του u πάνω από το K. Κάθε σώμα της μορφής $\mathbf{Q}(\zeta_m)$ όπου $\zeta_m=e^{2\pi i/m}$ για $m\in\mathbf{N}$ θα λέγεται κυκλοτομικό. Όπως είναι γνωστό , κάθε κυκλοτομική επέκταση πάνω από το $\mathbf{Q}$ είναι επέκταση του Galois. Η ομάδα των αντιστρέψιμών κλασματικών ιδεωδών του R_K θα συμβολίζεται με I(K) ή I_K και η υποομάδα της I_K των κυρίων ιδεωδών με θα συμβολίζεται με H(K) ή H_K. Η ομάδα πηλίκο της I(K) modulo H(K) θα συμβολίζεται C(K) ή C_K και το #C(K) θα συμβολίζεται με h_K. Ισχύει ότι $h_K=1$ αν και μόνο αν ο R_K είναι δακτύλιος μονοσήμαντης ανάλυσης.

<u>2.1.1.2 ΟΡΙΣΜΟΣ</u> : Έστω K ένα αλγεβρικό σώμα αριθμών.

- **<u>Πεπερασμένος πρώτος</u> του K θα λέγεται κάθε πρώτο ιδεώδες του R_K.**
- **<u>Άπειρος πρώτος</u> του K θα λέγεται κάθε $\mathbf{Q}$-εμφύτευση του K στο $\mathbf{C}$.**

Ένας άπειρος πρώτος $\mathfrak{p}$ του K θα λέγεται

- **<u>Πραγματικός</u> , αν $\mathfrak{p}(K)\subseteq\mathbf{R}$.**
- **<u>Μιγαδικός</u> , αν $\mathfrak{p}(K)\not\subseteq\mathbf{R}$.**

Το $P_o(K)$ θα συμβολίζει των πεπερασμένων πρώτων του K , ενώ το $P_\infty(K)$ θα συμβολίζει το σύνολο των απείρων πρώτων του K. Επίσης θέτουμε $P(K)=P_o(K)\cup P_\infty(K)$.

<u>2.1.1.3 ΟΡΙΣΜΟΣ</u> : 1. Αν L/K είναι επέκταση αλγεβρικών σωμάτων αριθμών και $\mathfrak{p}$ άπειρος πρώτος του K ,

τότε ο $\mathfrak{p}$ θα λέγεται διακλαδιζόμενος στο L αν και μόνο αν ο $\mathfrak{p}$ είναι πραγματικός , και υπάρχει επέκταση του στο L η οποία αποτελεί μιγαδικό πρώτο του L.

2. Μια επέκταση αλγεβρικών σωμάτων αριθμών L/K θα λέγεται διακλαδιζόμενη όταν

υπάρχει κάποιος πρώτος του K (πεπερασμένος ή άπειρος) ο οποίος διακλαδίζεται στο L.

<u>2.1.1.4 ΣΗΜΕΙΩΣΗ</u> : Όταν αναφερόμαστε αόριστα σε " πρώτο του K " - για κάποιο αλγεβρικό σώμα αριθμών K - ο πρώτος αυτός θα μπορεί να είναι πεπερασμένος ή άπειρος.

<u>2.1.1.5 ΠΡΟΤΑΣΗ</u> : Έστω τετραγωνικό σώμα αριθμών K (δηλαδή πεπερασμένη επέκταση του Q βαθμού 2), τότε ισχύουν τα ακόλουθα :

I. Υπάρχει $m \in Z$ με m ελεύθερο τετραγώνου ώστε $K=Q(\sqrt{m})$

II. $D_K \equiv \begin{cases} m & \text{αν } m \equiv 1 \pmod 4 \\ 4m & \text{αν } m \equiv 2,3 \pmod 4 \end{cases}$

III. $K=Q(\sqrt{D_K})$

IV. $R_K = \begin{cases} Z[\sqrt{m}] & \text{αν } m \equiv 2,3 \pmod 4 \\ Z\left[\frac{1+\sqrt{m}}{2}\right] & \text{αν } m \equiv 1 \pmod 4 \end{cases}$ **και συνεπώς** $R_K = Z\left[\frac{D_K + \sqrt{D_K}}{2}\right]$

V. Για κάθε αυτομορφισμό τ του C ισχύει $\tau(R_K)=R_K$ και $\tau(K)=K$.

VI. Αν $G(K|Q)=\{1,\tau\}$ τότε $\tau(R_K)=R_K$.

<u>2.1.1.6 ΠΡΟΤΑΣΗ</u> : Έστω $n \in N$. Αν $K=Q(\sqrt{-n})$, τότε τα ακόλουθα είναι ισοδύναμα :

I. $D_K=-4n$

II. $R_K=Z[\sqrt{-n}]$

III. Το n είναι ελεύθερο τετραγώνου και $n \not\equiv 3 \pmod 4$

<u>2.1.1.7 ΠΡΟΤΑΣΗ</u> (Νόμος ανάλυσης σε τετραγωνικά σώματα αριθμών) : Έστω σ η μιγαδική συζυγία. Αν $K=Q(\sqrt{m})$ είναι ένα τετραγωνικό σώμα αριθμών όπου m είναι ελεύθερος τετραγώνου και $p \in P$ τότε:

- **Αν $p \neq 2$ και**
  - $\left(\frac{m}{p}\right)_2 = 1$, **τότε $pR_K = p \cdot p'$ όπου p,p' πρώτα ιδεώδη του R_K και $p'=\sigma(p)$**
  - $\left(\frac{m}{p}\right)_2 = -1$, **τότε $pR_K = p$ όπου p πρώτο ιδεώδες του R_K**
  - $\left(\frac{m}{p}\right)_2 = 0$, **τότε $pR_K = p^2$ όπου p πρώτο ιδεώδες του R_K**

- **Αν p=2 και**
  - **$m \equiv 1 \pmod 8$, τότε $pR_K = p \cdot p'$ όπου p,p' πρώτα ιδεώδη του R_K και $p'=\sigma(p)$**
  - **$m \equiv 5 \pmod 8$, τότε $pR_K = p$ όπου p πρώτο ιδεώδες του R_K**
  - **$m \equiv 2,3,6,7 \pmod 8$, τότε $pR_K = p^2$ όπου p πρώτο ιδεώδες του R_K**

2.1.1.8 ΠΡΟΤΑΣΗ (Νόμος ανάλυσης σε κυκλοτομικά σώματα αριθμών) : Έστω $K=\mathbb{Q}(\zeta_m)$ όπου $\zeta_m=e^{2\pi i/m}$,

$m\in\mathbb{N}$ κυκλοτομικό σώμα αριθμών και $p\in\mathbb{P}$. Γράφουμε $m=p^k\cdot n$ για $n\in\mathbb{N}, k\geq 0$ όπου $p\nmid n$.

Αν με e συμβολίζουμε τον δείκτη διακλάδωσης της επέκτασης Galois K/Q και με f τον βαθμό αδρανείας της , τότε :

- **$e=\varphi(p^k)$**
- **$f=\min\{v\in\mathbb{N}|\ p^v\equiv 1(\mathrm{mod}m)\}$**
- **Η ανάλυση του pR_K σε πρώτα ιδεώδη του R_K είναι :**
  $pR_K=(p_1p_2\cdot\ldots p_r)^e$ και $N_K(p_j)=p^f\ \forall j\in\{1,2,\ldots,r\}$

2.1.1.9 ΠΡΟΤΑΣΗ : (Ειδική περίπτωση νόμου ανάλυσης) : Έστω L/K επέκταση Galois αλγεβρικών σωμάτων αριθμών και έστω $R=R_K$, $S=R_L$. Έστω επίσης ότι $L=K(u)$ για κάποιο $u\in S$.

Αν $\mathfrak{p}$ είναι πρώτο ιδεώδες του R και το ανάγωγο πολυώνυμο f(x) του u πάνω από το K

είναι διαχωρίσιμο θεωρούμενο σαν πολυώνυμο του $(\frac{R}{\mathfrak{p}})[x]$ τότε :

1. **Το $\mathfrak{p}$ δεν διακλαδίζεται στο L.**
2. **Αν $f(x)=f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_r(x)(\mathrm{mod}\mathfrak{p})$ όπου τα f_j είναι διακεκριμένα και ανάγωγα**

modulo $\mathfrak{p}$ $\forall j\in\{1,2,\ldots r\}$, τότε θέτοντας $\mathfrak{q}_j=\mathfrak{p}S+f_j(u)S\ \forall j\in\{1,\ldots,r\}$ έχουμε ότι τα $\mathfrak{q}_j$ είναι πρώτα ιδεώδη του S και διαφορετικά ανά δύο. Επίσης η ανάλυση του $\mathfrak{p}$ σε πρώτα ιδεώδη του L είναι η $\mathfrak{p}S=\mathfrak{q}_1\mathfrak{q}_2\cdot\ldots\cdot\mathfrak{q}_r$. Τέλος οι βαθμοί των f_j ταυτίζονται και η κοινή τιμή τους είναι ο βαθμός αδρανείας του $\mathfrak{p}$.

§2 ΤΑΞΕΙΣ ΤΕΤΡΑΓΩΝΙΚΩΝ ΣΩΜΑΤΩΝ ΑΡΙΘΜΩΝ

2.2.1 ΕΙΣΑΓΩΓΗ ΣΤΙΣ ΤΑΞΕΙΣ ΤΕΤΡΑΓΩΝΙΚΩΝ ΣΩΜΑΤΩΝ ΑΡΙΘΜΩΝ

2.2.1.1 ΠΡΟΤΑΣΗ : Αν K είναι αλγεβρικό σώμα αριθμών με (K:Q)=n και M ένα πεπερασμένα παραγόμενο

Z-υποmodule του K , τότε ισχύουν τα ακόλουθα :

1. **Το M είναι ελεύθερο Z-module.**
2. **rank(M)=n $\leftrightarrow$ "το M περιέχει μία Q-βάση του K".**

ΑΠΟΔΕΙΞΗ

Απλή άσκηση άλγεβρας.

2.2.1.2 ΟΡΙΣΜΟΣ : Αν K είναι τετραγωνικό σώμα αριθμών και O ένας υποδακτύλιος του K που ικανοποιεί τα ακόλουθα :

- **Το O είναι πεπερασμένα παραγόμενο Z-module**
- **$1 \in O$**
- **Το O περιέχει μια Q-βάση του K**

Τότε το O θα λέγεται τάξη του K.

2.2.1.3 ΠΑΡΑΤΗΡΗΣΕΙΣ : 1. Αν K είναι τετραγωνικό σώμα αριθμών και O ένας υποδακτύλιος του K με $1 \in O$, τότε ο O είναι τάξη του K αν και μόνο αν ο O είναι ελεύθερο Z-module με rank(O)=2.

2. Αν K είναι τετραγωνικό σώμα αριθμών και O μία τάξη του K , τότε K=quot(O).

3. Αν K είναι τετραγωνικό σώμα αριθμών τότε ο R_κ είναι μία τάξη του K και μάλιστα είναι η μέγιστη τάξη του K , με την διάταξη του εγκλεισμού , δηλαδή κάθε άλλη τάξη του K είναι υποσύνολο του R_K. Με τον όρο maximal τάξη ή maximum τάξη (μέγιστη τάξη) θα εννοούμε λοιπόν τον δακτύλιο ακεραίων αλγεβρικών τετραγωνικού σώματος αριθμών.

2.2.1.4 ΠΡΟΤΑΣΗ : Αν K είναι τετραγωνικό σώμα αριθμών και O μία τάξη του K , τότε ο δείκτης [R_K : O]

είναι πεπερασμένος και ειδικότερα αν θέσουμε f = [R_K : O] και $w_K := \frac{D_K + \sqrt{D_K}}{2}$

τότε

έχουμε $O = Z + f \cdot R_K = Z[fw_K]$

ΑΠΟΔΕΙΞΗ

Θέτουμε κατ' αρχήν $R=R_K$. Τα O,R τώρα είναι δύο Z-modules με rank ίσο με 2 και επίσης $O \subseteq R$,

συνεπώς ο $[R_K : O]$ είναι πεπερασμένος. Επειδή έχουμε $f = [R_K : O] = \# \frac{R}{O}$, θα ισχύει ότι

$f \cdot R \subseteq O$ και συνεπώς $Z+ f \cdot R \subseteq O$. Επίσης είναι εύκολο να δεί κανείς ότι $Z+f \cdot R=Z+fw_K \cdot Z$ (= $Z[fw_K]$) και

συνεπώς ότι $Z[fw_K] \subseteq O$. Όμως το $R=Z[w_K]$ και $[Z[w_K] : Z[fw_K]] =2$ και αφού τα O, $Z[fw_K]$ έχουν τον ίδιο

δείκτη στον R (ενώ $Z[fw_K] \subseteq O$) θα πρέπει να ταυτίζονται .

<u>2.2.1.5 ΠΟΡΙΣΜΑ</u> : Αν K είναι τετραγωνικό σώμα αριθμών , τότε οι τάξεις του K είναι ακριβώς τα σύνολα

$Z+f \cdot R_K$ όπου το f διατρέχει τους φυσικούς.

<u>2.2.1.6 ΠΡΟΤΑΣΗ</u> : Αν K είναι τετραγωνικό φανταστικό σώμα και O μία τάξη του K τότε $O^*=\{\pm 1\}$, εκτός

από τις περιπτώσεις

- **$K=Q(i)$ όπου για $O=R_K$ ισχύει $O^*=\{\pm 1,\pm i\}$.**
- **$K=Q(\omega)$ όπου για $O=R_K$ ισχύει $O^*=\{\pm 1,\pm \omega,\pm \omega^2\}$, $(\omega=e^{2\pi i/3})$.**

<u>ΑΠΟΔΕΙΞΗ</u>

Απλή άσκηση.

<u>2.2.1.7 ΟΡΙΣΜΟΣ</u> : Αν K είναι τετραγωνικό σώμα αριθμών και O μία τάξη του K , τότε ο δείκτης $[R_K : O]$

θα ονομάζεται οδηγός (conductor) της O και θα συμβολίζεται $cond(O)$.

<u>2.2.1.8 ΠΡΟΤΑΣΗ</u> : Αν O είναι μία τάξη του τετραγωνικού σώματος αριθμών $K=Q(\sqrt{m})$,για $m \in Z$ ελεύθερο τετραγώνου, και η ομάδα Galois $G(K|Q)$ του K υπέρ του Q είναι $G(K|Q)=\{1,\sigma\}$

τότε :

I. Για κάθε $a,b,c,d \in K$ και $A \in M_{2x2}(Z)$ με $\begin{pmatrix} a \\ b \end{pmatrix} = A \begin{pmatrix} c \\ d \end{pmatrix}$ ισχύει

$$\left(\det \begin{bmatrix} a & b \\ \sigma(a) & \sigma(b) \end{bmatrix} \right)^2 = \det A \cdot \left(\det \begin{bmatrix} c & d \\ \sigma(c) & \sigma(d) \end{bmatrix} \right)^2$$

II. Αν $O=aZ+bZ$ και $O=cZ+dZ$ τότε $\left(\det \begin{bmatrix} a & b \\ \sigma(a) & \sigma(b) \end{bmatrix} \right)^2 = \left(\det \begin{bmatrix} c & d \\ \sigma(c) & \sigma(d) \end{bmatrix} \right)^2$

III. $\forall \tau \in Aut(C)$ $\tau(O)=O$.

<u>ΑΠΟΔΕΙΞΗ</u>

Η απόδειξη είναι απλή εφαρμογή στοιχειωδών γνώσεων από την άλγεβρα γιαυτό και παραλείπεται.

<u>2.2.1.9 ΟΡΙΣΜΟΣ</u> : Αν O είναι μία τάξη του τετραγωνικού σώματος αριθμών $K=Q(\sqrt{m})$,για $m \in Z$ ελεύθερο τετραγώνου και $G(K|Q)=\{1,\sigma\}$, τότε για (a,b) μία Z- βάση του O, (δηλαδή για

$O=aZ+bZ$) ισχύει ότι ο αριθμός $\left(\det\begin{bmatrix} a & b \\ \sigma(a) & \sigma(b) \end{bmatrix}\right)^2$ είναι ανεξάρτητος της Z-βάσης (a,b) του O (βλ. το ΙΙ της πρότασης 2.2.1.8). Ο αριθμός αυτός θα λέγεται διακρίνουσα της τάξης O και θα συμβολίζεται D_O ή d_O.

<u>2.2.1.10 ΠΡΟΤΑΣΗ</u> : Έστω O τάξη του τετραγωνικού σώματος K και f = cond(O). Ισχύουν τα ακόλουθα :

1. **(a). $D_O=f^2 \cdot d_K$.**
   (b). $D_O \equiv 0,1 \pmod 4$.
   (c). $K=Q(\sqrt{D_O})$.
2. **Από το 1 έχουμε ότι $D_O \equiv 0,1 \pmod 4$. Διακρίνουμε τις περιπτώσεις :**
   <u>$D_O= 4m$</u> , για κάποιο $m \in Z$.
   Στην περίπτωση αυτή θέτοντας $\tau_o=\sqrt{m}$ ισχύει $O=Z[\tau_o]$.

   <u>$D_O= m$</u> , για κάποιο $m \in Z$ με $m \equiv 1 \pmod 4$.
   Στην περίπτωση αυτή θέτοντας $\tau_o=\frac{3+\sqrt{m}}{2}$ ισχύει $O=Z[\tau_o]$.

<u>ΑΠΟΔΕΙΞΗ</u>

Η απόδειξη είναι απλή εφαρμογή στοιχειωδών γνώσεων από την άλγεβρα γιαυτό και παραλείπεται.

<u>2.2.1.11 ΛΗΜΜΑ</u> : Το σύνολο $\{x \in Z \mid x \equiv 0,1 \pmod 4 , |x| \neq \square\}$ ισούται με την ένωση των δύο ακόλουθων συνόλων :
$S=\{f^2 m \in Z \mid f \in N, m \equiv 1 \pmod 4$ και m=ελεύθερο τετραγώνου$\}$ και
$T=\{4f^2 m \in Z \mid f \in N, m \equiv 2,3 \pmod 4$ και m=ελεύθερο τετραγώνου $m \neq -1\}$.

<u>ΑΠΟΔΕΙΞΗ</u>

Η απόδειξη είναι πολύ εύκολη και αφήνεται ως άσκηση.

<u>2.2.1.12 ΠΡΟΤΑΣΗ</u> : Αν $D \in Z$ με $D \equiv 0,1 \pmod 4$ και ο $|D|$ δεν είναι τέλειο τετράγωνο ακεραίου τότε υπάρχει μοναδικό τετραγωνικό σώμα αριθμών K και μοναδική τάξη O του K ώστε $D_O=D$. Μάλιστα ισχύει και η ακόλουθη ισοδυναμία : $D>0 \leftrightarrow$ "K είναι πραγματικό σώμα". Πιο συγκεκριμένα :

- **Αν $D \in \{f^2 m \in Z \mid f \in N, m \equiv 1 \pmod 4$ και m=ελεύθερο τετραγώνου$\}$ τότε $K=Q(\sqrt{D})=Q(\sqrt{m})$, με $D_K=m$ και $O=Z+fR_K$**
- **Αν $D \in \{4f^2 m \in Z \mid f \in N, m \equiv 2,3 \pmod 4$ και m=ελεύθερο τετραγώνου, $m \neq -1\}$ τότε $K=Q(\sqrt{D})=Q(\sqrt{m})$, με $D_K=4m$ και $O=Z+fR_K$.**

<u>ΑΠΟΔΕΙΞΗ</u>

Από το λήμμα 2.2.1.11 έχουμε ότι το D ανήκει στην ένωση των δύο ακόλουθων συνόλων :
$S=\{f^2 m \in Z \mid f \in N, m \equiv 1 \pmod 4$ και m=ελεύθερο τετραγώνου$\}$ και
$T=\{4f^2 m \in Z \mid f \in N, m \equiv 2,3 \pmod 4$ και m=ελεύθερο τετραγώνου$\}$.

Αν το D ανήκει στο σύνολο S, τότε παίρνουμε το σώμα $K=Q(\sqrt{m})$ και την τάξη του $O= Z+fR_K$ για τα οποία έχουμε $d_K=m$ και $d_O=f^2 d_K=D$. Αν πάλι το D ανήκει στο T , τότε παίρνουμε το σώμα $K=Q(\sqrt{m})$ και την τάξη του

$\mathcal{O}= \mathbb{Z}+fR_K$ οπότε $d_K=4m$ και $d_{\mathcal{O}}=f^2d_K=D$. Έχουμε λοιπόν δείξει την ύπαρξη και θέλουμε να δείξουμε ακόμα την

μοναδικότητα των K,$\mathcal{O}$. Έχουμε κατ' αρχήν από το 1(c) της πρότασης 2.2.1.10 ότι $K=\mathbb{Q}(\sqrt{D_{\mathcal{O}}})$ άρα $K=\mathbb{Q}(\sqrt{D})$

και συνεπώς το K είναι μοναδικό για το D , άρα και το d_K είναι μοναδικό για το D και συνεπώς και ο

cond($\mathcal{O}$)=D/d_K είναι μοναδικός για το D. Επειδή τώρα $\mathcal{O}=\mathbb{Z}+\text{cond}(\mathcal{O})\cdot R_K$ έχουμε τελικά ότι και η $\mathcal{O}$ ορίζεται

μονοσήμαντα από την D. Η τελευταία ισοδυναμία που αναφέρεται στην εκφώνηση είναι προφανής συνέπεια του

$K=\mathbb{Q}(\sqrt{D_D})=\mathbb{Q}(\sqrt{D})$.

<u>2.2.1.13 ΟΡΙΣΜΟΣ</u> : Θεμελιώδης διακρίνουσα θα λέγεται κάθε διακρίνουσα τετραγωνικού σώματος αριθμών.

<u>2.2.1.14 ΣΧΟΛΙΑ</u> : Είναι εύκολο να δει κανείς (βλ. λήμμα 2.2.1.11 και πρόταση 2.2.1.12) ότι κάθε $D\in\mathbb{Z}$

με $D\equiv 0,1 \pmod 4$ και $|D|\neq\square$, έχει μια μοναδική παράσταση σαν $D=f^2D_o$, όπου $f\in\mathbb{N}$ και

D_o είναι θεμελιώδης διακρίνουσα. Μάλιστα, υπάρχει μία "1-1" και "επί" αντιστοιχία μεταξύ των συνόλων $A=\{D\in\mathbb{Z} \mid D\equiv 0,1 \pmod 4 , |D|\neq\square\}$ και $B=\{f^2D_o \mid f\in\mathbb{N} , D_o=\text{θεμελιώδης διακρίνουσα}\}$ η οποία δίνεται μέσω του εγκλεισμού $B\to A$.

2.2.2 PROPER ΙΔΕΩΔΗ ΤΑΞΗΣ

2.2.2.1 ΛΗΜΜΑ : Έστω $\mathbf{O}$ τάξη ενός τετραγωνικού σώματος αριθμών Κ. Ισχύουν τα ακόλουθα :

1. **Κάθε ακέραιο ιδεώδες της τάξης $\mathbf{O}$ περιέχει ένα μη μηδενικό ακέραιο αριθμό.**
2. **Αν $\mathbf{a}$ ακέραιο ιδεώδες της τάξης $\mathbf{O}$ με $\mathbf{a\neq 0}$ τότε ο δακτύλιος $\frac{O}{a}$ είναι πεπερασμένος.**

ΑΠΟΔΕΙΞΗ

Λόγω της ομοιότητας του λήμματος με αντίστοιχη πρόταση για δακτυλίους ακεραίων αλγεβρικών αριθμών ,

θα δώσουμε απλά υποδείξεις.

Για το 1 : Αν $G(K|Q)=\{1,\sigma\}$ και $a\in a$ με $a\neq 0$ τότε $\sigma(a)\in O$ (λόγω του ΙΙΙ της πρότασης 2.2.1.8) και έτσι

$$a\cdot\sigma(a)\in a\cap Z.$$

Για το 2 : Αν $m\in Z\cap a$ (από το 1) με $m\neq 0$, τότε ο δακτύλιος $\frac{O}{mO}$ είναι πεπερασμένος. Έχουμε λοιπόν

$mO\subseteq a\subseteq O$, με τον $\frac{O}{mO}$ πεπερασμένο. Συνεπώς και ο $\frac{O}{a}$ είναι πεπερασμένος.

2.2.2.2 ΟΡΙΣΜΟΣ : Έστω $\mathbf{O}$ τάξη ενός τετραγωνικού σώματος αριθμών Κ και $\mathbf{a\triangleleft O}$ ακέραιο. Ο φυσικός αριθμός $\#\frac{O}{a}$ θα λέγεται νόρμα (norm) του $\mathbf{a}$ και θα συμβολίζεται $\mathbf{N(a)}$.

2.2.2.3 ΠΡΟΤΑΣΗ : Αν $\mathbf{O}$ είναι τάξη ενός τετραγωνικού σώματος αριθμών Κ τότε :

1. **Κάθε μη μηδενικό πρώτο ιδεώδες της $\mathbf{O}$ είναι maximal.**
2. **Ο δακτύλιος $\mathbf{O}$ είναι Noetherian.**

ΥΠΟΔΕΙΞΗ

Γίνεται χρήση του 1 του λήμματος 2.2.2.1 .

2.2.2.4 ΠΡΟΤΑΣΗ : Αν $\mathbf{O}$ τάξη ενός τετραγωνικού σώματος αριθμών Κ και $\mathbf{a\triangleleft O}$ ακέραιο με $\mathbf{N(a)\in P}$,

τότε το $\mathbf{a}$ είναι πρώτο ιδεώδες της $\mathbf{O}$.

ΑΠΟΔΕΙΞΗ

Ο δακτύλιος O είναι Noetherian και συνεπώς αν m είναι ιδεώδες της O maximal που περιέχει το a,

τότε $\#\frac{m}{a}=\frac{\#\frac{O}{a}}{\#\frac{O}{m}}=\frac{N(a)}{N(m)}$ και συνεπώς αφού $N(a)\in P$, θα έχουμε ότι $N(m)\in\{1, N(a)\}$. Επειδή το m

είναι maximal ιδεώδες θα έχουμε λοιπόν $N(m)=N(a)$ και έτσι $\#\frac{m}{a}=\frac{N(a)}{N(m)}=1$, δηλαδή $m=a$.

Έξάλλου το m ως maximal είναι και πρώτο ιδεώδες και έτσι έχουμε το ζητούμενο.

2.2.2.5 ΣΧΟΛΙΑ : 1. Εν γένει μία τάξη Ο σε τετραγωνικό σώμα αριθμών Κ με οδηγό f >1 δεν είναι ακέραια κλειστός δακτύλιος στο Κ και συνεπώς δεν είναι δακτύλιος του Dedekind. Προφανώς όμως υπάρχουν και τάξεις οι οποίες είναι δακτύλιοι του Dedekind (π.χ. οι δακτύλιοι των ακεραίων αλγεβρικών τετραγωνικών σωμάτων αριθμών.)

2. Αν Ο τάξη ενός τετραγωνικού σώματος αριθμών Κ , τότε επειδή quot(Ο)=Κ μπορούμε να θεωρήσουμε κλασματικά ιδεώδη του Ο τα οποία θα βρίσκονται στο Κ.

2.2.2.6 ΠΡΟΤΑΣΗ : Αν Ο τάξη ενός τετραγωνικού σώματος αριθμών Κ και a κλασματικό ιδεώδες της Ο με $a\neq 0$, τότε το a είναι ελεύθερο Z-module με rank ίσο με 2.

ΑΠΟΔΕΙΞΗ

Υπάρχει $u\in O$ ώστε το ua να είναι ακέραιο ιδεώδες της Ο. Άρα $a\subseteq \frac{1}{u}\cdot O$. Όμως το Ο είναι ελεύθερο Z-module με rank ίσο με 2 άρα και το $\frac{1}{u}\cdot O$ είναι ελεύθερο Z-module με rank 2 και συνεπώς και το a είναι ελεύθερο Z-module με rank 2 ή 1. Μένει λοιπόν να αποκλειστεί η περίπτωση rank=1. Αν rank=1 με π.χ. $a=vZ$, με $v\in O$, τότε γράφοντας $O=aZ+bZ$ παίρνουμε ότι $(uv)\cdot O\subseteq a$ (αφου $a\lhd O$) και έτσι $uva\in vZ$, $uvb\in vZ$. Άν τώρα $uva=\kappa v$ και $uvb=\lambda v$ με $\kappa,\lambda\in Z$ τότε αφού $a\neq 0$ θα έχουμε και $v\neq 0$ και συνεπώς $au=\kappa, bu=\lambda$ επομένως $(\lambda a-\kappa b)u=0 \xrightarrow{u\neq 0} \lambda a-\kappa b=0$ πράγμα άτοπο αφού τα a,b είναι Z-γραμμικώς ανεξάρτητα.

2.2.2.7 ΛΗΜΜΑ : Άν Ο τάξη ενός τετραγωνικού σώματος αριθμών Κ και a κλασματικό ιδεώδες της Ο , τότε $O\subseteq \{u\in K \mid u\cdot a\subseteq a\}\subseteq R_K$.

ΑΠΟΔΕΙΞΗ

Το ότι $O\subseteq \{u\in K \mid u\cdot a\subseteq a\}$ είναι προφανές. Για τον άλλο εγκλεισμό έχουμε ότι αν $u\in K$ με $u\cdot a\subseteq a$, τότε γράφοντας $a=aZ+bZ$ με $a,b\in O$ Z-γραμμικώς ανεξάρτητα (επειδή το a είναι Z-module με rank 2) , θα έχουμε $u\cdot a\in aZ+bZ$ οπότε θα υπάρχει $A\in M_{2x2}(Z)$ με $u\begin{pmatrix}a\\b\end{pmatrix}=A\begin{pmatrix}a\\b\end{pmatrix}$ και έτσι $(uI-A)\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$, με $\begin{pmatrix}a\\b\end{pmatrix}\neq 0$, επομένως $\det(uI-A)=0$. Αποδείξαμε δηλαδή ότι το u θα είναι ρίζα του πολυωνύμου $\det(xI-A)\in Z[x]$ και έτσι $u\in R_K$.

2.2.2.8 ΟΡΙΣΜΟΣ : Έστω Ο τάξη ενός τετραγωνικού σώματος αριθμών Κ και a κλασματικό ιδεώδες της Ο.

Αν $O = \{ u \in K \mid u \cdot a \subseteq a \}$ τότε το a θα λέγεται proper ιδεώδες της O.
(<u>ΣΗΜΕΙΩΣΗ</u> : Λόγω του λήμματος 2.2.2.7 η συνθήκη $O = \{ u \in K \mid u \cdot a \subseteq a \}$ είναι ισοδύναμη με την $\{ u \in K \mid u \cdot a \subseteq a \} \subseteq O$.)

<u>2.2.2.9 ΠΑΡΑΤΗΡΗΣΕΙΣ</u> : 1. Αν O τάξη ενός τετραγωνικού σώματος αριθμών K και a proper κλασματικό ιδεώδες της O , τότε $\forall \tau \in Aut(C)$, το $\tau(a)$ είναι είναι proper κλασματικό ιδεώδες της O (αφού $O=\tau(O)$ και $K=\tau(K)$).

2. Ο ορισμός του proper ιδεώδους μιάς τάξης ενός τετραγωνικού σώματος αριθμών έχει σημασία αφού υπάρχουν ιδεώδη σε τάξεις που δεν είναι proper. Αν πάρουμε για παράδειγμα την τάξη $O=Z[\sqrt{-3}]$ του $K=Q(\sqrt{-3})$ και το ιδεώδες $a=2O+(1+\sqrt{-3})O$ της O , τότε $O \neq \{ u \in K \mid u \cdot a \subseteq a \}$. Πράγματι $R_K=Z[\frac{1+\sqrt{-3}}{2}]$ οπότε $O \neq R_K$ (π.χ. $\frac{1+\sqrt{-3}}{2} \notin O$) ενώ $\{ u \in K \mid u \cdot a \subseteq a \} = R_K$ (Η τελευταία ισότητα ισχύει διότι κατ' αρχήν από 2.2.2.7 λήμμα έχουμε $\{ u \in K \mid u \cdot a \subseteq a \} \subseteq R_K$ και επίσης με πράξεις επαληθεύουμε απ'ευθείας ότι $\frac{1+\sqrt{-3}}{2} \in \{ u \in K \mid u \cdot a \subseteq a \}$, πράγμα που σημαίνει $R_K \subseteq \{ u \in K \mid u \cdot a \subseteq a \}$)

3. Τα κύρια κλασματικά ιδεώδη μιάς τάξης ενός τετραγωνικού σώματος αριθμών είναι proper.

4. Από τον εγκλεισμό $\{ u \in K \mid u \cdot a \subseteq a \} \subseteq R_K$ του λήμματος 2.2.2.7 προκύπτει ότι κάθε ιδεώδες μέγιστης τάξης ενός τετραγωνικού σώματος αριθμών είναι proper. (Αυτό θα γίνει καλύτερα κατανοητό παρακάτω που θα αποδείξουμε ότι τα proper ιδεώδη μιας τάξης είναι ακριβώς τα αντιστρέψιμα ιδεώδη της και συνεπώς αφού σε μέγιστες τάξεις κάθε ιδεώδες είναι αντιστρέψιμο , θα ισχύει ότι και κάθε ιδεώδες είναι proper.)

5. Έστω O τάξη ενός τετραγωνικού σώματος αριθμών K και a proper κλασματικό ιδεώδες της O. Αν $\alpha \in K-\{0\}$, τότε το $\alpha \cdot a$ είναι proper ιδεώδες της O.(Είναι προφανής συνέπεια του ότι $\{ u \in K \mid u\alpha \cdot a \subseteq \alpha \cdot a \} \subseteq \{ u \in K \mid u \cdot a \subseteq a \} = O$ που βλέπουμε εύκολα ότι ισχύει.)

2.2.2.10 ΛΗΜΜΑ : Άν $K=Q(\tau)$ τετραγωνικό σώμα αριθμών με $Irr(\tau,Z)(x)=ax^2+bx+c$ τότε το $a=Z+\tau Z$ είναι

proper κλασματικό ιδεώδες της τάξης $O=Z+a\tau Z$ του K.

ΑΠΟΔΕΙΞΗ

Κατ' αρχήν το O είναι υποδακτύλιος του K με $1\in O$. Επίσης το O είναι πεπερασμένα παραγόμενο Z-module και περιέχει μια Q-βάση του K (την $B=(1,a\tau)$) , συνεπώς εξ' ορισμού 2.2.1.2 θα έχουμε ότι το

O είναι μία τάξη του K. Τώρα για τον δακτύλιο $a=Z+\tau Z$ έχουμε ότι $a\cdot a\subseteq O$ και $u\cdot a\subseteq O, \forall u\in O$ οπότε το

a είναι ένα κλασματικό ιδεώδες της τάξης O. Θα δείξουμε ότι είναι και proper. Αρκεί να δείξουμε ότι $\{ u\in K \mid u\cdot a\subseteq a\}\subseteq O$. Έστω λοιπόν $u\in K$ με $u\cdot a\subseteq a$. Έχουμε $u\cdot(Z+\tau Z)\subseteq Z+\tau Z$ και έτσι $u\in Z+\tau Z$, $u\cdot\tau\in Z+\tau Z$.

Γράφοντας λοιπόν $u=m+n\tau$ με $m,n\in Z$, θα έχουμε $u\cdot\tau=m\tau+n\tau^2$. Όμως $a\tau^2+b\tau+c=0 \rightarrow n\tau^2=\frac{n}{a}(-b\tau-c)$

οπότε $u\cdot\tau=m\tau+\frac{n}{a}(-b\tau-c)$ και έτσι $u\cdot\tau=(\frac{-nc}{a})+(\frac{-bn}{a}+m)\cdot\tau$. Επειδή όμως $MK\Delta(a,b,c)=1$ θα έχουμε $a|n$

και έτσι $\frac{n}{a}\in Z$ με αποτέλεσμα $u=(m+n\tau)=[m+a\cdot(\frac{n}{a})\tau]\in Z+a\tau Z = O$.

2.2.2.11 ΛΗΜΜΑ : Έστω K τετραγωνικό σώμα αριθμών και O μια τάξη του K με proper κλασματικό

ιδεώδες a. Από την πρόταση 2.2.2.6 έχουμε ότι το a μπορεί να γραφεί στην μορφή $a=\alpha Z+\beta Z$ με $\alpha,\beta\in K$ γραμμικώς ανεξάρτητα. Αν θέσουμε $\tau=\frac{\beta}{\alpha}$ και $Irr(\tau|Z)(x)=ax^2+bx+c$

τότε ισχύουν τα ακόλουθα :

- **$K=Q(\tau)$**
- **$O=Z+a\tau Z$**
- **$a\cdot(\frac{a}{N(\alpha)}\cdot\bar{a})=O$.**

ΑΠΟΔΕΙΞΗ

Κατ' αρχήν $a=\alpha(Z+\tau Z)$. Ισχύει $[Q(\tau) : Q]\geq 2$ (αν $[Q(\tau) : Q]=1$, τότε $\tau\in Q$ και έτσι τα α,β είναι Z-γραμμικώς

εξαρτημένα , πράγμα άτοπο) , και έτσι αφού $2 = [K : Q]=[K : Q(\tau)]\cdot[Q(\tau) : Q]$ θα έχουμε τελικά ότι $[K : Q(\tau)]=1$

δηλαδή $K=Q(\tau)$. Στην συνέχεια δείχνουμε ότι $O=Z+a\tau Z$. Από το προηγούμενο λήμμα 2.2.2.10 έχουμε ότι το

$Z+a\tau Z$ είναι μία τάξη του K και ότι το $Z+\tau Z$ είναι ένα proper κλασματικό ιδεώδες της τάξης $Z+a\tau Z$. Όμως τότε

από το 5 των παρατηρήσεων 2.2.2.9 έχουμε ότι και το $\alpha(Z+\tau Z)=a$ είναι proper κλασματικό ιδεώδες της τάξης

$Z+a\tau Z$. Έχουμε τώρα :

Το a είναι proper ιδεώδες της $O \rightarrow \{u\in K \mid u\cdot a\subseteq a \} = O$ (Σ 2.2.2.11.1).

Το a είναι proper ιδεώδες της $Z+a\tau Z \rightarrow \{u\in K \mid u\cdot a\subseteq a \} = Z+a\tau Z$ (Σ 2.2.2.11.2).

Από τις Σ 2.2.2.11.1 και Σ 2.2.2.11.2 συμπεραίνουμε ότι $O=Z+a\tau Z$. Μένει τώρα να δείξουμε ότι

$\mathfrak{a}\cdot(\frac{\mathfrak{a}}{N(\mathfrak{a})}\cdot\bar{\mathfrak{a}})=\mathfrak{O}$. Για ευκολία στον συμβολισμό θα συμβολίζουμε με " ' " την μιγαδική συζυγία .Έχουμε ότι το

$\mathfrak{a}'=\bar{\mathfrak{a}}$ είναι proper ιδεώδες της τάξης $\mathfrak{O}'=\bar{\mathfrak{O}}=\mathfrak{O}$ του τετραγωνικού σώματος $K'=\bar{K}=K$ (βλ . πρόταση 2.2.1.8).

Ισχύει $a\cdot\mathfrak{a}\cdot\mathfrak{a}'=a\cdot[\alpha(Z+\tau Z)]\cdot[\alpha'(Z+\tau'Z)]=$
$aa\alpha\alpha'(Z+\tau Z)(Z+\tau'Z)=N(\alpha)\cdot a\cdot(Z+\tau Z+\tau'Z+\tau\tau'Z)=N(\alpha)\cdot(aZ+a\tau Z+a\tau'Z+a\tau\tau'Z)$

οπότε $a\cdot\mathfrak{a}\cdot\mathfrak{a}'=N(\alpha)\cdot(aZ+a\tau Z+a\tau'Z+a\tau\tau'Z)$. Όμως τα τ,τ' είναι ρίζες του $Irr(\tau,Z)(x)=ax^2+bx+c$ και έτσι $\tau+\tau'=\frac{-b}{a}$

και $\tau\cdot\tau'=\frac{c}{a}$ οπότε θα έχουμε $a\cdot\mathfrak{a}\cdot\mathfrak{a}'=N(\alpha)\cdot[aZ+(-b)Z+(-c)Z]$ που σημαίνει $a\cdot\mathfrak{a}\cdot\mathfrak{a}'=$
$N(\alpha)\cdot(aZ+bZ+cZ)$.

Επειδή τώρα $MK\Delta(a,b,c)=1$, θα ισχύει $aZ+bZ+cZ=Z$ (απλή άσκηση άλγεβας) και συνεπώς

$a\cdot\mathfrak{a}\cdot\mathfrak{a}'=N(\alpha)\cdot(Z+a\tau Z)=N(\alpha)\cdot\mathfrak{O}$. Εχουμε λοιπόν τελικά ότι $\mathfrak{a}\cdot(\frac{\mathfrak{a}}{N(\alpha)}\cdot\bar{\mathfrak{a}})=\mathfrak{O}$ που είναι το ζητούμενο.

<u>2.2.2.12 ΠΟΡΙΣΜΑ</u> : Τα proper ιδεώδη τάξης τετραγωνικού σώματος αριθμών είναι ακριβώς τα αντιστρέψιμα και μάλιστα αν $\mathfrak{a}$ είναι proper ιδεώδες τότε $\mathfrak{a}^{-1}=\frac{\mathfrak{a}}{N(\alpha)}\bar{\mathfrak{a}}$, όπου τα α,a είναι αυτά που ορίζονται στο λήμμα 2.2.2.11

<u>ΑΠΟΔΕΙΞΗ</u>

Έστω K τετραγωνικό σώμα αριθμών και $\mathfrak{O}$ μια τάξη του K. Από την προηγούμενη πρόταση έχουμε ότι κάθε

proper ιδεώδες της $\mathfrak{O}$ είναι αντιστρέψιμο και το $\mathfrak{a}^{-1}$ είναι ακριβώς το $\frac{\mathfrak{a}}{N(\alpha)}\bar{\mathfrak{a}}$. Μένει λοιπόν να δείξουμε ότι αν

$\mathfrak{a}$ είναι ένα αντιστρέψιμο ιδεώδες της $\mathfrak{O}$, τότε είναι και proper . Πράγματι , αν $\mathfrak{a}$ είναι ένα αντιστρέψιμο ιδεώδες

της $\mathfrak{O}$ τότε αν πάρουμε $\alpha\in K$ με $\alpha\cdot\mathfrak{a}\subseteq\mathfrak{O}$ θα έχουμε $\alpha\in\alpha\cdot\mathfrak{O}=\alpha\cdot(\mathfrak{a}\cdot\mathfrak{a}^{-1})=(\alpha\cdot\mathfrak{a})\cdot\mathfrak{a}^{-1}\subseteq\mathfrak{a}\cdot\mathfrak{a}^{-1}\subseteq\mathfrak{O}$ δηλαδή $\alpha\in\mathfrak{O}$.

Έτσι $\{u\in K\mid u\cdot\mathfrak{a}\subseteq\mathfrak{a}\}\subseteq\mathfrak{O}$ και έχουμε το ζητούμενο.

Στη συνέχεια αναφέρουμε ένα αποτέλεσμα από την θεωρία ελεύθερων αβελιανών ομάδων το οποίο θα χρησιμοποιήσουμε παρακάτω (βλ. [Αντων])

<u>2.2.2.13 ΘΕΩΡΗΜΑ</u> : Έστω (M,+) ελεύθερη αβελιανή ομάδα και (T,+) μία υποομάδα της M. Ισχύουν τα ακόλουθα :

1. **Η T είναι ελεύθερη αβελιανή ομάδα με $rank(T)\le rank(M)$**
2. **Αν $rank(M)=n$ και $rank(T)=d\le n$, τότε υπάρχει Z-βάση $B=(w_1,w_2,\ldots,w_n)$ της M και $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_d\in Z-\{0\}$ ώστε**
   - **Το $B'=(\varepsilon_1w_1,\varepsilon_2w_2,\ldots,\varepsilon_dw_d)$ να είναι Z-βάση του T**
   - **$\varepsilon_j\mid\varepsilon_{j+1}\ \forall j\in\{1,\ldots,d-1\}$**

3. **Άν rank(M)=rank(T)=n , και B,B' είναι Z-βάσεις για τις M,T αντίστοιχα ,**

τότε για τον μονοσήμαντα ορισμένο πίνακα $A\in M_{nxn}(Z)$ με $B'^{T}=A\cdot B^{T}$ ισχύει ότι [M : T] = | det(A) |.

<u>2.2.2.14 ΠΡΟΤΑΣΗ</u> (Ιδιότητες νόρμας ακεραίων ιδεωδών) Έστω K μιγαδικό τετραγωνικό σώμα αριθμών και O μία τάξη του K. Για κάθε ακέραια ιδεώδη a,b της D ισχύουν τα ακόλουθα :

1. **$N(\alpha O)=N(\alpha)$,$\forall\ \alpha\in O-\{0\}$**
2. **Αν σ είναι η μιγαδική συζυγία τότε $\sigma(a)\cdot a=N(a)\cdot O$. Συνεπώς αν το a είναι αντιστρέψιμο τότε $a^{-1}=\frac{1}{N(a)}\cdot\sigma(a)$.**
3. **$N(a\cdot b)=N(a)\cdot N(b)$.**

<u>ΑΠΟΔΕΙΞΗ</u>

<u>Για το 1</u> : Κατ' αρχήν από το πρόταση 2.2.1.10 έχουμε ότι υπάρχει $u\in O$ ώστε $O=Z+uZ$. Τώρα , το $B=(1,u)$ είναι βάση του K (K=quot(O)) , οπότε θεωρώντας τον πίνακα $A=\begin{pmatrix} x & y \\ z & w \end{pmatrix}\in M_{2x2}(Z)$ με $\alpha\cdot\begin{pmatrix}1\\u\end{pmatrix}=\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix}1\\u\end{pmatrix}$ θα έχουμε $N(\alpha)=detA=xw-yz\neq 0$ ($N(\alpha)\neq 0$ αφού $\alpha\neq 0$). Τώρα , $\alpha\in O\rightarrow \alpha O\subseteq O$.

Επειδή $\alpha\neq 0$, τα $\alpha,\alpha\cdot u$ είναι Z-γραμμικώς ανεξάρτητα. Συνεπώς , το $\alpha\cdot O=\alpha Z+\alpha uZ$ είναι ελεύθερη αβελιανή υποομάδα της (O,+) με $rank(\alpha O)=2=rank(O)$. Το 3 του θεωρήματος 2.2.2.13 θα μας δώσει τώρα ότι $N(\alpha O) = [O : \alpha O] = | detA | = |N(\alpha)|=N(\alpha)$.

<u>Για το 2</u> : Θα δείξουμε κατ' αρχήν ότι : $N(\beta c)=N(\beta)N(c)$ (Σ 2.2.2.14.1) για κάθε $\beta\in O-\{0\}$ και κάθε ακέραιο ιδεώδες c της O.

Πράγματι, έχουμε ότι το c είναι ακέραιο , οπότε $\beta c\subseteq\beta O\subseteq O$. Ο πυρήνας του επιμορφισμού προβολής $F:\frac{O}{\beta c}\rightarrow\frac{O}{\beta O}$ είναι ο $Ker(F)=\frac{\beta O}{\beta c}$ και έτσι από θεώρημα ισομορφισμού και λόγω του ότι $N(\beta c)=\#\frac{O}{\beta c}$, $N(\beta O)=\frac{O}{\beta O}$, θα έχουμε $N(\beta O)\cdot(\#\frac{\beta O}{\beta c})=N(\beta c)$.

Όμως $\beta\neq 0\rightarrow \#\frac{\beta O}{\beta c}=\#\frac{O}{c}=N(c)$ οπότε $N(\beta O)\cdot N(c)=N(\beta c)$. Χρησιμοποιώντας τώρα από το 1 ότι $|N(\beta)|=N(\beta O)$, έχουμε $N(\beta c)=N(\beta)N(c)$ και έτσι αποδείξαμε την Σ 2.2.2.14.1

Με βάση την πρόταση 2.2.2.11 τώρα αν γράψουμε $a=(\alpha Z+\beta Z)$, για $\alpha,\beta\in O$ (αφού a είναι ακέραιο) και θέσουμε $\tau=\frac{\beta}{\alpha}$ με $Irr(\tau|Z)(x)=ax^2+bx+c$ θα ισχύουν : $a=\alpha(Z+\tau Z)$, $K=Q(\tau)$, $O=Z+a\tau Z$, $a\cdot a\cdot\sigma(a)=N(\alpha)O$ (Σ 2.2.2.14.2) , όπου σ η μιγαδική συζυγία. Είναι εύκολο τώρα να δεί κανείς ότι

$a(Z+\tau Z)\subseteq O$ και $N(\ a(Z+\tau Z)\ ) = \#(\frac{O}{aZ+a\tau Z}) = \#\ (\frac{Z+a\tau Z}{aZ+a\tau Z}) = \#\ (\frac{Z}{aZ}) = a$ (αφού $a>0$). Έτσι , $N(\ a(Z+\tau Z)\ ) = a$ (Σ 2.2.2.14.3). Όμως τα a , $a(Z+\tau Z)$ είναι ακέραια ιδεώδη της O, οπότε η Σ 2.2.2.14.1 θα μας δώσει $N(a)N(a)=N(a\cdot a)$ και $N\ (\ \alpha\cdot[a(Z+\tau Z)]\ ) = N(\alpha)\cdot N(a(Z+\tau Z))$ και έτσι $N(a)N(a)=N(a\cdot a)=N(\ a\cdot\alpha\cdot(Z+\tau Z)\ )=N\ (\ \alpha\cdot[a(Z+\tau Z)]\ )=N(\alpha)\cdot N(a(Z+\tau Z))=N(\alpha)\cdot a$ (λόγω Σ 2.2.2.14.3). Δηλαδή $N(\alpha)\cdot a= N(a)N(a)=a^2N(a) \rightarrow N(\alpha)=aN(a)$. Η τελευταία ισότητα

σε συνδιασμό με την Σ 2.2.2.14.2 μας δίνει $\sigma(a)\cdot a=N(a)\cdot O$ που είναι η ζητούμενη σχέση.

Για το 3 : Από το 2 , έχουμε $N(ab)\cdot O = (ab)\cdot\sigma(ab) = a\cdot b\cdot\sigma(a)\cdot\sigma(b) = (N(a)\cdot O)\cdot(\ N(b)\cdot O) =(N(a)N(b))\cdot O$

Έτσι λοιπόν $N(ab)\cdot O=(N(a)N(b))\cdot O$ οπότε οι $N(ab)$, $N(a)\cdot N(b)$ είναι συνεταιρικοί στην O ,

όμως είναι και θετικοί ακέραιοι οπότε $N(ab) = N(a)\cdot N(b)$.

2.2.3 ΤΑΞΕΙΣ ΚΑΙ ΤΕΤΡΑΓΩΝΙΚΕΣ ΜΟΡΦΕΣ

2.2.3.1 ΟΡΙΣΜΟΣ : Έστω K τετραγωνικό σώμα αριθμών και O μία τάξη του K. Με I(O) ή I_O , θα συμβολίζεται το σύνολο των αντιστρέψιμων κλασματικών ιδεωδών της τάξης O και με H(O) ή H_O , θα συμβολίζεται το σύνολο των κυρίων κλασματικών ιδεωδών της O. Προφανώς , το I(O) είναι πολλαπλασιαστική ομάδα και το H(O) είναι υποομάδα της I(O). Η ομάδα πηλίκο $\frac{I(O)}{H(O)}$ θα συμβολίζεται με C(O) και θα ονομάζεται " ομάδα κλάσεων ιδεωδών της O ". Επίσης , με h_O ή h(O) , θα συμβολίζεται το #C(O). Ειδικά για την περίπτωση της μέγιστης τάξης R_K , έχουμε από τα σχόλια 2.1.1.1 ότι $I_K=I(R_K)$, $H_K=H(R_K)$ και $C(K)=C(R_K)$.

2.2.3.2 ΛΗΜΜΑ : Αν $\tau\in C$ και $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in M_{2x2}(R)$, τότε $Im(\frac{p\tau+q}{r\tau+s})= det\begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot |r\tau+s|^{-2} \cdot Im(\tau)$.

ΑΠΟΔΕΙΞΗ

$$Im(\frac{p\tau+q}{r\tau+s}) = \frac{1}{2i}(\frac{p\tau+q}{r\tau+s} - \frac{p\bar{\tau}+q}{r\bar{\tau}+s}) = |r\tau+s|^{-2} \cdot \frac{1}{2i} \cdot [(p\tau+q)(r\bar{\tau}+s) - (p\bar{\tau}+q)(r\tau+s)] =$$
$$= |r\tau+s|^{-2} \cdot Im[(p\tau+q)(r\bar{\tau}+s)] = |r\tau+s|^{-2} \cdot Im(pr|\tau|^2+ps\tau+qr\bar{\tau}+qs) = |r\tau+s|^{-2} \cdot (ps \cdot Im(\tau)-qr \cdot Im(\tau)) =$$
$$= |r\tau+s|^{-2} det\begin{pmatrix} p & q \\ r & s \end{pmatrix} Im(\tau).$$

2.2.3.3 ΛΗΜΜΑ : Έστω D διακρίνουσα με $|D|\neq\square$.

1. **Άν $f(x,y)=ax^2+bxy+cy^2$ είναι τετραγωνική μορφή διακρίνουσας $D_f=D$ με $a\neq0$ και τ μία ρίζα της εξίσωσης $f(x,1)=0$ τότε η f είναι θετικά ορισμένη αν και μόνο αν " $a>0$ και $\tau\notin R$ ".**
2. **Άν $f(x,y)=ax^2+bxy+cy^2$ είναι θετικά ορισμένη τετραγωνική μορφή διακρίνουσας $D_f=D$ με $a\neq0$ και τ είναι μία ρίζα της εξίσωσης $f(x,1)=0$, τότε το σώμα $Q(\tau)$ είναι τετραγωνικό φανταστικό και το $O=Z+a\tau Z$ είναι μία τάξη του $Q(\tau)$ με διακρίνουσα $D_O=D_f$ και το $Z+\tau Z$ είναι proper ιδεώδες της O.**
3. **Έστω δύο θετικά ορισμένες τετραγωνικές μορφές f(x,y),g(x,y) διακρίνουσας D ώστε οι συντελεστές του x^2 των f,g να μην είναι μηδέν. Άν οι εξισώσεις $f(x,1)=0$, $g(x,1)=0$ έχουν κοινή λύση , τότε οι μορφές f και g ταυτίζονται.**

ΑΠΟΔΕΙΞΗ

Για το 1 : Έχουμε $\tau\in\{\frac{-b+\sqrt{D_f}}{2a}, \frac{-b-\sqrt{D_f}}{2a}\}$ (Σ 2.2.3.3.1)

($\rightarrow$) Άν η f είναι θετικά ορισμένη , τότε η πρόταση 1.2.1.16 μας δίνει $a>0$ και $D<0$ (αφού $a\neq0$ και $D\neq\square \rightarrow D\neq0$). Επίσης $D<0 \rightarrow \tau\notin R$ λόγω της Σ 2.2.3.3.1 .

($\leftarrow$) Άν $\tau\notin R$ και $a>0$ τότε " $\tau\notin R \rightarrow D<0$ " και έτσι αφού $a>0$, πάλι η πρόταση 1.2.1.16 θα μας δώσει ότι η f είναι θετικά ορισμένη.

Για το 2 : Έχουμε $\tau\in\{\frac{-b+\sqrt{D_f}}{2a}, \frac{-b-\sqrt{D_f}}{2a}\}$. Από το 1 , αφού η f είναι πρωταρχική θετικά ορισμένη τετραγωνική μορφή , θα έχουμε $a>0$ και $\tau\notin R$. και συνεπώς το $Q(\tau)$ είναι τετραγωνικό φανταστικό σώμα. Επίσης από το λήμμα 2.2.2.10 έχουμε ότι το $O=Z+a\tau Z$ είναι μία τάξη του $Q(\tau)$ και το

$Z+\tau Z$ είναι proper ιδεώδες της O. Μένει να δείξουμε ότι $D_O=D_f$. Αυτό θα γίνει χρησιμοποιώντας την

πρόταση 2.2.1.12 :

- Αν $D_f\in\{k^2m\in Z \mid k\in N,\ m\equiv 1(\mathrm{mod}4)$ και m=ελεύθερο τετραγώνου$\}$ τότε D_f είναι η διακρίνουσα της

  τάξης $Z+kR_K$, του $K=Q(\sqrt{m})$ με $D_K=m$. Αλλά $R_K=Z+(\frac{D_K+\sqrt{D_K}}{2})Z=Z+(\frac{m+\sqrt{m}}{2})Z$

  και για $\tau=\frac{-b\pm\sqrt{D_f}}{2a}\rightarrow a\tau=\frac{-(b\pm km)}{2}\pm k\frac{m+\sqrt{m}}{2}$. Όμως $k^2m=D_f=b^2-4ac\rightarrow k^2m\equiv b^2(\mathrm{mod}4)$

  και επειδή $m\equiv 1(\mathrm{mod}4)$, θα έχουμε $k^2\equiv b^2(\mathrm{mod}4)\rightarrow k\equiv\pm b(\mathrm{mod}2)\rightarrow km\equiv\pm b(\mathrm{mod}2)$

  $\rightarrow\frac{-(b\pm km)}{2}\in Z$. Άρα $O=Z+a\tau Z=Z+(k\frac{m+\sqrt{m}}{2})Z=Z+kR_K$ και έτσι η διακρίνουσα D_f της τάξης $Z+kR_K$ είναι D_O.

- Αν $D_f\in\{4k^2m\in Z \mid k\in N,\ m\equiv 2,3(\mathrm{mod}4)$ και m=ελεύθερο τετραγώνου$\}$ τότε D_f είναι η διακρίνουσα της τάξης $Z+kR_K$, του $K=Q(\sqrt{m})$ με $D_K=4m$. Αλλά $R_K=Z+(\frac{D_K+\sqrt{D_K}}{2})Z$

  $=Z+\sqrt{m}Z$

  και $a\tau=\frac{-b+2k\sqrt{m}}{2}=-\frac{b}{2}+k\sqrt{m}$. Τώρα $b^2-4ac=D_f=4k^2m\rightarrow b^2\equiv 0(\mathrm{mod}4)\rightarrow b\equiv 0(\mathrm{mod}2)$

  $\rightarrow -\frac{b}{2}\in Z$ και έτσι $O=Z+a\tau Z=Z+(-\frac{b}{2}+k\sqrt{m})Z=Z+(k\sqrt{m})Z=Z+kR_K$, οπότε οι διακρίνουσα D_f της τάξης $Z+kR_K$ είναι D_O.

Για το 3 : Έστω $f(x,y)=ax^2+bxy+cy^2$ και $g(x,y)=a'x^2+b'xy+c'y^2$ και τ η κοινή ρίζα των $f(x,1)=0$ και $g(x,1)=0$.

Έχουμε $D_f=D_g$ και $\tau=\frac{-b\pm\sqrt{D_f}}{2a}=\frac{-b'\pm\sqrt{D_f}}{2a'}\rightarrow 2a\tau+b=\pm 2a'\tau+b'$. Επίσης από το 1 έχουμε $\tau\notin R$.

Διακρίνουμε τις περιπτώσεις :

- 1η περίπτωση : $2a\tau+b=2a'\tau+b'$.

  τότε $2(a-a')\tau=b'-b$ και έτσι $\tau\notin R\rightarrow a=a'$, $b=b'$, οπότε και αφού $b^2-4ac=D_f=b'^2-4a'c'$

  θα πάρουμε $c=c'$.
- 2η περίπτωση : $2a\tau+b=-(2a'\tau+b')$.

  τότε $2(a+a')\tau=-b'-b$ και έτσι $\tau\notin R\rightarrow a=-a'$, $b=-b'$. Όμως $a,a'>0$ (λόγω 1) οπότε $a=a'=0$ πράγμα άτοπο από την υπόθεση.

2.2.3.4 ΛΗΜΜΑ : Αν $f(x,y)=ax^2+bxy+cy^2$, $g(x,y)=a_1x^2+b_1xy+c_1y^2$ είναι πρωταρχικές θετικά ορισμένες τετραγωνικές μορφές διακρίνουσας D και $ΜΚΔ(a,a_1,\frac{b+b_1}{2})=1$, τότε η πρόταση 1.2.4.4 μας δίνει ότι υπάρχει ακέραιος B μοναδικός $\mathrm{mod}2aa_1$

$$\text{ώστε} \begin{cases} B \equiv b(\mathrm{mod} 2a) \\ B \equiv b_1(\mathrm{mod} 2a_1) \\ B^2 \equiv D(\mathrm{mod} 4aa_1) \end{cases}$$

Για τον B ισχύει επιπλέον ότι ΜΚΔ(a,a',B)=1

ΑΠΟΔΕΙΞΗ

Είναι απλή άσκηση στοιχειώδους θεωρίας αριθμών.

2.2.3.5 ΟΡΙΣΜΟΣ : Έστω D διακρίνουσα με D<0 ,|D|≠□και f(x,y) τετραγωνική μορφή διακρίνουσας D. Οι ρίζες της εξίσωσης f(x,1)=0 δεν είναι πραγματικές (αφού D<0) και μάλιστα (αφού είναι συζυγείς) η μία ακριβώς από αυτές -έστω τ- θα βρίσκεται στο άνω μιγαδικό ημιεπίπεδο : $h=\{z\in C|Im(z)>0\}$. Η τ θα καλείται " η ρίζα της μορφής f ". Μάλιστα , αν $f(x,y)=ax^2+bxy+cy^2$ τότε $a,c\neq 0$ (γιατί D<0) και η ρίζα της f είναι η $\tau = \frac{-b+\sqrt{D}}{2a}$. Τέλος όπως μπορεί να δεί κανείς , αν τ είναι η ρίζα μιας πρωταρχικής θετικά ορισμένης μορφής f διακρίνουσας D<0 , τότε f(x,1)=Irr(τ|Z)(x).

2.2.3.6 ΛΗΜΜΑ : Έστω D διακρίνουσα με D<0 και f,g τετραγωνικές μορφές διακρίνουσας D. Αν τ,τ' είναι οι ρίζες των f,g αντίστοιχα , τότε τα ακόλουθα είναι ισοδύναμα :

1. **Οι f,g είναι κανονικά ισοδύναμες.**
2. **Υπάρχει πίνακας $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in sl(2,Z)$ ώστε $\tau' = \frac{p\tau+q}{r\tau+s}$.**
3. **$Z+\tau Z=\lambda(Z+\tau' Z)$, για κάποιο $\lambda\in K^*$, όπου $K=Q(\tau)$.**

ΑΠΟΔΕΙΞΗ

Κατ' αρχήν έχουμε ότι οι συντελεστές του x^2 των f(x,y),g(x,y) δεν είναι μηδέν. Επίσης $\tau,\tau'\notin R$ (αφού D<0).

$1 \rightarrow 2$ Έστω $f(x,y)=g(px+qy,rx+sy)$, όπου $A=\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in sl(2,Z)$.

Έχουμε $r\tau+s\neq 0$

Πράγματι , αν $r\tau+s=0$, τότε επειδή $\tau\notin R$ θα έχουμε r=0 οπότε και s=0 και έτσι det(A)=0

πράγμα άτοπο αφού $A\in sl(2,Z)$.

Έτσι , $0=f(\tau,1)=g(p\tau+q,r\tau+s)=(r\tau+s)^2\cdot g(\frac{p\tau+q}{r\tau+s},1)$ και συνεπώς αφού $r\tau+s\neq 0$, θα έχουμε $g(\frac{p\tau+q}{r\tau+s},1)=0$.

Τώρα από το λήμμα 2.2.3.2 έχουμε $Im(\frac{p\tau+q}{r\tau+s})=de(\begin{pmatrix} p & q \\ r & s \end{pmatrix})\cdot|r\tau+s|^2\cdot Im(\tau)$. Άρα $\frac{p\tau+q}{r\tau+s}\in h=\{z\in C|$ $Im(z)>0\}$

Έτσι η $\frac{p\tau+q}{r\tau+s}$ είναι " ή ρίζα " της g και συνεπώς $\tau'=\frac{p\tau+q}{r\tau+s}$.

$\underline{2 \to 1}$ Άν $\tau'=\frac{p\tau+q}{r\tau+s}$ με $A=\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in sl(2,Z)$, τότε $g(p\tau+q,r\tau+s)=(r\tau+s)^2 \cdot g(\frac{p\tau+q}{r\tau+s},1)= (r\tau+s)^2 \cdot g(\tau',1)=0$. Άρα το τ είναι ρίζα του g(px+qy,rx+sy) και αφού $\tau \in \mathbf{h}$, το τ θα είναι " η ρίζα " του g(px+qy,rx+sy). Το 3 τώρα του λήμματος 2.2.3.3 μας δίνει f(x,y)= g(px+qy,rx+sy) και συνεπώς οι μορφές f,g είναι κανονικά ισοδύναμες.

$\underline{2 \to 3}$ Άν $\tau'=\frac{p\tau+q}{r\tau+s}$ με $A=\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in sl(2,Z)$, τότε θέτουμε $\lambda=r\tau+s \in K^*$, οπότε $\lambda(Z+\tau'Z) = (r\tau+s)[Z+\tau'Z] =$ $= (r\tau+s)Z+(p\tau+r)Z$. Θα δείξουμε ότι $(r\tau+s)Z+(p\tau+r)Z = Z+\tau Z$ οπότε και θα έχουμε το ζητούμενο.

Πράγματι , προφανώς : $(r\tau+s)Z+(p\tau+r)Z \subseteq Z+\tau Z$. Επίσης :

Αν $x+\tau y \in Z+\tau Z$, τότε επειδή $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in sl(2,Z) \to \det=\begin{pmatrix} p & q \\ r & s \end{pmatrix} \neq 0$, θα υπάρχουν $m,n \in Z$ με $\begin{pmatrix} q & s \\ p & r \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$. Έχουμε τώρα $x+\tau y = [(p\tau+q)m +(r\tau+s)n] \in [(r\tau+s)Z+(p\tau+r)Z]$.

$\underline{3 \to 2}$ Έστω $\lambda \in K^*$ με $\lambda(Z+\tau'Z) = Z+\tau Z$. Αφού $\tau,\tau' \notin R$, θα έχουμε ότι οι $B=(1,\tau)$ και $B'=(\lambda,\lambda\tau)$ είναι Z-βάσεις των ελεύθερων αβελιανών προσθετικών ομάδων $Z+\tau Z$, $\lambda Z+\lambda\tau Z$ αντίστοιχα. Επειδή $\lambda(Z+\tau'Z) = Z+\tau Z$, οι B,B' θα είναι βάσεις της ίδιας ομάδος και συνεπώς θα υπάρχει unimodular πίνακας (δηλαδή πίνακας ορίζουσας ± 1) $A=\begin{pmatrix} p & q \\ r & s \end{pmatrix}$, με $\begin{pmatrix} \lambda\tau' \\ \lambda \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix}$. Έχουμε λοιπόν $\tau'\lambda=p\tau+q$ και $\lambda=r\tau+s$.

Εξάλλου $\lambda \neq 0 \to r\tau+s \neq 0$ και συνεπώς $\tau'=\frac{p\tau+q}{r\tau+s}$. Αν $\det\begin{pmatrix} p & q \\ r & s \end{pmatrix} = -1$, τότε από 2.2.3.2 λήμμα έχουμε $Im(\tau') = - |r\tau+s|^{-2} \cdot Im(\tau)$. Επειδή όμως $\tau \in \mathbf{h}=\{z \in C | Im(z)>0\}$, θα έχουμε $Im(\tau)>0$ και συνεπώς $Im(\tau')<0$ πράγμα άτοπο αφού και $\tau' \in \mathbf{h}$.Η περίπτωση $\det\begin{pmatrix} p & q \\ r & s \end{pmatrix} = -1$ δίνει συνεπώς άτοπο και έτσι $\det\begin{pmatrix} p & q \\ r & s \end{pmatrix} =1$.

Άρα $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in sl(2,Z)$ και έχουμε το ζητούμενο.

$\underline{2.2.3.7\ \Theta\Epsilon\Omega\Rho\Eta\Mu\Alpha}$: Έστω D διακρίνουσα , με $D<0$ και $D \neq \square$. Άν O είναι τάξη διακρίνουσας D σε τετραγωνικό σώμα K , τότε $K=Q(\sqrt{D})$ και ισχύουν τα ακόλουθα :

1. **Αν $f(x,y)=ax^2+bxy+cy^2$ είναι πρωταρχική θετικά ορισμένη τετραγωνική μορφή διακρίνουσας D με $a \neq 0$, τότε το $aZ+(\frac{-b+\sqrt{D}}{2})Z$ είναι ακέραιο proper ιδεώδες**

της O με νόρμα ίση με a και μάλιστα , αν τ είναι η ρίζα του f , τότε $O=Z+\tau Z$ και

$aZ+(\frac{-b+\sqrt{D}}{2})Z = a(Z+\tau Z)$.

2. **Η απεικόνιση που στέλνει κάθε πρωταρχική θετικά ορισμένη τετραγωνική μορφή $f(x,y)=ax^2+bxy+cy^2$ διακρίνουσας D με $a\neq 0$ στο ακέραιο proper ιδεώδες $aZ+(\frac{-b+\sqrt{D}}{2})Z$ της τάξης O , επάγει ισομορφισμό ανάμεσα στην ομάδα κλάσεων τετραγωνικών μορφών C(D) και στην ομάδα κλάσεων ιδεωδών $C(O)$.**
3. **Ένας φυσικός αριθμός m παρίσταται από μία πρωταρχική θετικά ορισμένη μορφή f διακρίνουσας D αν και μόνο αν υπάρχει ακέραιο ιδεώδες a της O το οποίο να ανήκει στην κλάση της $C(O)$ που αντιστοιχεί στην κλάση της f στην C(D) - σύμφωνα με τον ισομορφισμό του 2 - με $N(a)=m$.**

<u>ΑΠΟΔΕΙΞΗ</u>

Κατ' αρχήν , το ότι $K=Q(\sqrt{D})$ προκύπτει από το 1 (c) της πρότασης 2.2.1.10.

<u>Για το 1</u> : Από ορισμό 2.2.3.5 έχουμε ότι η ρίζα της f είναι η $\tau = \frac{-b+\sqrt{D}}{2a}$. Έχουμε λοιπόν $K=Q(\sqrt{D}) \rightarrow \tau\in K$.

Θα δείξουμε ότι $K=Q(\tau)$ (Σ 2.2.3.7.1). Πράγματι ,

$\tau\notin R \rightarrow \tau\notin Q \rightarrow [Q(\tau) : Q]\geq 2$. Επίσης , $2 = [K : Q] = [K : Q(\tau)] \cdot [Q(\tau) : Q]$

και συνεπώς $[K : Q(\tau)] = 1$, πράγμα που σημαίνει ότι $K=Q(\tau)$.

Τώρα επειδή η f είναι πρωταρχική και το τ είναι ρίζα του $f(x,1)$, θα έχουμε ότι $Irr(\tau|Z)(x)=f(x,1)$.

Θα δείξουμε ότι $O = Z +a\tau Z$ (Σ 2.2.3.7.2). Πράγματι ,

Το λήμμα 2.2.3.3 μας δίνει ότι το $Z +a\tau Z$ είναι μια τάξη του K με διακρίνουσα D. Επειδή και η O έχει διακρίνουσα D θα έχουμε λόγω της πρότασης 2.2.1.12 ότι $O = Z +a\tau Z$.

Παρατηρούμε τώρα ότι το λήμμα 2.2.3.3 μας δίνει ότι το $Z+\tau Z$ είναι proper ιδεώδες της τάξης O , πράγμα που (λόγω του 5 των παρατηρήσεων 2.2.2.9) σημαίνει ότι και το $a(Z+\tau Z)$ είναι proper ιδεώδες της τάξης O. Όμως $\tau = \frac{-b+\sqrt{D}}{2a} \rightarrow a\tau = \frac{-b+\sqrt{D}}{2}$ και συνεπώς $a(Z +\tau Z) = aZ+(\frac{-b+\sqrt{D}}{2})Z$, οπότε έχουμε τελικά ότι το $aZ+(\frac{-b+\sqrt{D}}{2})Z$ είναι proper ιδεώδες της O.

Τέλος επειδή προφανώς $a(Z+\tau Z)\subseteq Z +a\tau Z=O$ έχουμε ότι το $aZ+(\frac{-b+\sqrt{D}}{2})Z$ είναι proper ακέραιο.

Στην συνέχεια δείχνουμε ότι $N(aZ+(\frac{-b+\sqrt{D}}{2})Z) = a$.

Έχουμε $N(aZ+(\frac{-b+\sqrt{D}}{2})Z) = N(a(Z+\tau Z)) = \#(\frac{O}{aZ+a\tau Z}) = \#(\frac{Z+a\tau Z}{aZ+a\tau Z}) = \#(\frac{Z}{aZ}) = a$ (αφού $a>0$).

<u>Για το 2</u> : Δείχνουμε κατ' αρχήν ότι η απεικόνιση $C(D) \rightarrow C(O)$ της εκφώνησης είναι καλά ορισμένη :

Αν $f(x,y)=ax^2+bxy+cy^2$, $g(x,y)=a'x^2+b'xy+c'y^2$ είναι κανονικά ισοδύναμες πρωταρχικές θετικά ορισμένες τετραγωνικές μορφές διακρίνουσας D με $a,a'\neq 0$ και ρίζες τ,τ' αντίστοιχα , τότε το λήμμα 2.2.3.6 μας δίνει ότι

υπάρχει $\lambda\in K$ με $\lambda\neq 0$ ώστε $\lambda(Z+\tau'Z) = Z+\tau Z$. Συνεπώς από το 1 έχουμε

$(Z+\tau'Z) \cdot (\lambda O) = Z+\tau Z$, πράγμα που σημαίνει ότι τα $Z+\tau'Z$, $Z+\tau Z$

ανήκουν στην ιδια κλάση στην C(D) , και συνεπώς λόγω του 1 , το ίδιο

θα συμβαίνει και με τα $a'Z+(\frac{-b'+\sqrt{D}}{2})Z$, $aZ+(\frac{-b+\sqrt{D}}{2})Z$. Τα f,g δηλαδή απεικονίζονται στο ίδιο στοιχείο της $C(\mathcal{O})$ και η απεικόνιση που μελετάμε είναι πράγματι καλά ορισμένη.

Δείχνουμε στην συνέχεια ότι η απεικόνιση $C(D) \to C(\mathcal{O})$ της εκφώνησης είναι " 1-1 " :

Αν οι εικόνες $aZ+(\frac{-b+\sqrt{D}}{2})Z$, $a'Z+(\frac{-b+\sqrt{D}}{2})Z$ των πρωταρχικών θετικά ορισμένων μορφών $f(x,y)=ax^2+bxy+cy^2$, $g(x,y)=a'x^2+b'xy+c'y^2$

ανήκουν στην ίδια κλάση της $C(\mathcal{O})$, τότε επειδή το 1 μας δίνει $aZ+(\frac{-b+\sqrt{D}}{2})Z = a(Z+\tau Z)$, $a'Z+(\frac{-b+\sqrt{D}}{2})Z = a(Z+\tau' Z)$, θα έχουμε τελικά από το λήμμα 2.2.3.6 ότι οι f,g είναι κανονικά ισοδύναμες και συνεπώς ανήκουν στην ίδια κλάση της C(D).

Θα δείξουμε τώρα ότι η απεικόνιση $C(D) \to C(\mathcal{O})$ της εκφώνησης είναι " επί " :

Έστω $\mathfrak{a}$ ένα proper κλασματικό ιδεώδες της τάξης $\mathcal{O}$. Ως proper , το $\mathfrak{a}$ θα είναι διάφορο του τετριμμένου ιδεώδους και συνεπώς η πρόταση 2.2.2.6 μας δίνει ότι το $\mathfrak{a}$ είναι Z-module με rank ίσο με 2. Έστω λοιπόν $\mathfrak{a}=uZ+vZ$, με $u,v\in K^*$. Επειδή $rank_Z(\mathfrak{a})=2$ θα έχουμε ότι τα $\frac{u}{v}$, $\frac{v}{u}$ δεν ανήκουν στο $R\cap K$. Όμως $\frac{v}{u} = \frac{1}{|\frac{u}{v}|}\overline{(\frac{u}{v})}$ και συνεπώς ένα ακριβώς από τα $\frac{u}{v}$, $\frac{v}{u}$ θα ανήκει στο $\mathbf{h}=\{z\in C \mid Im(z)>0\}$. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $\frac{v}{u}\in\mathbf{h}$. Θέτουμε $\tau := \frac{v}{u}\in\mathbf{h}$. Έστω ότι $Irr(\tau|Z)(x)=ax^2+bx+c$. Θεωρούμε τότε την μορφή $f(x,y)= ax^2+bxy+cy^2$.

Επειδή $MK\Delta(a,b,c)=1$, και $a>0$ (βλ . ορισμό του $Irr(\cdot|Z)$ στους συμβολισμούς) το 1 από το λήμμα 2.2.3.3 θα μας δώσει ότι η f είναι θετικά ορισμένη πρωταρχική μορφή. Επίσης από το 2 του ίδιου λήμματος , παίρνουμε ότι η f έχει διακρίνουσα ίση με την διακρίνουσα

της $\mathcal{O}=Z+a\tau Z$ η οποία είναι D και συνεπώς $f\in F_{pd}(D)$. Θα δείξουμε ότι η

$[f(x,y)]$ της C(D) αντιστοιχίζεται στο $\mathfrak{a}H(\mathcal{O})$ της $C(\mathcal{O})$. Πράγματι , η $[f(x,y)]$ αντιστοιχίζεται στο $aZ+(\frac{-b+\sqrt{D}}{2})Z$ και το τ είναι η ρίζα του f $(\tau\in\mathbf{h})$ οπότε από το 1 έχουμε ότι $aZ+(\frac{-b+\sqrt{D}}{2})Z=a(Z+\tau Z)$. Όμως $\mathfrak{a}H(\mathcal{O}) = (uZ+vZ)\,H(\mathcal{O}) = u(Z+\tau Z)H(\mathcal{O}) = a(Z+\tau Z)H(\mathcal{O})$ και έχουμε το

ζητούμενο.

Τέλος θα δείξουμε ότι η απεικόνιση $C(D) \to C(\mathcal{O})$ της εκφώνησης είναι ομομορφισμός :

Η σύνθεση Dirichlet δύο τετραγωνικών μορφών $f(x,y)=ax^2+bxy+cy^2$, $g(x,y)=a'x^2+b'xy+c'y^2$ διακρίνουσας D ορίστηκε ώς η μορφή

$F(x,y)=aa'x^2+Bxy+(\frac{B^2-D}{4aa'})y^2$, όπου B είναι τυχαία και μοναδική modulo 2aa' λύση του συστήματος $\left\{\begin{array}{l} B\equiv b(mod2a) \\ B\equiv b'(mod2a') \\ B^2\equiv D(mod4aa') \end{array}\right\}$. Οι εικόνες των f , g , F με την απεικόνιση της εκφώνησης είναι αντίστοιχα οι $aZ+(\frac{-b+\sqrt{D}}{2})Z$, $a'Z+(\frac{-b'+\sqrt{D}}{2})Z$, $aa'Z+(\frac{-B+\sqrt{D}}{2})Z$. Λόγω τώρα του πιο πάνω συστήματος ισοτιμιών έχουμε για $\Delta=\frac{-B+\sqrt{D}}{2}$ ότι $\Delta\equiv\frac{-b+\sqrt{D}}{2}(mod2a)$, $\Delta\equiv\frac{-b'+\sqrt{D}}{2}(mod2a')$, και συνεπώς οι εικόνες των f , g , F με την απεικόνιση της εκφώνησης είναι αντίστοιχα τα ιδεώδη $aZ+\Delta Z$, $a'Z+\Delta Z$, $aa'Z+\Delta Z$. Μένει να δείξουμε ότι $(aZ+\Delta Z)(a'Z+\Delta Z)=$ $=(aa'Z+\Delta Z)$. Πράγματι, $\Delta^2+B\Delta=\frac{B^2+D-2B\sqrt{D}}{4}+\frac{-B^2+B\sqrt{D}}{2}=\frac{-B^2+D}{4}$ και συνεπώς αφού το B είναι λύση του συστήματος ισοτιμιών θα έχουμε από την τελευταία ισοτιμία του συστήματος ότι $\Delta^2+B\Delta\equiv 0(modaa')$ (Σ 2.2.3.7.3) . Τώρα $(aZ+\Delta Z)(a'Z+\Delta Z)=$ $= aa'Z+a\Delta Z+a'\Delta Z+\Delta^2 Z$ οπότε από την Σ 2.2.3.7.3 θα έχουμε $(aZ+\Delta Z)(a'Z+\Delta Z)= aa'Z+a\Delta Z+a'\Delta Z+B\Delta Z$. Όμως από το λήμμα 2.2.3.4 έχουμε $MK\Delta(a,a',B)=1$ και έτσι $aZ+a'Z+BZ=Z$ (απλή άσκηση άλγεβρας) πράγμα που σημαίνει $\Delta Z= a\Delta Z+a'\Delta Z+B\Delta Z$ οπότε $(aZ+\Delta Z)(a'Z+\Delta Z)=$ $=aa'Z+\Delta Z$ και έχουμε τελειώσει.

Για το 3 : Πριν προχωρήσουμε στο κυρίως μέρος της απόδειξης θα κάνουμε πρώτα κάποιες παρατηρήσεις. Αν a είναι ακέραιο ιδεώδες της τάξης O , τότε και το σ(a) είναι ακέραιο ιδεώδες (όπου σ είναι η μιγαδική συζυγία) της O. Μάλιστα αν το a είναι proper τότε και το σ(a) είναι proper και μάλιστα $[a]^{-1}=[\sigma(a)]$ στην C(O). Πράγματι , το σ(O) είναι μία τάξη του K και το σ(a) είναι ακέραιο ιδεώδες της σ(O) . Από το 3 της πρότασης 2.2.1.8 όμως έχουμε σ(O)=O , και έτσι είναι ακέραιο ιδεώδες της O. Αν επιπλέον το a είναι proper , τότε προφανώς και το το σ(a) είναι proper της σ(O) , και συνεπώς και της O. Μάλιστα από την πρόταση 2.2.2.14 έχουμε $\sigma(a)\cdot a=N(a)\cdot O$ και συνεπώς $[a]^{-1}=[\sigma(a)]$.

Συνεχίζουμε τώρα με το κυρίως μέρος της απόδειξης.

($\rightarrow$) Έστω ότι ο φυσικός m παρίσταται από μία πρωταρχική θετικά ορισμένη μορφή f διακρίνουσας D. Ο m μπορεί να γραφεί $m=d^2a$ με $d,a\in N$ όπου ο a να παρίσταται από την f (βλ. παρατήρηση 1.2.1.8). Έχουμε ότι υπάρχουν $b,c\in Z$ ώστε η f είναι να είναι κανονικά ισοδύναμη με την μορφή $g(x,y)=ax^2+bxy+cy^2$ (βλ. πρόταση 1.2.1.9). Τώρα κανονικά ισοδύναμες μορφές έχουν την ίδια διακρίνουσα και έτσι $D_g=D<0$. Επίσης $a>0$ και συνεπώς από την πρόταση 1.2.1.16 έχουμε ότι η g είναι θετικά ορισμένη. Είναι επίσης πρωταρχική , λόγω του πορίσματος 1.2.1.6. Έχουμε λοιπόν ότι μέσω του ισομορφισμού $C(D)\rightarrow C(O)$ που ορίσαμε στο 2 η κλάση [g(x,y)] θα

απεικονίζεται στην κλάση του ιδεώδους $\mathfrak{a} = aZ+(\frac{-b+\sqrt{D}}{2})Z$ της O στην $C(O)$. Αν τ είναι η ρίζα της g , τότε από 2.2.3.5 έχουμε $\tau=\frac{-b+\sqrt{D}}{2a}$ και συνεπώς $\mathfrak{a} = aZ+\tau Z$. Από το 1 έχουμε ότι $O=Z+a\tau Z$ και ότι $\mathfrak{a}$ είναι ακέραιο ιδεώδες της O $aZ+(\frac{-b+\sqrt{D}}{2})Z$ με $N(\mathfrak{a}) = a$.

Έχουμε τώρα $m=d^2a=N(d)N(\mathfrak{a})=N(d\mathfrak{a})$ όπου προφανώς $[d\mathfrak{a}]=[\mathfrak{a}]$ στην $C(O)$. Συνοψίζοντας , έχουμε ότι ο m ισούται με την νόρμα του ακέραιου ιδεώδους $d\mathfrak{a}$ της O , και επίσης $[d\mathfrak{a}]=[\mathfrak{a}]$.

Αλλά το $[f(x,y)]=[g(x,y)] \in C(D)$ αντιστοιχεί στην κλάση $[\mathfrak{a}]= [d\mathfrak{a}]$ της $C(O)$ μέσω της $C(D) \to C(O)$, οπότε και έχουμε το ζητούμενο.

($\leftarrow$) Έστω ότι $N(\mathfrak{a})=m\in N$ όπου $\mathfrak{a}$ είναι ιδεώδες της O που ανήκει στην κλάση της εικόνας της $[f(x,y)]$ μέσω της $C(D) \to C(O)$. Θα δείξουμε ότι η f παριστά τον m. Πράγματι , αν γράψουμε $f(x,y)= =ax^2+bxy+cy^2$ και θέσουμε τ την ρίζα της f , τότε το $[f(x,y)]$ αντιστοιχίζεται (λόγω 1) στο ακέραιο ιδεώδες $aZ+(\frac{-b+\sqrt{D}}{2})Z=a(Z+\tau Z)$ νόρμας a της τάξης $O=Z+a\tau Z$. Έχουμε λοιπόν ότι $[\mathfrak{a}]=[a(Z+\tau Z)]$ στην $C(O)$ και συνεπώς θα υπάρχει $u\in O$ με $\mathfrak{a}=ua(Z+\tau Z)$ (Σ 2.2.3.7.4)

Εξάλλου τότε $aN(u) = N(a(Z+\tau Z))N(u) = N(ua(Z+\tau Z)) = N(\mathfrak{a}) = m \to m=aN(u)$ (Σ 2.2.3.7.5)

Τώρα επειδή το $\mathfrak{a}$ είναι ακέραιο και $O=Z+a\tau Z$, θα υπάρχουν (λόγω Σ 2.2.3.7.4) $p,q,r,s\in Z$ με $au=p+qa\tau$, $au\tau=r+sa\tau$. Οπότε $(p+qa\tau)\tau= r+sa\tau$. Όμως τ είναι ρίζα της f και έτσι $a\tau^2=-b\tau-c$, οπότε $(p+qa\tau)\tau= r+sa\tau \to p\tau+qa\tau^2=r+sa\tau \to p\tau-bq\tau-cq=r+sa\tau \to r+(sa+bq)\tau= -cq+p\tau$. Αλλά $\tau\notin R$ οπότε $r = -cq$ και $p=sa+bq$ (Σ 2.2.3.7.6). Έχουμε τώρα από την (Σ 2.2.3.7.5) ότι $m = aN(u) = \frac{N(au)}{a} = \frac{(p+qa\tau)\overline{(p+qa\tau)}}{a} = \frac{(p+qa\tau)(p+qa\bar{\tau})}{a}$. Εξάλλου $\tau=\frac{-b+\sqrt{D}}{2a}$ οπότε $\tau+\bar{\tau} = -\frac{b}{a}$, $\tau\cdot\bar{\tau} = \frac{c}{a}$ και συνεπώς $m = \frac{p^2 - \frac{pbqa}{a} + \frac{q^2a^2c}{a}}{a} = \frac{p^2 - pqb + q^2ca}{a}$.

Αντικαθιστώντας τέλος από την Σ 2.2.3.7.6 το p με sa+bq , θα πάρουμε m=f(s,q).

<u>ΑΣΚΗΣΗ</u> : Η αντίστροφη απεικόνιση της $C(D) \to C(O)$ είναι η εξής :

$[\mathfrak{a}] \to [\frac{1}{N(\mathfrak{a})}(ux-vy)(\bar{u}x-\bar{v}y)]$, όπου $\mathfrak{a}$ είναι proper ιδεώδες της O με $\mathfrak{a}=uZ+vZ$,$u,v\in C$

<u>2.2.3.8 ΠΑΡΑΤΗΡΗΣΗ</u> : Αν D διακρίνουσα , με $D<0|\neq\square$.τότε κάθε πρωταρχική τετραγωνική μορφή f διακρίνουσας D , που παριστά τουλάχιστο ένα φυσικό , είναι θετικά ορισμένη. (βλ. πρόταση 1.2.16)

<u>2.2.3.9 ΠΟΡΙΣΜΑ</u> : Ένας φυσικός αριθμός m παρίσταται από μία πρωταρχική μορφή f διακρίνουσας D<0,

$|D|\neq\square$ αν και μόνο αν υπάρχει ακέραιο ιδεώδες $\mathfrak{a}$ της O που να ανήκει στην κλάση της $C(O)$

στην οποία αντιστοιχεί στην κλάση της f στην C(D) - σύμφωνα με τον ισομορφισμό $C(D) \to C(O)$ του θεωρήματος 2.2.3.7 - με $N(\mathfrak{a})=m$.

(Το πόρισμα είναι άμεση συνέπεια του 3 του θεωρήματος 2.2.3.7 και της παρατήρησης 2.2.3.8)

<u>2.2.3.10 ΠΟΡΙΣΜΑ</u> : Αν $\mathbf{O}$ είναι τάξη σε φανταστικό τετραγωνικό σώμα και $m\in\mathbf{Z}-\{0\}$, τότε κάθε στοιχείο της $C(\mathbf{O})$ περιέχει ακέραιο proper ιδεώδες με νόρμα πρώτη προς το m.

<u>ΑΠΟΔΕΙΞΗ</u>

Άμεση συνέπεια του ισομορφισμού $C(D)\to C(\mathbf{O})$ του θεωρήματος 2.2.3.7 και της πρότασης 1.2.3.7

Παρακάτω θα αναφέρουμε τι ισχύει μεταξύ τάξεων και τετραγωνικών μορφών στην περίπτωση θετικής διακρίνουσας. Για λεπτομέρειες παραπέμπουμε στο βιβλίο του Cox : [COX] σελ. 142

<u>2.2.3.11 ΣΧΟΛΙΑ</u> : Ο ισομορφισμός $C(D)\to C(\mathbf{O})$ που αναφέρεται στο θεώρημα 2.2.3.7 για $D<0$, $|D|\neq\square$, δεν ισχύει γενικά για $D\in\mathbf{Z}$, $|D|\neq\square$. Πράγματι , ας θεωρήσουμε την περίπτωση D=12 στην οποία έχουμε $D\in\mathbf{Z}$, $|D|\neq\square$. Ισχύει $R_K=\mathbf{Z}[\sqrt{3}]$ και $d_K=12$, οπότε η τάξη $\mathbf{O}=R_K=\mathbf{Z}[\sqrt{3}]$ του τετραγωνικού σώματος $K=\mathbf{Q}(\sqrt{3})$ έχει διακρίνουσα 12. Ο $\mathbf{Z}[\sqrt{3}]$ είναι δακτύλιος μονοσήμαντης ανάλυσης και συνεπώς $h_K=1$, οπότε $\#C(\mathbf{O})=\#C(K)=1$. Όμως οι μορφές x^2-3y^2 , $-x^2+3y^2$ έχουν διακρίνουσα 12 και δεν είναι κανονικά ισοδύναμες

Πράγματι , αν ήταν , τότε θα υπήρχε πίνακας $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ της $sl(2,\mathbf{Z})$ με $u^2-3v^2=-x^2+3y^2$ για $\begin{pmatrix}u\\ v\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}$. Όμως τότε η παρατήρηση 1.2.1.5 θα μας δώσει $2ab-6cd=0$ και αφού $ad-bc=1$ (λόγω $A\in sl(2,\mathbf{Z})$) , θα έχουμε τελικά $4cd=1$ με $c,d\in\mathbf{Z}$ που είναι άτοπο.

Συνεπώς $\#C(D)>1$ και έτσι δεν είναι δυνατόν τα $C(D),C(\mathbf{O})$ να είναι ισόμορφα.

<u>2.2.3.12 ΟΡΙΣΜΟΣ</u> : 1. Έστω K τετραγωνικό σώμα και $\mathbf{O}$ μια τάξη του K. Με $H^+(\mathbf{O})$ θα συμβολίζεται το σύνολο $\{\mathbf{a}\mid\exists u\in\mathbf{O}: \mathbf{a}=u\mathbf{O}\text{ και }N(u)>0\}$. Είναι προφανές ότι το $H^+(\mathbf{O})$ είναι υποομάδα της $H(\mathbf{O})$. Η ομάδα πηλίκο $\frac{I(\mathbf{O})}{H^+(\mathbf{O})}$ θα συμβολίζεται $C^+(\mathbf{O})$ και θα ονομάζεται στενή ομάδα κλάσεων (strict class group , narrow class group) της $\mathbf{O}$.

2. Έστω D διακρίνουσα. Στο σύνολο $F(D)$ ορίζεται η σχέση $\sim$ ώς εξής : Για $f,g\in F(D)$,

$f\sim g$ αν και μόνο αν υπάρχει $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in sl(2,\mathbf{Z})$ ώστε για $\begin{pmatrix}u\\ v\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}$ να ισχύει $f(x,y)=(\det A)g(u,v)$. Η $\sim$ είναι σχέση ισοδυναμίας στο $F(D)$ και ονομάζεται "προσημασμένη ισοδυναμία" (signed equivalence). Η προσημασμένη ισοδυναμία είναι προφανώς και ισοδυναμία στο σύνολο των πρωταρχικών μορφών διακρίνουσας D και ορίζει εκεί ένα σύνολο πηλίκο. Το σύνολο πηλίκο αυτό θα συμβολίζεται $C_s(D)$ και θα ονομάζεται "προσημασμένη ομάδα κλάσεων"

(signed class group).

2.2.3.13 ΠΡΟΤΑΣΗ : (Σχέση $C^+(O)$ και $C(O)$) Αν O είναι τάξη τετραγωνικού σώματος K , τότε

1. **Αν συμβαίνει ένα εκ' των δύο ακόλουθων :**
   - **Το K είναι φανταστικό**
   - **Το K είναι πραγματικό και $\exists \varepsilon \in E(O)$ με $N(\varepsilon)=-1$**

   τότε $C(O)=C^+(O)$.
2. **Αν ο K είναι πραγματικό και δεν υπάρχει ενάδα του O με νόρμα -1 , τότε $|C^+(O)| = 2 \cdot |C(O)|$.**

2.2.3.14 ΠΡΟΤΑΣΗ : Έστω D διακρίνουσα. Τότε η $C_s(D)$ μπορεί να πάρει την δομή ομάδας.

2.2.3.15 ΘΕΩΡΗΜΑ : Αν K είναι τετραγωνικό σώμα αριθμών με τάξη O διακρίνουσας D , τότε

1. **Υπάρχει φυσικός ισομορφισμός $C(D) \cong C^+(O)$**
2. **Υπάρχει φυσικός ισομορφισμός $C_s(D) \cong C(O)$.**

2.2.4 ΙΔΕΩΔΗ ΠΡΩΤΑ ΠΡΟΣ ΤΟΝ ΟΔΗΓΟ

2.2.4.1 ΟΡΙΣΜΟΣ : Έστω O μια τάξη σε τετραγωνικό σώμα αριθμών K και a ακέραιο μη μηδενικό ιδεώδες της O. Αν m είναι ακέραιος αριθμός με $a+mO=O$, τότε το a θα λέγεται "πρώτο προς τον m".

2.2.4.2 ΛΗΜΜΑ : Έστω $(G,+)$ αβελιανή ομάδα με $|G|=n$. Προφανώς , ο πολλαπλασιασμός με $m\in N$ είναι ομομορφισμός. Ειδικότερα , τα ακόλουθα είναι ισοδύναμα :

1. **Ο πολλαπλασιασμός με $m\in N$ είναι ισομορφισμός**
2. **Ο πολλαπλασιασμός με $m\in N$ είναι επιμορφισμός**
3. **Ο πολλαπλασιασμός με $m\in N$ είναι μονομορφισμός**
4. **$MK\Delta(m,n)=1$.**

ΑΠΟΔΕΙΞΗ

Άμεση συνέπεια του θεμελιώδους θεωρήματος δομής πεπερασμένων αβελιανών ομάδων.

2.2.4.3 ΠΡΟΤΑΣΗ : Έστω O μια τάξη σε τετραγωνικό σώμα αριθμών K με $f=con(O)$.

1. **Αν a είναι ακέραιο ιδεώδες της O και $m\in Z$, τότε τα ακόλουθα είναι ισοδύναμα :**
   a. **Το a είναι πρώτο προς το m**
   b. **Ο πολλαπλασιασμός με m στην $\frac{O}{a}$ είναι ισομορφισμός.**
   c. **$(N(a),m)=1$.**
2. **Κάθε ακέραιο ιδεώδες της O , πρώτο προς το f είναι proper.**

ΑΠΟΔΕΙΞΗ

1. $a \leftrightarrow b$ Αν η απεικόνιση πολλαπλασιασμού με m στο O είναι ισομορφισμός , τότε θα είναι και επιμορφισμός , οπότε για κάθε $u\in O$, θα υπαρχει $v\in O$ με $mv+a=u+a$ και έτσι $u\in a+mO$. Συνεπώς $O\subseteq a+mO$ και έτσι αφού το a είναι ακέραιο θα έχουμε $O=a+mO$. Αν αντίστροφα $O=a+mO$, τότε για κάθε $u\in O$, θα υπαρχει $v\in O$ με $u\in mv+a \rightarrow mv+a=u+a$ και συνεπώς ο πολλαπλασιασμός με m είναι επιμορφισμός.Άρα από το λήμμα 2.2.4.2 είναι και ισομορφισμός.

   $b \leftrightarrow c$ Τώρα από το λήμμα 2.2.4.2 έχουμε ότι ο πολλαπλασιασμός με m στην ομάδα $(\frac{O}{a},+)$ είναι ισομορφισμός αν και μόνο αν $MK\Delta(N(a),m)=1$.

2. Αν a είναι ακέραιο ιδεώδες πρώτο προς το f , τότε εξ' ορισμού : $a+fO=O$. Επίσης αν $b\in K$ με $ba\subseteq a$ τότε $b\in R_K$.Πράγματι ,

   Το a είναι Z-module με rank 2 (βλ. προταση 2.2.2.6) και γράφοντας $a=uZ+vZ$ με $u,v\in K$ έχουμε λόγω του $ba\subseteq a$ ότι υπάρχει $A\in M_{2x2}(Z)$ με $b\begin{pmatrix}u\\v\end{pmatrix}=A\begin{pmatrix}u\\v\end{pmatrix}$.

   Τώρα $(bI_2-A)\begin{pmatrix}u\\v\end{pmatrix}=0$, όπου βέβαια $(u,v)\neq(0,0)$ και συνεπώς $\det(bI_2-A)=0$,

   οπότε το b είναι ρίζα του $\det(xI_2-A)\in Z[x]$, οπότε $b\in R_K$.

   Έχουμε λοιπόν $bO = b(a+fO) = ba+bfO \subseteq a+fR_K \subseteq O$ (γιατί a είναι ακέραιο και επίσης $O=Z+fR_K$.) Τελικά $bO \subseteq O$. Δείξαμε λοιπόν ότι $\{b\in K \mid ba\subseteq a\}\subseteq O$ και έτσι εξ' ορισμού 2.2.2.8 έχουμε ότι το a είναι proper.

2.2.4.4 ΠΑΡΑΤΗΡΗΣΕΙΣ : Αν O είναι μια τάξη σε τετραγωνικό σώμα αριθμών K με $f=con(O)$, τότε τα

ιδεώδη της $\mathbf{O}$ που είναι πρώτα προς το f βρίσκονται στο σύνολο $\mathbf{I(O)}$ των αντιστρεψίμων ιδεωδών της $\mathbf{O}$ και μάλιστα λόγω πολλαπλασιατικότητας της νόρμας (βλ. πρόταση 2.2.2.14) αποτελούν αβελιανή πολλαπλασιατική ημιομάδα. Με $\mathbf{I(O,f)}$ θα συμβολίζεται η πολλαπλασιαστική αβελιανή ομάδα που παράγεται από την ημιομάδα των ιδεωδών της $\mathbf{O}$ τα οποία είναι πρώτα προς το f . Με $\mathbf{H(O,f)}$, θα συμβολίζεται η υποομάδα της $\mathbf{I(O,f)}$ των κυρίων ιδεωδών. (Προφανώς από τους ορισμούς προκύπτει ότι $\mathbf{I(O,f) < I(O)}$ και ότι $\mathbf{H(O,f) = I(O,f)\cap H(O)}$.) Τέλος η ομάδα πηλίκο της $\mathbf{I(O,f)}$ modulo $\mathbf{H(O,f)}$ θα συμβολίζεται με $\mathbf{C(O,f)}$. Κάνοντας κατάχρηση συμβολισμού , για σκοπούς ευκολίας , θα συμβολίζουμε στην συνέχεια με $\mathbf{I(O,f)\cap O}$ το υποσύνολο των ακεραίων πρώτων πρός το f ιδεωδών του $\mathbf{I(O,f)}$ και όμοια με $\mathbf{I(R_K,f)\cap R_K}$ το σύνολο των ακεραίων πρώτων πρός το f ιδεωδών του $\mathbf{I_K(f)=I(R_K,f)}$.

<u>2.2.4.5 ΠΡΟΤΑΣΗ</u> : Έστω $\mathbf{O}$ τάξη διακρίνουσας D με $\mathbf{D<0}$ σε τετραγωνικό σώμα αριθμών K. Αν $\mathbf{f = cond(O)}$, τότε η κανονική ένθεση $\mathbf{I(O,f) \to I(O)}$ επάγει ισομορφισμό $\mathbf{C(O) \xrightarrow{\cong} C(O,f)}$ που δίνεται από την αντιστοιχία $\mathbf{a\cdot H(O) \to a_f\cdot H(O,f)\ \forall a\in O}$. όπου $\mathbf{a_f}$ είναι οποιοδήποτε ιδεώδες της $\mathbf{O}$ πρώτο προς το f που να ανήκει στην κλάση $\mathbf{[a]}$ του $\mathbf{a}$ στην $\mathbf{C(O)}$

<u>ΑΠΟΔΕΙΞΗ</u>

Από πόρισμα 2.2.3.10 έχουμε ότι κάθε κλάση της C(O) έχει ακέραιο ιδεώδες με νόρμα πρώτη προς το f.

Η κανονική ένθεση $I(O,f) \to I(O)$ επομένως , επάγει "επί" απεικόνιση $I(O,f) \to C(O)$. Ο πυρήνας της απεικόνισης αυτής είναι ακριβώς το $I(O,f)\cap H(O)$. Επειδή εξ' ορισμού $I(O,f)\cap H(O) = H(O,f)$, θα έχουμε ισομορφισμό $C(O,f) \xrightarrow{\cong} C(O)$, του οποίου ο αντίστροφος ισομορφισμός είναι ο αναφερόμενος στην εκφώνηση.

<u>2.2.4.6 ΠΡΟΤΑΣΗ</u> : Έστω τάξη $\mathbf{O}$ διακρίνουσας D σε τετραγωνικό σώμα αριθμών K. Έστω επίσης $\mathbf{f = cond(O)}$. Ισχύουν τα ακόλουθα :

1. **Αν $\mathbf{b}$ είναι ιδεώδες του $\mathbf{R_K}$ πρώτο πρός το f , τότε και το $\mathbf{b\cap O}$ είναι ιδεώδες της $\mathbf{O}$ πρώτο προς το f , και μάλιστα με νόρμα ίση με την νόρμα του $\mathbf{b}$. ($\mathbf{\#\frac{R_K}{b} = \#\frac{O}{b\cap O}}$)**
2. **Αν $\mathbf{a}$ είναι ιδεώδες της $\mathbf{O}$ πρώτο προς το f , τότε το $\mathbf{aR_K}$ είναι ιδεώδες του $\mathbf{R_K}$ πρώτο προς το f και μάλιστα με νόρμα ίση την νόρμα του $\mathbf{a}$. ($\mathbf{\#\frac{O}{a} = \#\frac{R_K}{aR_K}}$)**
3. **Τα $\mathbf{I(R_K,f)\cap R_K}$ και $\mathbf{I(O,f)\cap O}$ είναι πολλαπλασιαστικές ημιομάδες και οι ομάδες που παράγονται από αυτές είναι οι $\mathbf{I_K(f)}$, $\mathbf{I(O,f)}$ αντίστοιχα. Η απεικόνιση $\mathbf{F: I(R_K,f)\cap R_K \to I(O,f)\cap O}$ που σε κάθε ακέραιο ιδεώδες $\mathbf{b}$του $\mathbf{R_K}$ πρώτο προς τον f , αντιστοιχεί το ακέραιο , πρώτο προς το f ,ιδεώδες της $\mathbf{O}$: $\mathbf{b\cap O}$, είναι ισομορφισμός μεταξύ των ημιομάδων $\mathbf{I(R_K,f)\cap R_K}$ και $\mathbf{I(O,f)\cap O}$ και επάγει ισομορφισμό $\mathbf{I_K(f) \xrightarrow{\cong} I(O,f)}$. (Μάλιστα $\mathbf{F^{-1} : I(O,f)\cap O \to I(R_K,f)\cap R_K : F^{-1}(a)=aR_K}$.)**

<u>ΑΠΟΔΕΙΞΗ</u>

1. Αν $\mathfrak{b}$ είναι ιδεώδες του R_K πρώτο πρός το f , τότε κατ' αρχήν το $\mathfrak{b}\cap O$ είναι ακέραιο ιδεώδες της O. Από το 2 της πρότασης 2.2.4.3 , θα έχουμε το ζητούμενο αν η νόρμα του $\mathfrak{b}\cap O$ είναι ίση με την νόρμα του $\mathfrak{b}$. Αρκεί λοιπόν να δείξουμε ότι η απεικόνιση $\varphi : (\frac{O}{\mathfrak{b}\cap O},+) \to (\frac{R_K}{\mathfrak{b}},+) : u+\mathfrak{b}\cap O \to u+\mathfrak{b}$, $u\in O$, είναι ισομορφισμός. Πράγματι ,

   Κατ' αρχήν από το λήμμα 2.2.4.2 έχουμε ότι ο πολλαπαλασιασμός με f στο R_K είναι ισομορφισμός (αφού το $\mathfrak{b}$ είναι πρώτο προς το f). Αν $u\in R_K$ τότε υπάρχει $v\in R_K$ με $u=fv$ και έτσι $u+\mathfrak{b}=fv+\mathfrak{b}$ Όμως $f = \mathrm{cond}(O) = \#\frac{R_K}{O}$, και έτσι $fv\in O$, οπότε $fv+\mathfrak{b}\cap O \in \frac{O}{\mathfrak{b}\cap O}$ και $\varphi(fv+\mathfrak{b})=u+\mathfrak{b}$. Η απεικόνιση φ λοιπόν είναι "επι". Η φ όμως είναι προφανώς και ομομορφισμός πεπερασμένων ομάδων , οπότε είναι και ισομορφισμός.
2. Αν $\mathfrak{a}$ είναι ιδεώδες της O πρώτο προς το f , τότε κατ' αρχήν το $\mathfrak{a}R_K$ είναι ακέραιο ιδεώδες του R_K. Θα αποδείξουμε την σχέση $N(\mathfrak{a}R_K) = N(\mathfrak{a})$, που είναι η ζητούμενη , εφαρμόζοντας το 1. Παρατηρούμε κατ' αρχήν ότι επειδή $\mathfrak{a}+f\mathfrak{O}=O$ θα έχουμε $\mathfrak{a}R_K+fR_K \supseteq(\mathfrak{a}+f\mathfrak{O})R_K=OR_K=R_K \to \mathfrak{a}R_K+fR_K \supseteq R_K$. Εξάλλου προφανώς $\mathfrak{a}R_K+fR_K\subseteq R_K$, οπότε $\mathfrak{a}R_K+fR_K=R_K$ (Σ 2.2.4.6.1).
   Θα δείξουμε τώρα ότι $\mathfrak{a}R_K\cap O=\mathfrak{a}$ (Σ 2.2.4.6.2).

   Πράγματι , το $\mathfrak{a}R_K\cap O$ είναι ακέραιο ιδεώδες της O και προφανώς $\mathfrak{a}\subseteq\mathfrak{a}R_K\cap O$. Επίσης $f = \mathrm{cond}(O) = \#\frac{R_K}{O}$ και έτσι $fR_K\subseteq O$, οπότε

   $\mathfrak{a}R_K\cap O = (\mathfrak{a}R_K\cap O)O = (\mathfrak{a}R_K\cap O)(\mathfrak{a}+f\mathfrak{O}) = (\mathfrak{a}R_K\cap O)\mathfrak{a}+(\mathfrak{a}R_K\cap O)\, f\mathfrak{O} \subseteq \mathfrak{a}+f(\mathfrak{a}R_K\cap O) \subseteq$
   $\subseteq \mathfrak{a}+f\mathfrak{a}R_K\subseteq \mathfrak{a}+\mathfrak{a}O = \mathfrak{a}$.

   Τώρα η σχέση Σ 2.2.4.6.1 μας δίνει ότι το $\mathfrak{a}R_K$ είναι ιδεώδες του R_K πρώτο προς το f. Εφαρμόζοντας λοιπόν το 1 για $\mathfrak{b}=\mathfrak{a}R_K$, θα πάρουμε ότι $N(\mathfrak{a}R_K) = N(\mathfrak{a}R_K\cap O)$ και συνεπώς λόγω της σχέσης Σ 2.2.4.6.2
   θα ισχύει $N(\mathfrak{a}R_K) = N(\mathfrak{a})$.
3. Θα αποδείξουμε κατ' αρχήν ότι
   - $\mathfrak{a}R_K\cap O=\mathfrak{a}$, για κάθε ιδεώδες $\mathfrak{a}$ του O πρώτο προς το f (Σ 2.2.4.6.3)
   - $(\mathfrak{b}\cap O)R_K=\mathfrak{b}$, για κάθε ιδεώδες $\mathfrak{b}$ του R_K πρώτο προς το f (Σ 2.2.4.6.4)

   Πράγματι ,

   Η σχέση Σ 2.2.4.6.3 είναι ακριβώς η Σ 2.2.4.6.2 η οποία έχει ήδη αποδειχτεί. Όσο για την Σ 2.2.4.6.3 , έχουμε τα ακόλουθα : Για ιδεώδες $\mathfrak{b}$ του R_K πρώτο προς το f , το 1 μας δίνει ότι το $\mathfrak{b}\cap O$ είναι ιδεώδες του O πρώτο προς το f , οπότε $\mathfrak{b}\cap O + f\mathfrak{O} = O$. Έχουμε τώρα $\mathfrak{b} = \mathfrak{b}O = \mathfrak{b}(\mathfrak{b}\cap O + f\mathfrak{O}) = \mathfrak{b}(\mathfrak{b}\cap O)+f\mathfrak{b}O \subseteq R_K(\mathfrak{b}\cap O)+f\mathfrak{b} \to \mathfrak{b} \subseteq R_K(\mathfrak{b}\cap O)+f\mathfrak{b}$.Όμως $f = \mathrm{cond}(O) = \#\frac{R_K}{O} \to fR_K\subseteq O \to f\mathfrak{b}\subseteq fR_K\subseteq O$. Εξάλλου προφανώς $f\mathfrak{b}\subseteq\mathfrak{b}$, οπότε τελικά $f\mathfrak{b}\subseteq\mathfrak{b}\cap O$ και έτσι $\mathfrak{b} \subseteq R_K(\mathfrak{b}\cap O)+f\mathfrak{b} \subseteq R_K(\mathfrak{b}\cap O) + \mathfrak{b}\cap O \subseteq R_K(\mathfrak{b}\cap O) \to \mathfrak{b} \subseteq R_K(\mathfrak{b}\cap O)$.
   Τέλος το ότι $R_K(\mathfrak{b}\cap O) \subseteq \mathfrak{b}$ είναι προφανές και έτσι $(\mathfrak{b}\cap O)R_K=\mathfrak{b}$.

   Υπενθυμίζουμε ότι το $I_K(f)$ είναι η πολλαπλασιαστική ομάδα που παράγουν τα πρώτα ιδεώδη του K τα οποία δεν διαιρούν το fR_K (βλ. ορισμό 2.1.2.7). Όμως , τα πρώτα ιδεώδη του K τα οποία δεν διαιρούν το
   fR_K είναι ακριβώς τα πρώτα ιδεώδη του K , τα οποία είναι πρώτα προς το f. Η $I_K(f)$ επομένως , είναι η πολλαπλασιαστική ομάδα που παράγεται από το σύνολο
   $\{ \mathfrak{p} \triangleleft R_K \mid \mathfrak{p} =$ πρώτο ιδεώδες και πρώτο προς το f $\}$, οπότε η $I_K(f)$ θα είναι η πολλαπλασιαστική ομάδα που παράγεται από την ημιομάδα $\{ \mathfrak{a} \triangleleft R_K \mid \mathfrak{a} =$ πρώτο προς το f $\} = I(R_K,f) \cap R_K$. Επίσης , το $I(O,f)$ είναι εξ' ορισμού η ομάδα που παράγεται από την ημιομάδα $\{ \mathfrak{a} \triangleleft O \mid \mathfrak{a} =$ πρώτο προς το f $\} = I(O,f)\cap O$.

Θα δείξουμε ότι η απεικόνιση F που ορίστηκε στην εκφώνηση είναι ισομορφισμός των ημιομάδων $I(R_K,f)\cap R_K$ και $I(O,f)\cap O$, οπότε η F θα επεκτείνεται ισομορφικά και στις ομάδες που παράγονται από αυτές τις ημιομάδες , δηλαδή στις $I_K(f)$, $I(O,f)$ αντίστοιχα.

Για το "επί" :

Αν a είναι ιδεώδες του $I(O,f)\cap O$, δηλαδή ακέραιο ιδεώδες της O πρώτο προς το f , τότε το aR_K είναι , λόγω 2 , ιδεώδες του $I(R_K,f)\cap R_K$ (δηλαδή ακέραιο ιδεώδες του R_K πρώτο προς το f) και $F(aR_K)= aR_K\cap O = a$, λόγω Σ 2.2.4.6.3.

Για το "1-1" :

Αν b,b' είναι ιδεώδη του $I(R_K,f)\cap R_K$ (δηλαδή ακέραια ιδεώδη του R_K πρώτα προς το f), με $F(b)= F(b')$, τότε $b'= (b'\cap O)R_K =F(b')R_K= =F(b)R_K = (b\cap O)R_K =b$, λόγω Σ 2.2.4.6.4.

Για την ομομορφικότητα :

Επειδή έχουμε ήδη δείξει ότι η F είναι "1-1" και "επί" , μπορούμε να θεωρίσουμε την F^{-1} και να δείξουμε ότι είναι ομομορφισμός , οπότε και η F θα είναι ομομορφισμός. Έχουμε ,(βλ. απόδειξη του "επί") ότι για b πρώτο προς το f , ακέραιο ιδεώδες του R_K , ισχύει $F^{-1}(b)=bR_K$.
Αν λοιπόν b,b' είναι πρώτα προς το f , ακέραια ιδεώδη του R_K , τότε $F^{-1}(bb')=(bb')R_K=(bR_K)(b'R_K)=F^{-1}(b)F^{-1}(b')$.

2.2.4.7 ΛΗΜΜΑ : Αν K είναι τετραγωνικό σώμα αριθμών και $m\in Z$, $\alpha,\beta\in R_K$ με $\alpha\equiv\beta(\mathrm{mod} mR_K)$, τότε $N(\alpha)\equiv N(\beta)(\mathrm{mod} m)$.

ΑΠΟΔΕΙΞΗ

Αν η ομάδα Galois της $K|Q$ είναι $G(K|Q)=\{1,\sigma\}$, τότε (βλ. πρόταση 2.1.1.5) $\sigma(R_K)=R_K$, οπότε για $\alpha\equiv\beta(\mathrm{mod} mR_K)$ θα έχουμε $\sigma(\alpha)\equiv\sigma(\beta)(\mathrm{mod} mR_K)$ και συνεπώς $\alpha\sigma(\alpha)\equiv\beta\sigma(\beta)(\mathrm{mod} mR_K)\rightarrow N(\alpha)\equiv N(\beta)(\mathrm{mod} mR_K)$.

Οπότε υπάρχει $u\in R_K$ με $N(\alpha)-N(\beta)=mu$. Τώρα $[N(\alpha)-N(\beta)]\in Z\rightarrow mu\in Z$. Επειδή $R_K=Z\left[\frac{D_K+\sqrt{D_K}}{2}\right]=$

$=Z+\left[\frac{D_K+\sqrt{D_K}}{2}\right]Z$, αν θέσουμε $u=x+y\frac{D_K+\sqrt{D_K}}{2}$, $x,y\in Z$, τότε επειδή $mu\in Z$. και $\sqrt{D_K}\notin Z$, θα έχουμε $y=0$, οπότε $u\in Z$, και έτσι $N(\alpha)\equiv N(\beta)(\mathrm{mod} m)$.

2.2.4.8 ΛΗΜΜΑ : Αν K είναι τετραγωνικό σώμα αριθμών και O μία τάξη του K με οδηγό f , τότε για κάθε $\alpha\in R_K$, τα ακόλουθα είναι ισοδύναμα :

1. **Υπάρχει $a\in Z$ με $ΜΚΔ(a,f)=1$ ώστε $\alpha\equiv a(\mathrm{mod} fR_K)$.**
2. **$\alpha\in O$ και $ΜΚΔ(N(\alpha),f)=1$.**

ΑΠΟΔΕΙΞΗ

$1\rightarrow 2$ Έστω ότι υπάρχει $a\in Z$ με $ΜΚΔ(a,f)=1$ ώστε $\alpha\equiv a(\mathrm{mod} fR_K)$. Από το λήμμα 2.2.4.7 τότε , έχουμε $N(\alpha)=a^2(\mathrm{mod} f)\rightarrow ΜΚΔ(N(\alpha),f) =ΜΚΔ(a^2,f) = 1$ (αφού $ΜΚΔ(a,f)=1$). Επίσης $f = \mathrm{cond}(O) = = \#\frac{R_K}{O}$ και έτσι $fR_K\subseteq O$, οπότε $\alpha\equiv a(\mathrm{mod} fR_K)\rightarrow(\alpha-a)\in fR_K\rightarrow(\alpha-a)\in O$. Όμως $a\in Z\subseteq O$ και συνεπώς $\alpha\in O$.

$2\rightarrow 1$ Έστω $\alpha\in O$ και $ΜΚΔ(N(\alpha),f)=1$. Έχουμε $O=Z+fR_K$ (βλ. πρόταση 2.2.1.4) , οπότε $\alpha\in(Z+fR_K)$ και συνεπώς υπάρχει κάποιο $a\in Z$ με $\alpha\equiv a(\mathrm{mod} fR_K)$. Επίσης από το λήμμα 2.2.4.7 θα πάρουμε $N(\alpha)\equiv a^2(\mathrm{mod} f)$ οπότε επειδή $ΜΚΔ(N(\alpha),f)=1$, θα ισχύει $ΜΚΔ(a^2,f)=1\rightarrow ΜΚΔ(a,f)=1$.

2.2.4.9 ΘΕΩΡΗΜΑ : Αν Κ είναι τετραγωνικό φανταστικό σώμα αριθμών , και Ο μία τάξη του Κ με οδηγό

f , τότε υπάρχουν οι ακόλουθοι φυσικοί ισομορφισμοί :

$$C(O) \xrightarrow{\cong} C(O,f) \xrightarrow{\cong} \frac{I_K(f)}{H_{K,Z}(f)}$$

οι οποίοι δίνονται μέσω των αντιστοιχιών $a \cdot H(O) \to a_f \cdot H(O,f) \to (a_f R_K) \cdot H_{K,Z}(f)$ **,**$\forall a \in O$**.**

όπου με a_f **συμβολίζουμε τυχαίο πρώτο προς το f ιδεώδες της Ο το οποίο ανήκει στην** $[a] \in C(O)$**.**

ΑΠΟΔΕΙΞΗ

Από την πρόταση 2.2.4.5 έχουμε ότι η ένθεση $I(O,f) \to I(O)$, επάγει ισομορφισμό $C(O) \xrightarrow{\cong} C(O,f)$ ώστε κάθε κλάση ιδεώδους a της Ο να αντιστοιχίζεται στην κλάση τυχαίου πρώτου προς το f ιδεώδους a_f της Ο που να ανήκει στην κλάση [a] του a στην Ο. Μένει λοιπόν να αποδειχτεί ο ισομορφισμός $C(O,f) \xrightarrow{\cong} \frac{I_K(f)}{H_{K,Z}(f)} : b \cdot H(O,f) \to (bR_K) \cdot H_{K,Z}(f)$.Πράγματι , από την πρόταση 2.2.4.6 έχουμε ότι ο ισομορφισμός $P : I(O,f) \cap O \to I(R_K,f) \cap R_K : P(a)=aR_K$, των ημιομάδων $I(O,f) \cap O$, $I(R_K,f) \cap R_K$ επάγει ισομορφισμό $P' : I(O,f) \xrightarrow{\cong} I_K(f)$. Επειδή λοιπόν εξ' ορισμού $C(O,f) = \frac{I(O,f)}{H(O,f)}$, θα έχουμε το ζητούμενο αν δείξουμε ότι η υποομάδα H(O,f) της I(O,f) αντιστοιχείται μέσω του P' στην υποομάδα $H_{K,Z}(f)$ της $I_K(f)$. Πράγματι , η H(O,f) είναι η ομάδα των ιδεωδών της Ο που παράγεται από τα κύρια ιδεώδη της Ο που είναι πρώτα προς το f και συνεπώς (λόγω $a \leftrightarrow c$ του 1της πρότασης 2.2.4.3) η H(O,f) παράγεται από τα ιδεώδη της μορφής aO με $a \in O$ και $MK\Delta(N(a),f)=1$. Σύμφωνα λοιπόν τώρα με το λήμμα 2.2.4.8 , η H(O,f) θα είναι η ομάδα των ιδεωδών της Ο η οποία θα παράγεται από το σύνολο { aO | $a \in R_K$ και υπάρχει $\alpha \in Z$ με $MK\Delta(\alpha,f)=1$ ώστε $\alpha \equiv a (\mathrm{mod} f R_K)$ }. Το σύνολο όμως αυτό αντιστοιχείται μέσω της P' στο { aR_K | $a \in R_K$ και υπάρχει $\alpha \in Z$ με $MK\Delta(\alpha,f)=1$ ώστε $\alpha \equiv a (\mathrm{mod} f R_K)$ } το οποίο εξ' ορισμού είναι το $H_{K,Z}(f)$ (βλ. παρατήρηση 2.1.2.8).

2.2.5 ΥΠΟΛΟΓΙΣΜΟΣ ΤΟΥ ΑΡΙΘΜΟΥ ΚΛΑΣΣΕΩΝ

Στην παράγραφο αυτή αναφέρουμε για λογους πληρότητας μερικά χρήσιμα αποτελέσματα που αφορούν
αριθμούς κλάσεων τάξεων και τετραγωνικών μορφών. Για περισσότερες λεπτομέρειες παραπέμπουμε
στο : [COX] σελ. 146-149.

<u>2.2.5.1 ΘΕΩΡΗΜΑ</u> : Αν O είναι μία τάξη τετραγωνικού φανταστικού σώματος K , με οδηγό f , τότε

$$h_K \mid h(O) \text{ και ειδικότερα } h(O) = \frac{h_K \cdot f}{[R_K^* : O^*]} \prod_{\substack{p \mid f \\ p \in P}} \left(1 - \frac{1}{p} \cdot \left(\frac{d_K}{p}\right)_2\right).$$

<u>2.2.5.2 ΘΕΩΡΗΜΑ</u> (Siegel): Έστω D διακρίνουσα με D<0 , και m∈N.

1. **Υπάρχει φανταστικό τετραγωνικό σώμα K και τάξεις O , O' του K με διακρίνουσες D , m^2D αντίστοιχα , ώστε $O' \subseteq O$ και [O : O'] = m.**
2. **Αν K είναι φανταστικό τετραγωνικό σώμα K και τάξεις O , O' του K με διακρίνουσες D , m^2D αντίστοιχα ώστε $O' \subseteq O$ και [O : O'] = m , τότε**

$$h(m^2D) = \frac{h(D) \cdot m}{[O^* : O'^*]} \prod_{\substack{p \mid m \\ p \in P}} \left(1 - \frac{1}{p}\left(\frac{D}{p}\right)_2\right)$$

<u>2.2.5.3 ΘΕΩΡΗΜΑ</u> : Έστω K τετραγωνικό φανταστικό σώμα. Ισχύουν τα ακόλουθα :

1. $h(d_K) = \sum_{n=1}^{|d_K|-1} \left(n \cdot \left(\frac{d_K}{n}\right)_2\right)$.
2. $\lim_{d_K \to -\infty} \frac{\log[h(d_K)]}{\log|d_K|} = \frac{1}{2}$.
3. $\forall\, \varepsilon>0 \ , \ \exists\, c_\varepsilon>0 : \ h(d_K) > c_\varepsilon |d_K|^{\frac{1}{2}-\varepsilon}$.
4. $h(d_K) > \frac{1}{7000} \prod_{\substack{p \mid d_K \\ p \in P}} \left(1 - \frac{\left[2\sqrt{p}\right]}{p+1}\right) \log|d_K|$

<u>2.2.5.4 ΣΧΟΛΙΑ</u> : Το 2 του θεωρήματος 2.2.5.3 είναι γνωστο και ως θεώρημα του Siegel. Το 4 του ίδιου θεωρήματος είναι συνέπεια ενός σημαντικότατου αποτελέσματος των Gross και Zagier της δεκαετίας του 80.

§3 CLASS FIELD THEORY ΚΑΙ ΘΕΩΡΗΜΑ ΠΥΚΝΟΤΗΤΑΣ ΤΟΥ CEBOTAREV

Σε όλη την §3 δεν θα δοθούν αποδείξεις. Εκτός από τους απαραίτητους ορισμούς και τα σχόλια , θα γίνει απλή αναφορά των θεωρημάτων της Class field theory και του θεωρήματος πυκνότητας του Cebotarev. καθώς και των άμεσων εφαρμογών τους. Για αναλυτικές αποδείξεις των θεωρημάτων της παραγράφου 2.3.1 - οι οποίες σημειώνουμε ότι είναι αρκετά δύσκολες και μακροσκελείς- παραπέμπουμε στο βιβλίο του Janusz : [JANUSZ] κεφ. V. Μια σύντομη παρουσίαση της Class field theory υπάρχει στο βιβλίο του Cox : [Cox] σελ. 159-164 με πολύ καλές παραπομπές για τις αποδείξεις. Επίσης για τις αποδείξεις της παραγράφου 2.3.2 παραπέμπουμε στο : [Cox] σελ. 169-172.

2.3.1 CLASS FIELD THEORY

2.3.1.1 ΟΡΙΣΜΟΣ : Έστω K ένα αλγεβρικό σώμα αριθμών και $\mathfrak{m}$ ένα modulus του K. Μια υποομάδα P του $I_K(\mathfrak{m})$ θα λέγεται " υποομάδα ισοδυναμίας για το $\mathfrak{m}$ ", αν ισχύει $H_{K,1}(\mathfrak{m}) \subseteq P \subseteq I_K(\mathfrak{m})$.

Στην περίπτωση που η P είναι υποομάδα ισοδυναμίας για το $\mathfrak{m}$, η ομάδα πηλίκο $\frac{I_K(\mathfrak{m})}{P}$, θα ονομάζεται " γενικευμένη ομάδα κλάσεων ιδεωδών για το $\mathfrak{m}$ ".

2.3.1.2 ΣΧΟΛΙΑ : Το βασικό αποτέλεσμα της class field theory , το οποίο και θα φανεί στην συνέχεια είναι ότι για αλγεβρικό σώμα αριθμών K , οι γενικευμένες ομάδες κλάσεων ιδεωδών για τα διάφορα modulus του K είναι ακριβώς οι ομάδες Galois των αβελιανών επεκτάσεων του K. Στο αποτέλεσμα αυτό , κύριο ρόλο θα παίξει η απεικόνιση του Artin για αβελιανές επεκτάσεις του K η οποία και θα οριστεί παρακάτω.

2.3.1.3 ΠΡΟΤΑΣΗ : Έστω L/K αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών. Αν $\mathfrak{m}$ είναι ένα modulus του K διαιρέσιμο από όλους τους πρώτους του K (πεπερασμένους και άπειρους) που διακλαδίζονται στο L , τότε το σύμβολο του Artin $\left(\frac{L \mid K}{\cdot}\right)$, επεκτείνεται πολλαπλασιαστικά στο $I_K(\mathfrak{m})$ επάγοντας ομομορφισμό $I_K(\mathfrak{m}) \to G(L|K)$.

2.3.1.4 ΟΡΙΣΜΟΣ : Έστω L/K αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών και $\mathfrak{m}$ ένα modulus του K διαιρέσιμο από όλους τους πρώτους του K (πεπερασμένους και άπειρους) που διακλαδίζονται στο L. Η επέκταση του συμβόλου του Artin στο $I_K(\mathfrak{m})$, θα συμβολίζεται με $\Phi_{\frac{L}{K},\mathfrak{m}}$ ή πιο απλά $\Phi_{\mathfrak{m}}$ - όταν δεν υπάρχει περίπτωση σύγχυσης - .

2.3.1.5 ΘΕΩΡΗΜΑ ($1^{ο}$ θεώρημα της class field theory - Θεώρημα αντιστροφής του Artin) : Έστω L/K αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών. Αν $\mathfrak{m}$ είναι ένα modulus του K διαιρέσιμο από όλους τους πρώτους του K (πεπερασμένους και άπειρους) που διακλαδίζονται στο L , τότε ισχύουν τα ακόλουθα :

1. **Η απεικόνιση $\Phi_{\mathfrak{m}}$ του Artin είναι "επί".**

2. **Αν οι εκθέτες των πεπερασμένων πρώτων του K που διαιρούν το m είναι αρκετά μεγάλοι , τότε ο πυρήνας $Ker(\Phi_m)$ της Φ_m είναι υποομάδα ισοδυναμίας για το modulus m.**

2.3.1.6 ΣΧΟΛΙΑ : 1. Άμεση συνέπεια των θεωρημάτων 2.3.1.3 και 2.3.1.5 είναι ότι στην περίπτωση αβελιανής επέκτασης αλγεβρικών σωμάτων αριθμών L/K , και modulus m του K που διαιρείται από όλους τους πρώτους του K (πεπερασμένους και άπειρους) που διακλαδίζονται στο L με αρκετά μεγάλους εκθέτες , η ομάδα Galois G(L|K) της επέκτασης L/K είναι γενικευμένη ομάδα κλάσεων ιδεωδών για το m.

2. **Παρατηρούμε ότι για το modulus m του θεωρήματος 2.3.1.5 έχουμε υποθέσει ότι διαιρείται από όλους τους πρώτους του K που διακλαδίζονται στο L με αρκετά μεγάλους εκθέτες . Τέτοια moduli όμως υπάρχουν άπειρα και συνεπώς θα υπάρχουν και άπειρα moduli n ώστε το $Ker(\Phi_n)$ να είναι υποομάδα ισοδυναμίας για το n. Ωστόσο υπάρχει κάποιο modulus του K το οποίο είναι καλύτερο από τα άλλα , υπό την έννοια ότι έχει το λιγότερο δυνατό πλήθος διαιρετών ενώ διατηρεί την ιδιότητα η απεικόνιση του Artin για το modulus αυτό να έχει πυρήνα υποομάδα ισοδυναμίας. Το ακόλουθο θεώρημα θα ξεκαθαρίσει για τι ακριβώς μιλάμε.**

2.3.1.7 ΘΕΩΡΗΜΑ (Θεώρημα οδηγού) : Αν L/K είναι αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών ,

τότε υπάρχει modulus f του K μοναδικά ορισμένο από την επέκταση L/K , ώστε :

1. **Ένας πρώτος του K (πεπερασμένος ή άπειρος) διακλαδίζεται στο L αν και μόνο αν διαιρεί το f.**
2. **Αν m είναι modulus του K που περιέχει όλους τους πρώτους του K (πεπερασμένους και άπειρους) που διακλαδίζονται στο L , τότε το $Ker(\Phi_n)$ είναι υποομάδα ισοδυναμίας για το m αν και μόνο αν f|m.**

2.3.1.8 ΟΡΙΣΜΟΣ : Για αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών L/K , το μοναδικό modulus του K με τις ιδιότητες 1 και 2 του Θεωρήματος 2.3.1.7 , θα ονομάζεται "οδηγός" της επέκτασης L/K και θα συμβολίζεται με f(L|K).

2.3.1.9 ΣΧΟΛΙΑ : Το επόμενο θεώρημα που είναι και γνωστό ως "θεώρημα ύπαρξης" , έχει ως συνέπεια το γεγονός ότι κάθε γενικευμένη ομάδα κλάσεων ιδεωδών είναι ισόμορφη με ομάδα Galois κάποιας αβελιανής επέκτασης.

2.3.1.10 ΘΕΩΡΗΜΑ ($2^{ο}$ θεώρημα της class field theory) Έστω K αλγεβρικό σώμα αριθμών και m ένα modulus του K. Αν P είναι μια υποομάδα ισοδυναμίας για το m (δηλαδή , αν $H_{K,1}(m) \subseteq P \subseteq I_K(m)$) , τότε υπάρχει μοναδική αβελιανή επέκταση L του K ώστε το m να διαιρείται από όλους τους πρώτους του K που διακλαδίζονται στο L και επίσης $P = Ker(\Phi_{\frac{L}{K},m})$.

2.3.1.11 ΣΧΟΛΙΑ : Αν L/K είναι αβελιανή επέκταση , τότε για το modulus f(L|K) από τα σχόλια 2.3.1.6 εξάγουμε ότι η G(L|K) είναι υποομάδα ισοδυναμίας (για το f(L|K)). Αν πάλι P είναι υποομάδα ισοδυναμίας για κάποιο modulus m του K , τότε το θεώρημα 2.3.1.10 θα μας δώσει ότι η P είναι ισόμορφη με ομάδα Galois κάποιας αβελιανής επέκτασης του K. Με τα μέχρι τώρα λοιπόν αποτελέσματα φαίνεται αυτό που προείπαμε στα σχόλια 2.3.1.2 , ότι δηλαδή για αλγεβρικό σώμα αριθμών K , οι γενικευμένες ομάδες κλάσεων ιδεωδών για τα διάφορα modulus του K είναι ακριβώς οι ομάδες Galois των αβελιανών επεκτάσεων του K. Σαν εφαρμογή των παραπάνω θεωρημάτων αναφέρουμε την παρακάτω πρόταση 2.3.1.12 και το θεώρημα των Kronecker-Weber.

2.3.1.12 ΠΡΟΤΑΣΗ : Έστω L και M αβελιανές επεκτάσεις του αλγεβρικού σώματος αριθμών K. Τα ακόλουθα είναι ισοδύναμα :

- **$L \subseteq M$.**
- **Υπάρχει modulus m του K διαιρέσιμο από όλους τους πρώτους του K που διακλαδίζονται σε κάποιο από τα L,M ώστε :**

$$H_{K,1}(m) \subseteq \mathrm{Ker}(\Phi_{\frac{M}{K},m}) \subseteq \mathrm{Ker}(\Phi_{\frac{L}{K},m}).$$

2.3.1.13 ΘΕΩΡΗΜΑ (Kronecker-Weber) : Αν L είναι αλγεβρικό σώμα αριθμών και αβελιανή επέκταση του $\mathbb{Q}$, τότε υπάρχει $m \in \mathbb{N}$ με $L \subseteq \mathbb{Q}(\zeta_m)$, όπου ως συνήθως $\zeta_m = e^{2\pi i/m}$.

2.3.1.14 ΟΡΙΣΜΟΣ : Έστω K αλγεβρικό σώμα αριθμών και m ένα modulus του K. Επειδή η $H_{K,1}(m)$ είναι προφανώς μια υποομάδα ισοδυναμίας για το m (βλ. ορισμό 2.3.1.1) , από το θεώρημα ύπαρξης 2.3.1.10 έπεται ότι υπάρχει μοναδική αβελιανή επέκταση K_m του K ώστε κάθε διακλαδιζόμενος πρώτος του K στο K_m να διαιρεί το m , και επίσης $H_{K,1}(m) = \ker(\Phi_{\frac{K_m}{K},m})$. Το K_m θα ονομάζεται " σώμα ακτίνας κλάσης" (ray class field) για το modulus m. Το σώμα ακτίνας κλάσης για το modulus 1 θα ονομάζεται " Σώμα κλάσεως του Hilbert για το K" (Hilbert class field).

2.3.1.15 ΘΕΩΡΗΜΑ (Ιδιότητες του σώματος κλάσεων του Hilbert) :

1. **Αν L είναι το σώμα κλάσεων του Hilbert ενός αλγεβρικού σώματος αριθμών K**

   τότε :
   a. **$C(R_K) \cong G(L/K)$.**
   b. **Η επέκταση L/K είναι μη διακλαδιζόμενη.**
   c. **$f(L/K) = 1$.**
2. **Το σώμα κλάσεων του Hilbert ενός αλγεβρικού σώματος αριθμών είναι η**

μέγιστη αβελιανή μη διακλαδιζόμενη επέκταση του.

<u>2.3.1.16 ΠΟΡΙΣΜΑ</u> : Αν L/K είναι αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών , τότε ο οδηγός f(L/K)

είναι ο μέγιστος κοινός διαιρέτης όλων των moduli $\mathfrak{m}$ για τα οποία $L \subseteq K_{\mathfrak{m}}$.

2.3.2 ΘΕΩΡΗΜΑ ΠΥΚΝΟΤΗΤΑΣ ΤΟΥ CEBOTAREV

2.3.2.1 ΟΡΙΣΜΟΣ : Έστω K αλγεβρικό σώμα αριθμών και $S \subseteq P_o(K)$. Αν υπάρχει το

όριο $\lim_{x \to 1^+} \dfrac{\sum_{p \in S} N(p)^{-x}}{-\log(x-1)}$

τότε θα συμβολίζεται δ(S) και θα ονομάζεται " πυκνότητα Dirichlet " του S.

2.3.2.1 ΠΡΟΤΑΣΗ (Ιδιότητες πυκνότητας Dirichlet) : Έστω K αλγεβρικό σώμα αριθμών και $S,T \subseteq P_o(K)$.

1. **Το $\delta(P_o(K))$ υπάρχει και μάλιστα $\delta(P_o(K)) = 1$.**
2. **Αν $S \subseteq T$ και τα δ(S) , δ(T) υπάρχουν , τότε $\delta(S) \le \delta(T)$.**
3. **Αν το δ(S) υπάρχει , τότε $0 \le \delta(S) \le 1$.**
4. **Αν $S \cap T = \varnothing$ και τα δ(S) , δ(T) υπάρχουν , τότε $\delta(S \cup T) = \delta(S) + \delta(T)$.**
5. **Αν το S είναι πεπερασμένο , τότε δ(S) = 0.**
6. **Αν $S \overset{\bullet}{=} T$ (δηλαδή αν τα S , T διαφέρουν κατά πεπερασμένο πλήθος στοιχείων) και τα δ(S) , δ(T) υπάρχουν , τότε δ(S) = δ(T).**
7. **Αν θέσουμε $P_{o,1}(K)$ το σύνολο των πεπερασμένων πρώτων του K με βαθμό αδρανείας 1 και υπάρχει το δ(S) , τότε θα υπάρχει και το $\delta(S \cap P_{o,1}(K))$ και μάλιστα $\delta(S) = \delta(S \cap P_{o,1}(K))$.**

2.3.2.3 ΣΗΜΕΙΩΣΗ : Υπενθυμίζουμε από την στοιχειώδη αλγεβρική θεωρία αριθμών ότι αν L/K είναι Galois

επέκταση αλγεβρικών σωμάτων αριθμών και p είναι πεπερασμένος πρώτος του K μη διακλαδιζόμενος στο L με q,q' πεπερασμένους πρώτους του L πάνω από το p , τότε τα σύμβολα του Frobenius $\left[\frac{L|K}{q}\right]$ και $\left[\frac{L|K}{q'}\right]$ είναι συζυγή στοιχεία της G(L|K). Έτσι , γενικά το σύμβολο του Artin $\left[\frac{L|K}{p}\right]$ ορίζεται ως η κλάση συζυγίας

ενός από τα σύμβολα του Frobenius για κάποιο πρώτο του L πάνω από το p. Στην περίπτωση που η L/K είναι αβελιανή , τα σύμβολα του Frobenius για τους διάφορους πρώτους του L πάνω από το p θα ταυτίζονται , οπότε το σύμβολο του Artin θα είναι μονοσύνολο και έτσι θα μπορεί να ταυτιστεί με το μοναδικό του στοιχείο. Στην γενική περίπτωση πάντως το σύμβολο του Artin είναι κλάση συζυγίας.

2.3.2.4 ΘΕΩΡΗΜΑ (Πυκνότητας του Cebotarev) : Έστω L/K επέκταση Galois αλγεβρικών σωμάτων αριθμών και έστω $\sigma \in G(L|K)$. Αν με (σ) συμβολίσουμε την κλάση συζυγίας του σ

στην G(L|K) , τότε το σύνολο { $p\in P_o(K)$ | ο p δεν διακλαδίζεται στο L και $\left[\frac{L|K}{p}\right]=(\sigma)$ }

έχει πυκνότητα Dirichlet ίση με $\frac{\#(\sigma)}{[L:K]}$.

2.3.2.5 ΠΟΡΙΣΜΑ : Έστω L/K αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών. Το σύνολο των πεπερασμένων πρώτων του K που αναλύονται πλήρως στο L , έχει πυκνότητα Dirichlet $\frac{1}{[L:K]}$ και συνεπώς είναι άπειρο.

2.3.2.6 ΟΡΙΣΜΟΣ : Αν L/K είναι επέκταση αλγεβρικών σωμάτων αριθμών , τότε με $\tilde{spl}(L/K)$ ή με $\tilde{spl}(L/K)$

ή με $\tilde{spl}(\frac{L}{K})$, θα συμβολίζεται το σύνολο :

{ $p\in P_o(K)$ | ο p δεν διακλαδίζεται στο L και υπάρχει $q\in P_o(L)$ πάνω από το p, με $f\left(\frac{q}{p}\right)=1$ }

(Προφανώς αν η L/K είναι Galois , τότε $\tilde{spl}(L/K)=spl(L/K)$)

Επίσης με $\tilde{spl}(L)$ θα συμβολίζεται το $\tilde{spl}(L/Q)$

2.3.2.7 ΠΡΟΤΑΣΗ : Έστω L/K και M/K επεκτάσεις αλγεβρικών σωμάτων αριθμών. Ισχύουν τα ακόλουθα :

1. Αν M/K είναι Galois , τότε ισχύει η ισοδυναμία :

   " $L\subseteq M \leftrightarrow spl(M/K) \dot{\subseteq} spl(L/K)$ "
2. Αν L/K είναι Galois , τότε ισχύει η ισοδυναμία :

   " $L\subseteq M \leftrightarrow \tilde{spl}(M/K) \dot{\subseteq} spl(L/K)$ "

2.3.2.8 ΘΕΩΡΗΜΑ : Αν L/K και M/K είναι επεκτάσεις Galois αλγεβρικών σωμάτων αριθμών , τότε :

1. $L\subseteq M \leftrightarrow spl(M/K) \dot{\subseteq} spl(L/K)$.
2. $L=M \leftrightarrow spl(M/K) \dot{=} spl(L/K)$.

§4 RING CLASS FIELDS

2.4.1 RING CLASS FIELDS

2.4.1.1 ΣΧΟΛΙΑ : Έστω K τετραγωνικό σώμα αριθμών και O τάξη του K με f = cond(O). Από τον ορισμό 2.1.2.7 για τα $H_{K,1}(f)$, $H_{K,Z}(f)$ και από παρατήρηση 3 της 2.1.2.8 έχουμε ότι $H_{K,1}(f) \subseteq H_{K,Z}(f) \subseteq I_K(f)$. Συνεπώς , η $H_{K,Z}(f)$ είναι υποομάδα ισοδυναμίας για το modulus fR_K του K και η ομάδα $\frac{I_K(f)}{H_{K,Z}(f)}$ είναι γενικευμένη ομάδα κλάσεων ιδεωδών για το modulus fR_K του K (βλ. ορισμό 2.3.1.1). Έτσι στην περίπτωση που το K είναι φανταστικό , από το θεώρημα 2.2.4.7 θα έχουμε ότι η ομάδα C(O) είναι γενικευμένη ομάδα κλάσεων ιδεωδών για το modulus fR_K του K. Από την class field theory ξέρουμε ότι οι γενικευμένες ομάδες κλάσεων ιδεωδών είναι ισόμορφες μέσω της απεικόνισης του Artin με ομάδες Galois αβελιανών επεκτάσεων του K (βλ. σχόλια 2.3.1.9). Έτσι λοιπόν και στην περίπτωση της C(O) , θα βρούμε αβελιανή επέκταση του K (την οποία θα ονομάσουμε παρακάτω ring class field της O), με ομάδα Galois ισόμορφη με την C(O). Μάλιστα στην πρόταση 2.4.1.4 θα υπολογίσουμε και την απεικόνιση ισομορφισμού.

2.4.1.2 ΟΡΙΣΜΟΣ : Έστω K τετραγωνικό σώμα αριθμών και O τάξη του K με f = cond(O). Επειδή η ομάδα $H_{K,Z}(f)$ είναι υποομάδα ισοδυναμίας για το modulus fR_K του K (βλ. σχόλια 2.4.1.1) , το θεώρημα ύπαρξης 2.3.1.10 δίνει ότι υπάρχει μοναδική αβελιανή επέκταση L του K ώστε το modulus $m=fR_K$ του K να διαιρείται από όλους τους πρώτους του K που διακλαδίζονται στο L και επίσης να ισχύει $H_{K,Z}(f) \cong \mathrm{Ker}(\Phi_{\frac{L}{K},m})$. Το σώμα L θα ονομάζεται " ring class field " (σώμα κλάσης δακτυλίου) της τάξης O.

2.4.1.3 ΠΑΡΑΤΗΡΗΣΗ : Αν K είναι τετραγωνικό σώμα αριθμών , τότε από το 2 την παρατήρησης 2.1.2.8 και από τον ορισμό 2.3.1.11 προκύπτει ότι το σώμα κλάσεως του Hilbert είναι το ring class field της μέγιστης τάξης R_K.

2.4.1.4 ΠΡΟΤΑΣΗ (Ιδιότητες των ring class fields) : Έστω L το ring class field τάξης O τετραγωνικού σώματος αριθμών με cond(O)=f. Ισχύουν τα ακόλουθα :

1. **Κάθε πρώτος του K που διακλαδίζεται στο L διαιρεί το modulus fR_K του K.**
2. **Για K φανταστικό , η απεικόνιση του Artin επάγει ισομορφισμό**

$\frac{I_K(f)}{H_{K,Z}(f)} \xrightarrow{\cong} G(L|K)$ **ο οποίος με τη σειρά του επάγει ισομορφισμό**

$C(O) \xrightarrow{\cong} G(L|K)$ **που για** $m=fR_K$ **δίνεται από την αντιστοιχία** $a \to \Phi_{\frac{L}{K},m}(a_fR_K)$ **, όπου** a_f **είναι οποιοδήποτε ιδεώδες της** O **πρώτο προς το** f **που να ανήκει στην** $[a] \in C(O)$.

ΑΠΟΔΕΙΞΗ

1. Προκύπτει κατ' ευθείαν από τον ορισμό 2.4.1.2.
2. Κατ' αρχήν από 1 , το m διαιρείται από όλους τους πρώτους του K που διακλαδίζονται στο L.

   Ο ισομορφισμός $C(O) \xrightarrow{\cong} \frac{I_K(f)}{H_{K,Z}(f)}$ του θεωρήματος 2.2.4.7 δίνεται από την αντιστοιχία : $a \to (a_fR_K) \cdot H_{K,Z}(f)$, $\forall a \in O$ (όπου το a_f είναι τυχαίο ιδεώδες της O πρώτο προς το f που ανήκει στην [a]). Από το θεώρημα 2.3.1.5 τώρα έχουμε ότι η απεικόνιση του Artin $\Phi_{\frac{L}{K},m} : I_K(f) \to G(L|K)$: $a \to \Phi_{\frac{L}{K},m}(a)$, είναι επιμορφισμός και συνεπώς επειδή $H_{K,Z}(f) = \ker(\Phi_{\frac{L}{K},m})$ (βλ ορισμό 2.4.1.2) ,

   θα επάγει ισομορφισμό $\frac{I_K(f)}{H_{K,Z}(f)} \xrightarrow{\cong} G(L|K)$: $b \cdot H_{K,Z}(f) \to \Phi_{\frac{L}{K},m}(b)$, $\forall b \in I_K(f)$.

   Παίρνοντας λοιπόν την σύνθεση $C(O) \xrightarrow{\cong} \frac{I_K(f)}{H_{K,Z}(f)} \xrightarrow{\cong} G(L|K)$: $a \to \Phi_{\frac{L}{K},m}(a_fR_K)$

   θα έχουμε τον ζητούμενο ισομορφισμό $C(O) \cong G(L|K)$.

2.4.1.5 ΠΡΟΤΑΣΗ : Έστω O **τάξη σε φανταστικό τετραγωνικό σώμα K , με** $f = cond(O)$. **Άν** $m=fR_K$ **και "σ" είναι η μιγαδική συζυγία , τότε ισχύουν τα ακόλουθα :**

1. $\sigma(m)=m$ **και** $\sigma(H_{K,Z}(f)) = H_{K,Z}(f)$.
2. $\ker(\Phi_{\frac{\sigma(L)}{K},m}) = \ker(\Phi_{\frac{L}{K},m})$.

ΑΠΟΔΕΙΞΗ

1. Το ότι $\sigma(m)=m$, είναι άμεση συνέπεια τού ότι $\sigma(f)=f$ και του ότι $\sigma(R_K)=R_K$ (βλ. πρόταση 2.1.1.5). Επίσης

   Από παρατήρηση 2.1.2.8 έχουμε $H_{K,Z}(f) = < aR_K \mid a \in R_K , \exists i \in Z : " (i,m)=1$ και $a \equiv i (\mathrm{mod} fR_K) >$ και έτσι

   αν $aR_K \in H_{K,Z}(f)$, τότε $\exists i \in Z$ με $(i,m)=1$ και $a \equiv i (\mathrm{mod} fR_K)$. Έχουμε $\sigma(aR_K)=\sigma(a)R_K$ και $\sigma(a) \equiv i (\mathrm{mod} \sigma(fR_K))$

   $\to \sigma(a) \equiv i (\mathrm{mod} fR_K)$. Έτσι $\sigma(aR_K) \in H_{K,Z}(f)$ και συνεπώς $\sigma(H_{K,Z}(f)) \subseteq H_{K,Z}(f)$, οπότε και $\sigma(H_{K,Z}(f)) = H_{K,Z}(f)$.

2. Αρκεί να δείξουμε ότι $\ker(\Phi_{\frac{\sigma(L)}{K},m}) \subseteq \ker(\Phi_{\frac{L}{K},m})$ (αφού $\sigma^2=1$) και συνεπώς (λόγω του 1 και του ότι

   $\ker(\Phi_{\frac{L}{K},m}) = H_{K,Z}(f)$ αφού το L είναι το ring class field της O) αρκεί να δείξουμε ότι

$\ker(\Phi_{\frac{\sigma(L)}{K},m}) \subseteq \sigma(\ker(\Phi_{\frac{L}{K},m}))$. Επείδή η απεικόνιση του Artin $\Phi_{\frac{\sigma(L)}{K},m}$, είναι πολλαπλασιαστική επέκταση του συμβόλου του Artin $\left[\frac{\sigma(L)\mid K}{\cdot}\right]$, στο $I_K(m)$, θα έχουμε τελειώσει αν για p πεπερασμένο πρώτο του K που δεν διαιρεί το fR_K με $\left[\frac{\sigma(L)\mid K}{p}\right]=1$, ισχύει $p\in \sigma(\ker(\Phi_{\frac{L}{K},m}))$. Πράγματι, θα έχουμε ότι ο $\sigma(p)$ είναι πρώτος του $\sigma(K)=K$ και δεν διαιρεί το modulus $\sigma(fR_K)=fR_K$ (αφού το p δεν διαιρεί το fR_K). Επίσης

$\left[\frac{\sigma(L)\mid K}{p}\right]=1 \rightarrow \left[\frac{\sigma(\sigma(L))\mid \sigma(K)}{\sigma(p)}\right]=1 \rightarrow \left[\frac{L\mid K}{\sigma(p)}\right]=1$, και έχουμε ότι $\sigma(p)\in \ker(\Phi_{\frac{L}{K},m})$, πράγμα που σημαίνει ότι $p=\sigma(\sigma(p))\in\sigma(\ker(\Phi_{\frac{L}{K},m}))$ οπότε και έχουμε το ζητούμενο.

2.4.2 ΕΠΙΛΥΣΗ ΤΗΣ $p=x^2+ny^2$ ΓΙΑ ΟΛΑ ΤΑ $n\in\mathbb{N}$ ΕΚΤΟΣ ΠΕΠΕΡΑΣΜΕΝΟΥ ΠΛΗΘΟΥΣ

<u>2.4.2.1 ΛΗΜΜΑ</u> : Έστω Κ φανταστικό τετραγωνικό σώμα αριθμών και L/K μία Galois επέκταση αλγεβρικών σωμάτων αριθμών. Αν το "σ" συμβολίζει την μιγαδική συζυγία , τότε :

1. **Η επέκταση $L/\mathbb{Q}$ είναι Galois αν και μόνο αν σ(L)=L.**
2. **Αν το L είναι το σώμα κλάσεως του Hilbert για το Κ , τότε η επέκταση $L/\mathbb{Q}$ είναι Galois.**
3. **Αν η επέκταση $L/\mathbb{Q}$ είναι Galois , τότε**
   - **(a). $[L\cap\mathbb{R}:\mathbb{Q}]=[L:K]$, και η επέκταση $\frac{L\cap\mathbb{R}}{\mathbb{Q}}$ είναι Galois.**
   - **(b). Για κάθε στοιχείο u του $L\cap\mathbb{R}$ ισχύει η ισοδυναμία : " $L\cap\mathbb{R}=\mathbb{Q}(u)\leftrightarrow L=K(u)$".**

<u>ΑΠΟΔΕΙΞΗ</u>

1. ($\rightarrow$) Έστω ότι η επέκταση $L/\mathbb{Q}$ είναι Galois. Έστω ότι $K=\mathbb{Q}(\sqrt{m})$ (βλ πρόταση 2.1.1.5) με m<0. Υπάρχουν δύο εμφυτεύσεις του Κ στο $\mathbb{C}$. Η μία είναι η ταυτοτική απεικόνιση :1 και η άλλη η μιγαδική συζυγία :σ.

   Το σ(L) είναι υπέρσωμα του σ(K)=K. Θα δείξουμε ότι $\sigma(L)\subseteq L$ οπότε και θα έχουμε τελειώσει (αφού τότε $L=\sigma(\sigma(L))\subseteq\sigma(L)$). Έστω λοιπόν $w\in L$ και έστω $f(x)=Irr(w|\mathbb{Q})(x)$. Επειδή η $L/\mathbb{Q}$ είναι Galois , οι ρίζες του f θα ανήκουν στο L. Τώρα $f(w)=0\rightarrow\sigma(f(w))=0\rightarrow f(\sigma(w))=0$ (αφού $f(x)\in\mathbb{Q}(x)$). Άρα $\sigma(w)\in L$ και έτσι $\sigma(L)\subseteq L$.

   ($\leftarrow$) Αν $\sigma(L)=L$, τότε $\sigma_{|L}\in G(L|\mathbb{Q})$. Θα δείξουμε ότι το υπόσωμα της L του οποίου τα στοιχεία παραμένουν αναλλοίωτα από τους αυτομορφισμούς της $G(L|\mathbb{Q})$ είναι ακριβώς το $\mathbb{Q}$, οπότε εξ'ορισμού των επεκτάσεων Galois , θα έχουμε ότι η $L/\mathbb{Q}$ είναι Galois. Προφανώς τα στοιχεία του $\mathbb{Q}$ παραμένουν αναλλοίωτα από την $G(L|\mathbb{Q})$. Έστω τώρα $w\in L$ με $\tau(w)=w$, $\forall\tau\in G(L|\mathbb{Q})$. Επειδή το Κ είναι της μορφής $K=\mathbb{Q}(\sqrt{m})$ (βλ πρόταση 2.1.1.5) με m<0 , θα ισχύει $K=\mathbb{Q}(\sqrt{m})=\mathbb{Q}[\sqrt{m}]=\{x+y\sqrt{m}\mid x,y\in\mathbb{Q}\}$. Από την τελευταία σχέση φαίνεται εύκολα ότι $K\cap\mathbb{R}=\mathbb{Q}$ και συνεπώς για να έχουμε $w\in\mathbb{Q}$ που είναι και το ζητούμενο , αρκεί να δείξουμε ότι $w\in K\cap\mathbb{R}$. Έχουμε $\sigma_{|L}\in G(L|\mathbb{Q})$, οπότε $w=\sigma(w)$, και έτσι $w\in\mathbb{R}$. Επίσης επειδή το w παραμένει αναλλοίωτο από την $G(L/\mathbb{Q})$, θα παραμένει αναλλοίωτο και από την $G(L|K)$ (αφού $G(L|K)\subseteq G(L|\mathbb{Q})$). Όμως η L/K είναι Galois και έτσι τα στοιχεία του L που παραμένουν αναλλοίωτα από την $G(L|K)$ είναι ακριβώς τα στοιχεία του Κ. Θα έχουμε λοιπόν $w\in K$ και έτσι από τα παραπάνω $w\in K\cap\mathbb{R}=\mathbb{Q}$.

2. Αν το L είναι το σώμα κλάσεως του Hilbert για το Κ, τότε για να δείξουμε ότι η $L/\mathbb{Q}$ είναι Galois , αρκεί από το 1 να δείξουμε ότι σ(L)=L. Πράγματι , Το σ(L) είναι μη διακλαδιζόμενη αβελιανή απέκταση του σ(K)=K οπότε επειδή το L είναι η μέγιστη μη διακλαδιζόμενη επέκταση του Κ (βλ. θεώρημα 2.3.1.12) θα έχουμε

$\sigma(L)\subseteq L$. Όμως $[\sigma(L) : K] = [\sigma(L) : \sigma(K)] = [L : K]$ και έτσι $L=\sigma(L)$.

3. (a). Επειδή η L/Q είναι Galois , έχουμε από το 1 ότι $\sigma(L)=L$ και έτσι $\sigma_{|L}\in G(L|Q)$. Θεωρούμε την υποομάδα

$<\sigma_{|L}>$ της $G(L|Q)$ που παράγει η $\sigma_{|L}$. Προφανώς $<\sigma_{|L}> = \{ 1 , \sigma_{|L} \}$ και $L\cap R$ είναι το υπόσωμα του L των αναλλοίωτων στοιχείων του L από την $<\sigma_{|L}>$. Έχουμε τώρα $[L\cap R : Q] = \frac{[L : Q]}{[L : L\cap R]} =$

$= \frac{[L : K]\cdot[K : q]}{[L : L\cap R]}$. Θα δείξουμε ότι $[K : Q] = [L : L\cap R]$. Πράγματι , από θεωρία Galois έχουμε $[L : L\cap R] = \#G(L| L\cap R) = \#<\sigma_{|L}> = 2 = [K : Q]$. Συνεπώς από τα παραπάνω προκύπτει $[L\cap R : Q] = [L : K]$. Εξάλλου , το γεγονός ότι $2= [K : Q] = [L : L\cap R]$ συνεπάγεται ότι $[(G(L|Q) : G(L|L\cap R)] = 2$ και επομένως η $G(L|L\cap R)$ είναι κανονική υποομάδα της $G(L|Q)$, πράγμα που

σημαίνει ότι η επέκταση $L\cap R/Q$ είναι Galois.

(b). ($\rightarrow$) Αν $u\in L\cap R$ με $L\cap R =Q(u)$, τότε από το (a) έχουμε $[Q(u) : Q] = [Q(u)\cap R : Q] = [L : K] =$

$= [L : K(u)]\cdot[K(u) : K] =[L : K(u)]\frac{[K(u) : Q]}{[K : Q]} = [L : K(u)]\frac{[K(u) : Q(u)][Q(u) : Q]}{[K : Q]}$.

Όμως $[K :Q] = [K(u) : Q(u)] = 2$ και έτσι $[Q(u) : Q] =[L : K(u)]\cdot[Q(u) : Q] \rightarrow [L : K(u)] = 1 \rightarrow L=K(u)$.

($\leftarrow$) Αν $L=K(u)$ για $u\in L\cap R$, τότε από το (a) έχουμε $[K(u)\cap R : Q] = [K(u) : K]$, οπότε

$[K(u)\cap R : Q(u)]\cdot[Q(u) : Q] = \frac{[K(u) : Q]}{[K : Q]} = \frac{[K(u) : Q(u)][Q(u) : Q]}{[K : Q]}$, και επειδή $[K :Q] = [K(u) : Q(u)]$

θα έχουμε $[K(u)\cap R : Q(u)] =1$ συνεπώς $L\cap R = K(u)\cap R = Q(u)$.

<u>2.4.2.2 ΠΑΡΑΤΗΡΗΣΗ</u> : Από την πολλαπλασιαστικότητα του βαθμού αδρανείας και του δείκτη διακλάδωσης στα αλγεβρικά σώματα αριθμών έχουμε ότι αν M/L και L/K είναι επεκτάσεις Galois αλγεβρικών σωμάτων αριθμών και p είναι ένα πρώτο ιδεώδες του K , τότε τα ακόλουθα είναι ισοδύναμα :

- **Το p αναλύεται πλήρως στο M (δηλαδή $p\in spl(M/K)$).**
- **Το p αναλύεται πλήρως στο L (δηλαδή $p\in spl(L/K)$) και υπάρχει πρώτο ιδεώδες q του L πάνω από το p που αναλύεται πλήρως στο M (δηλαδή $q\in spl(M/L)$).**

<u>2.4.2.3 ΔΗΜΜΑ</u> : Έστω O τάξη φανταστικού τετραγωνικού σώματος K και L το ring class field της O. Έστω επίσης "σ" η μιγαδική συζυγία. Ισχύουν τα ακόλουθα :

1. **Η επέκταση L/Q είναι Galois με $\sigma_{|L}\in G(L|Q)$ και επίσης $\forall\tau\in G(L|K)$ ισχύει $\sigma_{|L}\cdot\tau\cdot\sigma_{|L} = \tau^{-1}$.**
2. **Αν $K=Q(\sqrt{-n})$ και $O=Z[\sqrt{-n}]$, τότε για κάθε p περιττό πρώτο αριθμό ισχύει η ισοδυναμία :**
   - **"$p\in spl(L)$" $\leftrightarrow$ "$\exists x,y\in Z : p=x^2+ny^2$"**

<u>ΑΠΟΔΕΙΞΗ</u>

1. Θα δείξουμε ότι σ(L)=L , όπου "σ" είναι η μιγαδική συζυγία.

Αν f=cond(O) , θεωρούμε το modulus m=fR$_K$ του K. Από πρόταση 2.4.1.5 έχουμε ker($\Phi_{\frac{\sigma(L)}{K},m}$) = ker($\Phi_{\frac{L}{K},m}$). Επίσης επειδή το m περιέχει τους πρώτους του K που διακλαδίζονται στο L (βλ. πρόταση 2.4.1.4) , το σ(m)=m (βλ πρόταση 2.4.1.5) θα περιέχει τους πρώτους του σ(K)=K (βλ πρόταση 2.1.1.5) που διακλάδίζονται στο σ(L) , έτσι η πρόταση 2.3.1.12 θα δώσει (αφού $H_{K,1}(m) \subseteq H_{K,\mathbf{Z}}(f) = \ker(\Phi_{\frac{L}{K},m})$, διότι το L είναι ring class field της O) ότι σ(L)⊆L. Ομοίως L=σ(σ(L))⊆σ(L) και έτσι L=σ(L).

Αφού σ(L)=L , το 1 του λήμματος 2.4.2.1 θα δώσει ότι η επέκταση L/Q είναι Galois και μάλιστα $\sigma_{|L} \in G(L|K)$.

Τώρα , έστω τ∈G(L|K). Από τον ισομορφισμό $C(O) \xrightarrow{\cong} G(L|K)$ που επάγει η απεικόνιση του Artin (βλ. πρόταση 2.4.1.4) , έχουμε ότι υπάρχει κλασματικό ιδεώδες a της O ώστε το a να αντιστοιχίζεται στο τ σύμφωνα με τον πιο πάνω ισομορφισμό. Μάλιστα αν a_f είναι ιδεώδες της O πρώτο προς το f που να ανήκει στην κλάση του a στην C(O) τότε η κλάση aH(O) του a στην C(O) αντιστοιχεί στο $\Phi_{\frac{L}{K},m}(a_f R_K)$ = τ.

Είναι προφανές τώρα ότι το $a^{-1}H(O)$ θα αντιστιχεί μέσω του $C(O) \xrightarrow{\cong} G(L|K)$ στο τ^{-1}. Παρατηρούμε όμως ότι $a_f+fO = O$ (αφού το a_f είναι πρώτο προς το f) και έτσι $\sigma(a_f+fO)=\sigma(O) \rightarrow \sigma(a_f)+\sigma(f)\sigma(O) = \sigma(O) \rightarrow \sigma(a_f)+fO=O$, οπότε το $\sigma(a_f)$ είναι πρώτο προς το f ιδεώδες της σ(O)=O (βλ. το III της πρότασης 2.2.1.8). Επίσης $\sigma(a)H(O) = a^{-1}H(O)$ (βλ. το 2 της πρότασης 2.2.2.14) και έτσι η κλάση $a^{-1}H(O)= \sigma(a)H(O)$ θα αντιστοιχεί μέσω του $C(O) \xrightarrow{\cong} G(L|K)$ στην $\Phi_{\frac{L}{K},m}(\sigma(a_f)R_K)$. Επειδή , όπως είπαμε προηγουμένως , το $a^{-1}H(O)$ θα αντιστιχεί μέσω του $C(O) \xrightarrow{\cong} G(L|K)$ στο τ^{-1} , θα έχουμε τελικά ότι $\Phi_{\frac{L}{K},m}(\sigma(a_f)R_K) = \tau^{-1}$. Συνεπώς $\Phi_{\frac{L}{K},m}(\sigma(a_f R_K)) = \tau^{-1}$ (βλ. το V της πρότασης 2.1.1.5). Από γνωστη ιδιότητα του συμβόλου του Artin και επειδή το $\Phi_{\frac{L}{K},m}$ αποτελεί επέκταση του στο $I_K(m)$, θα έχουμε $\sigma_{|L} \cdot (\Phi_{\frac{L}{K},m}(a_f R_K)) \cdot \sigma_{|L}^{-1} = \tau^{-1}$. Αλλά $\sigma^{-1}=\sigma$, και $\Phi_{\frac{L}{K},m}(a_f R_K) = \tau$, οπότε έχουμε $\sigma_{|L} \cdot \tau \cdot \sigma_{|L}=\tau^{-1}$.

2. Έστω $K=Q(\sqrt{-n})$ και $O=Z[\sqrt{-n}]$. Έστω επίσης p περιττός πρώτος. Διακρίνουμε τις περιπτώσεις

<u>1η Περίπτωση</u> : p|n.

Στην περίπτωση αυτή , από τον νόμο ανάλυσης σε τετραγωνικά σώματα αριθμών έχουμε ότι ο p δεν αναλύεται πλήρως στο K οπότε δεν θα αναλύεται πλήρως στο L. Επίσης προφανώς δεν υπάρχουν x,y∈Z με $p=x^2+ny^2$. Κανένα μέλος λοιπόν της αποδεικτέας ισοδυναμίας δεν είναι αληθές , οπότε η ισοδυναμία είναι αληθής.

<u>2η Περίπτωση</u> : p ∤ n.

Κατ' αρχήν από τον νόμο ανάλυσης σε τετραγωνικά σώματα (βλ. πρόταση 2.1.1.7) μπορούμε εύκολα να δούμε ότι οι πρώτοι αριθμοί που διακλαδίζονται σε τετραγωνικό σώμα , θα πρέπει να διαιρούν την διακρίνουσα του σώματος. Η διακρίνουσα της τάξης $O=Z[\sqrt{-n}]$ είναι -4n. Οπότε $-4n=f^2 d_K$. Επειδή p ∤ n , θα έχουμε p ∤ d_K και συνεπώς ο p δεν διακλαδίζεται στο K. Παρακάτω η $\overline{\cdot}$ θα εκφράζει την μιγαδική συζυγία.

Θα αποδείξουμε ότι οι ακόλουθες προτάσεις είναι ισοδύναμες

(a). $\exists x,y\in Z : p=x^2+ny^2$.

(b). $pR_K=\mathfrak{p}\cdot\bar{\mathfrak{p}}$, όπου $\mathfrak{p},\bar{\mathfrak{p}}$ είναι διαφορετικοί πρώτοι του K και $\mathfrak{p}$ είναι κύριο ιδεώδες του R_K της μορφής uR_K με $u\in O\subseteq R_K$.

(c). $pR_K=\mathfrak{p}\cdot\bar{\mathfrak{p}}$, όπου $\mathfrak{p},\bar{\mathfrak{p}}$ είναι διαφορετικοί πρώτοι του K και $p\in H_{K,Z}(f)$.

(d). $pR_K=\mathfrak{p}\cdot\bar{\mathfrak{p}}$, όπου $\mathfrak{p},\bar{\mathfrak{p}}$ είναι διαφορετικοί πρώτοι του K και $\left[\frac{L\mid K}{p}\right]=1$.

(e). $pR_K=\mathfrak{p}\cdot\bar{\mathfrak{p}}$, όπου $\mathfrak{p},\bar{\mathfrak{p}}$ είναι διαφορετικοί πρώτοι του K και $p\in spl(L/K)$..

(f). $p\in spl(L)$.

(a)→(b) Έστω $p=x^2+ny^2$ για $x,y\in Z$. Έχουμε $p=(x+\sqrt{-n}\,y)(x-\sqrt{-n}\,y)$. Θέτουμε $\mathfrak{p}=(x+\sqrt{-n}\,y)R_K$. Τότε $pR_K=\mathfrak{p}\cdot\bar{\mathfrak{p}}$. Τα $\mathfrak{p},\bar{\mathfrak{p}}$ έχουν νόρμα ίση με $N_{\frac{K}{Q}}(x+\sqrt{-n}\,y)=$ $=x^2+ny^2=p$, επομένως είναι πρώτα ιδεώδη του K. Επίσης επειδή ο p δεν διακλάδίζεται στο K έχουμε $\mathfrak{p}\neq\bar{\mathfrak{p}}$. Τέλος, το $\mathfrak{p}$ είναι κύριο ιδεώδες και $(x+\sqrt{-n}\,y)\in O=Z[\sqrt{-n}]$.

(b)→(a) Έστω $pR_K=\mathfrak{p}\cdot\bar{\mathfrak{p}}$, όπου $\mathfrak{p},\bar{\mathfrak{p}}$ είναι διαφορετικοί πρώτοι του K και $\mathfrak{p}$ είναι κύριο ιδεώδες του R_K της μορφής uR_K με $u\in O\subseteq R_K$. Γράφουμε $\mathfrak{p}=(x+\sqrt{-n}\,y)R_K$, οπότε $pR_k=\mathfrak{p}\cdot\bar{\mathfrak{p}}=(x+\sqrt{-n}\,y)(x-\sqrt{-n}\,y)R_K=(x^2+ny^2)R_K$. Συνεπώς $p=\varepsilon(x^2+ny^2)$, όπου ε είναι μονάδα του R_K. Όμως $n\in N$, οπότε $\varepsilon\in\{\pm1,\pm i,\pm\omega,\pm\omega^2\}$ και έτσι $p=x^2+ny^2$.

(b)→(c) Έστω $pR_K=\mathfrak{p}\cdot\bar{\mathfrak{p}}$, όπου $\mathfrak{p},\bar{\mathfrak{p}}$ είναι διαφορετικοί πρώτοι του K και $\mathfrak{p}$ είναι κύριο ιδεώδες του R_K της μορφής uR_K με $u\in O\subseteq R_K$. Γράφουμε $\mathfrak{p}=(x+\sqrt{-n}\,y)R_K$
Από τον ισομορφισμό του θεωρήματος 2.2.4.7, έχουμε ότι η εικόνα της κλάσης $\mathfrak{a}\cdot H(O)$ του ιδεώδους $\mathfrak{a}=uO$ της O είναι η $(\mathfrak{a}_fR_K)\cdot H_{K,Z}(f)$, όπου $\mathfrak{a}_f$ είναι τυχαίο ιδεώδες της O πρώτο πρός το f που ανήκει στην κλάση $\mathfrak{a}\cdot H(O)=H(O)$. Όμως η εικόνα του $\mathfrak{a}\cdot H(O)=H(O)$ είναι η $H_{K,Z}(f)$.

Πράγματι, το $\mathfrak{a}$ είναι κύριο ιδεώδες της O οπότε επειδή $\mathfrak{a}_f\in\mathfrak{a}\cdot H(O)$, θα έχουμε $\mathfrak{a}_f\in H(O,f)\rightarrow\mathfrak{a}_fH(O,f)=H(O,f)$ και συνεπώς τελικά μέσω του ισομορφισμού του θεωρήματος 2.2.4.7 το $\mathfrak{a}H(O)$ θα αντιστοιχιθεί στο $H_{K,Z}(f)$.

Έτσι $(\mathfrak{a}_fR_K)\in H_{K,Z}(f)$. Αν $\mathfrak{a}_f=vO$, $v\in O$, τότε $(\mathfrak{a}_fR_K)\in H_{K,Z}(f)\rightarrow(vR_K)\in H_{K,Z}(f)$ (αφού $O\subseteq R_K$). Έτσι $\mathfrak{p}=uR_K\in(vR_K)H_{K,Z}(f)=H_{K,Z}(f)\rightarrow\mathfrak{p}\in H_{K,Z}(f)$.

(c)→(b) Έστω $pR_K=\mathfrak{p}\cdot\bar{\mathfrak{p}}$, όπου $\mathfrak{p},\bar{\mathfrak{p}}$ είναι διαφορετικοί πρώτοι του K και $p\in H_{K,Z}(f)$. Γράφουμε $\mathfrak{p}=uR_K$ με $u\in R_K$. Από τους ισομορφισμούς του θεωρήματος 2.2.4.7 έχουμε ότι υπάρχει ιδεώδες $\mathfrak{a}$ της O ώστε κάθε ιδεώδες $\mathfrak{a}_f$ της O πρώτο προς το f που να ανήκει στην $\mathfrak{a}\cdot H(O)$ να δίνει $(\mathfrak{a}_f\cdot R_K)\,H_{K,Z}(f)=\mathfrak{p}\cdot H_{K,Z}(f)=H_{K,Z}(f)$. Θα δείξουμε κατ' αρχήν ότι μπορουμε να εκλέξουμε το $\mathfrak{a}_f$ ώστε $\mathfrak{a}_fR_K\neq R_K$

Πράγματι, αν $\mathfrak{a}_f=R_K$, τότε θεωρούμε $m\in N$ με $(m,f)=1$.

Το ιδεώδες $m\mathfrak{a}_f$ της O είναι πρώτο προς το f (βλ. πρόταση 2.2.4.3) και ανήκει στην $\mathfrak{a}\cdot H(O)$ (αφού το ίδιο κάνει και η $\mathfrak{a}_f$). Επίσης $(m\mathfrak{a}_f)R_K=fR_K\neq R_K$.

Παίρνουμε λοιπόν εξ' αρχής $\mathfrak{a}_fR_K\neq R_K$. Από τον ισομορφισμό

$C(O,f)\xrightarrow{\cong}\frac{I_K(f)}{H_{K,Z}(f)}$ που αναφέρεται στο θεώρημα 2.2.4.7 και λόγω του

ότι το H(O,f) (ουδέτερο στοιχείο της C(O,f)) αντιστοιχεί στο $H_{K,\mathfrak{Z}}(f)$ (ουδέτερο στοιχείο της $\frac{I_K(f)}{H_{K,\mathfrak{Z}}(f)}$) έχουμε ότι $a_f H(O,f)=H(O,f)$. Γράφουμε $a_f=vO$, $v\in O\subseteq R_K$ και έχουμε $(uR_K)\in(vR_K)H_{K,\mathfrak{Z}}(f)$ οπότε υπάρχει $w\in R_K$ με $p=uR_K=(vR_K)(wR_K)$. Επειδή το p είναι πρώτο ιδεώδες του R_K , από μονοσήμαντη ανάλυση θα έχουμε ότι κάποιο από τα vR_K , wR_K είναι το R_K. Αλλά $vR_K\neq R_K$ και έτσι $wR_K=R_K$ οπότε έχουμε $p=vR_K$ με $v\in O$ και έχουμε το ζητούμενο.

(c)→(d) Έστω $pR_K=p\cdot\bar{p}$, όπου $p,\bar{p}$ είναι διαφορετικοί πρώτοι του K και $p\in H_{K,\mathfrak{Z}}(f)$. Ο ισομορφισμός $\frac{I_K(f)}{H_{K,\mathfrak{Z}}(f)} \xrightarrow{\cong} G(L|K)$ που επάγει η απεικόνιση του Artin θα μας δώσει ,αφού $p\in H_{K,\mathfrak{Z}}(f)$, ότι $\Phi_{\frac{L}{K},m}(p)=1$, για $m=fR_K$. Επειδή p είναι ακέραιο , θα έχουμε $\left[\frac{L\mid K}{p}\right]=1$.

(d)→(c) Έστω $pR_K=p\cdot\bar{p}$, όπου $p,\bar{p}$ είναι διαφορετικοί πρώτοι του K και $\left[\frac{L\mid K}{p}\right]=1$. Έχουμε $-4n=f^2d_K$ και συνεπώς αφού ο p είναι περιττος και $p\nmid n$ θα έχουμε $p\nmid f$. Τώρα $N(p)=p$ και έτσι $(N(p),f)=1$. Είναι εύκολο να δει κανείς τώρα ότι $p\in I_K(f)$ (Αν $p|fR_K$ τότε $N(p)\mid N(fR_K)\rightarrow N(p)|f^2$ πράγμα άτοπο.). Μπορούμε λοιπόν για $m=fR_K$ να θεωρήσουμε το $\Phi_{\frac{L}{K},m}(p)$. Έχουμε : $\left[\frac{L\mid K}{p}\right]=1\rightarrow$ $\Phi_{\frac{L}{K},m}(p)=1$. Το $H_{K,\mathfrak{Z}}(f)$ είναι το ουδέτερο στοιχείο της $\frac{I_K(f)}{H_{K,\mathfrak{Z}}(f)}$, και το 1 είναι το ουδέτερο στοιχείο της G(L|K). Έτσι ισομορφισμός $\frac{I_K(f)}{H_{K,\mathfrak{Z}}(f)} \xrightarrow{\cong} G(L|K)$ που επάγει η απεικόνιση του Artin $\Phi_{\frac{L}{K},m}$ θά αντιστοιχίζει το $H_{K,\mathfrak{Z}}(f)$ στο 1. Επειδή λοιπόν $\Phi_{\frac{L}{K},m}(p)=1$ θα έχουμε $p\cdot H_{K,\mathfrak{Z}}(f)=H_{K,\mathfrak{Z}}(f)\rightarrow p\in H_{K,\mathfrak{Z}}(f)$.

(d)↔(e) Από στοιχειώδη αλγεβρική θεωρία αριθμών έχουμε ότι για αβελιανή επέκταση N/M αλγεβρικών σωμάτων αριθμών και u πρώτο μη διακλαδιζόμενο ιδεώδες του R_M ισχύει "$\left[\frac{N\mid M}{u}\right]=1\leftrightarrow u\in spl(N/M)$". Η ζητούμενη ισοδυναμία είναι τώρα προφανής.

(e)↔(f) Από τον νόμο ανάλυσης σε τετραγωνικά σώματα αριθμών (βλ. πρόταση 2.1.1.7) έχουμε ότι
" $p\in spl(K/Q)$ " ↔ " $pR_K=p\cdot\bar{p}$, όπου $p,\bar{p}$ είναι διαφορετικοί πρώτοι του K "
Η ισοδυναμία (e)↔(f)είναι τώρα προφανής λόγω της παρατήρησης 2.4.2.2

<u>2.4.2.4 ΛΗΜΜΑ</u> : Έστω K φανταστικό τετραγωνικό σώμα και L/K Galois επέκταση αλγεβρικών σωμάτων αριθμών. Ισχύουν τα ακόλουθα :

1. **Υπάρχει πραγματικός αλγεβρικός ακέραιος α_o ώστε $L=K(\alpha_o)$.**
2. **Αν α είναι πραγματικός αλγεβρικός ακέραιος ώστε $L=K(\alpha)$, τότε για $f(x)=Irr(\alpha|Q)(x)$ ιαχύουν τα ακόλουθα :**

- **$f(x) = Irr(\alpha|K)(x)$.**
- **Κάθε πρώτος αριθμός p που δεν διαιρεί την διακρίνουσα D_f του f ικανοποιεί την ακόλουθη ισοδυναμία :**

" $p \in spl(L)$" $\leftrightarrow$ " $\left(\frac{d_K}{p}\right)_2 = 1$ και η $f(x) \equiv 0 (mod p)$ είναι επιλύσιμη στο Z"

ΑΠΟΔΕΙΞΗ

1. Το $L \cap R$ είναι προφανώς αλγεβρικό σώμα αριθμών με δακτύλιο ακεραίων αλγεβρικών τον $R_{L\cap R} = R_L \cap R_R$. Η επέκταση $L\cap R/Q$ είναι πεπερασμένη και διαχωρίσιμη , άρα και απλή. Θα δείξουμε ότι υπάρχει $\alpha_o \in R_{L\cap R}$ με $L \cap R = Q(\alpha_o)$. Πράγματι ,

Η $L\cap R/Q$ είναι απλή οπότε υπάρχει $\alpha \in L \cap R$ με $L \cap R = Q(\alpha)$. Έστω ότι $Irr(\alpha|Q)(x) = a_o+a_1x+a_2x^2 \ldots a_{n-1}x^{n-1}+x^n$ με $a_o,a_1,\ldots,a_{n-1} \in Q$.

Άρα $a_o+a_1\alpha+a_2\alpha^2 \ldots a_{n-1}\alpha^{n-1}+\alpha^n = 0$. Γράφοντας $a_t = \frac{p_t}{q_t}$, t=0,1,2,,,n-1 όπου p_t,q_t είναι πρώτοι μεταξύ τους ακέραιοι αριθμοι και πολλαπλασιάζοντας με q^n , όπου $q = ΕΚΠ(q_1,q_2,\ldots,q_{n-1})$, θα πάρουμε $(\alpha q)^n + a_{n-1}q(\alpha q)^{n-1} + \ldots + a_2q^{n-2}(\alpha q)^2 + a_1q^{n-1}(\alpha q) +$

$+ a_oq^n = 0$, όπου βέβαια $x^n + (a_{n-1}q)x^{n-1} + \ldots + (a_2q^{n-2})x^2 + (a_1q^{n-1})x + (a_oq^n) \in Z[x]$.

Θέτουμε λοιπόν $\alpha_o = \alpha q$, οπότε $L \cap R = Q(\alpha) = Q(\alpha_o)$ και ο α_o είναι ακέραιος αλγεβρικός ,

δηλαδή $\alpha_o \in R_{L\cap R}$.

Από το 3 τώρα του λήμματος 2.4.2.1 έχουμε ότι $L = K(\alpha_o)$ και επειδή ο α_o είναι πραγματικός αλγεβρικός ακέραιος , έχουμε το ζητούμενο.

2. Έστω α πραγματικός αλγεβρικός ακέραιος με $L = K(\alpha)$ και έστω $f(x)= Irr(\alpha|Q)(x) \in Z[x]$. Έχουμε κατ'αρχήν

ότι $\alpha \in L \cap R$ και ειδικότερα $\alpha \in R_{L\cap R}$. Επίσης 3 του λήμματος 2.4.2.1 μας δίνει $L \cap R = Q(\alpha)$. Το f(x) ως πολυώνυμο του Q(x) είναι και πολυώνυμο του K(x). Θα δείξουμε ότι deg(f)=[L : K] οπότε επειδή το f έχει

ρίζα το α και L=K(α) θα έχουμε ότι $f(x) = Irr(\alpha|K)(x)$. Πράγματι ,

Επειδή $L \cap R = Q(a)$ και $f(x)= Irr(\alpha|Q)(x)$, θα έχουμε ότι $deg(f)=[L\cap R : Q]$. Όμως αφού $L=K(\alpha)$, το 3 του λήμματος 2.4.2.1 θα μας δώσει $[L\cap R : Q] = [L : K]$ και έχουμε το ζητούμενο.

Δείξαμε λοιπόν ότι $f(x) = Irr(\alpha|K)(x)$. Έστω τώρα πρώτος αριθμός p που δεν διαιρεί την διακρίνουσα D_f του f. Επειδή $p \nmid D_f$, το f(x) ειναι διαχωρίσιμο modulo p (δηλαδή είναι διαχωρίσιμο σαν πολυώνυμο του

$Z_p[x]$).

($\rightarrow$) Έστω $p \in spl(L)$. Εξ' ορισμού λοιπόν , το pZ αναλύεται πλήρως στο L , οπότε θα αναλύεται πλήρως και στο K (βλ παρατήρηση 2.4.2.2). Από το νόμο ανάλυσης στα τετραγωνικά σώματα αριθμών (βλ. πρόταση 2.1.1.7) έχουμε ότι $\left(\frac{d_K}{p}\right)_2 = 1$. Έστω τώρα p ένα πρώτο ιδεώδες του K πάνω από το pZ. Επείδή το pZ αναλύεται πλήρως στο K , ο βαθμός αδρανείας $f\left(\frac{p}{pZ}\right)$ στην

επέκταση K/Q θα είναι ισός με 1. Όμως το Z_p μέσω προβολής , εμφυτεύεται στο $\frac{R_K}{p}$ όπου εξ'ορισμού $f\left(\frac{p}{pZ}\right)=[\frac{R_K}{p}:Z_p]$ και έτσι η προαναφερόμενη ένθεση $Z_p\to\frac{R_K}{p}$ είναι ισομορφισμός σωμάτων. Αφού λοιπόν το f(x) ειναι διαχωρίσιμο modulo p θα είναι και διαχωρίσιμο modulo p. Επίσης επειδή $p\in spl(L)$, θα έχουμε ότι και ο p αναλύεται πλήρως στο L και από τον νόμο ανάλυσης της πρότασης 2.1.1.9 έχουμε ότι το f(x) έχει degf- το πλήθος ρίζες στο $\frac{R_K}{p}$,οπότε η f(x)≡0(modp) είναι επιλύσιμη στο Z λόγω του ισομορφισμού που επάγει η ένθεση $Z_p\to\frac{R_K}{p}$.

(←) Έστω $\left(\frac{d_K}{p}\right)_2=1$ και η f(x)≡0(modp) επιλύσιμη στο Z. Από νόμο ανάλυσης στα τετραγωνικά σώματα (βλ. πρόταση 2.1.1.7) , έχουμε ότι το pZ αναλύεται πλήρως στο K. Ο βαθμός αδρανείας $f\left(\frac{p}{pZ}\right)$ είναι ίσος επομένως με 1. Έτσι $f\left(\frac{p}{pZ}\right)=[\frac{R_K}{p}:Z_p]=1\to$ η ένθεση $Z_p\to\frac{R_K}{p}$ είναι ισομορφισμός σωμάτων. Επειδή λοιπόν f(x)≡0(modp) επιλύσιμη στο Z θα έχουμε ότι και f(x)≡0(modp) επιλύσιμη στο R_K. Επίσης το f είναι διαχωρίσιμο στο Z_p , άρα είναι διαχωρίσιμο και στο $\frac{R_K}{p}$. Λόγω του ότι η f(x)≡0(modp) είναι επιλύσιμη στο R_K και επειδή η L/K είναι επέκταση Galois,

το 2 της πρότασης 2.1.1.9 δίνει ότι το p αναλύεται πλήρως στο L. Έχουμε λοιπόν το ιδεώδες pZ το οποίο

αναλύεται πλήρως στο K και το ιδεώδες p του K πάνω από το pZ το οποίο διακλαδίζεται πλήρως στο L.

Η παρατήρηση 2.4.2.3 επόμενως θα δώσει ότι $p\in spl(L)$.

<u>2.4.2.5 ΘΕΩΡΗΜΑ</u> : Έστω $n\in N$ και έστω $K=Q(\sqrt{-n})$. Υπάρχει ανάγωγο μονικό πολυώνυμο $f_n(x)$ βαθμού h(-4n) ώστε για κάθε περιττό πρώτο αριθμό p που δεν διαιρεί την διακρίνουσα του f_n να ισχύει η παρακάτω ιδοδυναμία :

" $\exists x,y\in Z : p=x^2+ny^2$ " ↔ " $\left(\frac{-n}{p}\right)_2=1$ και η $f_n(x)\equiv 0(modp)$ έχει λύση στο Z " (Σ 2.4.2.5)

Επίσης σαν f_n μπορεί να εκλεγεί οποιοδήποτε ανάγωγο πολυώνυμο πανω από το Q πραγματικού αλγεβρικού ακεραίου α , ώστε το K(α) να είναι το ring class field της τάξης $Z[\sqrt{-n}]$ του τετραγωνικού φανταστικού σώματος K.

Τέλος , αν f(x) είναι μονικό πολυώνυμο βαθμού h(-4n) του Z[x] ώστε η ισοδυναμία Σ 2.4.2.5 να ικανοποιείται για κάθε p περιττό πρώτο που δεν διαιρεί την διακρίνουσα του f , τότε το f είναι ανάγωγο πολυώνυμο πάνω από το K και είναι το ανάγωγο πολυώνυμο πάνω από το K κάποιου στοιχείου b ώστε το K(b) να είναι το ring class field της τάξης $Z[\sqrt{-n}]$ του K.

<u>ΑΠΟΔΕΙΞΗ</u>

Έχουμε $n\in N$ και $K=Q(\sqrt{-n})$. Έστω L το ring class field της τάξης $Z[\sqrt{-n}]$ του K. Από το 1 του λήμματος 2.4.2.3 έχουμε ότι η επέκταση L/Q είναι Galois , οπότε από το λήμμα 2.4.2.4 έχουμε ότι υπάρχει πραγματικός αλγεβρικός ακέραιος α_o , ώστε $L=K(\alpha_o)$. Θέτουμε $f_n(x)=Irr(a_o|K)(x)$. Από το λήμμα 2.4.2.4 πάλι έχουμε ότι κάθε πρώτος αριθμός που δεν διαιρεί την διακρίνουσα του f_n ικανοποιεί την ακόλουθη

ισοδυναμία : " $p\in spl(L)$ " $\leftrightarrow$ " $\left(\frac{-n}{p}\right)_2=1$ και η $f_n(x)\equiv 0(\mathrm{mod}p)$ έχει λύση στο Z " (Σ 2.4.2.5)

Όμως από το 2 του λήμματος 2.4.2.3 έχουμε ότι για κάθε περιττό πρώτο αριθμό p ισχύει η ακόλουθη ισοδυναμία " $p\in spl(L)$ " $\leftrightarrow$ " $\exists x,y\in Z : p=x^2+ny^2$ " (Σ 2.4.2.6).

Οι σχέσεις Σ 2.4.2.5 και Σ 2.4.2.6 μας δίνουν τώρα ότι για κάθε περιττό πρώτο p που δεν διαιρεί την διακρίνουσα του f_n ισχύει η ισοδυναμία Σ 2.4.2.5 που αναφέρεται στην εκφώνηση του θεωρήματος.

Επίσης ο βαθμός του f_n είναι h(-4n) διότι κατ' αρχήν η διακρίνουσα της τάξης $Z[\sqrt{-n}]$ είναι -4n (απλή επαλήθευση) και έτσι $C(Z[\sqrt{-n}])\cong C(-4n)$ (βλ. θεώρημα 2.2.3.7). Επίσης $f_n(x)=\mathrm{Irr}(a_o|K)(x)$, $L=K(a_o)$ και $[L:K]=\#G(L|K)=\#C(O)=\#C(-4n)=h(-4n)$ (βλ. πρόταση 2.4.1.4).

Παρατηρούμε από την παραπάνω αποδεικτική διαδικασία ότι σαν f_n μπορεί να εκλεγεί οποιοδήποτε ανάγωγο πολυώνυμο πανω από το Q πραγματικού αλγεβρικού ακεραίου α , ώστε το K(α) να είναι το ring class field της τάξης $Z[\sqrt{-n}]$ του τετραγωνικού φανταστικού σώματος K. Θα αποδείξουμε τώρα την - κατά κάποιο τρόπο - μοναδικότητα των πολυωνύμων f_n που αναφέρεται στο θεώρημα. Έστω λοιπόν f(x) μονικό πολυώνυμο του Z[x] βαθμού h(-4n) ώστε η ισοδυναμία Σ 2.4.2.5 να ικανοποιείται για κάθε p περιττό πρώτο που δεν διαιρεί την διακρίνουσα του f. Θα δείξουμε ότι το f είναι ανάγωγο πολυώνυμο πάνω από το K και είναι το ανάγωγο πολυώνυμο πάνω από το K κάποιου στοιχείου b ώστε το K(b) να είναι το ring class field της τάξης $Z[\sqrt{-n}]$ του K.

Έστω g(x) ένας ανάγωγος παράγοντας του f(x) πάνω από το K[x] και έστω u μία ρίζα του g(x). Θέτουμε M=K(u). Επειδή το u είναι ρίζα του g(x) , θα είναι και ρίζα του f(x) και συνεπώς το u θα είναι αλγεβρικός ακέραιος (αφού το f(x) είναι μονικό πολυώνυμο του Z[x]).

Θα αποδείξουμε στην συνέχεια τα ακόλουθα :

(α). $spl(L)\overset{\bullet}{=}\{ p\in P \mid p\in spl(K) \text{ και } f(x)\equiv 0(\mathrm{mod}p) \text{ επιλύσιμη στο } Z \}$.

(β). $\tilde{spl}(M)\overset{\bullet}{\subseteq} spl(L)$.

(γ). $L = M$.

Για το (α) : Κατ' αρχήν από τον νόμο ανάλυσης σε τετραγωνικά σώματα αριθμών έχουμε ότι

$spl(Q(\sqrt{-n}))-\{2\}=\{ p\in P^* \mid \left(\frac{-n}{p}\right)_2=1\}$ (βλ. πρόταση 2.1.1.7) και συνεπώς

$spl(K)=spl(Q(\sqrt{-n}))\overset{\bullet}{=}\{ p\in P \mid \left(\frac{-n}{p}\right)_2=1\}$. Έτσι θα ισχύει ότι

$\{ p\in P \mid p\in spl(K) \text{ και } f(x)\equiv 0(\mathrm{mod}p) \text{ επιλύσιμη στο } Z \}\overset{\bullet}{=}$

$\overset{\bullet}{=}\{ p\in P \mid \left(\frac{-n}{p}\right)_2=1 \text{ και } f(x)\equiv 0(\mathrm{mod}p) \text{ επιλύσιμη στο } Z \}$.

Λόγω λοιπόν της Σ 2.4.2.5 έχουμε ότι $\{ p\in P \mid p\in spl(K) \text{ και } f(x)\equiv 0(\mathrm{mod}p) \text{ επιλύσιμη στο } Z \}$

$\overset{\bullet}{=}$

$\overset{\bullet}{=} spl(L)$ που είναι και το ζητούμενο.

Για το (β) : Αν $p\in \tilde{spl}(M)$, τότε το p δεν διακλαδίζεται στο M και υπάρχει πρώτο ιδεώδες q του R_M ώστε $f\left(\frac{q}{pZ}\right)=1$. Θέτουμε $p=q\cap R_K$, οπότε από πολλαπλασιαστικότητα των βαθμών αδρανείας έχουμε $f\left(\frac{p}{pZ}\right)=1$. Όμως το pZ δεν διακλαδίζεται στο M , άρα δεν διακλαδίζεται ούτε στο K.

Επειδή τώρα η επέκταση K/Q είναι Galois , θα έχουμε λόγω του ότι $f\left(\frac{p}{pZ}\right)=1$ ότι $p\in spl(K)$

Τώρα $g(u)=0\rightarrow f(u)=0$, οπότε $u\in R_M$. Η $f(x)\equiv 0(\mathrm{mod}q)$ είναι επομένως επιλύσιμη στο R_M.

Συνεπώς επειδή $[\frac{R_M}{q} : \frac{Z}{pZ}] = f\left(\frac{q}{pZ}\right) = 1$, ο μονομορφισμός $\frac{Z}{pZ} \to \frac{R_M}{q}$ που επάγει η εμφύτευση $Z_p \to R_M$ είναι ισομορφισμός. Έτσι λοιπόν και η $f(x) \equiv 0 (\mathrm{mod} p)$ θα είναι επιλύσιμη στο Z. Συνοψίζοντας έχουμε ότι $p \in \{ q \in P \mid q \in spl(K)$ και $f(x) \equiv 0 (\mathrm{mod} q)$ επιλύσιμη στο $Z \}$, οπότε το (α) μας δίνει ότι $\tilde{spl}(M) \subseteq spl(L)$.

Για το (γ) : Η επέκταση L/Q είναι Galois (βλ. λήμμα 2.4.2.3) , οπότε το 2 της πρότασης 2.3.2.7 μας δίνει λόγω του (β) ότι $L \subseteq M$. Τώρα $[L : K] = h(-4n)$ (αφού $L = K(a_o)$ και ο βαθμός του $f_n(x) = Irr(a_o|K)(x)$ είναι $h(-4n)$), οπότε επειδή $L \subseteq M$, θα ισχύει :
$h(-4n) = [L : K] \leq [M : K] = deg(g) \leq deg(f) = h(-4n)$ και συνεπώς $[L : K] = [M : K]$, πράγμα που σημαίνει ότι M = L.

Δείξαμε λοιπόν ότι L=M , επομένως $deg(f) = h(-4n) = [L : K] = [M : K] = [K(u) : K] = deg(g)$, που σημαίνει (λόγω του ότι το g διαιρεί το f) ότι $f(x) = g(x)$. Αφού το g(x) εκλέκτηκε ανάγωγος παράγοντας του f(x) στο K[x] με ρίζα το u , θα έχουμε ότι $f(x) = Irr(u|K)(x)$. Επίσης το L=M=K(u) είναι το ring class field της τάξης $Z[\sqrt{-n}]$ του K.

<u>2.4.2.6 ΣΧΟΛΙΑ</u> : Για λόγους πληρότητας αναφέρουμε ότι ισχύει ανάλογο θεώρημα με το 2.4.2.5 για την κύρια μορφή διακρίνουσας D με D<0 και D≡1(mod4). Για λεπτομέρειες παραπέμπουμε στο βιβλίο του [COX].

§5 ΕΦΑΡΜΟΓΕΣ ΤΩΝ RING CLASS FIELDS ΣΕ ΣΥΓΚΕΚΡΙΜΕΝΑ ΠΑΡΑΔΕΙΓΜΑΤΑ

2.5.1 ΥΠΟΛΟΓΙΣΜΟΣ ΤΩΝ RING CLASS FIELDS ΤΩΝ ΤΑΞΕΩΝ $Z[\sqrt{-14}]$, $Z[\sqrt{-27}]$ ΚΑΙ $Z[\sqrt{-64}]$

2.5.1.1 ΛΗΜΜΑ : Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών και $u \in R_K$. Αν $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες του R_K και ν μία λύση της εξίσωσης $x^2=u$ με $L=K(v)$, τότε ισχύουν τα ακόλουθα:

1. **Αν $2u \notin \mathfrak{p}$, τότε το $\mathfrak{p}$ δεν διακλαδίζεται στο L.**
2. **Αν $u \notin \mathfrak{p}$ και υπάρχουν $b,c \in R_K$ με $u^2=b^2-4c$, τότε το $\mathfrak{p}$ δεν διακλαδίζεται στο L.**

ΑΠΟΔΕΙΞΗ

Έχουμε ότι το πολυώνυμο $f(x)=x^2-u$ του $K[x]$ είναι διαχωρίσιμο και έχει ρίζα το ν. Η επέκταση L/K επομένως (αφού $L=K(v)$) είναι Galois. Προχωρούμε τώρα στο κυρίως μέρος της απόδειξης :

1. Αν $2u \notin \mathfrak{p}$, τότε $4u \notin \mathfrak{p}$

   Πράγματι , Αν $4u \in \mathfrak{p}$ τότε επειδή $2u \notin \mathfrak{p}$ θα έχουμε $2 \in \mathfrak{p}$ και συνεπώς $2u \in \mathfrak{p}$, πράγμα άτοπο. Επειδή η διακρίνουσα του f είναι $-4u \notin \mathfrak{p}$, θα έχουμε ότι το πολυώνυμο $f(x)=(x^2-u) \in R_K[x]$ είναι διαχωρίσιμο modulo $\mathfrak{p}$, και συνεπώς από το 1 της πρότασης 2.1.1.9 έχουμε ότι το $\mathfrak{p}$ δεν διακλαδίζεται στο L.

2. Το πολυώνυμο $g(x)=x^2+bx+c$ του $R_K[x]$ έχει διακρίνουσα $b^2-4c=u^2 \notin \mathfrak{p}$ και είναι συνεπώς διαχωρίσιμο modulo $\mathfrak{p}$. Οι ρίζες του g(x) , είναι οι $\frac{-b+v}{2}$, $\frac{-b-v}{2}$ και επομένως , αφού $g(x) \in R_K[x]$, θα έχουμε ότι $\frac{-b+v}{2} \in R_L$. Είναι προφανές τώρα ότι $L=K(v)=K(\frac{-b+v}{2})$, οπότε το 1 της πρότασης 2.1.1.9 θα μας δώσει ότι $\mathfrak{p}$ δεν διακλαδίζεται στο L.

2.5.1.2 ΛΗΜΜΑ : Αν M είναι κυβική επέκταση (δηλαδή επέκταση βαθμού 3) του $K=Q(\sqrt{-3})$, ώστε η επέκταση M/Q να είναι Galois και $G(M|Q) \cong S_3$, τότε υπάρχει φυσικός αριθμός m ελεύθερος κύβου ώστε $M=K(\sqrt[3]{m})$.

ΑΠΟΔΕΙΞΗ

Έστω M κυβική επέκταση του $K=Q(\sqrt{-3})$, ώστε η επέκταση M/Q να είναι Galois και $G(M|Q) \cong S_3$. Έχουμε $\#G(M|K)=[M : K]=3$ και συνεπώς $G(M|K) \cong Z_3$. Έστω τ γεννήτορας της $G(M|K)$. Θα έχουμε λοιπόν και $\tau \in G(M|Q)$. Η μιγαδική συζυγία "σ" ανήκει προφανώς στην $G(M|Q)$. Θα αποδείξουμε ότι :

$\tau\sigma = \sigma\tau^{-1}$ (Σ 2.5.1.2.1)

Πράγματι , η τάξη του τ είναι 3 και η τάξη του σ είναι 2. Τα $1,\sigma,\tau,\tau^2,\tau\sigma,\tau^2\sigma$ έχουν πλήθος 6 και είναι μεταξύ τους διαφορετικά (αν π.χ. $\tau\sigma=\tau^2\sigma$, τότε $\tau\sigma^2=\tau^2\sigma^2 \rightarrow \tau=\tau^2$ πράγμα άτοπο). Συνεπώς $G(M|Q)=\{1,\sigma,\tau,\tau^2,\tau\sigma,\tau^2\sigma\}$. Τώρα προφανώς $\sigma\tau \in G(M|Q)$ και με το μάτι βλέπουμε ότι $\sigma\tau \neq 1,\sigma,\tau,\tau^2$. Αν $\sigma\tau = \tau\sigma$, τότε $(\tau\sigma)^2=\tau\sigma$, οπότε η υποομάδα της $G(M|Q)$ που παράγεται από τα σ,τ είναι η $V_4 = \langle \sigma,\tau \mid \sigma^2=1 , \tau^3=1, \sigma\tau=\tau\sigma \rangle$ η οποία έχει πλήθος στοιχείων 4. Όμως $\#G(M|Q) = \#S_3 = 6$ που σημαίνει ότι $4 \nmid \#G(M|Q)$ και έτσι η V_4 δεν μπορεί να είναι υποομάδα της $G(M|Q)$, άρα έχουμε άτοπο.

Δεν είναι λοιπόν δυνατόν να ισχύει τσ=στ , οπότε από τα παραπάνω θα έχουμε αναγκαστικά ότι στ=τ^2σ. Τώρα στσ = $\tau^2\sigma^2 = \tau^2 = \tau^{-1} \rightarrow$ τσ=στ^{-1}.

Παρατηρούμε τώρα ότι από το 1 του λήμματος 2.4.2.4 έχουμε ότι υπάρχει πραγματικός αλγεβρικός ακέραιος α_o ώστε M=K(α_o). Θέτουμε $u_j = \alpha_o + \omega^j\tau^{-1}(\alpha_o) + \omega^{2j}\tau^{-2}(\alpha_o)$, j$\in$ {0,1,2} , όπου ως συνήθως $\omega=e^{2\pi i/3}$. Θα αποδείξουμε τα ακόλουθα :

1. $u_j \in R_M$, $\forall j \in \{0,1,2\}$.
2. $\tau(u_j)=\omega^j u_j$, $\forall j \in \{0,1,2\}$.
3. $\sigma(u_j)=u_j$, $\forall j \in \{0,1,2\}$.
4. $u_j^3 \in Z$, $\forall j \in \{1,2\}$ και $u_o \in Z$.
5. Αν $u_1 \neq 0$, τότε M=K(u_1).
6. Αν $u_2 \neq 0$, τότε M=K(u_2).
7. Δεν μπορεί ταυτόχρονα $u_1=0$ και $u_2=0$.

Για το 1 : Έχουμε $\alpha_o \in R_M$ (αφού M=K(α_o) και ο α_o είναι πραγματικός αλγεβρικός ακέραιος). Επίσης $\tau \in G(M|Q) \rightarrow \tau^{-1}(\alpha_o), \tau^{-2}(\alpha_o) \in R_M$. Εξάλλου $\omega = \frac{-1+i\sqrt{3}}{2} = \frac{-1+\sqrt{-3}}{2} \in K \subseteq M \rightarrow \omega \in R_M$ (αφού $\omega^2+\omega+1=0$). Εξ' ορισμού τώρα των u_j για j$\in$ {0,1,2} , έχουμε ότι $u_j \in R_M$.

Για το 2 : Κατ αρχήν $\omega=\frac{-1+\sqrt{-3}}{2} \in K$ και έτσι επειδή $\tau \in G(M|K)$ έχουμε $\tau(\omega)=\omega$. Τώρα $\tau(u_j) = \tau(\alpha_o)+\omega^j\alpha_0+ +\omega^{2j}\tau^{-1}(\alpha_o) = \omega^j[\alpha_o+\omega^j\tau^{-1}(\alpha_o)+\omega^{-j}\tau(\alpha_o)]$. Όμως $\omega^{-j}=\omega^{2j}$ (αφού $\omega^3=1$) , και έτσι τελικά $\tau(u_j)= \omega^j[\alpha_o+\omega^j\tau^{-1}(\alpha_o)+\omega^{2j}\tau(\alpha_o)]= \omega^j u_j$.

Για το 3 : Προκύπτει με πράξεις όπως ακριβώς και προηγουμένως στο 2 και χρησιμοποιώντας την σχέση Σ 2.5.1.2.1 .

Για το 4 : Για j$\in$ {1,2} , τα 2 και 3 μας δίνουν $\sigma(u_j^3)=u_j^3$, $\tau(u_j^3)=u_j^3$, οπότε αφού τα σ,τ παράγουν την G(M|Q) , θα έχουμε ότι το u_j παραμένει αναλλοίωτο από τους αυτομορφισμούς της G(M|Q). Επειδή η επέκταση M|Q είναι Galois θα έχουμε τότε $u_j^3 \in Q$. Εξάλλου το 1 δίνει ότι $u_j^3 \in R_M$, οπότε τελικά $u_j^3 \in Z$. Επίσης τα 2,3 δίνουν $\sigma(u_o)=u_o$, $\tau(u_o)=u_o$. Όπως λοιπόν και προηγουμένως , το u_o παραμένει αναλλοίωτο από την G(M|Q) , οπότε $u_o \in Q$ και έτσι από 1 έχουμε $u_o \in Z$.

Για το 5 : Έστω $u_1 \neq 0$. Επειδή [M : K] = 3 , έχουμε [K(u_1) : K] = 1ή 3 και συνεπώς K(u_1) = K ή K(u_1)=M. Αν K(u_1)=K , τότε $u_1 \in K$ και επειδή $\tau \in G(M|K)$, θα έχουμε $\tau(u_1)=u_1$, που σημαίνει από το 1 ότι $\omega u_1=u_1$, πράγμα άτοπο για $u_1 \neq 0$. Συνεπώς M=K(u_1).

Για το 6 : Εντελώς όμοια με το 5.

Για το 7 : Αν $u_1=0$, τότε $u_1 = \alpha_o + \omega\tau^{-1}(\alpha_o) + \omega^2\tau^{-2}(\alpha_o) = 0$. Αν $u_2=0$, τότε $u_2 = \alpha_o + \omega^2\tau^{-1}(\alpha_o) + \omega\tau^{-2}(\alpha_o) = 0$. Προσθέτοντας κατά μέλη τις παραπάνω ισότητες παίρνουμε : $2\alpha_o+(\omega^2+\omega)\tau^{-1}(\alpha_o)+(\omega^2+\omega)\tau^{-2}(\alpha_o)=0$. Επειδή $\omega^2+\omega+1=0$, η τελευταία ισότητα γίνεται $2\alpha_o=\tau^{-1}(\alpha_o)+\tau^{-2}(\alpha_o)$. Όμως επειδή $u_o=\alpha_o+\tau^{-1}(\alpha_o)+\tau^{-2}(\alpha_o)$, θα έχουμε $3\alpha_o=u_o$. Τώρα από το 4 έχουμε $u_o \in Z$, και η σχέση $3\alpha_o=u_o$ θα μας δώσει $\alpha_o \in Q$ οπότε και $\alpha_o \in K$. Έτσι M=K(α_o)=K , που είναι άτοπο αφού [M : K]=3.

Από το 7 , έχουμε ότι $u_1 \neq 0$ ή $u_2 \neq 0$. Διακρίνουμε τώρα τις περιπτώσεις :

1η Περίπτωση : $u_1 \neq 0$

Από το 4 έχουμε $u_1^3 \in Z$. Γράφουμε $u_1^3=k^3m$, με k,m$\in$ Z και m ελεύθερο κύβου. Το u_1 είναι λοιπόν μία λύση της εξίσωσης $x^3-k^3m=0$. Οι άλλες λύσεις της $x^3-k^3m=0$ είναι οι ωu_1, $\omega^2 u_1$. Επειδή και το $k\sqrt[3]{m}$ είναι ρίζα της εξίσωσης $x^3-k^3m=0$, θα έχουμε $k\sqrt[3]{m} \in \{u_1, \omega u_1, \omega^2 u_1\}$. Επειδή $\omega=\frac{-1+\sqrt{-3}}{2} \in K$, θα έχουμε λόγω του 5 ότι $M=K(u_1)=K(\omega u_1)=K(\omega^2 u_1)$. Συνεπώς $K(\sqrt[3]{m}) = K(k\sqrt[3]{m}) = M$.

$2^{η}$ Περίπτωση : $u_2 \neq 0$

Ομοίως με την πρώτη περίπτωση , χρησιμοποιώντας το 6 μπορούμε να δείξουμε ότι υπάρχει $m \in Z$ ελεύθερο κύβου ώστε $M=K(\sqrt[3]{m})$.

2.5.1.3 ΘΕΩΡΗΜΑ : 1. To ring class field της τάξης $Z[\sqrt{-14}]$ είναι το $K(\sqrt{2\sqrt{2}-1})$.

2. To ring class field της τάξης $Z[\sqrt{-27}]$ είναι το $K(\sqrt[3]{2})$.

3. To ring class field της τάξης $Z[\sqrt{-64}]$ είναι το $K(\sqrt[4]{2})$.

ΑΠΟΔΕΙΞΗ

1. Ο δακτύλιος $O=Z[\sqrt{-14}]$ είναι τάξη στο σώμα $K = quot(Z[\sqrt{-14}]) = Q(\sqrt{-14})$ (βλ. το 2 της παρατήρησης 2.2.1.3). Επίσης το 14 είναι ελεύθερο τετραγώνου και $(-14) \equiv 2 (mod 4)$. Συνεπώς $R_K = Z[\sqrt{-14}] = O$ (βλ. πρόταση 2.1.1.5). Ζητάμε λοιπόν το ring class field της μέγιστης τάξης του τετραγωνικού φανταστικού σώματος $K= Q(\sqrt{-14})$. Από την παρατήρηση 2.4.1.3 τώρα φαίνεται ότι το ζητούμενο ring class field είναι το σώμα κλάσεως του Hilbert για το σώμα K.
Έτσι λόγω του 2 του θεωρήματος 2.3.1.15 έχουμε να υπολογίσουμε την μέγιστη μη διακλαδιζόμενη αβελιανή επέκταση του K. Θέτουμε $\alpha := \sqrt{2\sqrt{2}-1}$ και $L=K(\alpha)$. Θα δείξουμε ότι το L είναι η μέγιστη μη διακλαδιζόμενη αβελιανή επέκταση του K , και συνεπώς το L θα είναι το ζητούμενο ring class field.
Έστω H η μέγιστη αβελιανή μη διακλαδιζόμενη επέκταση του K. Από τον πίνακα της εφαρμογής 1.2.2.8 παίρνουμε ότι $h(-56)=4$. Η διακρίνουσα της O είναι $d_O = d_{R_K} = -4 \cdot 14 = -56$.
Από τον ισομορφισμό $C(d_O) \cong C(O)$ του θεωρήματος 2.2.3.7 θα πάρουμε τώρα ότι $\#C(O) = \#C(-56) = h(-56) = 4$. Εξάλλου η πρόταση 2.4.1.4 μας δίνει ισομορφισμό $C(O) \cong G(H|K)$ και έτσι $[H : K] = \# G(H|K) = 4$ (Σ 2.5.1.3.1). Το ανάγωγο πολυώνυμο του α πάνω από το Q μπορεί να επαληθευτεί εύκολα ότι είναι το x^4+2x^2-7. Επαληθεύεται επίσης εύκολα ότι το x^4+2x^2-7 είναι και το ανάγωγο πολυώνυμο του α πάνω από το $K = Q(\sqrt{-14}) = Q[\sqrt{-14}]$.
Έχουμε λοιπόν $[L : K] = 4$ (Σ 2.5.1.3.2). Επίσης $\#G(L|K) = [L : K] = 4$. Όμως κάθε ομάδα τάξεως 4 είναι
αβελιανή (Υπάρχουν δύο ομάδες τάξεως 4. Η μία είναι η Z_4 και η άλλη είναι η $V_4=<a,b \mid a^2=b^2=1, ab=ba>$.) , οπότε η G(L|K) είναι αβελιανή. Επειδή τώρα το x^4+2x^2-7 έχει ρίζες ακριβώς τα $\alpha = \sqrt{2\sqrt{2}-1}$, $b = \sqrt{-2\sqrt{2}-1}$, $-\alpha$, $-b$, είναι διαχωρίσιμο.
Θα δείξουμε τώρα ότι $b \in L$

Πράγματι , $b = i(\sqrt{2\sqrt{2}+1}) = \frac{i\sqrt{7}}{\sqrt{2\sqrt{2}-1}} = \frac{i\sqrt{7}}{\alpha} = \frac{\sqrt{-14}}{2\alpha} \in L$ (αφού $K=Q(\sqrt{-14})$).

Συνεπώς η επέκταση L/K , ως σώμα ριζών πάνω από το K ενός διαχωρισίμου πολυωνύμου , είναι επέκταση του Galois. Επειδή η G(L|K) είναι αβελιανή , θα έχουμε ότι η επέκταση L/K είναι αβελιανή.
Θα δείξουμε τώρα ότι η επέκταση L/K είναι μη διακλαδιζόμενη.

Κατ' αρχήν επειδή το K είναι τετραγωνικό φανταστικό σώμα , οι άπειροι πρώτοι του είναι η ταυτοτική απεικόνιση του K και η μιγαδική συζυγία. Οι πρώτοι αυτοί δεν διακλαδίζονται στο L εξ'ορισμού (βλ. ορισμό 2.1.1.3). Μένει να δειχτεί ότι και οι πεπερασμένοι πρώτοι του K δεν διακλαδίζονται στο L. Έχουμε $\alpha^2 = 2\sqrt{2} - 1 \rightarrow \sqrt{2} \in L$.
Θέτουμε $K_1 := K(\sqrt{2})$. Λόγω πολλαπλασιαστικότητας του δείκτη διακλάδωσης , αρκεί
να δειχτεί ότι στις επεκτάσεις L/K_1 και K_1/K δεν υπάρχουν πεπερασμένοι πρώτοι που να διακλαδίζονται.
Για την K_1/K : Αν p είναι πρώτο ιδεώδες του R_K , τότε για $2 \notin p$ από το 1 του λήμματος
2.5.1.1 έχουμε ότι ο p δεν διακλαδίζεται στο L. Μένει η περίπτωση $2 \in p$. Αν $2 \in p$, τότε επειδή $i\sqrt{14} = \sqrt{-14} \in K \subseteq K_1$ θα έχουμε και

$i \in K_1$. Άρα $\sqrt{-2} \in K_1 \rightarrow \sqrt{7} = \frac{\sqrt{-14}}{\sqrt{-2}} \in K_1 \rightarrow \sqrt{-7} \in K_1$. Ισχύει τώρα ότι $K_1=K(\sqrt{-7})$. (Πράγματι, έχουμε $K(\sqrt{-7}) \subseteq K_1$ και επίσης $\sqrt{2} = \frac{\sqrt{-14}}{\sqrt{-7}} \in Q(\sqrt{-7}, \sqrt{-14}) = K(\sqrt{-7})$, οπότε $K_1=K(\sqrt{2}) \subseteq K(\sqrt{-7})$.)

Αν $-7 \in p$, τότε επειδή $2 \in p$ θα έχουμε $1 = (-7+2 \cdot 3) \in p$, άτοπο γιατί το p είναι πρώτο ιδεώδες του R_K. Έτσι $-7 \notin p$. Επειδή τώρα $-7=1^2-4 \cdot 2$, το 2 του λήμματος 2.5.1.1 θα δώσει ότι το p δεν διακλαδίζεται στο $K_1=K(\sqrt{-7})$.

Για την L/K_1 : Θέτουμε $\mu=\alpha^2= 2\sqrt{2} -1$, $\mu'= -2\sqrt{2} -1$. Έχουμε λοιπόν $K_1= K(\sqrt{2}) = K(\mu) = K(\mu')$ και $L=K(\sqrt{\mu})$.Επίσης , όπως δείξαμε και στην περίπτωση της επέκτασης K_1/K , ισχύει $\sqrt{-7} \in K_1$ (πράγματι, $i \in K_1 \rightarrow \sqrt{-2} \in K_1 \rightarrow \sqrt{7} = \frac{\sqrt{-14}}{\sqrt{-2}} \in K_1 \rightarrow \sqrt{-7} \in K_1$) και συνεπώς $\sqrt{\mu\mu'} = \sqrt{-7} \in K_1$. Η τελευταία σχέση συνεπάγεται ότι $\sqrt{\mu'} \in L$. Μάλιστα $L=K_1(\sqrt{\mu})=K_1(\frac{\sqrt{-7}}{\sqrt{\mu'}})=K_1(\sqrt{\mu'})$. Αν τώρα p_1 είναι πεπερασμένος πρώτος του K_1 , διακρίνουμε τις περιπτώσεις:

1η Περίπτωση : $2 \notin p_1$.
Τότε αφού $\mu+\mu'=-2$, θα έχουμε ότι κάποιο από τα μ,μ' δεν ανήκει στο p_1. Αν $\mu \notin p_1$, τότε $2\mu \notin p_1$ και επειδή $L=K_1(\sqrt{\mu})$, το 1 του λήμματος 2.5.1.1 μας δίνει ότι το p_1 δεν διακλαδίζεται στο L.

2η Περίπτωση : $2 \in p_1$.
Στην περίπτωση αυτή επειδή το $\sqrt{2}$ είναι ακέραιος αλγεβρικός και ανήκει στο K_1 , θα έχουμε ότι $\mu \notin p_1$. (Πράγματι , αν $(2\sqrt{2} -1)=\mu \in p_1$, τότε $1 \in p_1$, πράγμα άτοπο γιατί το p_1 είναι πρώτο ιδεώδες.). Τώρα γράφουμε $\mu = (1+\sqrt{2})^2-4 \cdot 1$ και έτσι το 2 του λήμματος 2.5.1.1 θα δώσει τελικά ότι το p_1 δεν διακλαδίζεται στο L.

Συνοψίζοντας λοιπόν έχουμε ότι η L/K είναι αβελιανή επέκταση του K , μη διακλαδιζόμενη με $[L : K]=4$.

Επίσης η σχέση (Σ 2.5.1.3.1) μας δίνει ότι $[H : K]=4$. Τέλος $L \subseteq H$, αφού H είναι η μέγιστη αβελιανή μη διακλαδιζόμενη επέκταση του K. Συμπεραίνουμε επομένως από τα παραπάνω ότι L=H που είναι και η σχέση που θέλαμε να αποδείξουμε.

2. Ο δακτύλιος $O=Z[\sqrt{-27}]$ είναι τάξη στο φανταστικό τετραγωνικό σώμα $K=Q(\sqrt{-27})=Q(\sqrt{-3})=Q(i\sqrt{3})$. Έστω L το ring class field της τάξης O. Θα δείξουμε κατ' αρχήν τα ακόλουθα :
   a. Το L είναι κυβική αβελιανή επέκταση Galois του K.
   b. Η επέκταση L/Q είναι Galois με ομάδα Galois την S_3.
   c. Οι πρώτοι του K που διακλαδίζονται στο L διαιρούν το modulus $6R_K$.

Για το a : Έχουμε $d_O = -4 \cdot 27$. Επίσης από τον πίνακα της εφαρμογής 1.2.2.8 έχουμε $h(-4 \cdot 27)=h(-108)=3$.

Από τους ισομορφισμούς $C(O) \cong C(d_O)$, $C(O) \cong G(L|K)$ του θεωρήματος 2.2.3.7 και της πρότασης 2.4.1.4 αντίστοιχα , θα πάρουμε επομένως ότι $[L : K]=\#G(L|K)= h(-108)=3$. Το ότι η L/K είναι αβελιανή προκύπτει από τον ορισμό των ring class fields (βλ. ορισμό 2.4.1.2).

Για το b : Το 1 του λήμματος 2.4.2.3 δίνει ότι επέκταση $L/\mathbb{Q}$ είναι Galois. Έχουμε τώρα $\#G(L|\mathbb{Q})= =[L : \mathbb{Q}]=[L : K][K : \mathbb{Q}] =3 \cdot 2=6 \rightarrow \#G(L|\mathbb{Q})=6$. Υπάρχουν δύο "τύποι"ομάδων τάξεως 6 : η κυκλική και η S_3. Θα αποκλείσουμε την περίπτωση η $G(L|\mathbb{Q})$ να είναι κυκλική. Έστω ότι η $G(L|\mathbb{Q})$ είναι κυκλική και παράγεται από το $\rho_o \in G(L|\mathbb{Q})$. Θα δείξουμε ότι $\rho_o^2=1$, που είναι άτοπο.

Έχουμε ότι $\rho_o^2 \in G(L|K)$ (λόγω του ότι $[G(L|\mathbb{Q}) : G(L|K)] = 2$) και επίσης $\sigma_{|L} \cdot \rho_o^2 \cdot \sigma_{|L}=\rho_o^{-2}$ με $\sigma_{|L} \in G(L|\mathbb{Q})$ (βλ. το 1 του λήμματος 2.4.2.3). Επειδή η τάξη της σ είναι 2 , θα έχουμε $\sigma_{|L}=\rho_o^3$ και συνεπώς θα έχουμε $\rho_o^3 \rho_o^2 = \rho_o^{-2}=\rho_o^4 \rightarrow \rho_o^2=1$.

Για το c : Έχουμε $K=\mathbb{Q}(\sqrt{-3})$, οπότε $R_K=\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ (βλ. πρόταση 2.1.1.5) Τώρα $\frac{1+\sqrt{-3}}{2}=\omega-1$ ($\omega=e^{2\pi i/3}$) και έτσι $R_K=\mathbb{Z}[\omega]$. Έχουμε $d_K=3$ (βλ. πρόταση 2.1.1.5) οπότε επειδή $\frac{d_O}{d_K}=\frac{108}{3}=36=6^2$, έχουμε ότι ο οδηγός της O είναι το 6. Η πρόταση 2.4.1.4 τώρα θα μας δώσει ότι κάθε πρώτος του K που διακλαδίζεται στο L διαιρεί το modulus $6R_K$.

Παρατηρούμε τώρα ότι από το λήμμα 2.5.1.2 και το γεγονός ότι η L/K είναι κυβική επέκταση ώστε η επέκταση $L/\mathbb{Q}$ να είναι Galois με ομάδα Galois την S_3 μας δίνει ότι υπάρχει ακέραιος αριθμός m ελεύθερος κύβου ώστε $L=K(\sqrt[3]{m})$. Θα δείξουμε στην συνέχεια ότι οι μόνοι πρώτοι αριθμοί που διαιρούν το m είναι ο 2 και ο 3.

Πράγματι, κατ' αρχήν $K=\mathbb{Q}(\sqrt{-3})=K(\frac{-1+\sqrt{-3}}{2})=K(\omega)$, οπότε $L=K(\sqrt[3]{m})=\mathbb{Q}(\sqrt[3]{m},\omega)$.

Αν p είναι πρώτος αριθμός που διαιρεί το m , τότε διακλαδίζεται στο L και συνεπώς και το pR_K διακλαδίζεται στο L. Από το c παραπάνω έχουμε ότι $pR_K \mid 6R_K$ και επομένως από μονοσήμαντη ανάλυση σε πρώτα ιδεώδη στον δακτύλιο του Dedekind R_K , έχουμε ότι p=2 , ή p=3 (βλ. υπενθυμίσεις 1.3.1.1 για τους πρώτους του R_K).

Από το γεγονός ότι το m είναι ελεύθερο κύβου έχουμε ότι $m \in \{2,3,4,6,9,12,18,36\}$

Επειδή $K(\sqrt[3]{4}) \subseteq K(\sqrt[3]{2})$, $K(\sqrt[3]{9}) \subseteq K(\sqrt[3]{3})$ και $\sqrt[3]{2}=\frac{\sqrt[3]{2^3}}{\sqrt[3]{4}}=\frac{2}{\sqrt[3]{4}} \in K(\sqrt[3]{4})$, $\sqrt[3]{3}=\frac{\sqrt[3]{3^3}}{\sqrt[3]{9}}=\frac{3}{\sqrt[3]{9}} \in K(\sqrt[3]{9})$, θα έχουμε $K(\sqrt[3]{4})=K(\sqrt[3]{2})$, $K(\sqrt[3]{9})=K(\sqrt[3]{3})$. Εξάλλου $K(\sqrt[3]{18})=K(\sqrt[3]{2} \cdot \sqrt[3]{9})=K(\sqrt[3]{6})$ και $K(\sqrt[3]{36})=K(\sqrt[3]{2} \cdot \sqrt[3]{18})=K(\sqrt[3]{2} \cdot \sqrt[3]{6})=K(\sqrt[3]{12})$. Συνεπώς για τα διάφορα m που ανήκουν στο σύνολο $\{2,3,4,6,9,12,18,36\}$ παίρνουμε $L \in \{ K(\sqrt[3]{2}) , K(\sqrt[3]{3}) , K(\sqrt[3]{6}) , K(\sqrt[3]{12}) \}$. Θα αποκλείσουμε την περίπτωση $L=K(\sqrt[3]{3})$:

Αν $L=K(\sqrt[3]{3})$, τότε εκλέγουμε το πολυώνυμο f_{27} του θεωρήματος 2.4.2.5 να είναι το ανάγωγο πολυώνυμο του πραγματικού αλγεβρικού ακέραιου $\sqrt[3]{3}$. Ο αριθμός 31 είναι πρώτος και το $f_{27}(x)=x^3-3$, έχει διακρίνουσα -3^5 η οποία επομένως δεν διαιρείται από το 31. Επειδή $31=2^2+27 \cdot 1^2$, το θεώρημα 2.4.2.5 θα μας δώσει

τώρα ότι η ισοδυναμία $x^3-3\equiv 0(\mathrm{mod}31)$ θα έχει λύση στο Z. Αυτό όμως όπως μπορεί κάποιος να αποδείξει εύκολα με απλό υπολογισμό είναι άτοπο.

Εντελώς όμοια μπορούμε να αποκλείσουμε τις περιπτώσεις $L= K(\sqrt[3]{6})$ και $L= K(\sqrt[3]{12})$, οπότε θα έχουμε

$L= K(\sqrt[3]{2})$.

3. Όμοια με το 2 και χρησιμοποιώντας ανάλογο λήμμα με το 2.5.1.2 μπορεί να δειχτεί ότι το ring class field

της τάξης $Z[\sqrt{-64}]$ είναι το $K(\sqrt[4]{2})$. Η απόδειξη παραλείπεται λόγω της μεγάλης της ομοιότητας με την περίπτωση 2 της τάξης $Z[\sqrt{-27}]$.

2.5.2 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ ΤΩΝ ΜΟΡΦΩΝ x^2+14y^2 , x^2+27y^2 ΚΑΙ x^2+64y^2

<u>2.5,2.1 ΘΕΩΡΗΜΑ</u> : Για κάθε πρώτο αριθμό p ισχύουν οι ακόλουθες ισοδυναμίες :

1. " $\exists x,y\in Z : p=x^2+14y^2$ " $\leftrightarrow$ "$\left(\frac{-14}{p}\right)_2=1$ και η $(x^2+1)^2\equiv 8(\mathrm{mod}p)$ είναι επιλύσιμη στο Z".

2. " $\exists x,y\in Z : p=x^2+27y^2$ " $\leftrightarrow$ " $p\equiv 1(\mathrm{mod}3)$ και η $x^3\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη στο Z ".

3. " $\exists x,y\in Z : p=x^2+64y^2$ " $\leftrightarrow$ " $p\equiv 1(\mathrm{mod}4)$ και η $x^4\equiv 2(\mathrm{mod}p)$ είναι επιλύσιμη στο Z ".

<u>ΑΠΟΔΕΙΞΗ</u>

1. Κατ' αρχήν είναι προφανές ότι για p=7,2 , το αριστερό μέλος της αποδεικτέας ισοδυναμίας δεν ισχύει.

   Επειδή $\left(\frac{-14}{2}\right)=\left(\frac{-14}{7}\right)_2=0$, έχουμε ότι ούτε το δεξιό μέλος ισχύει. Συνεπώς η αποδεικτέα ισοδυναμία ισχύει για p=7 και p=2. Έστω τώρα p≠2,7. Από το θεώρημα 2.5.1.3 έχουμε ότι το ring class field της τάξης $Z[\sqrt{-14}\,]$ του φανταστικού τετραγωνικού σώματος $K=Q(\sqrt{-14}\,)$ είναι το $K(\sqrt{2\sqrt{2}-1}\,)$. Το ανάγωγο πολυώνυμο πάνω από το Q του πραγματικού αλγεβρικού ακέραιου $\sqrt{2\sqrt{2}-1}$ επαληθεύεται εύκολα ότι είναι το $(x^2+1)^2-8$. Επειδή η διακρίνουσα του $(x^2+1)^2-8$ είναι $-2^{14}\cdot 7$ (επαληθεύεται εύκολα) , το θεώρημα 2.4.2.5 θα μας δώσει ότι για κάθε πρώτο αριθμό p με p≠2,7 ισχύει η ακόλουθη ισοδυναμία

   " $\exists x,y\in Z : p=x^2+14y^2$ " $\leftrightarrow$ "$\left(\frac{-14}{p}\right)_2=1$ και η $(x^2+1)^2\equiv 8(\mathrm{mod}p)$ είναι επιλύσιμη στο Z".

   που είναι ακριβώς αυτή που θέλουμε να αποδείξουμε.

2. Είναι προφανές ότι για p=2,3 το αριστερό μέλος της αποδεικτέας ισοδυναμίας δεν ισχύει. Επειδή $2\not\equiv 1(\mathrm{mod}3)$ και $3\not\equiv 1(\mathrm{mod}3)$, δεν ισχύει και το δεξιό μέλος. . Συνεπώς η αποδεικτέα ισοδυναμία ισχύει για p=2 και p=3. Έστω τώρα p≠2,3. Από το θεώρημα 2.5.1.3 έχουμε ότι το ring class field της τάξης $Z[\sqrt{-27}\,]$ του φανταστικού τετραγωνικού σώματος $K=(\sqrt{-27}\,)$ είναι το $K(\sqrt[3]{2}\,)$.Το ανάγωγο πολυώνυμο πάνω από το Q του πραγματικού αλγεβρικού ακέραιου $\sqrt[3]{2}$ επαληθεύεται εύκολα ότι είναι το x^3-2. Επειδή η διακρίνουσα του x^3-2 είναι $-2^2\cdot 3^3$ (επαληθεύεται εύκολα) , το θεώρημα 2.4.2.5 θα μας δώσει ότι για κάθε πρώτο αριθμό p με p≠2,3 ισχύει η ακόλουθη ισοδυναμία

   " $\exists x,y\in Z : p=x^2+27y^2$ " $\leftrightarrow$ "$\left(\frac{-27}{p}\right)_2=1$ και η είναι $x^3\equiv 2(\mathrm{mod}p)$ επιλύσιμη στο Z".

   Επειδή $\left(\frac{-27}{p}\right)_2=\left(\frac{-3^3}{p}\right)_2=\left(\frac{-1}{p}\right)_2\left(\frac{3}{p}\right)_2=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right)_2=\left(\frac{p}{3}\right)_2$, θα έχουμε ότι $\left(\frac{-27}{p}\right)_2=1$ αν και μόνο αν η $\left(\frac{p}{3}\right)_2=1$. Έχουμε όμως ότι το p modulo 3 είναι 1 ή 2. Επειδή $\left(\frac{2}{3}\right)_2=-1$ και $\left(\frac{1}{3}\right)_2=1$, θα έχουμε $\left(\frac{-27}{p}\right)_2=1\leftrightarrow\left(\frac{p}{3}\right)_2=1\leftrightarrow p\equiv 1(\mathrm{mod}3)$. Οι τελευταίες σχέσεις σε συνδιασμό με τα παραπάνω μας δίνουν το αποδεικτέο.

3. Η περίπτωση είναι εντελώς όμοια με τις προηγούμενες και αφήνεται ως άσκηση.

§1 ΕΛΛΕΙΠΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΙ ΜΙΓΑΔΙΚΟΣ ΠΟΛΛΑΠΛΑΣΙΑΣΜΟΣ

3.1.1 ΕΛΛΕΙΠΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΙ Η $\wp$-ΣΥΝΑΡΤΗΣΗ ΤΟΥ WEIERSTRASS

Αποδείξεις για την παράγραφο 3.1.1 μπορούν να βρεθουν στο : [Cox] σελ. 200-208 , ενώ περισσότερες ιδιότητες της $\wp$-συνάρτησης του Weierstrass υπάρχουν στο κεφάλαιο 1 του [Lang].

3.1.1.1 ΟΡΙΣΜΟΣ : Κάθε σύνολο L της μορφής $L= w_1\mathbf{Z}+w_2\mathbf{Z}$, όπου οι w_1,w_2 είναι μιγαδικοί αριθμοί γραμμικά ανεξάρτητοι στο $\mathbf{R}$, θα ονομάζεται lattice του $\mathbf{C}$ ή απλά lattice.

3.1.1.2 ΟΡΙΣΜΟΣ : Έστω L ένα lattice του $\mathbf{C}$. Κάθε μιγαδική συνάρτηση $f : \mathbf{C} \to \mathbf{C}$ θα λέγεται ελλειπτική συνάρτηση του L (elliptic function) αν είναι μερόμορφη και $f(z+w)=f(z)$ $,\forall z\in \mathbf{C},\forall w\in L$.

3.1.1.3 ΠΡΟΤΑΣΗ : Κάθε ελλειπτική συνάρτηση με ολόμορφη επέκταση στο $\mathbf{C}$ είναι σταθερή.

3.1.1.4 ΟΡΙΣΜΟΣ : Άν L είναι ένα lattice του $\mathbf{C}$ και $r\in\mathbf{N}$ με $r>2$, τότε η σειρά $\sum_{w\in L-\{0\}} \frac{1}{w^r}$ συγκλίνει απόλυτα. Η σειρά αυτή θα συμβολίζεται $G_r(L)$ και θα ονομάζεται σειρά του Eisenstein.
Επίσης , με $g_2(L)$ και $g_3(L)$ θα συμβολίζονται αντίστοιχα τα $60G_4(L)$, $140G_6(L)$.

3.1.1.5 ΛΗΜΜΑ : Άν L είναι ένα lattice του $\mathbf{C}$, τότε η σειρά $\sum_{w\in L-\{0\}} \left(\frac{1}{(z-w)^2}-\frac{1}{w^2}\right)$ συγκλίνει στο $\mathbf{C}$-L.
Η συνάρτηση $\frac{1}{z^2}+\sum_{w\in L-\{0\}} \left(\frac{1}{(z-w)^2}-\frac{1}{w^2}\right)$ είναι άρτια ελλειπτική συνάρτηση του L που είναι ολόμορφη στο $\mathbf{C}$-L και στα στοιχεία του L έχει πόλους τάξης 2.

3.1.1.6 ΟΡΙΣΜΟΣ : Άν L είναι ένα lattice του $\mathbf{C}$, τότε η άρτια ελλειπτική συνάρτηση $\wp(\cdot;L) : (\mathbf{C}-L) \to \mathbf{C}$:

$\wp(z;L)= \frac{1}{z^2} + \sum_{w\in L-\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$ **θα ονομάζεται <u>$\wp$ - συνάρτηση του Weierstrass για το lattice L</u>.**

<u>3.1.1.7 ΠΡΟΤΑΣΗ</u> : Άν L είναι ένα lattice του C , τότε

$$\wp(z;L) = \frac{1}{z^2} + \sum_{n=1}^{\infty} [(2n+1)G_{2n+2}(L)z^{2n}] \quad (\Sigma\ 3.1.1.7.1)$$

<u>3.1.1.8 ΠΡΟΤΑΣΗ</u> : 1. Άν L είναι ένα lattice του C και θέσουμε για ευκολία στους συμβολισμούς $\wp(\cdot) := \wp(\cdot;L)$, τότε η $\wp$ ικανοποιεί την διαφορική εξίσωση :

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L) \quad (\Sigma\ 3.1.1.8.1)$$

2. Στην έκφραση Σ 3.1.1.7.1 της $\wp(z;L)$ σαν σειρά Laurent τοπικά στο (0,0) οι συντελεστές της σειράς $a_n := (2n+1)G_{2n+2}(L)$ ανήκουν στο $Q(g_2(L),g_3(L))$

(Μάλιστα $a_1 = \frac{g_2(L)}{20}$, $a_2 = \frac{g_3(L)}{28}$, $a_3 = \frac{g_2(L)^2}{1200}$).

<u>3.1.1.9 ΠΟΡΙΣΜΑ</u> : Άν L είναι ένα lattice του C , τότε τα $g_2(L)$, $g_3(L)$ χαρακτηρίζουν πλήρως την συνάρτηση του Weierstrass $\wp(\cdot\ ; L)$ για το lattice L.

<u>3.1.1.10 ΠΡΟΤΑΣΗ</u> : Αν L είναι ένα lattice του C και θέσουμε $\wp(\cdot) := \wp(\cdot;L)$, τότε ισχύουν τα ακόλουθα :

1. **" $\wp(z)=\wp(w) \leftrightarrow z \equiv \pm w (\mathrm{mod} L)$ " , $\forall z,w \in (C-L)$.**
2. **Για $w \in (C-L)$, η εξίσωση $\wp(z)=\wp(w)$ ως προς z έχει το πολύ δύο λύσεις modulo L. Οι λύσεις αυτές είναι οι w,-w.**

<u>3.1.1.11 ΠΟΡΙΣΜΑ</u> : Αν L είναι ένα lattice του C κσι θέσουμε $\wp(\cdot) := \wp(\cdot;L)$, τότε για $w \notin L$ ισχύει η ακόλουθη ισοδυναμία : " $\wp'(z)=0 \leftrightarrow 2w \in L$ ".

<u>3.1.1.12 ΠΡΟΤΑΣΗ</u> : Άν L είναι ένα lattice του C και θέσουμε $\wp(\cdot) := \wp(\cdot;L)$, τότε για κάθε $z,w \in C$ με $z,w \notin L$ και $z \not\equiv \pm w (\mathrm{mod} L)$ ισχύει ο ακόλουθος προσθετικός κανόνας :

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2$$

<u>3.1.1.13 ΠΡΟΤΑΣΗ</u> : Άν L είναι ένα lattice του C , τότε ισχύουν τα ακόλουθα :

1. **Κάθε άρτια ελλειπτική συνάρτηση του L , η οποία είναι ολόμορφη στο C-L**

ανήκει στο $\mathbf{C}[\wp(\cdot\,;L)]$. Είναι δηλαδή πολυωνυμική έκφραση της $\wp(\cdot\,;L)$.

2. Κάθε άρτια ελλειπτική συνάρτηση ανήκει στο $\mathbf{C}(\wp(\cdot\,;L))$. Είναι δηλαδή ρητή έκφραση της $\wp(\cdot\,;L)$.

3.1.1.14 ΠΡΟΤΑΣΗ : Άν L είναι ένα lattice του **C** , τότε η $\wp(\cdot\,;L)$ είναι "επί" του **C**.

3.1.1.15 ΣΧΟΛΙΑ : Είναι εύκολο να δεί κανείς ότι αν η $\bar{\cdot}$ εκφράζει την μιγαδική συζυγία , ισχύουν οι ακόλουθες ιδιότητες :

1. $\wp(\bar{z}\,;\bar{L}) = \overline{\wp(z\,;L)}$, $\forall z \in (\mathbf{C}\text{-}L)$
2. $g_2(\bar{L}) = \overline{g_2(L)}$.
3. $g_3(\bar{L}) = \overline{g_3(L)}$.

3.1.2 Η j-ΑΝΑΛΛΟΙΩΤΗ ΕΝΟΣ LATTICE

Αποδείξεις για τις ιδιότητες της j-αναλλοίωτης μπορούν να βρεθούν στο : [Cox] σελ. 205-208.

3.1.2.1 ΟΡΙΣΜΟΣ : Δύο lattices L,L' θα λέγονται ομοιόθετα αν υπάρχει $\lambda \in \mathbb{C}-\{0\}$ με $L'=\lambda \cdot L$.

3.1.2.2 ΠΑΡΑΤΗΡΗΣΕΙΣ : 1. Η ομοιοθεσία των lattices είναι σχέση ισοδυναμίας.

2. Αν $f(z)$ είναι ελλειπτική συνάρτηση για κάποιο lattice L και $\lambda \in \mathbb{C}-\{0\}$, τότε

η $f(\lambda z)$ είναι ελλειπτική συνάρτηση για το lattice λL.

Ειδικότερα, ισχύουν οι ακόλουθες σχέσεις :

a. $\wp(\lambda z ; \lambda L) = \lambda^{-2}\wp(z ; L)$, $\forall z \in (\mathbb{C}-L)$.

b. $g_2(\lambda L) = \lambda^{-4} g_2(L)$.

c. $g_3(\lambda L) = \lambda^{-6} g_3(L)$.

3.1.2.3 ΟΡΙΣΜΟΣ : Αν L είναι lattice του $\mathbb{C}$, τότε ο αριθμός $g_2(L)^3 - 27g_3(L)^2$ θα συμβολίζεται με $\Delta(L)$ και θα λέγεται διακρίνουσα του lattice L.

3.1.2.4 ΠΑΡΑΤΗΡΗΣΕΙΣ : 1. Παρατηρούμε ότι για lattice L, το $\Delta(L)$ είναι η διακρίνουσα του πολυωνύμου

$$4x^3 - g_2(L)x - g_3(L).$$

2. Άν η $\bar{\cdot}$ εκφράζει την μιγαδική συζυγία, τότε $\Delta(\bar{L}) = \overline{\Delta(L)}$.

3.1.2.5 ΠΡΟΤΑΣΗ : Άν L είναι lattice του $\mathbb{C}$, τότε $\Delta(L) \neq 0$.

3.1.2.6 ΟΡΙΣΜΟΣ : Άν L είναι lattice του $\mathbb{C}$, τότε ο μιγαδικός αριθμός $1728\frac{g_2(L)^3}{\Delta(L)}$ θα συμβολίζεται με $j(L)$ και θα ονομάζεται j - αναλλοίωτη του lattice L. (Στην αμέσως επόμενη πρόταση θα φανεί από που προέρχεται ο χαρακτηρισμός "αναλλοίωτη".)

3.1.2.7 ΠΡΟΤΑΣΗ : Άν L,L' είναι lattices του $\mathbb{C}$, τότε $j(L)=j(L)$ αν και μόνο αν τα L,L' είναι ομοιόθετα.

3.1.2.8 ΠΑΡΑΤΗΡΗΣΗ : Άν L είναι lattice του C , και η $\bar{\cdot}$ εκφράζει την μιγαδική συζυγία , τότε $j(\bar{L}) = \overline{j(L)}$.

3.1.2.9 ΠΡΟΤΑΣΗ : Άν L είναι lattice του C , τότε ισχύουν τα ακόλουθα :

1. $g_2(L)=0$ αν και μόνο αν το L είναι ομοιόθετο με το lattice $Z+iZ$, ($i^2=1$).
2. $g_3(L)=0$ αν και μόνο αν το L είναι ομοιόθετο με το lattice $Z+\omega Z$, ($\omega=e^{2\pi i/3}$) .
3. Αν $g_2(L), g_3(L)\neq 0$, τότε υπάρχουν $\lambda,\mu\in C-\{0\}$ με
   - $g_2(\lambda L) = \lambda^{-4} g_2(L) = 20\mu$ και
   - $g_3(\lambda L) = \lambda^{-6} g_3(L) = 28\mu$.

3.1.3 ΜΙΓΑΔΙΚΟΣ ΠΟΛΛΑΠΛΑΣΙΑΣΜΟΣ

3.1.3.1 ΠΡΟΤΑΣΗ : Έστω K φανταστικό τετραγωνικό σώμα και O μια τάξη του K. Άν a είναι κλασματικό ιδεώδες της O , τότε (λόγω πρότασης 2.2.2.6) το a είναι ελεύθερο Z-module με rank ίσο με 2. Αν a=αZ+βZ ,για κάποια α,β∈ K , τότε τα α,β είναι R-γραμμικώς ανεξάρτητα.

ΑΠΟΔΕΙΞΗ

Αν τα α,β ήταν γραμμικώς εξαρτημένα , θα έπρεπε το $\tau=\frac{\beta}{\alpha}$ να ανήκει στο R. Όμως $[Q(\tau):Q]\geq 2$ (αν $\tau\in Q$ τότε τα α,β θα ήταν Q-γραμμικώς εξαρτημένα , οπότε θα ήταν και Z-γραμμικώς εξαρτημένα που είναι άτοπο αφού το a έχει rank ίσο με 2). Επίσης $Q\subseteq Q(\tau)\subseteq K$ με $[K:Q]=2$ και συνεπώς $K=Q(\tau)$, οπότε αφού $\tau\in R$, θα είχαμε $K\subseteq R$ που είναι άτοπο αφού το K είναι φανταστικό σώμα.

3.1.3.2 ΠΟΡΙΣΜΑ : Κάθε proper ιδεώδες τάξης φανταστικού τετραγωνικού σώματος είναι lattice του C.

3.1.3.3 ΠΑΡΑΤΗΡΗΣΗ : Από την παρατήρηση 3.1.2.8 συνάγουμε εύκολα ότι αν a είναι proper ιδεώδες τάξης φανταστικού τετραγωνικού σώματος , τότε $j(a)\in R$ αν και μόνο αν η τάξη της κλάσης του a modulo την υποομάδα H(O) στην C(O) είναι 2.

3.1.3.4 ΠΡΟΤΑΣΗ : Αν L είναι lattice του C , τότε η συνάρτηση $z\to\wp(kz;L)$ είναι ρητή έκφραση της $z\to\wp(z;L)$ για κάθε ακέραιο αριθμό k. Μάλιστα μπορούμε να γράψουμε $\wp(kz)=\frac{A(\wp(z))}{B(\wp(z))}$ με $A(x),B(x)\in C[x]$, όπου το A να έχει βαθμό k^2 , και το B να έχει βαθμό k^2-1.

ΑΠΟΔΕΙΞΗ

Κατ' αρχήν θα συμβολίζουμε με $\wp(\cdot)$ την $\wp(\cdot;L)$ και με g_2 , g_3 τα $g_2(L)$, $g_3(L)$ αντίστοιχα. Από την πρόταση 3.1.1.12 έχουμε ότι για μιγαδικούς αριθμούς z,w με $z,w,2z\notin L$ και $z\not\equiv\pm w(\mathrm{mod}L)$ ισχύει ότι $\wp(z+w)=-\wp(z)-\wp(w)+\frac{1}{4}\left(\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right)^2$. Εφαρμόζοντας τώρα το θεώρημα de l' Hospital παίρνοντας $w\to z$, θα προκύψει ότι $\wp(2z)=-2\wp(z)+\frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2$. Τώρα αν παραγωγίσουμε τη διαφορική εξίσωση Σ 3.1.1.8.1 της πρότασης 3.1.1.8 παίρνουμε $\wp''(z)=6\wp(z)^2-\frac{g_2}{2}$ και συνεπώς η προηγούμενη σχέση θα δώσει $\wp(2z)=-2\wp(z)+\frac{1}{16}\left(\frac{(12\wp(z)-g_2)^2}{4\wp(z)^3-g_2\wp(z)-g_3}\right)$. Η τελευταία σχέση μας δίνει ότι η $z\to\wp(2z)$ είναι ρητή έκφραση της $z\to\wp(z)$. Το συμπέρασμα του θεωρήματος που αφορά τους βαθμούς είναι προφανές ότι ικανοποιείται. Έστω τώρα ότι για κάποιο φυσικό $n\in N$ έχουμε ότι η $z\to\wp(nz)$ είναι ρητή έκφραση της $\wp$. Τότε από τον προσθετικό κανόνα της πρότασης 3.1.3.4 θα πάρουμε ότι

$\wp((n+1)z) = -\wp(z) - \wp(nz) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(nz)}{\wp(z) - \wp(nz)}\right)^2$ για κάθε μιγαδικό αριθμό z με $z,nz \notin L$ και $z \not\equiv nz(\mathrm{mod}L)$. Από την επαγωγική υπόθεση έχουμε το ζητούμενο για το $\wp((n+1)z)$. Όσο αφορά το συμπέρασμα του θεωρήματος για τους βαθμούς , είναι δουλειά ρουτίνας να αποδειχτεί χρησιμοποιώντας την επαγωγική υπόθεση και το ότι $\wp((n+1)z) = -\wp(z) - \wp(nz) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(nz)}{\wp(z) - \wp(nz)}\right)^2$.

<u>3.1.3.5 ΠΡΟΤΑΣΗ</u> : Έστω L = αZ+βZ lattice του C για α,β∈C. Θέτουμε $\tau=\frac{\alpha}{\beta} \in (C-R)$ και συνεπώς το L είναι ομοιόθετο με το lattice L' = Z+τZ. Αν υπάρχει $u_o \in C-Z$ ώστε $u_oL' \subseteq L'$, τότε ισχύουν τα ακόλουθα :

- **Το σώμα K=Q(τ) είναι τετραγωνικό φανταστικό και το σύνολο O={u∈K | uL'⊆L' } είναι μία τάξη του K.**
- **Το L' είναι proper κλασματικό ιδεώδες της τάξης O.**
- **∀u∈(O-Z) , K=Q(u).**

<u>ΑΠΟΔΕΙΞΗ</u>

Έχουμε $u_oL' \subseteq L' \rightarrow \exists a,b,c,d \in Z$ με $u_o=a+b\tau$, $u_o\tau=c+d\tau$. Επειδή $u_o \notin Z$, θα έχουμε $b \neq 0$. Εξάλλου $\tau = \frac{u_o\tau}{u_o} = \frac{c+d\tau}{a+b\tau}$, οπότε $b\tau^2+(a-d)\tau-c=0$. Επειδή $b \neq 0$, θα έχουμε επομένως ότι το $K=Q(\tau)$ είναι τετραγωνικό και φανταστικό (αφού $\tau \notin R$) σώμα. Το σύνολο $O=\{u \in K \mid uL' \subseteq L'\}$ φαίνεται αμέσως ότι είναι υποδακτύλιος του K και $1 \in O$. Επίσης , το O είναι Z-module με rank ίσο με 2.

Πράγματι , $K=Q(\tau)=Q(a+b\tau)=Q(u_o)$. Επειδή $[K : Q]=2$, υπάρχουν το πολύ δύο Q-γραμμικώς ανεξάρτητα στοιχεία του K και συνεπώς υπάρχουν το πολύ δύο Z-γραμμικώς ανεξάρτητα στοιχεία του O. Έχουμε εξ' ορισμού $u_o \in O$. Επειδή $\tau \notin R$, έχουμε επίσης ότι τα $1,u_o$ είναι Z-γραμμικώς ανεξάρτητα. Αφού υπάρχουν το πολύ δύο Z-γραμμικώς ανεξάρτητα στοιχεία του O , θα έχουμε ότι $O=Z+u_oZ$. Εξάλλου αφού τα $1,u_o$ είναι Z-γραμμικώς ανεξάρτητα , το rank του ελεύθερου Z-module $O=Z+u_oZ$ είναι 2.

Λόγω του 1 των παρατήρησεων 2.2.1.3 τώρα έχουμε ότι το O είναι τάξη του K. Αποδεικνύουμε τώρα ότι το L' είναι κλασματικό ιδεώδες της O.

Κατ' αρχήν το L' βλέπουμε εύκολα ότι είναι O-υποmodule του K. Επίσης $u_o \in O \rightarrow (bu_o) \in O$. Για το ζητούμενο , αρκεί επομένως να δειχτεί ότι $(bu_o)L' \subseteq O$ ή ισοδύναμα ότι $(bu_o\tau) \in O$ (αφού $L'=Z+\tau Z$). Από τον ορισμό της O προκύπτει ότι το $(bu_o\tau) \in O$ είναι ισοδύναμο με το $(bu_o\tau) \in \{u \in K \mid uL' \subseteq L'\}$. Ο τελευταίος εγκλεισμος ισχύει γιατί αν $(x+y\tau) \in L'$,

με $x,y\in Z$, τότε $bu_o\tau(x+y\tau) = (bu_ox)\tau+ u_oy(b\tau^2)$ οπότε αφού $u_oL'\subseteq L'$ και $b\tau^2=c+(a-d)\tau$, θα έχουμε $bu_o\tau(x+y\tau)\in L'$.

Το L' είναι proper ιδεώδες της O εξ' ορισμού της O. Τέλος , για κάθε $u\in O-Z$ έχουμε $uL'\subseteq L'$, οπότε θα υπάρχουν $x,y\in Z$ με $u=x+y\tau$ και συνεπώς $K=Q(\tau)=Q(x+y\tau)=Q(u)$.

<u>3.1.3.6 ΟΡΙΣΜΟΣ</u> : Έστω $L = \alpha Z+\beta Z$ lattice του C για $\alpha,\beta\in C$. Θέτουμε $\tau=\frac{\alpha}{\beta}\in(C-R)$ και $L' = Z+\tau Z$.

1. **Κάθε μιγαδικός αριθμός u με την ιδιότητα $uL'\subseteq L'$, θα λέγεται ότι έχει <u>μιγαδικό πολλαπλασισμό με το lattice L</u>.**
   Επειδή αν ένα lattice L έχει μιγαδικό πολλαπλασιασμό με κάποιον μιγαδικό αριθμό , τότε και κάθε ομοιόθετο με το L lattice έχει μιγαδικό πολλαπλασιασμό με τον ίδιο αριθμό , μπορούμε να αναφερόμεστε σε <u>μιγαδικό πολλαπλασιασμό αριθμού με κλάση ομοιοθεσίας ενός lattice</u>.
2. **Αν υπάρχει μιγαδικός αριθμός u_o που δεν ανήκει στο Z ώστε το u_o να έχει μιγαδικό πολλαπλασιασμό με το L , τότε η τάξη O που ορίζεται στην πρόταση 3.1.3.5 θα ονομάζεται <u>πλήρης δακτύλιος μιγαδικού πολλαπλασιασμού του L</u>.**

<u>3.1.3.7 ΠΡΟΤΑΣΗ</u> (Ιδιότητες πλήρους δακτυλίου μιγαδικού πολλαπλασιασμού) :

1. **Έστω lattice L. Θεωρούμε $\tau\in C-Z$, ώστε το L να είναι ομοιόθετο με το latice $L'=Z+\tau Z$**

   (βλ. εκφώνηση πρότασης 3.1.3.5). Έστω ότι υπάρχει ο πλήρης δακτύλιος μιγαδικού πολλαπλασιασμού του L. Αν με O συμβολιστεί ο δακτύλιος αυτός , τότε ισχύουν τα ακόλουθα :

   (a). **$O=\{u\in K \mid uL'\subseteq L'\}$..**

   (b). **Αν το L είναι ομοιόθετο με lattice L_1 , τότε και για το L_1 υπάρχει πλήρης δακτύλιος μιγαδικού πολλαπλασιασμού , ο οποίος μάλιστα είναι ο O.**
2. **Αν O είναι τάξη σε φανταστικό τετραγωνικό σώμα K και a είναι ένα proper κλασματικό ιδεώδες της O , τότε το a είναι lattice του C με πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το O.**

<u>ΑΠΟΔΕΙΞΗ</u>

1. Αν $\lambda\in C-\{0\}$, τότε $\forall u\in C$, $uL\subseteq L \leftrightarrow u\lambda L\subseteq\lambda L$. Τα (a),(b) είναι τώρα προφανή
2. Για το lattice a έχουμε ότι υπάρχει $u_o\in O-Z$, με $u_oa\subseteq a$ (μάλιστα οποιοδήποτε στοιχείο του O-Z έχει αυτήν την ιδιότητα) και συνεπώς από την πρόταση 3.1.3.5 θα υπάρχει ο πλήρης δακτύλιος μιγαδικού πολλαπλασιασμού του lattice a. Έστω O' ο δακτύλιος αυτός και έστω K' το τετραγωνικό φανταστικό

σώμα στο οποίο ο O' είναι τάξη (βλ. πρόταση 3.1.3.5). Γράφοντας $a=\alpha Z+\beta Z$ και θέτοντας $\tau=\frac{\beta}{\alpha}$ θα έχουμε σύμφωνα με την πρόταση 3.1.3.5 ότι $K'=Q(\tau)$. Επόμενως $K'=Q(\tau)\subseteq K$, οπότε αφού $[K' : Q] =$ $= [K : Q] = 2$, θα έχουμε $K=K'$. Τώρα επειδή το a είναι proper ιδεώδες της O θα έχουμε ότι $O = \{u\in K \mid ua\subseteq a\}$. Εξάλλου από το (a) του 1 έχουμε ότι $O'= \{u\in K \mid ua\subseteq a\}$, οπότε και $O=O'$.

<u>3.1.3.8 ΛΗΜΜΑ</u> : Αν A(x),B(x) είναι πολυώνυμα του $C[x]$ πρώτα μεταξύ τους , τότε υπάρχει πεπερασμένο πλήθος μιγαδικών αριθμών λ ώστε το πολυώνυμο A(x)-λB(x) να έχει πολλαπλή ρίζα.

<u>ΑΠΟΔΕΙΞΗ</u> :

Έστω μιγαδικός αριθμός λ και έστω ότι το A(x)-λB(x) έχει πολλαπλή ρίζα $z\in C$. Έχουμε επομένως ότι A'(z)=λB'(z) και συνεπώς A(z)B'(z)-A'(z)B(z)=0. Έχουμε λοιπόν δείξει τον ακόλουθο εγκλεισμό : $\{ z\in C \mid \exists\lambda\in C$: το z είναι πολλαπλή ρίζα του A(x)-λB(x) $\} \subseteq \{ z\in C \mid$ A(z)B'(z)-A'(z)B(z)=0 $\}$

Όμως το σύνολο $\{ z\in C \mid$ A(z)B'(z)-A'(z)B(z)=0 $\}$ είναι πεπερασμένο.

Πράγματι , το πολυώνυμο A(x)B'(x)-A'(x)B(x) είναι διάφορο του μηδενικού πολυωνύμου διότι τα πολυώνυμα A(x) και B(x) είναι πρώτα μεταξύ τους.

Έχουμε λοιπόν ότι το σύνολο $\{ z\in C \mid \exists\lambda\in C$: το z είναι πολλαπλή ρίζα του A(x)-λB(x) $\}$ είναι πεπερασμένο. Αν λοιπόν υπάρχει άπειρο πλήθος μιγαδικών λ ώστε τα A(x)-λB(x) να έχουν πολλαπλή ρίζα , θα υπάρχει $z_o\in C$ και ακολουθία ξένων ανά δύο μιγαδικών αριθμών $(\lambda_n)_{n\in N}$ ώστε το z_o να είναι πολλαπλή ρίζα των πολυωνύμων $A(x)-\lambda_n B(x)$, $\forall n\in N$. Αυτό κατ΄αρχήν σημαίνει ότι $A(z_o)-\lambda_n B(z_o)=0$, $\forall n\in N$. Επειδή η ακολουθία $(\lambda_n)_{n\in N}$ αποτελείται από ξένους ανά δύο μιγαδικούς αριθμούς , θα υπάρχει κάποιος όρος της λ_o διάφορος του μηδενός. Θα έχουμε λοιπόν $A(z_o)-\lambda_o B(z_o)=0$ και συνεπώς επειδή τα A(x),B(x) είναι πρώτα μεταξύ τους δεν μπορεί τα $A(z_o)$ και $B(z_o)$ να είναι ταυτόχρονα μηδέν. Αν $B(z_o)\neq 0$, τότε $\forall n\in N$, $\lambda_n=\frac{A(z_o)}{B(z_o)}$, οπότε η ακολουθία $(\lambda_n)_{n\in N}$ είναι σταθερή , πράγμα άτοπο.

Αν πάλι $A(z_o)\neq 0$, τότε $\forall n\in N$. $\lambda_n=\frac{B(z_o)}{A(z_o)}$, οπότε η ακολουθία $(\lambda_n)_{n\in N}$ είναι σταθερή και έχουμε πάλι άτοπο.

<u>3.1.3.9 ΘΕΩΡΗΜΑ</u> : Έστω L lattice του C και $\wp$ η συνάρτηση του Weierstrass για το L. Αν $\alpha\in C-Z$, τότε :

1. **Τα ακόλουθα είναι ισοδύναμα :**
   - **(i). Η $\wp(\alpha z)$ είναι ρητή έκφραση της $\wp(z)$.**
   - **(ii). $\alpha L\subseteq L$.**
   - **(iii). Το L έχει πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού ο οποίος περιέχει α .**

(iv). Υπάρχει τάξη O σε φανταστικό τετραγωνικό σώμα Κ ώστε να ισχύουν τα ακόλουθα :

- **$\alpha\in\mathsf{O}$.**
- **Το L ομοιόθετο με proper κλασματικό ιδεώδες της O.**

2. Αν ισχύει το (iv) του 1 , τότε τα O,Κ είναι μοναδικά και ο O είναι ο πλήρης δακτύλιος μιγαδικού πολλαπλασιασμού του L.

3. Αν ισχύει το (i) του 1 , τότε η συνάρτηση $\wp(\alpha z)$ μπορεί να έρθει στην μορφή $\wp(\alpha z)=\frac{A(\wp(z))}{B(\wp(z))}$, για πρώτα μεταξύ τους πολυώνυμα A[x],B[x] του C[x] όπου deg(A[x]) = deg(B[x])+1 = [L : αL] = N(α). (Η νόρμα N(α) του α αφορά την επέκταση K/Q όπου το Κ είναι το τετραγωνικό σώμα του (iv) του 1).

ΑΠΟΔΕΙΞΗ

1. (i) → (ii) Έστω ότι $\wp(\alpha z)=\frac{A(\wp(z))}{B(\wp(z))}$ για κάποια πολυώνυμα A[x],B[x] του C[x] , τα οποία (χωρίς περιορισμό της γενικότητας) είναι πρώτα μεταξύ τους. Θα έχουμε λοιπόν $A(\wp(z)) = \wp(\alpha z)\cdot B(\wp(z))$. Επειδή το 0 είναι πόλος τάξης 2 της $\wp$, θα είναι και πόλος τάξης 2 της $\wp(\alpha z)$. Έχουμε τώρα ότι η συνάρτηση $A(\wp(z))$ έχει πόλο στο 0 τάξης $2\cdot\deg(A[x])$ και η συνάρτηση $\wp(\alpha z)\cdot B(\wp(z))$ θα έχει πόλο στο 0 τάξης $2\cdot\deg(B[x])+2$. Συμπεραίνουμε λοιπόν ότι $2\cdot\deg(A[x]) = 2\cdot\deg(B[x])+2$ και επομένως $\deg(A[x])=\deg(B[x])+1$. Η τελευταία σχέση μας δίνει ότι η συνάρτηση $\frac{A(\wp(z))}{B(\wp(z))}$ έχει πόλο σε κάθε σημείο w του lattice L (λόγω του ότι η $\wp$ έχει πόλους στα σημεία του L) και έτσι η $\wp(\alpha z)$ έχει πόλο σε κάθε σημείο w του lattice L , πράγμα που σημάινει ότι η $\wp$ έχει πόλους σε κάθε σημείο του αL. Από το λήμμα 3.1.1.5 όμως έχουμε ότι η $\wp$ έχει πόλους ακριβώς στα σημεία του L και συνεπώς $\alpha L\subseteq L$.

(ii) → (iii) Αν $\alpha L\subseteq L$, τότε επειδή $\alpha\in\mathsf{C}-\mathsf{Z}$, ικανοποιούνται οι υποθέσεις του ορισμού 3.1.3.6 και συνεπώς το L έχει πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού. Εξάλλου από τον ορισμό του πλήρους δακτυλίου μιγαδικού πολλαπλασιασμού έχουμε ότι το α περιέχεται σ'αυτόν τον δακτύλιο.

(iii) → (iv) Αν το L έχει πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού ο οποίος περιέχει α, τότε από την πρόταση 3.1.3.5 έχουμε ότι ο δακτύλιος αυτός αποτελεί τάξη για το τετραγωνικό φανταστικό σώμα $K=\mathsf{Q}(\alpha)$ και μάλιστα το L είναι ομοιόθετο με proper κλασματικό ιδεώδες της προαναφερόμενης τάξης.

(iv) → (i) Έστω ότι υπάρχει τάξη O σε φανταστικό τετραγωνικό σώμα Κ ώστε $\alpha\in\mathsf{O}$ και το L να είναι ομοιόθετο με proper κλασματικό ιδεώδες a της O. Έχουμε κατ' αρχήν ότι το a έχει πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το O (βλ. το 2 της πρότασης 3.1.3.7). Συνεπώς $\mathsf{O}=\{ u\in K \mid u\mathsf{a}\subseteq\mathsf{a} \}$ (βλ. το 1(a) της πρότασης 3.1.3.7) και επομένως $\mathsf{O}=\{ u\in K \mid uL\subseteq L \}$ (βλ. το 1(b) της πρότασης 3.1.3.7). Επειδή $\alpha\in\mathsf{O}$, θα ισχύει $\alpha L\subseteq L$. Άρα η συνάρτηση $\wp(\alpha z)$ είναι περιοδική ως πρός τα στοιχεία του αL (αφού η $\wp$ είναι περιοδική ως προς το L) και είναι μερόμορφη στο C (αφού και η $\wp$ είναι μερόμορφη στο C) , οπότε θα είναι ελλειπτική συνάρτηση του L και μάλιστα άρτια (αφού και η $\wp$ είναι άρτια). Το 2 της

πρότασης 3.1.1.13 θα μας δώσει τώρα ότι η $\wp(\alpha z)$ έιναι ρητή έκφραση της $\wp$.

2. Αν ισχύει το (iv) του 1, και το L είναι ομοιόθετο με proper κλασματικό ιδεώδες $\mathfrak{a}$ του $\mathfrak{O}$, τότε από το 2 της πρότασης 3.1.3.7 έχουμε ότι το $\mathfrak{a}$ έχει πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το $\mathfrak{O}$, πράγμα που σημαίνει $\mathfrak{O}=\{ u\in K \mid u\mathfrak{a}\subseteq\mathfrak{a} \}$ (βλ. το 1(a) της πρότασης 3.1.3.7) και επομένως $\mathfrak{O}=\{ u\in K \mid uL\subseteq L \}$ (βλ. το 1(b) της πρότασης 3.1.3.7). Από την πρόταση 3.1.3.5 όμως έχουμε $K=\mathbb{Q}(\alpha)$, συνεπώς το K είναι μοναδικό , πράγμα που σημαίνει λόγω της ισότητας $\mathfrak{O}=\{ u\in K \mid uL\subseteq L \}$ ότι και το $\mathfrak{O}$ είναι μοναδικό. Εξάλλου επειδή το L είναι ομοιόθετο με το $\mathfrak{a}$ και το $\mathfrak{a}$ έχει πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το $\mathfrak{O}$, από το 1 της πρότασης 3.1.3.7 έχουμε ότι ο $\mathfrak{O}$ είναι ο πλήρης δακτύλιος μιγαδικού πολλαπλασιασμού του L.

3. Έστω ότι $\wp(\alpha z)=\frac{A(\wp(z))}{B(\wp(z))}$ για κάποια πολυώνυμα A[x],B[x] του $\mathbb{C}[x]$, τα οποία (χωρίς περιορισμό της γενικότητας) είναι πρώτα μεταξύ τους. Στην απόδειξη της συνεπαγωγής (i) → (ii) του 1 , δείξαμε με επειχείρημα πόλων ότι deg(A[x])=deg(B[x])+1. Εξάλλου από την ισοδυναμία των προτάσεων του 1 έχουμε ότι το L είναι ομοιόθετο με proper κλασματικό ιδεώδες $\mathfrak{a}$ τάξης $\mathfrak{O}$ τετραγωνικού φανταστικού σώματος αριθμών K με $\alpha\in\mathfrak{O}$. Είναι εύκολο να δεί κανείς ότι αφού τα L και $\mathfrak{a}$ είναι ομοιόθετα , ισχύει

$[L : \alpha L] =[\mathfrak{a} : \alpha\mathfrak{a}]= \#\frac{\mathfrak{a}}{\alpha\mathfrak{a}} = \frac{\#\left(\frac{\mathfrak{O}}{\alpha\mathfrak{a}}\right)}{\#\left(\frac{\mathfrak{O}}{\mathfrak{a}}\right)} = \frac{N(\alpha\mathfrak{a})}{N(\mathfrak{a})}= N(\alpha)\frac{N(\mathfrak{a})}{N(\mathfrak{a})}= N(\alpha)$. Μένει λοιπόν να δειχτεί ότι

$[L : \alpha L]=\deg(A[x])$. Έχουμε $\alpha\in\mathbb{C}-Z \rightarrow \alpha\neq 0$. Θα δείξουμε ότι υπάρχει μιγαδικός αριθμός z_o με $2\alpha z_o\notin L$ (Σ 3.1.3.9.1) ώστε το πολυώνυμο $P(x)=A(x)-\wp(\alpha z_o)B(x)$ να μήν έχει πολλαπλή ρίζα.

Κατ' αρχήν από το λήμμα 3.1.3.8 έχουμε ότι υπάρχει θετικός πραγματικός αριθμός r ώστε για κάθε μιγαδικό αριθμό u που δεν ανήκει στο σύνολο $B(0,r)=\{ v\in\mathbb{C} \mid |v|<r \}$, το $A(x)-uB(x)$ να μην έχει πολλαπλή ρίζα.

Παρατηροούμε όμως ότι επειδή το σύνολο $\wp(\frac{1}{2}L)$ είναι αριθμήσιμο , ισχύει $(\mathbb{C}-B(0,r))-\wp(\frac{1}{2}L) \neq\varnothing$. Υπάρχει λοιπόν μιγαδικός αριθμός u ώστε $u\notin B(0,r)$ και $u\notin\wp(\frac{1}{2}L)$. Αλλά η $\wp$ είναι "επί" του $\mathbb{C}$ (βλ. πρόταση 3.1.1.14) και έχει πόλους στο L , οπότε αν πάρουμε μιγαδικό αριθμό $w\in(\mathbb{C}-L)$ ώστε $\wp(w)=u$ και θέσουμε $z_o:=\frac{w}{\alpha}$, τότε αφ' ενός θα έχουμε $\wp(z_o\alpha)=\wp(w)=u\notin\wp(\frac{1}{2}L)$ που θα δώσει $2\alpha z_o\notin L$, αφ' ετέρου το $A(x)-uB(x) = A(x)-\wp(w)B(x) = A(x)-\wp(z_o\alpha)B(x)$ δεν έχει πολλαπλή ρίζα.

Έχουμε τώρα ότι deg(A[x])=deg(B[x])+1 και συνεπώς θα ισχύει deg(P(x))=deg(A(x)). Εξάλλου $\alpha L\subseteq L$ οπότε $L\subseteq\frac{1}{\alpha}L$. Αν $\{w_t\}_{t\in I}$ είναι πλήρες σύνολο αντιπροσώπων των κλάσεων της ομάδας $(\frac{1}{\alpha}L,+)$ modulo την υποομάδα της (L,+) , τότε θα δείξουμε κατ' αρχήν ότι τα $\wp(z_o+w_t)$,$t\in I$ είναι διακεκριμένα.

Πράγματι , αν $\wp(z_o+w_i) = \wp(z_o+w_j)$, όπου $i,j\in I$ με $i\neq j$, τότε από το 1 της πρότασης 3.1.1.10 έχουμε ότι $(z_o+w_i) \equiv \pm(z_o+w_j)(\mathrm{mod}L)$.
Αν $(z_o+w_i) \equiv (z_o+w_j)(\mathrm{mod}L)$, τότε $w_i\equiv w_j(\mathrm{mod}L)$ πράγμα άτοπο λόγω της εκλογής των w_t , $t\in I$. Αν πάλι $(z_o+w_i) \equiv -(z_o+w_j)(\mathrm{mod}L)$, τότε

$-2z_o \equiv (w_j+w_i) (\mathrm{mod} L)$, όμως $\{w_t \mid t\in I\} \subseteq \frac{1}{\alpha}L \rightarrow \alpha(w_j+w_i)\in L$ και συνεπώς $-2\alpha z_o \equiv \alpha(w_j+w_i) \equiv 0 (\mathrm{mod} L)$, οπότε $2z_o\alpha \in L$ που είναι άτοπο από την σχέση Σ 3.1.3.9.1.

Θα αποδείξουμε τώρα ότι τα $\wp(z_o+w_t)$, $t\in I$ είναι ρίζες του P(x) :

Πράγματι , κατ' αρχήν δείχνουμε ότι $\forall t\in I$, $(z_o+w_t)\notin L$ και $\alpha(z_o+w_t)\notin L$

Έχουμε $w_t\in \frac{1}{\alpha}L \rightarrow \alpha w_t\in L$, οπότε αν $(z_o+w_t)\in L$, τότε $\alpha(z_o+w_t)\in(\alpha L)\subseteq L \rightarrow \alpha z_o\in L \rightarrow 2\alpha z_o\in L$, πράγμα άτοπο από Σ 3.1.3.9.1. Αν πάλι $\alpha(z_o+w_t)\in L$, τότε $\alpha z_o\in L$ οπότε $2\alpha z_o\in L$, πράγμα άτοπο από Σ 3.1.3.9.1.

Έχουμε τώρα $\forall t\in I$, $w_t\in \frac{1}{\alpha}L \rightarrow \alpha w_t\in L \rightarrow \alpha(z_o+w_t)\in(\alpha L)\subseteq L \rightarrow \wp(\alpha(z_o+w_t))=$

$\wp(\alpha z_o)$. Αλλά όμως $\wp(\alpha z)=\frac{A(\wp(z))}{B(\wp(z))} \rightarrow A(\wp(z))=\wp(\alpha z)\cdot B(\wp(z)) \rightarrow$

$A(\wp(z_o+w_t)) = \wp(\alpha(z_o+w_t))B(\wp(z_o+w_t))=\wp(\alpha z_o)B(\wp(z_o+w_t)) \rightarrow A(\wp(z_o+w_t))=$

$=\wp(\alpha z_o)B(\wp(z_o+w_t)) \rightarrow P(\wp(z_o+w_t))=0$, $\forall t\in I$.

Στην συνέχεια θα δείξουμε ότι τα $\wp(z_o+w_t)$, $t\in I$ είναι οι μοναδικές ρίζες του P(x) :

Έστω u_o ρίζα του P(x). Υπάρχει $w_o\in C\text{-}L$ με $\wp(w_o)=u_o$ (βλ. πρόταση 3.1.1.14) Έχουμε $0=P(u_o)=A(u_o)-\wp(\alpha z_o)B(u_o)= A(\wp(w_o))-\wp(\alpha z_o)B(\wp(w_o))$

Άρα $A(\wp(w_o))-\wp(\alpha z_o)B(\wp(w_o))=0$ (Σ 3.1.3.9.2). Ισχύει ότι $B(\wp(w_o))\neq 0$

Αν $B(\wp(w_o))=0$, τότε από Σ 3.1.3.9.2 έχουμε ότι και $A(\wp(w_o))=0$, που είναι άτοπο γιατί τα πολυώνυμα A[x] , B[x] είναι πρώτα μεταξύ τους.

Μπορούμε λοιπόν να γράψουμε $\wp(\alpha z_o)= \frac{A(\wp(w_o))}{B(\wp(w_o))}$. Αλλά $\wp(\alpha z)=\frac{A(\wp(z))}{B(\wp(z))}$ και έτσι $\wp(\alpha z_o)=\wp(\alpha w_o) \rightarrow (\alpha z_o)\equiv \pm(\alpha w_o)(\mathrm{mod} L)$ (βλ. το 1 της πρότασης 3.1.1.10). Επειδή $\wp(-w_o)=\wp(w_o)$ (η $\wp$ συνάρτηση είναι άρτια), θα μπορούσαμε χωρίς περιορισμό της γενικότητας ασχοληθούμε μόνο με την περίπτωση $(\alpha z_o)\equiv(\alpha w_o)(\mathrm{mod} L)$, η οποία θα μας δώσει $(w_o-z_o)\in \frac{1}{\alpha}L$ και συνεπώς από την εκλογή των w_t , $t\in I$, θα έχουμε ότι $\exists t_o\in I$ με $(w_o-z_o)\equiv w_{t_o} (\mathrm{mod} L)$ πράγμα που σημαίνει ότι $u_o=\wp(w_o)=\wp(z_o+w_{t_o})$.

Επειδή επομένως το σύνολο των ριζών του P(x) είναι το $\{\wp(z_o+w_t) \mid t\in I\}$, θα έχουμε ότι $\deg(A(x)) = \deg(P(x)) = \#\{\wp(z_o+w_t) \mid t\in I\}$. Από την άλλη τα $\wp(z_o+w_t)$ είναι διακεκριμένα , οπότε $\#\{\wp(z_o+w_t) \mid t\in I\} =$

$= \#\{w_t \mid t\in I\} = [\frac{1}{\alpha}L : L] = [L : \alpha L]$. Συνεπώς $\mathrm{dag}(A(x))=[L : \alpha L]$.

3.1.3.10 ΠΑΡΑΤΗΡΗΣΕΙΣ : Αν K είναι τετραγωνικό φανταστικό σώμα και O είναι μία τάξη του K , τότε ισχύουν τα ακόλουθα :

1. **Αν a,b είναι proper κλασματικά ιδεώδη της O , τότε τα a,b είναι ομοιόθετα ως lattices αν και μόνο αν aH(O)=bH(O).**
2. **Αν a είναι proper κλασματικό ιδεώδες της O , τότε $j(a)\in R$ αν και μόνο αν η τάξη του aH(O) στην C(O) είναι 2.**
   (Προκύπτει από το 1 , την πρόταση 3.1.2.7 , την παρατήρηση 3.1.2.8 και το γεγονός ότι $a^{-1}H(O) = \bar{a}\, H(O)$ που συνεπάγεται το πόρισμα 2.2.2.12)

3.1.3.11 ΠΡΟΤΑΣΗ : Αν O είναι τάξη σε τετραγωνικό φανταστικό σώμα K , τότε υπάρχει "1-1" και "επί" αντιστοιχία ανάμεσα στην ομάδα κλάσεων ιδεωδών C(O) και στις κλάσεις ομοιοθεσίας των lattices με πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το O , ώστε κάθε κλάση aH(O) της C(O) (για proper ιδεώδες a της O) να ανιστοιχεί στην κλάση ομοιοθεσίας του lattice a.

ΑΠΟΔΕΙΞΗ

Θεωρούμε την απεικόνιση που αναφέρεται στην εκφώνηση. Η απεικόνιση αυτή είναι καλά ορισμένη και "1-1" λόγω του 1 της παρατήρησης 3.1.3.10. Επίσης είναι "επί" αφού αν C είναι κλάση ομοιοθεσίας lattices με πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το O , τότε αν L είναι ένας αντιπρόσωπος της κλάσης C , από το 2 του θεωρήματος 3.1.3.9 θα έχουμε ότι το L είναι ομοιόθετο με proper κλασματικό ιδεώδες a της O. Επόμένως το a έχει πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το O (βλ. ο 2 της πρότασης 3.1.3.7) και η κλάση ομοιοθεσίας που ορίζει το a είναι η C.

3.1.3.12 ΠΟΡΙΣΜΑ : Αν O είναι τάξη σε τετραγωνικό φανταστικό σώμα K , τότε υπάρχει πεπερασμένο σύνολο μιγαδικών αριθμών A , με πλήθος #A=h(O) ώστε για κάθε lattice L με πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το O να ισχύει $j(L)\in A$.

ΑΠΟΔΕΙΞΗ

Έστω $\{a_1,a_2,\ldots,a_{h(O)}\}$ πλήρες σύστημα αντιπροσώπων της ομάδας πηλίκο $C(O)=\frac{I(O)}{H(O)}$. Θέτουμε $A = \{ j(a_1),j(a_2),\ldots,j(a_{h(O)}) \}$. Λόγω της αντιστοιχίας που αναφέρεται στην πρόταση 3.1.3.11 και της πρότασης 3.1.2.7 έχουμε ότι το A έχει πληθάριθμο h(O) και για κάθε lattice L με πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού το O , ισχύει $j(L)\in A$.

3.1.3.13 ΠΑΡΑΔΕΙΓΜΑ-ΕΦΑΡΜΟΓΗ : Είναι προφανές ότι αν ένα lattice έχει μιγαδικό πολλαπλασιασμό με κάποιον μιγαδικό αριθμό α , τότε και κάθε ομοιόθετο του lattice έχει μιγαδικό πολλαπλασιασμό με το α. Παραδείγματος χαριν

τα lattices που έχουν μιγαδικό πολλαπλασιασμό με το $\sqrt{-5}$ είναι τα $L_1= \mathbb{Z}+\sqrt{-5}\,\mathbb{Z}$, $L_2=2\mathbb{Z}+(1+\sqrt{-5})\mathbb{Z}$ και όλα τα ομοιόθετα τους.

ΑΠΟΔΕΙΞΗ

Έστω lattice L το οποίο έχει μιγαδικό πολλαπλασιασμό με το $\sqrt{-5}$. Από το θεώρημα 3.1.3.9 έχουμε ότι το L έχει πλήρη δακτύλιο μιγαδικού πολλαπλασιασμού $\mathcal{O}$ με $\sqrt{-5} \in \mathcal{O}$ σε τετραγωνικό φανταστικό σώμα K. Επειδή $\sqrt{-5} \notin \mathbb{Z}$, θα έχουμε από την πρόταση 3.1.3.5 ότι $K=\mathbb{Q}(\sqrt{-5})$. Από θεωρία τετραγωνικών επεκτάσεων του $\mathbb{Q}$ (βλ. πρόταση 2.1.1.5) παίρνουμε ότι $R_K=\mathbb{Z}[\sqrt{-5}]$. Τώρα αν $f=\mathrm{cond}(\mathcal{O})$, θα ισχύει $\mathcal{O} = \mathbb{Z}+fR_K = \mathbb{Z}+f\mathbb{Z}[\sqrt{-5}]$. Επειδή όμως πρέπει $\sqrt{-5} \in \mathcal{O}$, με στοιχειώδεις πράξεις μπορούμε να δείξουμε ότι $\mathcal{O}=\mathbb{Z}[\sqrt{-5}]$ και συνεπώς $d_{\mathcal{O}}= -20$. Από τον πίνακα της εφαρμογής 1.2.2.8 έχουμε ότι $C(-20) = \{ [x^2+5y^2] , [2x^2+2xy+3y^2])$, πράγμα που σημαίνει ότι $C(\mathcal{O}) = \{ (\mathbb{Z}+\sqrt{-5}\,\mathbb{Z})H(\mathcal{O}) , (2\mathbb{Z}+(1+\sqrt{-5})\mathbb{Z})H(\mathcal{O}) \}$ και συνεπώς η πρόταση 3.1.3.11 θα μας δώσει ότι τα lattices που έχουν μιγαδικό πολλαπλασιασμό με το $\sqrt{-5}$ είναι τα $L_1= \mathbb{Z}+\sqrt{-5}\,\mathbb{Z}$, $L_2=2\mathbb{Z}+(1+\sqrt{-5})\mathbb{Z}$ και όλα τα ομοιόθετα τους. Μάλιστα η πρόταση 3.1.3.11 μας δίνει επιπλέον ότι υπάρχουν ακρίβώς δύο κλάσεις ομοιοθεσίας lattices τα οποία έχουν μιγαδικό πολλαπλασιασμό με το $\sqrt{-5}$.

§2 MODULAR ΣΥΝΑΡΤΗΣΕΙΣ

3.2.1 ΟΙ ΣΥΝΑΡΤΗΣΕΙΣ j , g_2 , g_3 , Δ

Αποδείξεις για την παράγραφο 3.2.1 μπορούν να βρεθούν στις σελίδες 220-224 του [Cox].

3.2.1.1 ΟΡΙΣΜΟΣ : 1. **Η j - συνάρτηση ορίζεται στο πάνω μιγαδικό ημιεπίπεδο $\mathfrak{h}=(z\in\mathbb{C} \mid Im(z)>0\}$ ως εξής : Για $\tau\in\mathfrak{h}$, το $j(\tau)$ είναι η j - αναλλοίωτη του lattice $\mathbb{Z}+\tau\mathbb{Z}$. Δηλαδή $j(\tau) := j(\mathbb{Z}+\tau\mathbb{Z})$.**

2. **Η g_2 - συνάρτηση ορίζεται στο πάνω μιγαδικό ημιεπίπεδο $\mathfrak{h}=(z\in\mathbb{C} \mid Im(z)>0\}$ ως εξής : $\forall\tau\in\mathfrak{h}$, $g_2(\tau) := g_2(\mathbb{Z}+\tau\mathbb{Z})$.**
3. **Η g_3 - συνάρτηση ορίζεται στο πάνω μιγαδικό ημιεπίπεδο $\mathfrak{h}=(z\in\mathbb{C} \mid Im(z)>0\}$ ως εξής : $\forall\tau\in\mathfrak{h}$, $g_3(\tau) := g_3(\mathbb{Z}+\tau\mathbb{Z})$.**
4. **Η Δ - συνάρτηση ορίζεται στο πάνω μιγαδικό ημιεπίπεδο $\mathfrak{h}=(z\in\mathbb{C} \mid Im(z)>0\}$ ως εξής : $\forall\tau\in\mathfrak{h}$, $\Delta(\tau) := \Delta(\mathbb{Z}+\tau\mathbb{Z})$.**

3.2.1.2 ΠΑΡΑΤΗΡΗΣΕΙΣ : 1. **$\Delta(\tau)\neq 0$, $\forall\tau\in\mathfrak{h}$.**

2. **Αν $\tau\in(i\mathbb{R}\cap\mathfrak{h})$, τότε $g_2(\tau), g_3(\tau), \Delta(\tau), j(\tau)\in\mathbb{R}$ (βλ. σχόλια 3.1.1.15 και παρατήρηση 3.1.2.8).**

3.2.1.3 ΣΧΟΛΙΑ : **Οι ιδιότητες της j συνάρτησης είναι στενά συνδεδεμένες με την δράση της ομάδας $sl(2,\mathbb{Z})$ στο σύνολο $\mathfrak{h}$.Η δράση αυτή ορίζεται ως εξής : Για πίνακα $\gamma=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in sl(2,\mathbb{Z})$ και στοιχείο $\tau\in\mathfrak{h}$, ορίζουμε $\gamma\cdot\tau = \frac{a\tau+b}{c\tau+d}\in\mathfrak{h}$. Τα στοιχεία $\tau,\gamma\cdot\tau$ θα λέγονται <u>sl(2,Z)-ισοδύναμα</u>. Είναι εύκολο να δεί κανείς ότι η $sl(2,\mathbb{Z})$-ισοδυναμία είναι σχέση ισοδυναμίας στο $\mathfrak{h}$ και ότι για $\gamma,\gamma'\in sl(2,\mathbb{Z})$ και $\tau\in\mathfrak{h}$ ισχύει $\gamma\cdot(\gamma'\cdot\tau) = (\gamma\gamma')\cdot\tau$.**

3.2.1.4 ΛΗΜΜΑ : 1. **Κάθε στοιχείο του $\mathfrak{h}$ είναι $sl(2,\mathbb{Z})$-ισοδύναμο με κάποιο $\tau'\in\mathfrak{h}$ ώστε $|Re(\tau')|\leq\frac{1}{2}$ και $|Im(\tau')|\geq\frac{1}{2}$.**

2. **Αν $\tau,\tau'\in\mathfrak{h}$, τότε υπάρχουν περιοχές U του τ και V του τ' ώστε το σύνολο $\{\gamma\in sl(2,\mathbb{Z}) \mid \forall z\in U , (\gamma\cdot z)\notin V\}$ να είναι πεπερασμένο.**
3. **Αν $\tau\in\mathfrak{h}$, τότε υπάρχει περιοχή U του τ ώστε για κάθε στοιχείο γ της $sl(2,\mathbb{Z})$ να ισχύει η ακόλουθη ισοδυναμία : " $\forall\exists z\in U : (\gamma\cdot z)\in U$" $\leftrightarrow$ "$\gamma\cdot\tau=\tau$"**

3.2.1.5 ΠΡΟΤΑΣΗ : Αν $\tau,\tau' \in \mathbf{h}$, τότε τα lattices $\mathbf{Z}+\tau\mathbf{Z}$, $\mathbf{Z}+\tau'\mathbf{Z}$ είναι ομοιόθετα αν και μόνο αν υπάρχει $\gamma \in sl(2,\mathbf{Z})$ με $\gamma \cdot \tau = \tau'$. (Η πρόταση αυτή είναι ακριβώς η ισοδυναμία $2 \leftrightarrow 3$ του λήμματος 2.2.3.6 και έχει αποδειχτεί.)

3.2.1.6 ΠΡΟΤΑΣΗ (Ιδιότητες της συνάρτησης j) :

1. Η j συνάρτηση είναι ολόμορφη στο $\mathbf{h}$.
2. Αν $\tau,\tau' \in \mathbf{h}$, τότε ισχύει η ακόλουθη ισοδυναμία : " $j(\tau)=j(\tau') \leftrightarrow \exists \gamma \in sl(2,\mathbf{Z}) : \gamma \cdot \tau = \tau'$ ".
3.
   - $\lim_{Im(\tau) \to +\infty} g_3(\tau) = \frac{8}{27}\pi^6$
   - $\lim_{Im(\tau) \to +\infty} g_2(\tau) = \frac{4}{3}\pi^4$
   - $\lim_{Im(\tau) \to +\infty} \Delta(\tau) = 0$
   - $\lim_{Im(\tau) \to +\infty} j(\tau) = \infty$
4. Η j συνάρτηση είναι "επί" του $\mathbf{C}$.
5. Για κάθε $\tau \in \mathbf{h}$ ισχύει $j'(\tau) \neq 0$, εκτός από τις ακόλουθες περιπτώσεις
   (a). Υπάρχει $\gamma \in sl(2,\mathbf{Z})$ με $\tau = \gamma \cdot i$.
   Στην περίπτωση αυτή ισχύει ότι $j'(\tau)=0$ και επιπλέον $j''(\tau) \neq 0$.
   (b). Υπάρχει $\gamma \in sl(2,\mathbf{Z})$ με $\tau = \gamma \cdot \omega$.
   Στην περίπτωση αυτή ισχύει ότι $j'(\tau) \neq 0$ και επιπλέον $j''(\tau)=0$, $j'''(\tau) \neq 0$.
6. Δεν υπάρχει πολυώνυμο $P(x) \in \mathbf{C}[x]$ με $P(j(\tau))=0$.
   (Αφού από την ανάλυση Fourier της j - βλ. [COX] θεώρ. 11.8 σελ. 225 - προκύπτει ότι $\lim_{Im(\tau) \to +\infty} P(j(\tau)) = \infty$)

3.2.1.7 ΠΟΡΙΣΜΑ : Αν g_2,g_3 είναι μιγαδικοί αριθμοί με $g_2^3 - 27g_3^2 \neq 0$, τότε υπάρχει lattice L με $g_2(L)=g_2$ και $g_3(L)=g_3$. (Η πρόταση αυτή προκύπτει από το ότι η j είναι "επί" του $\mathbf{C}$.)

3.2.2 ΕΙΣΑΓΩΓΗ ΣΤΙΣ MODULAR ΣΥΝΑΡΤΗΣΕΙΣ

3.2.2.1 ΟΡΙΣΜΟΣ : Έστω $m\in N$. Οι υποομάδες $\Gamma_o(m)$ και $\Gamma_o(m)^t$ και $\bar{\Gamma}(m)$ της $SL(2,Z)$ ορίζονται ως εξής :

$$\Gamma_o(m) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,Z) \mid c\equiv 0 (mod m) \}$$

$$\Gamma_o(m)^t := \{ A\in SL(2,Z) \mid A^t\in \Gamma_o(m) \} = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,Z) \mid b\equiv 0 (mod m) \}$$

$$\bar{\Gamma}(m) := \Gamma_o(m)\cap \Gamma_o(m)^t.$$

Επίσης ορίζεται το υποσύνολο $C(m)$ του $M_{2x2}(Z)$ ως εξής :

$$C(m) := \{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_{2x2}(Z) \mid ad=m , a>0 , 0\le b<d , \text{ΜΚΔ}(a,b,d)=1 \}$$

Ο πληθάριθμος του $C(m)$ θα συμβολίζεται με $c(m)$.

3.2.2.2 ΠΡΟΤΑΣΗ : 1. $\Gamma_o(1) = SL(2,Z)$.

2. $$c(m) = m\cdot \prod_{\substack{p\in P \\ p \mid m}} \left(1 + \frac{1}{p}\right).$$ **(Βλ. [Cox] , άσκηση 11.9 , σελ 245).**

3.2.2.3 ΣΧΟΛΙΑ : Υπενθυμίζουμε ότι αν $S\subseteq SL(2,Z)$ και f είναι μια μιγαδική συνάρτηση ορισμένη σε

υποσύνολο A του C λέγεται αναλλοίωτη από την S στο A αν $f(\gamma\bullet\tau)=f(\tau)$, $\forall\tau\in A,\forall\gamma\in S$.

3.2.2.4 ΠΡΟΤΑΣΗ : Άν $m\in N$ και f είναι συνάρτηση ορισμένη στο $h=\{z\in C \mid Im(z)>0\}$ ώστε να ισχύουν τα

ακόλουθα :

(a). Η f είναι μερόμορφη στο C.

(b). Η f είναι αναλλοίωτη από την $\Gamma_o(m)$.

και στην οριζόντια λωρίδα $L=\{z\in C \mid a_o\le Im(z)\le b_o\}$, με $a_o,b_o\in R$, $a_o<b_o$, του h η f

δεν έχει πόλο , τότε η $f_{|L}$ γράφεται κατά μοναδικό τρόπο σαν σειρά Fourier :

$$f_{|L}(\tau)= \sum_{n=-\infty}^{+\infty} \alpha_n e^{\frac{2\pi i\tau}{m}n} = \sum_{n=-\infty}^{+\infty} \alpha_n q^{\frac{1}{m}n} \quad , q=e^{2\pi i\tau}.$$

(Βλ. [Cox] σελ. 225).

3.2.2.5 ΛΗΜΜΑ : Έστω $m \in \mathbb{N}$ και μιγαδική συνάρτηση $f : h \to \mathbb{C}$ με τις ιδιότητες (a) και (b) της πρότασης 3.2.2.4. Αν $\gamma \in SL(2,\mathbb{Z})$, τότε και η συνάρτηση $\tau \to f(\gamma \cdot \tau)$ έχει τις ιδιότητες (a) και (b) και συνεπώς σε οριζόντιες λωρίδες του h στις οποίες η $f(\gamma \cdot \tau)$ δεν έχει πόλους , έχει έκφραση σε σειρά Fourier. (Βλ. [Cox] σελ. 225).

3.2.2.6 ΟΡΙΣΜΟΣ : Μια μιγαδική συνάρτηση $f(\tau)$ ορισμένη στο πάνω μιγαδικό επίπεδο $h=\{z \in \mathbb{C} \,|\, Im(z)>0\}$ για την οποία η σειρά Fourier της $f(\gamma \cdot \tau)$ (όπου υπάρχει) , $\forall \gamma \in SL(2,\mathbb{Z})$ έχει πεπερασμένο πλήθος αρνητικών εκθετών ονομάζεται " meromorphic at the cusps ".

3.2.2.7 ΟΡΣΜΟΣ : Έστω $m \in \mathbb{N}$. Μια μιγαδική συνάρτηση $f(\tau)$ ορισμένη στο πάνω μιγαδικό επίπεδο

$h=\{z \in \mathbb{C} | Im(z)>0$ που ικανοποιεί τις ακόλουθες ιδιότητες :

(a). Η f είναι μερόμορφη στο $\mathbb{C}$.

(b). Η f είναι αναλλοίωτη από την $\Gamma_o(m)$.

(c). Η f είναι meromorphic at the cusps.

λέγεται "modular συνάρτηση για την $\Gamma_o(m)$ ".

3.2.2.8 ΠΡΟΤΑΣΗ (Ιδιότητες modular συναρτήσεων) : Έστω $m \in \mathbb{N}$. Ισχύουν τα ακόλουθα :

1. Άθροισμα , γινόμενο και πηλίκο modular συναρτήσεων για την $\Gamma_o(m)$ είναι modular συνάρτηση για την $\Gamma_o(m)$.
2. Οι σταθερές συναρτήσεις είναι modular συναρτήσεις της $\Gamma_o(m)$.
3. Αν f είναι ολόμορφη modular συνάρτηση για την $\Gamma_o(m)$ στο h , τότε τα ακόλουθα είναι ισοδύναμα :
   - $\lim_{\substack{Im(\tau) \to +\infty \\ \tau \in h}} f(\tau) \in \mathbb{C}$.
   - Η έφραση fourier της f στο h έχει την μορφή $\sum_{n=0}^{+\infty} \alpha_n q^{\frac{1}{m}n}$, $q=e^{2\pi i \tau}$.
4. Αν f είναι ολόμορφη modular συνάρτηση για την SL(2,Z) στο h , ώστε $\lim_{\substack{Im(\tau) \to +\infty \\ \tau \in h}} f(\tau) \in \mathbb{C}$, τότε η f είναι σταθερή.

(Τα 1,2,3 είναι απλές ασκήσεις , ενώ για το 4 παραπέμπουμε στο λήμμα 11.10 του [Cox] σελ.226).

3.2.2.9 ΠΡΟΤΑΣΗ : Η j συνάρτηση είναι modular για την $SL(2,Z)$ και μάλιστα η έκφραση Fourier της

είναι : $j(\tau)=\frac{1}{q}+\sum_{n=0}^{+\infty} c_n q^n$, όπου $q=e^{2\pi i\tau}$ και $c_n\in Z$, $\forall n\geq 0$ με $c_0=744, c_1=196884$.

(Για την απόδειξη παραπέμπουμε στα [Lang] §4.1 και [Apostol] §1.15).

3.2.2.10 ΣΧΟΛΙΑ : Στην πιο πάνω πρόταση φαίνεται γιατί υπάρχει ο συντελεστής 1728 στον ορισμό

3.1.2.6 της j - αναλλοίωτης. Πολλαπλασιάζοντας με το 1728 , οι συνελεστές της έκφρασης fourier της j συνάρτησης γίνονται ακέραιοι αριθμοί.

3.2.2.11 ΛΗΜΜΑ : Έστω $\sigma_o=\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}\in C(m)$. Ισχύουν τα ακόλουθα :

1. **$\Gamma_o(m) = (\sigma_o^{-1}\cdot SL(2,Z)\cdot\sigma_o)\cap SL(2,Z)$.**
2. **Υπάρχει "1-1" και "επί" αντιστοιχία μεταξύ των στοιχείων της $C(m)$ και των δεξιών cosets της $\Gamma_o(m)$ στην $SL(2,Z)$. Η αντιστοιχία αυτή δίνεται από το παρακάτω διάγραμμα :**

$$\sigma \rightarrow (\sigma_o^{-1}\cdot SL(2,Z)\cdot\sigma)\cap SL(2,Z) .$$

(Βλ. [Cox] άσκηση 11.8 σελ. 245).

3.2.2.12 ΛΗΜΜΑ : Έστω $m\in N$ και $\gamma\in SL(2,Z)$. Αν σ είναι το μοναδικό στοχείο του $C(m)$ με $(\sigma_o^{-1}\cdot SL(2,Z)\cdot\sigma)\cap SL(2,Z) = \Gamma_o(m)\cdot\gamma$ (βλ. Λήμμα 3.2.2.11) , τότε ισχύει ότι :

$$j(m\cdot\gamma\cdot\tau) = j(\sigma\tau) , \forall\tau\in h. \quad (\Sigma\ 3.2.2.12.1).$$

Μάλιστα , το σ είναι το μοναδικό στοιχείο του $C(m)$ με την ιδιότητα Σ 3.2.2.12.1 και αν $\sigma=\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, τότε :

$$j(\sigma\tau)=\frac{\zeta_m^{-ab}}{\left(q^{\frac{1}{m}}\right)^{a^2}}+\sum_{n=0}^{\infty}c_n\zeta_m^{abn}\left(q^{\frac{1}{m}}\right)^{a^2n}\quad,\ \forall\tau\in h\ \ (\Sigma\ 3.2.2.12.2)$$

όπου $q=e^{2\pi i\tau}$, $\zeta_m=e^{2\pi i/m}$ και $(c_n)_{n=0}^{\infty}$ η ακολουθία συντελεστών Fourier της *j* συνάρτησης (βλ. πρόταση 3.2.2.9).

(Απόδειξη του λήμματος υπάρχει στην σελίδα 229 του [Cox]).

<u>3.2.2.13 ΠΡΟΤΑΣΗ</u> (Αρχή q- αναπτύγματος του Hasse) : Έστω A προσθετική υποομάδα της (C,+) και

f(τ) ολόμορφη modular συνάρτηση για την SL(2,Z). Αν το ανάπτυγμα Fourier της f

είναι $f(\tau)=\sum_{n=-M}^{+\infty}\alpha_n q^n$, όπου $q=e^{2\pi i}$, $M\in N$, και $\alpha_{-M},\alpha_{-M+1},\ldots,\alpha_0\in A$, τότε η f είναι

πολυωνυμική έκφραση της *j* συνάρτησης με συντελεστές από το Α.

(Βλ. [Cox] άσκηση 11.12 , σελ. 246).

3.2.3 Η MODULAR ΕΞΙΣΩΣΗ

3.2.3.1 ΠΡΟΤΑΣΗ : Από το 2 της πρότασης 3.2.2.2 έχουμε $c(m)=\#\mathbf{C}(m)<\infty$. Άν f είναι ένα συμμετρικό πολυώνυμο των $j(\sigma\tau)$, $\sigma\in\mathbf{C}(m)$, τότε η $f(\tau)$ είναι modular συνάρτηση για την $SL(2,\mathbf{Z})$ και ειδικότερα υπάρχει πολυώνυμο $A(x)$ του $\mathbf{Z}[x]$ ώστε $f(\tau)=A(j(\tau))$.

ΑΠΟΔΕΙΞΗ

Από το 2 του λήμματος 3.2.2.11 έχουμε ότι $c(m)=\#\mathbf{C}(m)=[SL(2,\mathbf{Z}),\Gamma_o(m)]$. Έστω λοιπόν ότι τα δεξιά cosets της $\Gamma_o(m)$ στην $SL(2,\mathbf{Z})$ είναι τα $\Gamma_o(m)\gamma_1,\Gamma_o(m)\gamma_2,\ldots,\Gamma_o(m)\gamma_{c(m)}$, για $\gamma_1,\gamma_2,\ldots,\gamma_{c(m)}\in SL(2,\mathbf{Z})$.

Το $f(\tau)$ είναι επομένως συμμετρικό πολυώνυμο των $j(m\cdot\gamma_t\cdot\tau)$, $t=1,2,..,c(m)$. Θα δείξουμε κατ' αρχήν ότι το $f(\tau)$ είναι αναλλοίωτο από την $SL(2,\mathbf{Z})$, δηλαδή ότι $f(\gamma\tau)=f(\tau)$,$\forall\gamma\in SL(2,\mathbf{Z})$.

Πράγματι , αν $\gamma\in SL(2,\mathbf{Z})$ τότε το $\{\gamma_1\cdot\gamma,\gamma_2\cdot\gamma,\ldots,\gamma_{c(m)}\cdot\gamma\}$ (λόγω της εκλογής του $\{\gamma_t\,|\,t=1,2..c(m)\}$ ως πλήρους σύστηματος αντπροσώπων δεξιών κλάσεων modulo $\Gamma_o(m)$) είναι και αυτό πλήρες σύστημα αντπροσώπων δεξιών κλάσεων modulo $\Gamma_o(m)$. Συνεπώς για κάθε συμετρικό πολυώνυμο $c(m)$- μεταβλητών $P(x_1,x_2,\ldots,x_{c(m)})$ με συντελεστές από τον δακτύλιο $\mathbf{H}(\mathbf{h};\mathbf{C})$ των ολόμορφων συναρτήσεων στο πάνω μιγαδικό ημιεπίπεδο $\mathbf{h}$ ισχύει :

$$P(j(m\gamma_1\cdot\gamma\cdot\tau),j(m\gamma_2\cdot\gamma\cdot\tau),\ldots,j(m\gamma_{c(m)}\cdot\gamma\cdot\tau))=P(j(m\gamma_1\cdot\tau),j(m\gamma_1\cdot\tau),\ldots,j(m\gamma_1\cdot\tau)).$$

Αυτό σημαίνει ότι $f(\gamma\cdot\tau)=f(\tau)$.

Εχουμε επίσης ότι η $f(\tau)$ είναι ολόμοφη συνάρτηση στο $\mathbf{h}$ αφού η j - συνάρτηση είναι ολόμορφη στο $\mathbf{h}$ (βλ. το 1 ης πρότασης 3.2.1.6). Η f επόμένως είναι ολόμορφη στο $\mathbf{h}$ και αναλλοίωτη από την $SL(2,\mathbf{Z})$ και έχει κατά συνπεπεια ανάπτυξη Fourier στο $\mathbf{h}$ της μορφής $\sum_{n=-\infty}^{+\infty}\alpha_n e^{2\pi i\tau n}$, $\alpha_n\in\mathbf{C}$,$\forall n\in\mathbf{Z}$. Θα δείξουμε τώρα ότι η f είναι meromorphic at the cusps.

Πράγματι , η σχέση Σ 3.2.2.12.1 του λήμματος 3.2.2.12 και η αντιστοιχία του 2 του λήμματος 3.2.2.11 μας δίνει ότι οι συναρτήσεις $j(m\cdot\gamma_t\cdot\tau)$, $t=1,2,\ldots,c(m)$ εκφράζονται σε σειρά Fourier με πεπερασμένο πλήθος αρνητικών εκθετών. Επειδή το $f(\tau)$ είναι πολυώνυμο των $j(m\cdot\gamma_t\cdot\tau)$, $t=1,2,..,c(m)$, θα μπορεί να γραφεί ως σειρά Fourier με πεπερασμένο πλήθος αρνητικών εκθετών. Από τη μοναδικότητα της έκφρασης σε σειρά Fourier , έχουμε ότι η σειρά Fourier της f θα έχει πεπερασμένο πλήθος αρνητικών εκθετών. Επειδή $f(\gamma\tau)=f(\tau)$,$\forall\gamma\in SL(2,\mathbf{Z})$, θα έχουμε επιπλέον ότι ότι για κάθε $\gamma\in SL(2,\mathbf{Z})$, η σειρά Fourier της $f(\gamma\tau)$ θα έχει πεπερασμένο πλήθος αρνητικών εκθετών και έτσι η f είναι meromorphic at the cusps (βλ. ορισμό 3.2.2.6).

Η $f(\tau)$ επομένως σύμφωνα με τον ορισμό 3.2.2.7 θα είναι modular συνάρτηση για την $SL(2,\mathbf{Z})$.

Από την αρχή του q - αναπτύγματος του Hasse (βλ. πρόταση 3.2.2.13) έχουμε ότι υπάρχει πολυώνυμο $A(x)\in\mathbf{C}[x]$ με $f(\tau)=A(j(\tau))$. Θα δείξουμε στην συνέχεια ότι $A(x)\in\mathbf{Z}[x]$. Το λήμμα 3.2.2.12 δίνε ότι για κάθε $\sigma\in\mathbf{C}(m)$, το $j(\sigma\tau)$ είναι μερομορφική έκφραση του $q^{\frac{1}{m}}$, (όπου $q=e^{2\pi i\tau}$) με συντελεστές από το $\mathbf{Q}(\zeta_m)$,

($\zeta_m=e^{2\pi i/m}$). Ως πρώτο βήμα θα δείξουμε ότι κάθε στοιχείο της ομάδας Galois $G(\mathbb{Q}(\zeta_m) \mid \mathbb{Q})$ επάγει μετάθεση του συνόλου $\{ j(\sigma\tau) \mid \sigma\in C(m) \}$ δρώντας στους συντελεστες των εκφράσεων Fourier των $j(\sigma\tau)$, $\sigma\in C(m)$.

Πράγματι, αν φ είναι στοιχείο της ομάδας Galois $G(\mathbb{Q}(\zeta_m) \mid \mathbb{Q})$, τότε υπάρχει $k\in N$ με ΜΚΔ(k,m)=1 ώστε $\varphi(\zeta_m)=\zeta_m^{\,k}$. Είναι εύκολο να δεί κανείς ότι ο φ επάγει αυτομορφισμό $\hat{\varphi}$ στο σύνολο των μερομορφικών εκφράσεων του $q^{\frac{1}{m}}$ με συντελεστές από το $\mathbb{Q}(\zeta_m)$, δρώντας στους συντελεστές. Έστω τώρα $\sigma=\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$. Έχουμε λοιπόν ad=m , 0≤b<d , ΜΚΔ(a,b,d)=1 (βλ. ορισμό 3.2.2.1). Τώρα , το λήμμα 3.2.2.12 θα μας δώσει ότι

$\hat{\varphi}(j(\sigma\tau)) = \dfrac{\zeta_m^{-abk}}{\left(q^{\frac{1}{m}}\right)^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abnk} \left(q^{\frac{1}{m}}\right)^{a^2 n}$. Θέτουμε b' το μοναδικό στοιχείο του συνόλου { 0,1,2,…, d-1} με b'≡bk(modd) , οπότε αφού ad=m θα έχουμε $\zeta_m^{\,abk} = \zeta_m^{\,ab'}$. Συνοψίζοντας , ισχύει $\hat{\varphi}(j(\sigma\tau)) = \dfrac{\zeta_m^{-ab'}}{\left(q^{\frac{1}{m}}\right)^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{ab'n} \left(q^{\frac{1}{m}}\right)^{a^2 n}$.

Παρατηρούμε όμως ότι $\begin{pmatrix} a & b' \\ 0 & d \end{pmatrix} \in C(m)$, οπότε θέτοντας $\sigma'=\begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}$ θα πάρουμε $\hat{\varphi}(j(\sigma\tau)) = j(\sigma'\tau)$ (βλ. λήμμα 3.2.2.12).

Η τελευταία σχέση μας δίνει ότι κάθε στοιχείο της ομάδας Galois $G(\mathbb{Q}(\zeta_m) \mid \mathbb{Q})$ επάγει μετάθεση του συνόλου $\{ j(\sigma\tau) \mid \sigma\in C(m) \}$ δρώντας στους συντελεστες των εκφράσεων Fourier.

Θα δείξουμε στην συνέχεια ότι η f(τ) έχει μερομορφική έκφραση Fourier με ακέραιες δυνάμεις του $q=e^{2\pi i\tau}$ και με συντελεστές ακεραίους αριθμούς.

Αφού το f(τ) είνα συμμετρικό πολυώνυμο των $j(\sigma\tau)$, $\sigma\in C(m)$ θα έχουμε ότι κάθε στοιχείο της ομάδας $G(\mathbb{Q}(\zeta_m) \mid \mathbb{Q})$ δρώντας στους συντελεστές της έκφρασης Fourier της f(τ) θα τους αφήνει αναλλοίωτους. Αυτό σημαίνει ότι οι συντελεστές της έκφρασης Fourier της f(τ) ανήκουν στο $\mathbb{Q}$. Παρατηρούμε όμως ότι οι συντελεστές των εκφράσεων Fourier των $j(\sigma\tau)$, $\sigma\in C(m)$ είναι αλγεβρικοί ακέραιοι (βλ. λήμμα 3.2.2.12) και συνεπώς και οι συντελεστές της έκφρασης Fourier της f(τ) πρέπει να είναι αλγεβρικοί ακέραιοι. Συνοψίζοντας, οι συντελεστές της έκφρασης Fourier της f(τ) πρέπει να είναι αλγεβρικοί ακέραιοι και ταυτόχρονα ρητοί αριθμοι , οπότε θα ανήκουν στο $\mathbb{Z}$. Εξάλλου στην αρχή της απόδειξης δείξαμε ότι η f(τ) έχει έκφραση σε σειρά Fourier με ακέραιες δυνάμεις του $q=e^{2\pi i\tau}$, οπότε έχουμε το ζητούμενο .

Γράφοντας τωρα $A(x)=A_r x^r+A_{r-1}x^{r-1}+\ldots+A_1 x+A_0$, με $r\in N$, $A_r\neq 0$, $A_t\in C$,t=0,1,…,r και θεωρώντας τις εκφράσεις Fourier των f(τ) , $j(\sigma\tau)$, $\sigma\in C(m)$ (βλ. λήμμα 3.2.2.12) είναι εύκολο - λαμβάνοντας υπ'όψιν ότι $f(\tau)=A(j(\tau))$, καθώς και ότι η f(τ) έχει μερομορφική έκφραση Fourier με ακέραιες δυνάμεις του $q=e^{2\pi i\tau}$ και με συντελεστές ακεραίους αριθμούς - ελέγχοντας τους συντελεστές Fourier αρνητικών δυνάμεων του $q=e^{2\pi i\tau}$ - να δούμε ότι $A_t\in Z$, t=0,1,…,r.

Υπενθυμίζουμε ότι για τυχαία υποσύνολα S,T *του* $\mathbb{C}$ *, ώστε το* T *να είναι ανοιχτό , το σύμβολο* $H(T ; S)$ *εκφράζει το σύνολο των ολόμορφων συναρτήσεων* $T \to S$. *Είναι εύκολο να δειχτεί (λόγω ανοιχτής απεικόνισης) ότι το* $H(T ; S)$ *είναι αντιμεταθετικός δακτύλιος χωρίς μηδενοδιαιρέτες.*

3.2.3.2 ΟΡΙΣΜΟΣ : Το πολυώνυμο $\Phi_m(x ; \tau) := \prod_{\sigma \in C(m)} (x - j(\sigma\cdot\tau)) \in H(h ; C)(x)$ **έχει συντελεστές συμμετρικά πολυώνυμα των** $j(\sigma\tau)$ **,** $\sigma \in C(m)$**. Σύμφωνα λοιπόν με την πρόταση 3.2.3.1 , θα υπάρχει πολυώνυμο** $\Phi_m(x,y) \in Z[x,y]$ **ώστε** $\Phi_m(x,j(\tau)) = \prod_{\sigma \in C(m)} (x - j(\sigma\cdot\tau))$**.**

Η εξίσωση $\Phi_m(x,y)=0$ **θα ονομάζεται modular εξίσωση. Επίσης - κάνοντας κατάχρηση ορολογίας - θα ονομάζεται modular εξίσωση το πολυώνυμο** $\Phi_m(x,y)$ **, καθώς και το** $\Phi_m(x ; j(\tau))$**.**

3.2.3.3 ΠΑΡΑΤΗΡΗΣΕΙΣ : Λόγω της αντιστοιχίας μεταξύ $C(m)$ **και των δεξιών coset της** $\Gamma_o(m)$ **στην** $SL(2,Z)$

που αναφέρεται στο 2 του λήμματος 3.2.2.11 , βέπουμε ότι ισχύει

$$\Phi_m(x,j(\tau)) = \prod_{\sigma \in C(m)} (x - j(\sigma\cdot\tau)) = \prod_{t=1}^{c(m)} (x - j(m\cdot\gamma_t\cdot\tau)) \qquad (\Sigma \ 3.2.3.3.1)$$

όπου $\gamma_1,\gamma_2,\ldots,\gamma_{c(m)}$ **είναι πλήρες σύστημα δεξιών αντιπροσώπων της** $SL(2,Z)$ **modulo την** $\Gamma_o(m)$**. Εξάλλου η σχέση Σ 3.2.3.3.1 συνεπάγεται αμέσως ότι για** $\sigma_o = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in C(m)$ **ισχύει (αφού** $\sigma_o \cdot \tau = m\tau$ **) ότι**

$$\Phi_m(j(m\tau),j(\tau)) = 0 \quad , \forall \tau \in h \qquad (\Sigma \ 3.2.3.3.2).$$

3.2.3.4 ΠΡΟΤΑΣΗ (Ιδιότητες modular εξίσωσης) : Έστω $m \in N$**. Ισχύουν τα ακόλουθα :**

1. **Το** $\Phi_m(x,y)$ **είναι ανάγωγο πολυώνυμο μεταβλητής** x **με συντελεστές από το σώμα** $C(y)$**. Έχει βαθμό** $c(m)$ **και μάλιστα :**

   $\Phi_m(x,j(\tau)) = Irr(j(m\tau) \mid C(j(\tau))(x)$**.**
2. $\Phi_m(x,y)=\Phi_m(y,x)$**.**

3. **Αν $m\neq\square$, τότε το $\Phi_m(x,x)$ είναι πολυώνυμο βαθμού μεγαλύτερου του 1 και με μεγιστοβάθμιο συντελεστή 1 ή -1.**
4. **Αν $m=p\in P$, τότε $\Phi_p(x,y)\equiv(x^p-y)(x-y^p)$ (mod $pZ[x,y]$)**
5. **$\Phi_m(j(m\tau)\,;j(\tau))=0$ και $\Phi_m(j(\sigma\cdot\tau)\,;j(\tau))=0$, $\forall\tau\in h$, $\forall\sigma\in C(m)$.**

(Η ιδιότητα 4 είναι γνωστή ως " σχέση ισοδυναμίας του Kronecker ".)

ΑΠΟΔΕΙΞΗ

1. Θέτουμε F_m το σώμα συναρτήσεων των ρητών εκφράσεων των $j(\tau), j(m\tau)$ με συντελεστές από το C. Δηλαδή $F_m = C(j(\tau),j(m\tau))$. Επειδή $\Phi_m(x,y)\in Z[x,y]$, θα έχουμε $\Phi_m(x,j)\in Z[j][x]$. Θα δείξουμε κατ' αρχήν ότι $[F_m : C(j(\tau))] \le c(m)$.

Πράγματι, από την Σ 3.2.3.3.1 έχουμε ότι η συνάρτηση $j(m\tau)$ είναι ρίζα του $\Phi_m(x,j(\tau))$.

Από τον ορισμό όμως της modular εξίσωσης (βλ. ορισμό 3.2.3.2) έχουμε ότι $\deg(\Phi_m(x,j(\tau)))=c(m)$, οπότε $[F_m : C(j(\tau))] = [C(j(m\tau),j(\tau)) : C(j(\tau))] \le \deg(\Phi_m(x,j(\tau)))=$

$= c(m)$.

Στην συνέχεια δείχνουμε ότι $[F_m : C(j(\tau))] \ge c(m)$.

Αν θέσουμε με F το σώμα των μερόμορφων συναρτήσεων στο h , τότε το F_m είναι προφανώς υπόσωμα του F. Θεωρούμε την αντιστοιχία $F_\gamma : F_m \to F$ ώστε κάθε στοιχείο $f(\tau)$ του F_m να αντιστοιχεί στο στοιχείο $f(\gamma\cdot\tau)$ του F. Η F_γ είναι μία $C(j(\tau))$ - εμφύτευση του F_m στο F.

Πράγματι, η F_γ είναι καλά ορισμένη γιατί για κάθε μερόμορφη συνάρτηση $g(\tau)$ του h η $g(\gamma\cdot\tau)$ είναι μερόμορφη (επαληθεύεται εύκολα). Επίσης η j συνάρτηση είναι $SL(2,Z)$-αναλλοίωτη (βλ. το 2 της πρότασης 3.2.1.6) , οπότε η F_γ είναι σταθερή στο $C(j(\tau))$. Εξάλλου η F_γ είναι προφανώς ομομορφισμός , οπότε για το "1-1" αρκεί να δειχτεί ότι $\mathrm{Ker}(F_\gamma)=\{0\}$. Αν $P(x,y)\in C[x,y]$ πολυώνυμο δύο μεταβλητών με $P(j(m\cdot\gamma\cdot\tau),j(\gamma\cdot\tau))=0$, τότε αντικαθιστώντας το τ με το $\gamma^{-1}\cdot\tau$ προκύπτει ότι $P(j(m\tau), j(\tau)) = 0$. Δείξαμε λοιπόν την συνεπαγωγή : " $P(j(m\cdot\gamma\cdot\tau),j(\gamma\cdot\tau))=0 \to P(j(m\tau), j(\tau)) = 0$ " από την οποία προκύπτει κατευθείαν ότι $\mathrm{Ker}(F_\gamma)=\{0\}$.

Θα δείξουμε τώρα ότι αν $\{\gamma_1,\gamma_2,\ldots,\gamma_{c(m)}\}$ είναι πλήρες σύστημα δεξιών αντιπροσώπων της SL(2,Z) modulo $\Gamma_o(m)$, τότε οι εμφυτεύσεις $F_{\gamma_1}, F_{\gamma_2}, \ldots, F_{\gamma_{c(m)}}$ είναι διαφορετικές.

Αν για κάποια $t,s\in\{1,2,\ldots,c(m)\}$ με $t\neq s$ ίσχυε $F_{\gamma_t}=F_{\gamma_s}$ τότε θα ίσχυε και $F_{\gamma_t}(j(m\tau))=F_{\gamma_s}(j(m\tau))$, οπότε εξ'ορισμού των F_{γ_t} , F_{γ_s} θα είχαμε $j(m\cdot\gamma_t\cdot\tau)=j(m\cdot\gamma_s\cdot\tau)$. Αλλά τότε από το λήμμα 3.2.2.12 θα είχαμε ότι θα υπήρχε μοναδικό $\sigma\in C(m)$ ώστε $j(\sigma\cdot\tau)=j(m\cdot\gamma_t\cdot\tau)=j(m\cdot\gamma_s\cdot\tau)$, όπου το σ θα ικανοποιούσε

την : $\Gamma_o(m)\cdot\gamma_s = (\sigma_o^{-1}\cdot SL(2,Z)\cdot\sigma)\cap SL(2,Z) = \Gamma_o(m)\cdot\gamma_t$,

κάτι

που είναι άτοπο από την εκλογή των γ_t,γ_s.

Έχουμε λοιπόν τουλάχιστο c(m) - το πλήθος εμφυτεύσεις του F_m στο F , οπότε αφού $F_m = C(j(\tau),j(m\tau))$, θα έχουμε ότι $[F_m : C(j(\tau))] \geq c(m)$.

Συνεχίζουμε δείχνοντας ότι το $\Phi_m(x,j(\tau))$ είναι το ανάγωγο πολυώνυμο του $j(m\tau)$ πάνω από το $C(j(\tau))$:

Από τις σχέσεις που έχουμε δείξει προκύπτει ότι $[F_m : C(j(\tau))] = c(m)$. Συνεπώς επειδή $\Phi_m(x,j(\tau))\in Z[j(\tau)][x]$ και το $j(m\tau)$ είναι ρίζα του $\Phi_m(x,j(\tau))$ με $\deg(\Phi_m(x,j(\tau))) = c(m)$, θα έχουμε $\Phi_m(x,j(\tau)) = \mathrm{Irr}(j(m\tau) \mid C(j(\tau)))(x)$.

Τέλος , παρατηρούμε ότι η απεικόνιση $C(x) \to C(j(\tau))$ με $x \to j(\tau)$, (όπου το $C(y)$ είναι ο δακτύλιος πολυωνύμων μεταβλητής y με συντελεστές από ο C) είναι ισομορφισμός

Πράγματι , από το 6 της πρότασης 3.2.1.6 έχουμε ότι η αντιστοιχία $x \to j(\tau)$ επάγει ισομορφισμό μεταξύ των $C[x]$ και $C[j(\tau)]$. Ο ισομορφισμός αυτός θα επεκτείνεται προφανώς και στα αντίσοιχα σώματα πηλίκων $C(x)$ και $C(j(\tau))$.

Αφού τώρα το $\Phi_m(x,j(\tau))$ είναι ανάγωγο θεωρούμενο σαν πολυώνυμο του x με συντελεστές από το σώμα $C(j(\tau))$, θα ισχύει ότι και το $\Phi_m(x,y)$ είναι ανάγωγο θεωρούμενο σαν πολυώνυμο του x με συντελεστές από το σώμα $C(y)$.

2. Εξ' ορισμού της modular εξίσωσης έχουμε ότι $\forall\sigma\in C(m)$ ισχύει $\Phi_m(j(\sigma\tau),j(\tau)) = 0$. Επειδή λοιπόν $\begin{pmatrix}1 & 0\\ 0 & m\end{pmatrix}\in C(m)$ και $\begin{pmatrix}1 & 0\\ 0 & m\end{pmatrix}\cdot\tau = \frac{\tau}{m}$, θα έχουμε ότι $\Phi_m(j(\frac{\tau}{m}), j(\tau)) = 0$, $\forall\tau\in h$. Επομένως $\Phi_m(j(\tau),j(m\tau))=0$

και έτσι λόγω της σχέσης Σ 3.2.3.3.2 της παρατήρησης 3.2.3.3 θα έχουμε ότι τα πολυώνυμα $\Phi_m(t,j)$, $\Phi_m(j,t)$ με μεταβλητή t και συντελεστές από το $Z[j]$ έχουν κοινή ρίζα. Επίσης , από το 1 έχουμε ότι το $\Phi_m(t,j)$ είναι ανάγωγο στο $Z[j]$. Θα δείξουμε ότι υπάρχει πολυώνυμο δύο μεταβλητών $g(x,y)$ ώστε $\Phi_m(y,x) = \Phi_m(x,y)\cdot g(x,y)$ (Σ 3.2.3.4.1)

Πράγματι , λόγω της ιδιότητας 6 της πρότασης 3.2.1.6 έχουμε ότι η ταυτοτική απεικόνιση στο Z επεκτείνεται σε ισομορφισμό μεταξύ του δακτύλιου $Z[j]$ και του δακτυλίου πολυωνύμων $Z[s]$ μέσω της αντιστοιχίας $j \to s$. Αυτό σημαίνει ότι δρώντας ο ισομορφισμός αυτός στους συντελεστές των πολυωνύμων $\Phi_m(t,j)$, $\Phi_m(j,t)$ και με βάση το ότι αυτά τα πολυώνυμα έχουν κοινή ρίζα στο $Z[j]$ ενώ το $\Phi_m(t,j)$ είναι ανάγωγο στο $Z[j]$, θα ισχύει $\Phi_m(t,s) \mid \Phi_m(s,t)$ στο $(Z[t])[s]$ Υπάρχει επομένως πολυώνυμο $g(t,s)\in Z[t,s]$ με $\Phi_m(s,t) = \Phi_m(t,s)\cdot g(t,s)$. Το αποδεικτέο είναι τώρα προφανές.

Παρατηρούμε στην συνέχεια ότι η σχέση Σ 3.2.3.4.1 συνεπάγεται ότι $\Phi_m(y,x) = \Phi_m(x,y)\cdot g(x,y) = \Phi_m(y,x)\cdot g(y,x)\cdot g(x,y)$. Συνεπώς $\Phi_m(y,x)\cdot[g(x,y)\cdot g(y,x) - 1] = 0$, οπότε $g(x,y)\cdot g(y,x) = 1$. Με απλό επειχείρημα βαθμών πολυωνύμων έχουμε από την τελευταία σχέση $g(x,y)\in\{\pm 1\}$. Μένει λοιπόν να αποκλείσουμε την περίπτωση $g(x,y) = -1$.

Αν $g(x,y) = -1$, τότε η σχέση Σ 3.2.3.4.1 δίνει $\Phi_m(y,x) = -\Phi_m(x,y)$, οπότε $\Phi_m(y,y)=0$. Αυτό όμως σημαίνει ότι το πολυώνυμο $\Phi_m(x,y)$ μεταβλητης x με συντελεστές από το σώμα $C(y)$, έχει ρίζα το $y\in C(y)$, κάτι που είναι άτοπο από το 1.

3. Έστω ότι το m δεν είναι τέλειο τετράγωνο. Προφανώς τότε $m\neq 1$, οπότε $c(m)>1$ (βλ. πρόταση 3.2.2.2). Έχουμε λοιπόν κατ' αρχήν $\deg(\Phi_m(x,y)) = c(m) > 1$ (βλ. ορισμό 3.2.3.2). Από την σχέση Σ 3.2.2.12.2 του λήμματος 3.2.2.12 και από την Fourier έκφραση της j συνάρτησης (βλ. πρόταση 3.2.2.9) προκύπτει

ότι υπάρχει ακολουθία μιγαδικών αριθμών $(A_n)_{n=1}^{\infty}$ ώστε για κάθε $\sigma\in C(m)$ να ισχύει :

$$j(\tau) - j(\sigma\tau) = \frac{1}{q} - \frac{\zeta_m^{-ab}}{\left(q^{\frac{1}{m}}\right)^{a^2}} + \sum_{n=0}^{\infty} A_n \left(q^{\frac{1}{m}}\right)^{a^2 n} = \frac{1}{\left(q^{\frac{1}{m}}\right)^{m}} - \frac{\zeta_m^{-ab}}{\left(q^{\frac{1}{m}}\right)^{a^2}} + \sum_{n=0}^{\infty} A_n \left(q^{\frac{1}{m}}\right)^{a^2 n} \quad , q = e^{2\pi i\tau}.$$

Τώρα επειδή $m\neq\square$, θα έχουμε $m\neq a^2 \rightarrow \frac{a^2}{m}\neq 1$, οπότε ο συντελεστής της περισσότερο αρνητικής δύναμης του $q^{\frac{1}{m}}$ ανήκει στο $\{1,-\zeta_m^{-ab}\}$ και επομένως είναι ρίζα της μονάδας. Εξάλλου , εξ' ορισμού της modular εξίσωσης έχουμε $\Phi_m(x,j(\tau)) = \prod_{\sigma\in C(m)}(x - j(\sigma\tau))$ (βλ. σχέση Σ 3.2.3.3.1) , οπότε $\Phi_m(j(\tau),j(\tau)) = \prod_{\sigma\in C(m)}(j(\tau) - j(\sigma\tau))$ και συνεπώς ο συντελεστής της περισσότερο αρνητικής δύναμης του $q^{\frac{1}{m}}$ στην έκφραση Fourier (που προκύπτει από τις εκφράσεις Fourier των διαφορών $j(\tau) - j(\sigma\tau)$, $\sigma\in C(m)$ που υπολογίστηκαν προηγουμένως) είναι ρίζα της μονάδος . Τώρα , επειδή $\Phi_m(x,x)\in Z[x]$, ο συντελεστής της περισσότερο αρνητικής δύναμης του $q^{\frac{1}{m}}$ στην έκφραση Fourier της modular για την SL(2,Z) συνάρτησης $\Phi_m(j(\tau),j(\tau))$ (βλ. το 1 της πρότασης 3.2.2.8) είναι ο μεγιστοβάθμιος συντελεστής του $\Phi_m(x,x)$. Προκύπτει λοιπόν από τα παραπάνω ότι ο μεγιστοβάθμιος συντελεστής του $\Phi_m(x,x)$ είναι ρίζα της μονάδος. Αλλά οι μόνες ρίζες της μονάδος που υπάρχουν στο Z είναι οι 1,-1 , οπότε θα έχουμε τελικά ότι ο μεγιστοβάθμιος συντελεστής του $\Phi_m(x,x)$ είναι 1 ή -1. Τέλος , ο εκθέτης της περισσότερο αρνητικής δύναμης του $q^{\frac{1}{m}}$ στην έκφραση Fourier της $\Phi_m(j(\tau),j(\tau))$ είναι μικρότερος του -1 (αφού $\deg(\Phi_m(x,j(\tau)) = c(m)>1$) , οπότε $\deg(\Phi_m(x,x)) > 1$.

4. Σε όλο το 4 , το q θα συμβολίζει το $e^{2\pi i\tau}$, για $\tau\in h$.

Έστω $m=p\in P$. Τότε $C(m) = C(p) = \left\{ \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix} \mid k\in\{0,1,\ldots,p-1\} \right\} \cup \left\{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right\}$. Πρίν αρχίσουμε την απόδειξη κάνουμε πρώτα κάποιες παρατηρήσεις:

Παρατήρηση 1 : $p=(1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$.

Πράγματι , $x^{p-1}+x^{p-2}+\ldots+x+1 = (x-\zeta_p)(x-\zeta_p^2)\ldots(x-\zeta_p^{p-1})$, οπότε για $x=1$ παίρνουμε $p=(1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$.

Παρατήρηση 2 : $(f(x)^p-g(x)^p)\equiv(f(x)-g(x))^p \pmod{(1-\zeta_p)(Z[\zeta_p])<q^{\frac{1}{p}}>}$, για κάθε $f(x),g(x)\in ((Z[\zeta_p])<q^{\frac{1}{p}}>)[x]$.

Πράγματι , στον δακτύλιο πολυωνύμων μεταβλητής x με συντελεστές από το $(Z[\zeta_p])<q^{\frac{1}{p}}>$ ισχύει $(f(x)^p-g(x)^p)\equiv(f(x)-g(x))^p \pmod{p(Z[\zeta_p])<q^{\frac{1}{p}}>}$, για κάθε $f(x),g(x)\in ((Z[\zeta_p])<q^{\frac{1}{p}}>)[x]$. Επομένως , λόγω της παρατήρησης 1 , θα έχουμε :

$(g(x)^p-f(x)^p)\equiv(g(x)-f(x))^p \pmod{(1-\zeta_p)(Z[\zeta_p])<q^{\frac{1}{p}}>}$.

Προχωράμε τώρα στην κύρια απόδειξη : Θέτουμε $\sigma_k = \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}$, $k\in\{0,1,\ldots,p-1\}$ και $\sigma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

Προφανώς τότε $C(m) = C(p) = \{ \sigma_k \mid 0\le k\le p \}$. Από το λήμμα 3.2.2.12 προκύπτει κατ' αρχήν ότι

$j(\sigma_k \cdot \tau) = \frac{\zeta_p^{-k}}{q^{\frac{1}{p}}} + \sum_{n=0}^{\infty} c_n \zeta_p^{kn} \left(q^{\frac{1}{p}} \right)^n$, όπου οι ακέραιοι αριθμοί c_n , $n \in \mathbb{N}$ είναι οι συντελεστές του ολόμορφου μέρους της έκφρασης Fourier της j συνάρτησης (βλ. πρόταση 3.2.2.9). Συνεπώς ,

$j(\sigma_k \cdot \tau) \equiv (\frac{1}{q^{\frac{1}{p}}} + \sum_{n=0}^{\infty} c_n \left(q^{\frac{1}{p}} \right)^n) \pmod{(1-\zeta_p)(Z[\zeta_p])< q^{\frac{1}{p}} >}$ και επομένως ισχύει η ακόλουθη σχέση :

$j(\sigma_k \cdot \tau) \equiv j(\sigma_0 \cdot \tau) \pmod{(1-\zeta_p)(Z[\zeta_p])< q^{\frac{1}{p}} >}$ (Σ 3.2.3.4.2)

Θα δείξουμε στην συνέχεια ότι :

$j(\sigma_p \cdot \tau) \equiv j(\tau)^p \pmod{(1-\zeta_p)(Z[\zeta_p])< q^{\frac{1}{p}} >}$ (Σ 3.2.3.4.3)

Πράγματι , το λήμμα 3.2.2.12 δίνει $j(\sigma_p \cdot \tau) = \frac{1}{q^p} + \sum_{n=0}^{\infty} c_n q^{pn}$. Όμως $c_n \in Z$, $\forall n \in \mathbb{N}$, οπότε για κάθε $n \in \mathbb{N}$ ισχύει $c_n^p \equiv c_n (\mathrm{mod} p)$. Η τελευταία ισοτιμία συνεπάγεται ότι για κάθε n , ισχύει $c_n^p \equiv c_n \pmod{p(Z[\zeta_p])< q^{\frac{1}{p}} >}$ που σημαίνει ότι $j(\sigma_p \cdot \tau) \equiv \left(\frac{1}{q}\right)^p + \sum_{n=1}^{\infty} (c_n q^n)^p \pmod{p(Z[\zeta_p])< q^{\frac{1}{p}} >}$.

Επομένως $j(\sigma_p \cdot \tau) \equiv \left(\frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n \right)^p \pmod{p(Z[\zeta_p])< q^{\frac{1}{p}} >}$ και έτσι

$j(\sigma_p \cdot \tau) \equiv j(\tau)^p \pmod{p(Z[\zeta_p])< q^{\frac{1}{p}} >}$ (βλ. πρόταση 3.2.2.9). Από την παρατήρηση 1 τώρα , έχουμε ότι $j(\sigma_p \cdot \tau) \equiv j(\tau)^p \pmod{(1-\zeta_p)(Z[\zeta_p])< q^{\frac{1}{p}} >}$, που είναι το ζητούμενο.

Συνεχίζουμε βάζοντας στο "παιχνίδι" την modular εξίσωση με την παρακάτω σχέση :

$\Phi_p(x, j(\tau)) \equiv (x^p - j(\sigma_0 \cdot \tau)^p)(x - j(\tau)^p) \pmod{(1-\zeta_p)(Z[\zeta_p])< q^{\frac{1}{p}} >[x]}$ (Σ 3.2.3.4.4)

Η σχέση Σ 3.2.3.4.4 αποδεικνύεται ως εξής : Οι σχέσεις Σ 3.2.3.4.2 και Σ 3.2.3.4.3 μας δίνουν δεδομένου ότι $C(p) = \{ \sigma_k \mid 0 \le k \le p \}$ και ότι $\Phi_p(x, j(\tau)) = \prod_{\sigma \in C(m)} (x - j(\sigma \cdot \tau)) = \prod_{k=0}^{p-1} (x - j(\sigma_k \cdot \tau))$, την ακόλουθη ισοτιμία :

$\Phi_p(x, j(\tau)) \equiv (x - j(\sigma_0 \cdot \tau))^p (x - j(\tau)^p) \pmod{(1-\zeta_p)(Z[\zeta_p])< q^{\frac{1}{p}} >[x]}$. Από την παρατήρηση 2 έχουμε επομένως ότι

$\Phi_p(x, j(\tau)) \equiv (x^p - j(\sigma_0 \cdot \tau)^p)(x - j(\tau)^p) \pmod{(1-\zeta_p)(Z[\zeta_p])< q^{\frac{1}{p}} >[x]}$.

Θα αποδείξουμε τώρα ότι

$j(\sigma_0 \cdot \tau)^p \equiv j(\tau) \pmod{(1-\zeta_p)(Z[\zeta_p])< q^{\frac{1}{p}} >}$ (Σ 3.2.3.4.5)

Έχουμε $j(\sigma_0 \cdot \tau) = \frac{\zeta_p^{-k}}{q^{\frac{1}{p}}} + \sum_{n=0}^{\infty} c_n \zeta_p^{kn} \left(q^{\frac{1}{p}} \right)^n$ (βλ. λήμμα 3.2.2.12). Επομένως ,

$$j(\sigma_0\cdot\tau)^p=\left(\frac{\zeta_p^{-k}}{q^{\frac{1}{p}}}+\sum_{n=0}^{\infty}c_n\left(q^{\frac{1}{p}}\right)^n\right)^p\equiv\frac{1}{q}+\sum_{n=0}^{\infty}c_n{}^pq^n\ (\mathrm{mod}\ p(Z[\zeta_p])<q^{\frac{1}{p}}>)$$

(λόγω παρατήρησης 2). Όμως $c_n{}^p\equiv c_n(\mathrm{mod}p)\rightarrow c_n{}^p\equiv c_n\ (\mathrm{mod}\ p(Z[\zeta_p])<q^{\frac{1}{p}}>)$ για κάθε $n\in N$, πράγμα που σημαίνει ότι

$$j(\tau)=\frac{1}{q}+\sum_{n=0}^{\infty}c_nq^n\equiv j(\sigma_0\cdot\tau)^p\ (\mathrm{mod}\ p(Z[\zeta_p])<q^{\frac{1}{p}}>).$$

Είναι εύκολο να δεί κανείς τώρα ότι οι σχέσεις Σ 3.2.3.4.4 και Σ 3.2.3.4.5 συνεπάγονται ότι

$\Phi_p(x,j(\tau))\equiv(x^p-j(\tau))(x-j(\tau)^p)\ (\mathrm{mod}\ (1-\zeta_p)(Z[\zeta_p])<q^{\frac{1}{p}}>[x])$ (Σ 3.2.3.4.6)

Παρατηρούμε τώρα ότι και τα δύο μέλη της ισοτιμίας Σ 3.2.3.4.6 είναι στοιχεία του $(Z<q>)[x]$. Οπότε ,

επειδή $[(1-\zeta_p)(Z[\zeta_p])<q^{\frac{1}{p}}>\ \cap\ Z<q>]=[(1-\zeta_p)(Z[\zeta_p])<q>\ \cap\ Z<q>]=pZ<q>$ (βλ. παρατήρηση 1) θα έχουμε ότι $\Phi_p(x,j(\tau))\equiv(x^p-j(\tau))(x-j(\tau)^p)\ (\mathrm{mod}\ pZ<q>[x])$. (Σ 3.2.3.4.7)

Θέτουμε $F(x\ ;j(\tau)):=\Phi_p(x,j(\tau))-(x^p-j(\tau))(x-j(\tau)^p)$. Οι συντελεστές του πολυωνύμου $F(x\ ;j(\tau))\in(Z[j(\tau)])[x]$ είναι πολυώνυμα του $j(\tau)$ και συνεπώς , όπως μπορεί εύκολα να δεί κανείς , θα είναι modular συναρτήσεις για την SL(2,Z). Επίσης η σχέση Σ 3.2.3.4.7 μας δίνει ότι οι συντελεστές του πολυωνύμου $F(x\ ;j(\tau))$ ανήκουν στο $pZ<q>$, πράγμα που σημαίνει ότι οι συντελεστές Fourier τους θα ανήκουν στο pZ. Από την αρχή του Hasse (βλ. πρόταση 3.2.2.13) για $(A,+)=(pZ,+)$, παίρνουμε ότι οι συντελεστές του $F(x\ ;j(\tau))$ είναι πολυώνυμα της $j(\tau)$ με συντελεστές από το pZ. Αυτό σημαίνει ότι υπάρχει πολυώνυμο $F_1(x,y)$ μεταβλητών x,y με συντελεστές από το $pZ[j(\tau)]$ με $F_1(x,j(\tau))=F(x\ ;j(\tau))$. Έτσι , $\Phi_p(x,j(\tau))\equiv(x^p-j(\tau))(x-j(\tau)^p)$ (mod $pZ[x,j(\tau)]$). Εφαρμόζοντας τώρα την Z-ισομορφία $Z[j(\tau)]\cong Z[y]$ η οποία προκύπτει από την αντιστοιχία $j(\tau)\rightarrow y$ (βλ. το 6 της πρότασης 3.2.1.6) έχουμε ότι $\Phi_p(x,y)\equiv(x^p-y)(x-y^p)$ (mod pZ[x,y]).

5 Οι αποδεικτέες σχέσεις είναι προφανείς συνέπειες των σχέσεων Σ 3.2.3.3.1 και Σ 3.2.3.3.2 της παρατήρησης 3.2.3.3.

Στην συνέχεια θα αναφέρουμε για λόγους πληρότητας ένα ισχυρό θεώρημα της complex multiplication μαζί με ένα λήμμα απαραίτητο για την απόδειξη του , καθώς και κάποιες σημαντικές προτάσεις που αφορούν την modular εξίσωση.

<u>3.2.3.5 ΛΗΜΜΑ</u> : Αν f(τ) είναι modular συνάρτηση για την SL(2,Z) και η f(τ) έχει πόλο στο $\omega=e^{2\pi i/3}$ τάξης m , για κάποιο $m\in N$, τότε ισχύουν τα ακόλουθα :

1. **3 | m.**
2. **Η συνάρτηση $j(\tau)^{m/3}f(\tau)$ είναι ολόμορφη στο σημείο ω.**
   (Βλ. [Cox] άσκηση 11.7 σελ. 245).

3.2.3.6 ΘΕΩΡΗΜΑ : Αν $m\in\mathbf{N}$, τότε ισχύουν τα ακόλουθα :

1. **Η j - συνάρτηση είναι modular συνάρτηση για την SL(2,Z) και κάθε modular συνάρτηση της SL(2,Z) είναι ρητή έκφραση της $j(\tau)$.**
2. **Αν $m\in\mathbf{N}$, τότε οι $j(\tau)$, $j(m\tau)$ είναι modular συναρτήσεις για την $\Gamma_o(m)$ και κάθε modular συνάρτηση για την $\Gamma_o(m)$ είναι ρητή έκφραση των $j(\tau)$, $j(m\tau)$ (δηλαδή ανήκει στο $\mathbf{C}(j(\tau), j(m\tau))$.**
   Πιο συγκεκριμένα , αν $f(\tau)$ είναι modular συνάρτηση για την $\Gamma_o(m)$, τότε η ρητή έκφραση του x με παράμετρο τ :
   $$G(x;\tau)=\Phi_m(x,j(\tau))\sum_{t=1}^{c(m)}\frac{f(\gamma_t(\tau))}{x-j(m\gamma_t\tau)}$$ **(όπου $\{\gamma_1,\gamma_2,\ldots,\gamma_{c(m)}\}$ είναι πλήρες σύστημα δεξιών αντιπροσώπων της SL(2,Z) modulo την $\Gamma_o(m)$) είναι ειδικότερα πολυώνυμο μεταβλητής x με συντελεστές πολυωνυμικές εκφράσεις της $j(\tau)$ και η $f(\tau)$ δίνεται ως ρητή έκφραση των συναρτήσεων $j(\tau)$, $j(m\tau)$ από την ακόλουθη σχέση :**
   $$f(\tau)=\frac{P(j(m\tau),\ j(\tau))}{\frac{d\Phi_m}{dx}(j(m\tau),j(\tau))}$$ **, όπου το $P(x,y)\in\mathbf{C}[x,y]$ είναι πολυώνυμο με $P(x,j(\tau))=G(x;j(\tau))$.**

(Απόδειξη του θεωρήματος υπάρχει στο βιβλίο του Cox : [Cox] θεώρ. 11.9 σελ. 226).

3.2.3.7 ΠΡΟΤΑΣΗ : Αν $f(\tau)$ είναι modular συνάρτηση για την $\Gamma_o(m)$ και $\tau_o\in\mathbf{h}=\{z\in\mathbf{C}\mid Im(z)>0\}$, τότε :

1. **Αν οι fourier εκφράσεις της $f(\tau)$ - όπου ορίζονται - έχουν ρητούς συντελεστές, τότε η $f(\tau)$ είναι ρητή έκφραση των συναρτήσεων $j(\tau)$, $j(m\tau)$, με συντελεστές ρητούς αριθμούς.**
2. **Αν ισχύει το 1 και επιπλέον ισχύουν τα ακόλουθα :**
   - **η $f(\tau)$ είναι ολόμορφη στο πάνω μιγαδικό ημιεπίπεδο $\mathbf{h}$**
   - $\frac{d\Phi_m}{dx}(j(m\tau_o),j(\tau_o))\neq 0$

   τότε ισχύει $f(\tau_o)=\frac{P(j(m\tau_o),\ j(\tau_o))}{\frac{d\Phi_m}{dx}(j(m\tau_o),j(\tau_o))}$ **, όπου το πολυώνυμο $P(x,y)$ του $\mathbf{C}[x,y]$ είναι αυτό που αναφέρεται στο θεώρημα 3.2.3.6.**

(Για την απόδειξη της πρότασης παραπέμπουμε στο βιβλίο του Cox : [Cox] πρότ. 12.7 σελ. 252)

3.2.3.8 ΠΡΟΤΑΣΗ : Έστω $\mathbf{O}$ μία τάξη σε φανταστικό τετραγωνικό σώμα K για την οποία ισχύει ότι $E(\mathbf{O})=\{\pm 1\}$. Αν υπάρχουν $\alpha\in\mathbf{C}$ και $s\in\mathbf{Z}$ ώστε να ισχύουν τα ακόλουθα :

- $\mathbf{O}=\mathbf{Z}+\alpha\mathbf{Z}$.
- $s \mid Tr(\alpha)$ **(όπου $Tr(\alpha)$ είναι το ίχνος του α στο K).**
- **ο ΜΚΔ$(s^2, N(\alpha))$ είναι ελεύθερος τετραγώνου.**

τότε για κάθε φυσικό αριθμό m ισχύει : $\frac{d\Phi_m}{dx}(j(\frac{m\alpha}{s}),j(\frac{\alpha}{s}))\neq 0$.

(Βλ. [Cox] λήμμα 12.11 σελ. 254)

3.2.4 ΡΙΖΕΣ ΤΗΣ MODULAR ΕΞΙΣΩΣΗΣ

3.2.4.1 ΟΡΙΣΜΟΣ : Έστω L , L' lattices με $L' \subseteq L$. Αν $[L : L'] = m$ και η προσθετική ομάδα $(\frac{L}{L'},+)$ είναι κυκλική , τότε το L θα λέγεται κυκλικό υπολattice τάξης m του L.

3.2.4.2 ΛΗΜΜΑ : Έστω lattice L με $L=Z+\tau Z$, για κάποιο $\tau \in h=\{z \in C \mid Im(z)>0\}$. Έστω επίσης L' υπολattice του C. Ισχύουν τα ακόλουθα :

1. **Αν $L' = (a\tau+b)Z+(c\tau+d)Z$ για $a,b,c,d \in Z$, τότε $[L : L'] = |ad-bc|$**
2. **Αν $L' = (a\tau+b)Z+(c\tau+d)Z$ για $a,b,c,d \in Z$, τότε ισχύει η ακόλουθη ισοδυναμία**
   " Η ομάδα $(\frac{L}{L'},+)$ είναι κυκλική " $\leftrightarrow$ " MKD(a,b,c,d)=1 "
3. **Αν $\{k \in N \mid k \in L'\} \neq \varnothing$, τότε υπάρχουν $a,b \in Z$ ώστε $L'=(a\tau+b)Z+d_oZ$, όπου $d_o=\min\{ k \in N \mid k \in L'\}$.**

ΑΠΟΔΕΙΞΗ

Το 1 είναι άμεση συνέπεια του 3 του θεωρήματος 2.2.2.13 , ενώ τα 2 και 3 είναι απλές ασκήσεις και η απόδειξη τους παραλείπεται.

3.2.4.3 ΠΡΟΤΑΣΗ : Έστω $\tau \in h=\{z \in C \mid Im(z)>0\}$ και $L=Z+\tau Z$. Ισχύουν τα ακόλουθα :

1. **Αν L' είναι κυκλικό υπολattice του L τάξης m , τότε υπάρχει μοναδικό στοιχείο $\sigma=\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$ με $L' = d(Z+\sigma \cdot \tau Z)$. Επίσης $d= \min\{ k \in N \mid k \in L'\}$.**
2. **Αν $\sigma=\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$, τότε το $d(Z+\sigma \cdot \tau Z)$ είναι κυκλικό υπολattice του L τάξης m και $d= \min\{ k \in N \mid k \in L'\}$.**

ΑΠΟΔΕΙΞΗ

1. Έχουμε ότι το L' είναι κυκλικό υπολattice του L. Από το 3 του λήμματος 3.2.4.2 έχουμε ότι αν θέσουμε $d= \min\{ k \in N \mid k \in L'\}$, τότε υπάρχουν ακέραιοι αριθμοί a,b ώστε $L'=(a\tau+b)Z+dZ$. Προφανώς χωρίς περιορισμό της γενικότητας μπορούμε να θεωρήσουμε $a>0$. Από το 1 του λήμματος 3.2.4.2 έχουμε ότι $m = |ad|$. Αλλά $a,d>0$ και συνεπώς $m=ad$. Επίσης , για κάθε ακέραιο αριθμό k , ισχύει $L'= (a\tau+b)Z+dZ = (a\tau+b+kd)Z+dZ = [a\tau+(b+kd)]Z+dZ$, και συνεπώς μπορούμε χωρίς περιορισμό της γενικότητας να υποθέσουμε ότι $0 \le b < d$ (Ευκλείδεια διαίρεση). Τέλος το 2 του λήμματος 3.2.4.2 δίνει ότι ΜΚΔ(a,b,d)=1 , πράγμα που σημαίνει ότι το $\sigma=\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ ανήκει στο C(m). Μάλιστα, $L' = (a\tau+b)Z+dZ =$

$= d(\frac{a\tau+b}{d}Z+Z) = d(Z+\sigma \cdot \tau Z)$.

2. Έχουμε ότι το $\sigma =\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ ανήκει στο C(m) , οπότε ΜΚΔ(a,b,d)=1. Επειδή $L' = d(Z+\sigma \cdot \tau Z)= d(Z+\frac{a\tau+b}{d}Z) =$ $(a\tau+b)Z+dZ$, έχουμε από το 2 του λήμματος 3.2.4.2 ότι η ομάδα $(\frac{L}{L'},+)$ είναι κυκλική. Εξάλλου $|ad|=m$ (αφού $\sigma \in C(m)$) , οπότε το 1 του λήμματος 3.2.4.2 δίνει $[L : L']=m$. Σύμφωνα λοιπόν με τα

παραπάνω έχουμε ότι το L' είναι κυκλικό υπολattice του L.

3.2.4.4 ΘΕΩΡΗΜΑ : Έστω $m\in N$. Αν $u,v\in C$, τότε τα ακόλουθα είναι ισοδύναμα :

1. **$\Phi_m(u,v)=0$**
2. **Υπάρχει lattice L και κυκλικό υπολattice L' του L τάξης m ώστε $u=j(L')$ και $v=j(L)$.**

ΑΠΟΔΕΙΞΗ

$1 \to 2$ Η j - συνάρτηση είναι "επί" του C (βλ. το 4 της πρότασης 3.2.1.6) , οπότε υπάρχει $\tau_o\in h$ ($h=\{z\in C \mid Im(z)>0\}$) με $j(\tau_o)=v$. Θέτουμε $L=Z+\tau_oZ$, οπότε $j(L)=v$. Έχουμε τώρα ότι

$0 = \Phi_m(u,v) = \Phi_m(u,,j(\tau_o))$. Όμως $\forall\tau\in h$, $\Phi_m(x,j(\tau)) = \prod_{\sigma\in C(m)}(x - j(\sigma\cdot\tau))$ (βλ. ορισμο 3.2.3.2)

και συνεπώς $\prod_{\sigma\in C(m)}(u - j(\sigma\cdot\tau_o))= 0$. Συνεπώς υπαρχει στοιχείο $\sigma_o=\begin{pmatrix} a_o & b_o \\ 0 & d_o \end{pmatrix}$ του $C(m)$ με $u=j(\sigma_o\cdot\tau_o)$. Θέτουμε $L'= d_o(Z+\sigma_o\cdot\tau_oZ)$. Από το 2 της πρότασης 3.2.4.3 έχουμε ότι το L' είναι κυκλικό υπολattice του L τάξης m. Επίσης $j(L') = j(d_o(Z+\sigma_o\cdot\tau_oZ)) = j(Z+\sigma_o\cdot\tau_oZ)$ (βλ. πρόταση 3.1.2.7) , οπότε $j(L') = j(Z+\sigma_o\cdot\tau_oZ) = j(\sigma_o\tau_o) = u$.

$2 \to 1$ Έστω ότι $u = j(L)$ και $v = j(L')$, για κυκλικό υπολattice L' του L τάξης m.
Γράφουμε $L=aZ+bZ$, με $a,b\in C$. Επειδή τα a,b είναι γραμμικώς ανεξάρτητα στο R , θα έχουμε $a,b\neq 0$ και $\frac{b}{a}\notin R$. Εκλέγουμε λοιπόν τ_o το μοναδικό στοιχείο του $\{\frac{b}{a}, -\frac{b}{a}\}$ το οποίο ανήκει στο h.
Έχουμε $L = a(Z+\tau_oZ) \to (Z+\tau_oZ) = \frac{1}{a}L$. Είναι προφανές ότι το $\frac{1}{a}L'$ θα είναι κυκλικό υπολattice του $(Z+\tau_oZ) = \frac{1}{a}L$ τάξης m. Από το 1 της πρότασης 3.2.4.3 έχουμε ότι υπάρχει στοιχείο $\sigma_o=\begin{pmatrix} a_o & b_o \\ 0 & d_o \end{pmatrix}$ του $C(m)$, ώστε $\frac{1}{a}L' = d_o(Z+\sigma_o\cdot\tau_oZ)$.
Θα δείξουμε ότι $u = j(\tau_o)$ και ότι $v=j(\sigma_o\cdot\tau_o)$.

Πράγματι , $u = j(L) = j(a(Z+\tau_oZ)) = j(Z+\tau_oZ) = j(\tau_o)$. Επίσης , $v = j(L') = j(\frac{1}{a}L') = j(d_o(Z+\sigma_o\cdot\tau_oZ)) = j(Z+\sigma_o\cdot\tau_oZ)$.

Συνεπώς , $v = j(\sigma_o\cdot\tau_o)$.

Τώρα επειδή $\Phi_m(j(\sigma_o\cdot\tau_o), j(\tau_o))=0$ (βλ. ορισμό 3.2.3.2) θα έχουμε ότι $\Phi_m(v,u)=0$, οπότε από το 2 της πρότασης 3.2.3.4 προκύπτει $\Phi_m(u,v)=0$.

§3 ΜΙΓΑΔΙΚΟΣ ΠΟΛΛΑΠΛΑΣΙΑΣΜΟΣ ΚΑΙ RING CLASS FIELDS

3.3.1 ΠΡΩΤΑΡΧΙΚΑ ΣΤΟΙΧΕΙΑ ΚΑΙ ΙΔΕΩΔΗ ΤΑΞΗΣ

3.3.1.1 ΟΡΙΣΜΟΣ : Αν O είναι τάξη σε φανταστικό τετραγωνικό σώμα αριθμών και a είναι ένα proper κλασματικό ιδεώδες της O , τότε το a θα λέγεται πρωταρχικό αν δεν είναι δυνατόν να γραφεί στην μορφή $a=db$, όπου $d\in N$, $d>1$ και b είναι ακέραιο proper ιδεώδες της O.

3.3.1.2 ΟΡΙΣΜΟΣ : Αν O είναι τάξη σε φανταστικό τετραγωνικό σώμα αριθμών και $\alpha\in O$, τότε το α θα λέγεται πρωταρχικό αν δεν είναι δυνατόν να γραφεί στην μορφή $\alpha=db$, όπου $d\in N$, $d>1$ και $b\in O$.

3.3.1.3 ΠΑΡΑΤΗΡΗΣΕΙΣ : Άμεση συνέπεια των παραπάνω ορισμών και των ιδιοτήτων της νόρμας ιδεωδών (βλ. πρόταση 3.2.2.14) είναι τα ακόλουθα :

1. **Αν O είναι τάξη σε φανταστικό τετραγωνικό σώμα αριθμών και a είναι ένα proper ακέραιο ιδεώδες της O , τότε το a θα είναι πρωταρχικό αν και μόνο αν η νόρμα του $N(a)$ είναι ελεύθερη τετραγώνου.**
2. **Αν O είναι τάξη σε φανταστικό τετραγωνικό σώμα αριθμών και $\alpha\in O$, τότε το α είναι πρωταρχικό στοιχείο της O αν και μόνο αν η νόρμα του α είναι ελεύθερη τετραγώνου.**
3. **Αν O και a είναι όπως στο 1 και επίσης το a είναι κύριο ιδεώδες με $a=\alpha O$, για $\alpha\in O$, τότε το a θα είναι πρωταρχικό ιδεώδες της O αν και μόνο αν το α είναι πρωταρχικό στοιχείο της O.**

3.3.1.4 ΛΗΜΜΑ : Αν G είναι πεπερασμένη αβελιανή ομάδα , τότε η G είναι κυκλική αν και μόνο αν δεν υπάρχει $d\in N$, $d>1$ ώστε η $(Z_d x Z_d,+)$ να είναι ισόμορφη με υποομάδα της G.

ΑΠΟΔΕΙΞΗ

Είναι άμεση συνέπεια του γεγονότος ότι $\forall\kappa\in N$ με $k>1$, η $Z_k x Z_k$ δεν είναι κυκλική και του θεωρήματος δομής

των πεπερασμένων αβελιανών ομάδων.

<u>3.3.1.5 ΠΡΟΤΑΣΗ</u> : Αν O είναι τάξη σε φανταστικό τετραγωνικό σώμα αριθμών και a,b είναι proper

κλασματικά ιδεώδη της O , τότε :

1. **Το ιδεώδες ab είναι υπolattice του b με [b : ab] = N(a).**
2. **Το ab είναι κυκλικό υπolattice του b αν και μόνο αν το a είναι πρωταρχικό ιδεώδες της τάξης O.**

<u>ΑΠΟΔΕΙΞΗ</u>

1. Το ab ως κλασματικό ιδεώδες είναι lattice και επειδή $ab \subseteq b$, θα έχουμε ότι το ab είναι υπolattice του b.

Επειδή το b είναι κλασματικό ιδεώδες της τάξης , θα υπάρχει $b \in O$ με $bb \subseteq O$. Η απεικόνιση προβολής

$\frac{O}{ab} \to \frac{O}{b}$ έχει πυρήνα το $\frac{b}{ab}$ και συνεπώς (επειδή η απεικόνιση είναι "επί") θα έχουμε

$(\#\frac{O}{b})(\#\frac{b}{ab}) =$

$= \#(\frac{O}{ab}) \to N(a) \cdot [b : ab] = N(ab) = N(a)N(b) \to [b : ab] = N(a).$

2. ($\leftarrow$) Έστω ότι το a είναι πρωταρχικό ενώ το ab δεν είναι κυκλικό υπolattice του b. Τότε από το λήμμα

3.3.1.4 προκύπτει ότι η ομάδα $(\frac{b}{ab},+)$ έχει υποομάδα ισόμορφη με την $(Z_d x Z_d,+)$, για κάποιο $d \in N$

με d>1. Αυτό σημαίνει ότι υπάρχει προσθετική υποομάδα b' της b με $ab \subseteq b' \subseteq b$, ώστε $(\frac{b'}{ab},+) \cong (Z_d x Z_d,+)$. Όμως η σχέση $ab \subseteq b' \subseteq b$, μας δίνει ότι το b' είναι ελεύθερη προσθετική υποομάδα του C με rank ίσο με 2 (αφού και τα ab,b είναι ελεύθερες προσθετικές ομάδες με rank

ίσο με 2). Θα δείξουμε ότι db'=ab

Έχουμε $\#\frac{b'}{ab} = \#(Z_d x Z_d) = d^2$. Εξάλλου επειδή

$(\frac{b'}{ab},+) \cong (Z_d x Z_d,+)$ και

επειδή κάθε στοιχείο της $(Z_d x Z_d,+)$ έχει τάξη διαιρέτη του d , θα ισχύει ότι

$db' \subseteq ab$. Όμως είναι προφανές ότι $\#\frac{b'}{db'} = d^2$, οπότε $\#\frac{b'}{ab} = \#\frac{b'}{db'}$ και

έτσι η σχέση $db' \subseteq ab$ δίνει db'=ab.

Η σχέση db'=ab , μας δίνει κατ' αρχήν ότι το b' είναι proper κλασματικό ιδεώδες της O.

Έχουμε τώρα $db'=ab \to a=d(bb'^{-1})$. Εξάλλου $bb'^{-1} \subseteq bb^{-1} = O$, οπότε το ιδεώδες bb'^{-1} είναι

ακέραιο και έχουμε άτοπο επειδή έχουμε υποθέσει το a να είναι πρωταρχικό.

($\rightarrow$) Έστω ότι η ομάδα $(\frac{b}{ab},+)$ είναι κυκλική αλλά το a δεν είναι πρωταρχικό ιδεώδες της τάξης O.

Θα υπάρχει λοιπόν $d\in N$ με $d>1$ και proper ιδεώδες c της O ώστε $a=dc$. Έχουμε συνεπώς ότι η

ομάδα $(\frac{b}{dcb},+)$ είναι κυκλική. Άρα και η υποομάδα της : $(\frac{cb}{dcb},+)$ είναι κυκλική. Παρατηρούμε όμως

ότι κάθε στοιχείο της ομάδας $(\frac{cb}{dcb},+)$ έχει τάξη που διαιρεί ο d , ενώ $\#(\frac{cb}{dcb},+) = d^2$. Κατά συνέπεια

η $(\frac{cb}{dcb},+)$ δεν μπορεί να είναι κυκλική και καταλήγουμε σε άτοπο.

<u>3.3.1.6 ΠΟΡΙΣΜΑ</u> : Αν O είναι τάξη σε φανταστικό τετραγωνικό σώμα αριθμών με $\alpha\in O$ και a είναι ένα

proper κλασματικό ιδεώδες της O , τότε ισχύουν τα ακόλουθα :

1. **Το αa είναι υπolattice του a τάξεως $N(\alpha)$.**
2. **Το αa είναι κυκλικό υπolattice του b αν και μόνο αν το α είναι πρωταρχικό στοιχείο της τάξης O.**

<u>ΑΠΟΔΕΙΞΗ</u>

Άμεση εφαρμογή της πρότασης 3.3.1.5 για το proper ιδεώδες $a := \alpha O$ και λαμβάνοντας υπ'όψιν ότι
$N(a)=N(\alpha)$, και το 3 των παρατηρήσεων 3.3.1.3.

3.3.2 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΤΩΝ RING CLASS FIELDS ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΗΝ j - ΑΝΑΛΛΟΙΩΤΗ

3.3.2.1 ΛΗΜΜΑ : Αν L είναι το ring class field τάξης $\mathcal{O}$ σε φανταστικό τετραγωνικό σώμα αριθμών K ,

τότε $spl(L) \dot{=} \{ p\in\mathbb{P} \mid \exists \alpha\in\mathcal{O} : N(\alpha)=p \}$ και ειδικότερα

$spl(L)-\{2\} = \{ p\in\mathbb{P} \mid \exists \alpha\in\mathcal{O} : N(\alpha)=p \}-\{2\}$.

ΑΠΟΔΕΙΞΗ

Η απόδειξη θα γίνει μόνο στην περίπτωση που $d_{\mathcal{O}}\equiv 0(\mathrm{mod}4)$.

Για την περίπτωση $d_{\mathcal{O}}\equiv 1(\mathrm{mod}4)$ παραπέμπουμε στην άσκηση 9.3 σελ.192 του [Cox].

Έστω λοιπόν $d_{\mathcal{O}}\equiv 0(\mathrm{mod}4)$. Από την πρόταση 2.2.1.10 έχουμε ότι για $d_{\mathcal{O}}=-4n$, με $n\in\mathbb{N}$, ισχύει $\mathcal{O}=\mathbb{Z}[\sqrt{-n}\,]$ και $K=\mathbb{Q}(\sqrt{-n}\,)$. Από το 2 του λήμματος 2.4.2.3 προκύπτει ότι οι περιττοί πρώτοι αριθμοί που γράφονται στην μορφή x^2+ny^2 , $x,y\in\mathbb{Z}$ είναι ακριβώς οι περιττοί πρώτοι του spl(L). Συνεπώς $spl(L) \dot{=} \{ x^2+ny^2 \mid x,y\in\mathbb{Z} , (x^2+ny^2)\in\mathbb{P} \}$. Μάλιστα $spl(L)-\{2\} = \{ x^2+ny^2 \mid x,y\in\mathbb{Z} , (x^2+ny^2)\in\mathbb{P} \}-\{2\}$.

Παρατηρούμε τώρα ότι αν $\alpha\in\mathcal{O}-\{0\}$, τότε υπάρχουν $x,y\in\mathbb{Z}$ με $\alpha=x+y\sqrt{-n}$, οπότε $N(\alpha)=x^2+ny^2$.

Συνεπώς , $spl(L) \dot{=} \{ p\in\mathbb{P} \mid \exists \alpha\in\mathcal{O} : N(\alpha)=p \}$ και ειδικότερα $spl(L)-\{2\} = \{ p\in\mathbb{P} \mid \exists \alpha\in\mathcal{O} : N(\alpha)=p \}-\{2\}$.

3.3.2.2 ΠΡΟΤΑΣΗ : Αν $\mathcal{O}$ είναι τάξη φανταστικού τετραγωνικού σώματος K , τότε ισχύουν τα ακόλουθα :

1. **Αν $\mathfrak{a}$ είναι proper κλασματικό ιδεώδες της $\mathcal{O}$, τότε ο $j(\mathfrak{a})$ είναι αλγεβρικός ακέραιος.**
2. **Ο $j(\mathcal{O})$ είναι πραγματικός αλγεβρικός ακέραιος.**

ΑΠΟΔΕΙΞΗ

1. Θα δείξουμε κατ' αρχήν ότι υπάρχει στοιχείο α της $\mathcal{O}$ με νορμα $N(\alpha)$ ελεύθερη τετραγώνου.

Πράγματι , Από πόρισμα 2.3.2.5 έχουμε ότι αν L είναι το ring class field της $\mathcal{O}$, τότε το σύνολο spl(L) είναι άπειρο. Επομένως και το σύνολο $\{ p\in\mathbb{P} \mid \exists \alpha\in\mathcal{O} : N(\alpha)=p \}$ είναι άπειρο (βλ. λήμμα 3.3.2.1). Υπάρχει λοιπόν $\alpha\in\mathcal{O}$ με $N(\alpha)\in\mathbb{P}$. Συνεπώς το $N(\alpha)$ είναι ελεύθερο τετραγώνου.

Θέτουμε $m:=N(\alpha)$. Από το 2 της παρατήρησης 3.3.1.3 και λόγω του ότι ο φυσικός $N(\alpha)$ είναι ελεύθερος τετραγώνου , έχουμε ότι το στοιχείο α είναι πρωταρχικό. Εφαρμόζοντας το πόρισμα 3.3.1.6 λοιπόν θα πάρουμε ότι το $\alpha\mathfrak{a}$ είναι κυκλικό υπolattice του $\mathfrak{a}$ τάξης $N(\alpha)=m$. Το θεώρημα 3.2.4.4 επομένως θα δώσει ότι $\Phi_m(j(\alpha\mathfrak{a}),j(\mathfrak{a}))=0$. Επειδή $j(\alpha\mathfrak{a})=j(\mathfrak{a})$ (βλ. πρόταση 3.1.2.7) , θα έχουμε ότι $\Phi_m(j(\mathfrak{a}),j(\mathfrak{a}))=0$. Το

$j(\mathsf{a})$ κατά συνέπεια είναι ρίζα της εξίσωσης $\Phi_m(x,x)=0$, οπότε λόγω του 3 της πρότασης 3.2.3.4 έχουμε

ότι το $j(\mathsf{a})$ είναι ακέραιος αλγεβρικός αριθμός.

2. Έχουμε $\mathsf{O}=\overline{\mathsf{O}}$ (βλ. το III της πρότασης 2.2.1.8) , οπότε λόγω της παρατήρησης 3.1.2.8 ισχύει $j(\mathsf{O})=j(\overline{\mathsf{O}})=\overline{j(\mathsf{O})}$, πράγμα που σημαίνει ότι $j(\mathsf{O})\in \mathsf{R}$. Λόγω του 1 τώρα έχουμε το ζητούμενο.

3.3.2.3 ΛΗΜΜΑ : Έστω O τάξη φανταστικού τετραγωνικού σώματος K , και a ένα proper κλασματικό ιδεώδες της O. Έστω επίσης L το ring class field της τάξης O. Θέτουμε $\mathsf{M}:=\mathsf{K}(j(\mathsf{a}))$.

1. Αν υπάρχει περιττός πρώτος αριθμός p ο οποίος να ικανοποιεί τα ακόλουθα :

- **$\mathsf{p}\in spl(\mathsf{L})$.**
- **Ο p δεν διακλαδίζεται στο M.**

τότε το πρώτο ιδεώδες $\mathfrak{q}_M$ του R_K , που είναι πάνω από το $p\mathsf{Z}$ (δηλ. $p\mathsf{Z}=\mathfrak{q}_M\cap\mathsf{Z}$) ικανοποιεί τα ακόλουθα :

a. $j(\mathsf{a})^p\equiv j(\mathsf{a}) \pmod{\mathfrak{q}_M}$.

b. $R_K[j(\mathsf{a})]\subseteq R_M$ και μάλιστα $[R_M : R_K[j(\mathsf{a})]]<\infty$.

Αν επιπλέον $p\nmid [R_M : R_K[j(\mathsf{a})]]$, τότε

(ι). $\alpha^p\equiv\alpha \pmod{\mathfrak{q}_M}$, $\forall\alpha\in R_M$.

(ιι). $N(\mathfrak{q}_M)=p$ και $f\left(\frac{\mathfrak{q}_M}{p\mathsf{Z}}\right)=1$.

2. $spl(\mathsf{L})\dot{\subseteq} spl(\mathsf{M})$.

3. $\mathsf{M}\subseteq\mathsf{L}$.

ΑΠΟΔΕΙΞΗ

1. a. Θα δείξουμε κατ' αρχήν ότι υπάρχει στοιχείο α_o της O με νορμα ίση με p.

Πράγματι , Από λήμμα 3.3.2.1 έχουμε (επειδή το L είναι το ring class field της O) ότι $spl(\mathsf{L})-\{2\}=\{q\in\mathsf{P}\mid\exists\alpha\in\mathsf{O} : N(\alpha)=q\}-\{2\}$. Επειδή $p\in spl(\mathsf{L})-\{2\}$, θα υπάρχει $\alpha_o\in\mathsf{O}$ με $N(\alpha_o)=p$.

Στην συνέχεια δείχνουμε ότι το $\alpha_o\mathsf{a}$ είναι κυκλικό υπολattice του a τάξης $N(\alpha_o)=p$.

Πράγματι , η νόρμα του α_o , ως πρώτος αριθμός είναι ελεύθερος τετραγώνου και συνεπώς το α_o είναι πρωταρχικό στοιχείο της O. Το πόρισμα 3.3.1.6 τώρα μας δίνει το ζητούμενο.

Το θεώρημα 3.2.4.4 τώρα , μας δίνει ότι $\Phi_p(j(\alpha_o\mathsf{a}),j(\mathsf{a}))=0$. Συνεπώς $\Phi_p(j(\mathsf{a}),j(\mathsf{a}))=0$ (βλ. πρόταση 3.1.2.7). Από την ισοδυναμία του Kronecker (βλ. το 4 της πρότασης 3.2.3.4) προκύπτει ότι $0\equiv -(j(\mathsf{a})^p-j(\mathsf{a}))^2 \pmod{p\mathsf{Z}[j(\mathsf{a}),j(\mathsf{a})]}$. Συνεπώς υπάρχει πολυώνυμο δύο μεταβλητών $f(x,y)\in\mathsf{Z}[x,y]$ ώστε $0=-(j(\mathsf{a})^p-j(\mathsf{a}))^2+pf(j(\mathsf{a}),,j(\mathsf{a}))$. Όμως το $j(\mathsf{a})$ είναι αλγεβρικός ακέραιος (βλ. το 1 της πρότασης 3.3.2.2) , οπότε αφού $j(\mathsf{a})\in M$ ($M=K(j(\mathsf{a}))$) , θα έχουμε $j(\mathsf{a})\in R_M$. Κατά συνέπεια $f(j(\mathsf{a}),,j(\mathsf{a}))\in R_M$.

Επειδή τώρα το q_M βρίσκεται πάνω από το pZ , θα έχουμε $pZ \subseteq q_M$, οπότε $p \in q_M$, που σημαίνει ότι $pf(j(a),,j(a)) \in q_M$. Άρα λόγω του ότι $0 = -(j(a)^p - j(a))^2 + pf(j(a),,j(a))$, θα έχουμε $j(a)^p \equiv j(a) \pmod{q_M}$.

b. Προφανώς $R_K[j(a)] \subseteq R_M$ (βλ. πρότ. 3.3.2.2). Το R_M είναι ελεύθερη αβελιανή ομάδα με rank ίσο με $[M : K]$. Επίσης επειδή το πολυώνυμο $Irr(j(a)|K)$ έχει βαθμό ίσο με $[M :K]$, τα $1, j(a), j(a)^2, \ldots, j(a)^{[M : K]-1}$ είναι Z-γραμμικώς ανεξάρτητα. Λόγω επομένως του λόγω του 1 του θεωρήματος 2.2.2.13 έχουμε ότι και το $R_K[j(a)]$ είναι ελεύθερη αβελιανή ομάδα με rank ίσο με $[M : K]$. Από το 3 του θεωρήματος 2.2.2.13 προκύπτει τώρα ότι $[R_M : R_K[j(a)]] < \infty$.

Έστω ότι $p \nmid [R_M : R_K[j(a)]]$.

(ι). Έχουμε $p \in spl(L) \rightarrow p \in spl(K)$. Έστω $p = q_M \cap K$. Το p έχει νόρμα ίση με p (αφού $p \in spl(K)$) και $pZ \subseteq p \subseteq q_M$. Έχουμε $\alpha^p \equiv \alpha \pmod{p}$, $\forall \alpha \in R_K \rightarrow \alpha^p \equiv \alpha \pmod{q_M}$, $\forall \alpha \in R_K$. Λόγω συνεπώς του a. θα έχουμε ότι $\alpha^p \equiv \alpha \pmod{q_M}$, $\forall \alpha \in R_K[j(a)]$. (Σ 3.3.2.3.1)

Έστω $n := [R_M : R_K[j(a)]]$. Θα δείξουμε ότι η απεικόνιση $L : \frac{R_M}{q_M} \rightarrow \frac{R_M}{q_M} : \alpha + q_M \rightarrow n\alpha + q_M$, $\forall \alpha \in R_M$ είναι ισομορφισμός σωμάτων.

Πράγματι , η L είναι "1-1" γιατί αν $n(\alpha-\beta) \in q_M$ για κάποια $\alpha, \beta \in R_M$, τότε επειδή $n \notin q_M$ (αν $n \in q_M$, τότε $n \in q_M \cap Z = pZ \rightarrow p|n$, κάτι που είναι άτοπο από την υπόθεση) θα έχουμε αναγκαστικά $(\alpha-\beta) \in q_M$ και συνεπώς $\alpha \equiv \beta \pmod{q_M}$.

Επίσης η L είναι προφανώς ομομορφισμός σωμάτων , οπότε μένει να αποδείξουμε ότι είναι και συνάρτηση "επί". Αν $\alpha \in R_M$, τότε $(n\alpha) \in R_K[j(a)]$ και έτσι η σχέση Σ 3.3.2.3.1 θα δώσει $(n\alpha)^p \equiv (n\alpha) \pmod{q_M}$. Η τελευταία ισοτιμία συνεπάγεται ότι $n(n^{p-1}\alpha-\alpha) \in q_M$. Αλλά επειδή $n \notin q_M$ (λόγω του ότι $q_M \cap Z = pZ$ και $p \nmid n$) , θα έχουμε $(n^{p-1}\alpha-\alpha) \in q_M$ και συνεπώς $L(\alpha n^{p-1} + q_M) = \alpha + q_M$.

Έστω τώρα $\alpha \in R_M$. Επειδή η L είναι ισομορφισμός , θα υπάρχει $\beta \in R_M$ με $n\beta \equiv \alpha \pmod{q_M}$. Εξάλλου $n = [R_M : R_K[j(a)]]$, (που σημαίνει ότι $n\beta \in R_K[j(a)]$) οπότε θα ισχύει $(n\beta)^p \equiv (n\beta) \bmod (q_M)$ (βλ. Σ 3.3.2.3.1). Έχουμε λοιπόν συνολικά $\alpha \equiv n\beta \equiv (n\beta)^p \equiv \alpha^p \pmod{q_M}$.

(ιι). Από το (ι) έχουμε ότι $\forall c \in \frac{R_M}{q_M}$ ισχύει $c^p = c$. Κατά συνέπεια , $\forall c \in \frac{R_M}{q_M} - \{0\}$ ισχύει $c^{p-1} = 1$ (Σ 3.3.2.3.2)

Όμως η πολλαπλασιαστική ομάδα $(\frac{R_M}{q_M} - \{0\}, \cdot)$ είναι κυκλική (αφού το σώμα $\frac{R_M}{q_M}$ είναι πεπερασμένο)

οπότε αν c_o είναι γεννήτορας της $(\frac{R_M}{q_M}-\{0\}, \cdot)$, επειδή από την σχέση Σ 3.3.2.3.2 έχουμε $c_o^{p-1}=1$

,

θα ισχύει $\#(\frac{R_M}{q_M}-\{0\}) \mid (p-1)$. Αλλά $N(q_M)=\#\frac{R_M}{q_M}$ και συνεπώς $(N(q_M)-1) \mid (p-1)$. Εξάλλου ο αριθμός

$N(q_M)$ είναι δύναμη του p $(q_M \cap Z=pZ)$, οπότε αναγκαστικά $N(q_M)=p$. Επίσης $N(q_M)=p^{f\left(\frac{q_M}{pZ}\right)}$, οπότε

$f\left(\frac{q_M}{pZ}\right)=1$.

2. Αν $p \in spl(L)$ με $p \nmid [R_M : R_K[j(a)]]$ και ο p δεν διακλαδίζεται στο M, τότε από το (ιι) του 1 έχουμε
   $p \in spl(M)$.

   Πράγματι, επειδή ο p δεν διακλαδίζεται στο M ισχύει $e\left(\frac{q_M}{pZ}\right)=1$, για κάθε πρώτο

   ιδεώδες q_M του R_M πάνω από το pZ. Εξάλλου από το (ιι) του 1 έχουμε ότι και

   $f\left(\frac{q_M}{pZ}\right)=1$, για κάθε πρώτο ιδεώδες q_M του R_M πάνω από το pZ. Συνεπώς

   $p \in spl(M)$.

   Όμως οι πρώτοι αριθμοί που διακλαδίζονται στο M είναι πεπερασμένοι (βλ. θεώρημα 2.3.1.7) και επίσης οι πρώτοι αριθμοί που διαιρούν το $[R_M : R_K[j(a)]]$ είναι πεπερασμένοι, οπότε εκτός από πεπερασμένο πλήθος πρώτων αριθμών, τα στοιχεία του spl(L) βρίσκονται στο spl(M).
   Δηλαδή $spl(L) \dot{\subseteq} spl(M)$.
3. Από το 1 του λήμματος 2.4.2.3 έχουμε ότι η επέκταση L/K είναι Galois. Το 1 της πρότασης 2.3.2.7 επομένως δίνει την ακόλουθη ισοδυναμία "$M \subseteq L$" $\leftrightarrow$ "$spl(L) \dot{\subseteq} spl(M)$" και το ζητούμενο τώρα είναι άμεση
   συνπέπεια του 2.

<u>3.3.2.4 ΛΗΜΜΑ</u> : Έστω O τάξη φανταστικού τετραγωνικού σώματος K, με οδηγό $f = cond(O)$ και a_o ένα

proper κλασματικό ιδεώδες της O. Έστω επίσης L το ring class field της τάξης O και $M=K(j(a_o))$. Ισχύουν τα ακόλουθα :

1. **Για κάθε proper κλασματικό ιδεώδες της O : a, ισχύει $j(a) \subseteq L$.**
2. **Αν $a_1, a_2, \ldots, a_h$ είναι αντιπρόσωποι κλάσεων για την C(O), τότε ο αριθμός $\Delta := \prod_{1 \le i < j \le h} (j(a_i) - j(a_j))$ είναι στοιχείο του $R_L-\{0\}$. Μάλιστα κάθε παράγοντας του Δ $(j(a_i) - j(a_j))$, $1 \le i < j \le h$ ανήκει στο R_L.**
3. **Αν $p \in \tilde{spl}(M)$, με $p \nmid f$ ώστε $MK\Delta(pR_L, \Delta R_L)=1$, τότε για κάθε πρώτο ιδεώδες p του R_K πάνω από το p ισχύουν τα ακόλουθα :**
   a. **$p = N(p) = N(p \cap O)$.**
   b. **Το ιδεώδες $(p \cap O)a$ είναι proper κλασματικό ιδεώδες της O και τα a, $(p \cap O)a$ δίνουν την ίδια κλάση στην C(O).**

4. $\tilde{spl}(M) \dot{\subseteq} spl(L)$.
5. $L \subseteq M$.

ΑΠΟΔΕΙΞΗ

1. Από το 3 του λήμματος 3.3.2.3 έχουμε ότι για κάθε proper κλασματικό ιδεώδες a της O ισχύει $K(j(a)) \subseteq L$.

Συνεπώς $j(a) \subseteq L$. Επειδή τα a_i , a_j για $i \neq j$ δεν είναι ομοιόθετα (βλ. το 1 των παρατηρήσεων 3.1.3.10) θα έχουμε $j(a_i) \neq j(a_j)$ (βλ. πρόταση 3.1.2.7). Εξάλλου $\forall i \in \{1,..,h\}$ ισχύει ότι ο $j(a_i)$ είναι αλγεβρικός ακέραιος (βλ. πρόταση 3.3.2.2) οπότε αφού $j(a_i) \in L$, θα έχουμε τελικά $\forall i \in \{1,\ldots,h\}$ $j(a_i) \in R_L$. Επομένως $\Delta \in R_L$.

2. Κατ' αρχήν ισχύει $M \subseteq L$ (βλ. λήμμα 3.3.2.3). Έχουμε $p \in \tilde{spl}(M)$ οπότε το p δεν διακλαδίζεται στο M και υπάρχει πρώτο ιδεώδες q_M του R_M πάνω από το pZ ώστε $f\left(\frac{q_M}{pZ}\right)=1$ (βλ. ορισμό 2.3.2.6).

Θα δείξουμε αρχικά ότι για κάθε πρώτο ιδεώδες p του R_K πάνω από το pZ ισχύει $f\left(\frac{p}{pZ}\right)=1$.

Πράγματι , οι βαθμοί αδρανείας των πρώτων ιδεωδών του K πάνω από το pZ ταυτίζονται αφού η επέκταση K/Q είναι Galois , οπότε επειδή $f\left(\frac{q_M \cap K}{pZ}\right)=1$ (λόγω πολλαπλασιαστικότητας των βαθμών αδρανείας και του γεγονότος ότι $f\left(\frac{q_M}{pZ}\right)=1$) οι βαθμοί αδρανείας όλων των πρώτων ιδεωδών του K πάνω από το pZ θα είναι 1.

Άμεση συνέπεια της πρότασης που μόλις αποδείξαμε είναι ότι αν p είναι πρώτο ιδεώδες του R_K πάνω από το pZ , τότε $N(p) = p$. $(N(p) = p^{f\left(\frac{p}{pZ}\right)} = p)$.

Στην συνέχεια παρατηρούμε ότι $p \in spl(K)$.

Πράγματι , οι βαθμοί αδρανείας των πρώτων ιδεωδών του K πάνω από το pZ

Επίσης το pZ δεν διακλαδίζεται στο M άρα ούτε και στο K.

Δείχνουμε τώρα ότι κάθε πρώτο ιδεώδες p του R_K πάνω από το pZ είναι πρώτο προς το f και επίσης $p = N(p) = N(p \cap O)$.

Επειδή έχουμε εξ'υποθέσεως ότι $p \nmid f$, θα ισχύει $MK\Delta(p,f)=1 \rightarrow MK\Delta(N(p),f)$.

Από το 1 της πρότασης 2.2.4.3 προκύπτει ότι το ιδεώδες p του R_K είναι πρώτο

πρός το f , οπότε από το 1 της πρότασης 2.2.4.6 προκύπτει ότι και το ιδεώδες $p \cap O$ της O είναι πρώτο προς το f και μάλιστα $N(p) = N(p \cap O)$.

Μένει λοιπόν να δείξουμε ότι αν p είναι πρώτο ιδεώδες του R_K πάνω από το pZ , τότε το ιδεώδες $(p \cap O)a$ είναι proper κλασματικό ιδεώδες της O και τα a , $(p \cap O)a$ δίνουν την ίδια κλάση στην $C(O)$.

Πράγματι , το p όπως δείξαμε προηγουμένως είναι πρώτο προς το f. Συνεπώς $(N(p),f)=1 \rightarrow (N(p \cap O),f)=1$. Το ιδεώδες $p \cap O$ της O επομένως είναι πρώτο πρός τον οδηγό f της O και συνεπώς είναι ακέραιο proper ιδεώδες της O (βλ. το 2 της πρότασης 2.2.4.3). Τώρα επειδή $N(p \cap O) = N(p) = p$,

το ιδεώδες $\mathfrak{p}\cap\mathfrak{O}$ της θα είναι πρωταρχικό (βλ. το 1 των παρατηρήσεων 3.3.1.3) και η πρόταση 3.3.1.5 δίνει ότι το $(\mathfrak{p}\cap\mathfrak{O})\mathfrak{a}$ είναι κυκλικό υπολattice του $\mathfrak{a}$ και μάλιστα τάξης p. Το θεώρημα 3.2.4.4 επομένως συνεπάγεται ότι $\Phi_p(j(\mathfrak{a}'),j(\mathfrak{a}))=0$, όπου $\mathfrak{a}' = (\mathfrak{p}\cap\mathfrak{O})\mathfrak{a}$. Από την σχέση ισοδυναμίας του Kronecker (βλ. το 4 της πρότασης 3.2.3.4) έχουμε ότι υπάρχει πολυώνυμο δυο μεταβλητών $P(x,y)\in\mathbb{Z}[x,y]$ ώστε $0 = \Phi_p(j(\mathfrak{a}'),j(\mathfrak{a})) = (j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) + pP(j(\mathfrak{a}'),j(\mathfrak{a}))$ (Σ 3.3.2.4.1) Από το 3 του 3.3.2.3 λήμματος έχουμε $M\subseteq L$. Θεωρούμε λοιπόν πρώτο ιδεώδες $\mathfrak{q}_L$ του R_L πάνω από το $\mathfrak{q}_M$ (Υπενθιμίζουμε ότι το $\mathfrak{q}_M$ εκλέχτηκε ως πρώτο ιδεώδες του R_M πάνω από το $p\mathbb{Z}$ ώστε $f\left(\frac{\mathfrak{q}_M}{p\mathbb{Z}}\right)=1$.) Θα δείξουμε ότι $MK\Delta(p , (j(\mathfrak{a}) - j(\mathfrak{a}')))\neq 1$ στο R_L.

Πράγματι , επειδή τα $j(\mathfrak{a}), j(\mathfrak{a}')$ είναι αλγεβρικοί ακέραιοι (βλ. πρόταση 3.3.2.2) και από το 1 προκύπτει ότι ανήκουν στο L , θα έχουμε $j(\mathfrak{a}'), j(\mathfrak{a})$, $P(j(\mathfrak{a}'),j(\mathfrak{a}))\in R_L$. Αλλά το $\mathfrak{q}_L$ είναι πάνω από το $\mathfrak{q}_M$ και συνεπώς πάνω από το $p\mathbb{Z}$. Αυτό σημαίνει ότι $p\in\mathfrak{q}_L$, οπότε $pR_L\subseteq\mathfrak{q}_L \rightarrow pP(j(\mathfrak{a}'),j(\mathfrak{a}))\in\mathfrak{q}_L$. Η σχέση Σ 3.3.2.4.1 τώρα θα δώσει

$(j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) = pP(j(\mathfrak{a}'),j(\mathfrak{a}))\in\mathfrak{q}_L$. . Παρατηρούμε όμως ότι το $f\left(\frac{\mathfrak{q}_M}{p\mathbb{Z}}\right)$ είναι η διάσταση του $\mathbb{Z}_p$ - διανυσματικού χώρου $\frac{R_M}{\mathfrak{q}_M}$. Επειδή $f\left(\frac{\mathfrak{q}_M}{p\mathbb{Z}}\right)=1$, θα έχουμε ότι η κανονική προβολή $\mathbb{Z}_p \rightarrow \frac{R_M}{\mathfrak{q}_M} : k+p\mathbb{Z} \rightarrow k+\mathfrak{q}_M$, $k\in\mathbb{Z}$ είναι ισομορφισμός. Άρα $\#(\frac{R_M}{\mathfrak{q}_M} - \{0\}) = p-1 \rightarrow \begin{cases} j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{q}_M} \\ j(\mathfrak{a}')^p \equiv j(\mathfrak{a}') \pmod{\mathfrak{q}_M} \end{cases} \rightarrow \begin{cases} j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{q}_L} \\ j(\mathfrak{a}')^p \equiv j(\mathfrak{a}') \pmod{\mathfrak{q}_L} \end{cases}$, οπότε $(j(\mathfrak{a}') - j(\mathfrak{a}))^2 \equiv pP(j(\mathfrak{a}'),j(\mathfrak{a})) \equiv 0 \pmod{\mathfrak{q}_L}$ και επειδή το $\mathfrak{q}_L$ είναι πρώτο ιδεώδες του R_L θα πάρουμε $(j(\mathfrak{a}') - j(\mathfrak{a})) \in \mathfrak{q}_L$.

Αν λοιπόν τα $\mathfrak{a}'$, $\mathfrak{a}$ ανήκαν σε διαφορετικές κλάσεις της $C(\mathfrak{O})$, τότε το $(j(\mathfrak{a}') - j(\mathfrak{a}))$ θα διαιρούσε το Δ (που ορίστηκε στο 2) στο R_L. Άρα $\Delta\in\mathfrak{q}_L \rightarrow \mathfrak{q}_L \mid \Delta R_L$. Όμως $\mathfrak{q}_L \mid pR_L$ και έτσι $MK\Delta(pR_L ,\Delta R_L)\neq 1$, πράγμα άτοπο εξ'υποθέσεως.

3. Έστω περιττός πρώτος p με $p\in \tilde{spl}(M)$, $p\nmid f$ και $MK\Delta(pR_L,\Delta R_L)=1$. Τα ιδεώδη $\mathfrak{a}$, $\mathfrak{a}':=(\mathfrak{p}\cap\mathfrak{O})\mathfrak{a}$ (από το 2) ανήκουν στην ίδια κλάση της $C(\mathfrak{O})$. Συνεπώς $\mathfrak{a}'\mathfrak{a}^{-1}\in H(\mathfrak{O}) \rightarrow (\mathfrak{p}\cap\mathfrak{O})\in H(\mathfrak{O})$. Γράφουμε $(\mathfrak{p}\cap\mathfrak{O})=\alpha\mathfrak{O}$,για $\alpha\in\mathfrak{O}$. Έχουμε $p = N(\mathfrak{p}\cap\mathfrak{O}) = N(\alpha)$ (βλ. το 2) και συνεπώς $p\in\{q\in\mathbb{P} \mid \exists\beta\in\mathfrak{O} : p=N(\beta)\}$, που σημαίνει ότι $p\in spl(L)$ (βλ. λήμμα 3.3.2.1). Όμως οι συνθήκες $p\nmid f$ και $MK\Delta(pR_L,\Delta R_L)\neq 1$ ικανοποιούνται για πεπερασμένο πλήθος πρώτων αριθμών p.

Πράγματι , ο R_L είναι δακτύλιος μονοσήμαντης ανάλυσης σε πρώτα ιδεώδη , οπότε αν p είναι πρώτος αριθμός με $MK\Delta(pR_L,\Delta R_L)\neq 1$, τότε τα πρώτα ιδεώδη του R_L που θα διαιρούσαν τον $MK\Delta(pR_L,\Delta R_L)$ θα ήταν ακριβώς (πεπερασμένους το πλήθος) οι πρώτοι διαιρέτες του ΔR_L που είναι πάνω από το p. Επειδή κάθε πρώτο ιδεώδες έχει ακριβώς ένα πρώτο αριθμό από κάτω του , οι πρώτοι αριθμοί που βρίσκονται κάτω από τα πρώτα ιδεώδη της ανάλυσης του ΔR_L είναι πεπερασμένοι το πλήθος.

Συνεπώς $\tilde{spl}(M) \dot{\subseteq} spl(L)$.

4. Άμεση συνέπεια του 3 και του 2 της πρότασης 2.3.2.7 (η $L/\mathbb{Q}$ είναι Galois λόγω του 1 του λήμματος 2.4.2.3).

3.3.2.5 ΘΕΩΡΗΜΑ : Άν $\mathbf{O}$ είναι τάξη φανταστικού τετραγωνικού σώματος K , και $\mathfrak{a}$ είναι proper κλασματικό ιδεώδες της $\mathbf{O}$, τότε το σώμα $K(j(\mathfrak{a}))$ είναι το ring class field της $\mathbf{O}$.

ΑΠΟΔΕΙΞΗ

Το θεώρημα είναι προφανής συνέπεια των λημμάτων 3.3.2.3 και 3.3.2.4

3.3.2.6 ΠΟΡΙΣΜΑ : Αν K είναι τετραγωνικό φανταστικό σώμα αριθμών , τότε το $K(j(R_K))$ είναι το σώμα κλάσεως του Hilbert.

ΑΠΟΔΕΙΞΗ

Το σώμα κλάσεως του Hilbert είναι το ring class field της μέγιστης τάξης : R_K (βλ. παρατήρηση 2.4.1.3).

Το ζητούμενο έπεται τώρα άμεσα από το θεώρημα 3.3.2.5.

Είναι γνωστό από την πρόταση 2.4.1.4 ότι αν L είναι το ring class field μιας τάξης $\mathbf{O}$ τετραγωνικού φανταστικού σώματος K , τότε η απεικόνιση του Artin επάγει ισομορφισμό $C(\mathbf{O}) \to G(L|K)$. Τώρα που το θεώρημα 3.3.2.5 μας έχει χαρακτηρίσει το ring class field , είναι φυσικό ότι μπορεί να προσδιοριστεί πιο συγκεκριμένα και ο ισομορφισμός $C(\mathbf{O}) \to G(L|K)$. Αναφέρουμε στην συνέχεια ένα θεώρημα από το οποίο προκύπτει εύκολα η μορφή του ισομορφισμού $C(\mathbf{O}) \to G(L|K)$. Αποδείξεις του θεωρήματος μπορούν να βρεθούν στο [Lang] Κεφ. 12 §3 , Κεφ. 10 §3 , καθώς και στο [Cox] θεώρ. 11.36 σελ. 240.

3.3.2.7 ΘΕΩΡΗΜΑ : Έστω $\mathbf{O}$ μία τάξη σε φανταστικό τετραγωνικό σώμα K και L τό ring class field της $\mathbf{O}$. Αν $\mathfrak{a}$ είναι ένα proper κλασματικό ιδεώδες της $\mathbf{O}$ και $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες του R_K που δεν διακλαδίζεται στο L , τότε $\left(\frac{L \mid K}{\mathfrak{p}}\right)(j(\mathfrak{a})) = j(\overline{\mathfrak{p} \cap \mathbf{O}} \cdot \mathfrak{a})$.

Σαν άμεσο πόρισμα του παραπάνω θεωρήματος αναφέρουμε παρακάτω πως μπορεί να χαρακτηριστεί ο ισομορφισμός $C(\mathbf{O}) \to G(L|K)$ της πρότασης 2.4.1.4

3.3.2.8 ΠΟΡΙΣΜΑ : Έστω $\mathbf{O}$ μία τάξη σε φανταστικό τετραγωνικό σώμα K με οδηγό f και L τό ring class field της $\mathbf{O}$. Για κάθε proper κλασματικό ιδεώδες $\mathfrak{a}_f$ της $\mathbf{O}$ πρώτο προς το f , το στοιχείο το $\Phi_{L/K,m}(\mathfrak{a}_f R_K)$ της $G(L|K)$, για $m=fR_K$, προκύπτει ώς εξής :

Θεωρούμε τυχαίο proper κλασματικό ιδεώδες $\mathfrak{b}$ της $\mathbf{O}$ (π.χ. το $\mathfrak{a}_f$) Από θεώρημα 3.3.2.5 ισχύει $L=K(j(\mathfrak{b}))$, οπότε αρκεί να προσδιοριστεί η τιμή της $\Phi_{L/K,m}(\mathfrak{a}_f R_K)$ στο $j(\mathfrak{b})$. Ισχύει λόγω του θεωρήματος 3.3.2.7 ότι $\Phi_{L/K,m}(\mathfrak{a}_f R_K)(j(\mathfrak{b})) = j(\bar{\mathfrak{a}}\,\mathfrak{b})$.

Αφού λοιπόν έχουμε χαρακτηρίσει πλήρως το $\Phi_{L/K,m}(\mathfrak{a}_f R_K)$, χαρακτηρίζεται αυτόματα και ο ισομορφισμός $C(\mathbf{O}) \to G(L|K)$ της πρότασης 2.4.1.4 όπως φαίνεται παρακάτω (βλ. πρόταση 2.4.1.4) :

Για κάθε αντιπρόσωπο $\mathfrak{a}$ κλάσης της $C(\mathbf{O})$, παίρνουμε τυχαίο πρώτο πρός το f ιδεώδες $\mathfrak{a}_f$ που να ανήκει στην κλάση και ορίζουμε το στοιχείο $\sigma_{\mathfrak{a}}$ της $G(L|K)$ να είναι το $\Phi_{L/K,m}(\mathfrak{a}_f R_K)$.

Η αντιστοιχία $\mathfrak{a} \cdot H(\mathbf{O}) \to \sigma_{\mathfrak{a}}$ επάγει τον ισομορφισμό της πρότασης 2.4.1.4.

3.3.3 Η MODULAR ΕΞΙΣΩΣΗ

3.3.3.1 ΟΡΙΣΜΟΣ : 1. Έστω τάξη O σε φανταστικό τετραγωνικό σώμα αριθμών K. Με $H_O(x)$ θα συμβολίζεται το ανάγωγο πολυώνυμο του $j(O)$ πάνω από το $\mathbb{Q}$. Η εξίσωση $H_O(x)=0$ θα ονομάζεται εξίσωση κλάσεων . Εξίσωση κλάσεων θα ονομάζεται καταχρηστικά και το πολυώνυμο $H_O(x)$.

2. Αν $D\in\mathbb{Z}$ και υπάρχει τάξη O σε τετραγωνικό σώμα αριθμών με διακρίνουσα ίση με D , τότε ορίζουμε $H_D(x) := H_O(x)$.

3.3.3.2 ΠΑΡΑΤΗΡΗΣΗ : Επειδή για τάξη O σε φανταστικό τετραγωνικό σώμα αριθμών K , το $j(O)$ είναι αλγεβρικός ακέραιος (βλ. πρόταση 3.3.2.2) , έχουμε ότι $H_O(x)\in\mathbb{Z}[x]$.

3.3.3.3 ΠΡΟΤΑΣΗ : Έστω O μία τάξη σε φανταστικό τετραγωνικό σώμα αριθμών K. Θέτουμε h:=h(O). Άν $\{a_1,a_2,\ldots,a_h\}$ είναι πλήρες σύνολο αντιπροσώπων κλάσεων της C(O) , τότε

$$H_O(x) = \prod_{i=1}^{h} (x - j(a_i)) .$$

ΑΠΟΔΕΙΞΗ

Από το θεώρημα 3.3.2.5 έχουμε ότι το L:=K(j(O)) είναι το ring class field της O και από το 1 του λήμματος 2.4.2.3 προκύπτει ότι η επέκταση L/K είναι Galois. Επίσης , το 3b του λήμματος 2.4.2.1 συνεπάγεται ότι $L\cap R = \mathbb{Q}(j(O))$ και το 3a του ίδιου λήμματος δίνει ότι η επέκταση $L\cap R / \mathbb{Q}$ είναι Galois.

Από τον ορισμό της εξίσωσης κλάσεων έχουμε επομένως $H_O(x) = \prod_{\sigma\in G(\mathbb{Q}(j(O)) \mid \mathbb{Q})} (x - \sigma(j(O)))$. Θα δείξουμε ότι $H_O(x) = \prod_{\sigma\in G(L|K)} (x - \sigma(j(O)))$.

Αρχικά δείχνουμε ότι $\{ \sigma_{|L\cap R} \mid \sigma\in G(L|K)\} \subseteq G(L\cap R \,|\mathbb{Q})$.

Πράγματι , $\sigma\in G(L|K)$, τότε $\sigma\in G(L|\mathbb{Q})$. Επειδή η επέκταση $L\cap R / \mathbb{Q}$ είναι Galois , το σώμα $L\cap R$ είναι ευσταθής ενδιάμεση επέκταση της $L/\mathbb{Q}$ και επομένως το $\sigma_{|L\cap R}$ είναι αυτομορφισμός του $L\cap R$. Εξάλλου $\sigma\in G(L|K)$, οπότε η $\sigma_{|R}$ αφήνει αναλλοίωτα τα στοιχεία του $K\cap R=\mathbb{Q}$ και συνεπώς $\sigma\in G(L\cap R \,|\mathbb{Q})$.

Στην συνέχεια δείχνουμε ότι $\#\{ \sigma_{|L\cap R} \mid \sigma\in G(L|K)\} = \#G(L|K)$.

Προφανώς $\#\{ \sigma_{|L\cap R} \mid \sigma\in G(L|K)\} \le \#G(L|K)$. Αρκεί λοιπόν να δειχτεί

ότι αν $\sigma,\sigma'\in G(L|K)$ με $\sigma_{|L\cap R} = \sigma'_{|L\cap R}$, τότε $\sigma=\sigma'$. Επειδή $j(O)\in L\cap R$ (βλ. το 2 της πρότασης 3.3.2.2) , θα έχουμε $\sigma_{|L\cap R}(j(O)) = \sigma'_{|L\cap R}(j(O)) \rightarrow \sigma(j(O)) = \sigma'(j(O))$. Επειδή όμως

σ,σ'∈ G(L|K) και L= K(j(O)) , θα ισχύει τελικά σ=σ'.

Έχουμε επομένως $\{ \sigma_{|L\cap R} \mid \sigma\in G(L|K)\} = G(L\cap R\,|\mathbb{Q})$ (βλ. το 3a του λήμματος 2.4.2.1.).

Από το 2 της πρότασης 3.3.2.2 έχουμε ότι ο $j(O)\in R$, οπότε

$$\{ \sigma(j(O)) \mid \sigma\in G(L|K) \} = \{ \sigma_{|L\cap R}(j(O)) \mid \sigma\in G(L|K) \} = \{ \sigma(j(O)) \mid \sigma\in G(L\cap R\,|\mathbb{Q}\}.$$

Συνεπώς θα έχουμε $\{ \sigma(j(O)) \mid \sigma\in G(L|K) \} = \{\sigma(j(O)) \mid \sigma\in G(\mathbb{Q}(j(O))|\mathbb{Q})\}$,

πράγμα

που σημαίνει $H_O(x) = \prod_{\sigma\in G(\mathbb{Q}(j(O))\,|\,\mathbb{Q})} (x - \sigma(j(O))) = \prod_{\sigma\in G(L|K)} (x - \sigma(j(O)))$.

Από τον ισομορφισμό $C(O) \to G(L|K)$ του πορίσματος 3.3.2.8 προκύπτει ότι $G(L|K) = \{ \sigma_{a_t} \mid 1\le t\le h \}$ και έτσι $H_O(x) = \prod_{1\le t\le h} [x - \sigma_{a_t}(j(O))]$. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι όλα τα a_t , $1\le t\le h$, είναι πρώτα πρός το f (βλ. πόρισμα 2.2.3.10). Από το πόρισμα 3.3.2.8 θα πάρουμε ότι $\forall t\in \{1,2,\ldots h\}$, $\sigma_{a_t}(j(O)) = j(\overline{a_t}\cdot O) = j(\overline{a_t\cdot O}) = j(\overline{a_t})$ (λόγω του ότι $O=\overline{O}$ από την πρόταση 2.2.1.8). Τώρα το $\{\overline{a_1},\overline{a_2},\ldots,\overline{a_h}\}$ είναι πλήρες σύνολο αντιπροσώπων κλάσεων για την τάξη $\overline{O}=O$, και συνεπώς $\{j(a_t) \mid 1\le t\le h\} = \{j(\overline{a_t}) \mid 1\le t\le h\}$. Συνοψίζοντας τα παραπάνω έχουμε :

$$H_O(x) = \prod_{1\le t\le h} [x - \sigma_{a_t}(j(O))] = \prod_{1\le t\le h} (x - j(\overline{a_t})) = \prod_{1\le t\le h} (x - j(a_t)).$$

<u>3.3.3.4 ΠΟΡΙΣΜΑ</u> : Έστω O μία τάξη σε φανταστικό τετραγωνικό σώμα αριθμών K. Αν a είναι ένα proper κλασματικό ιδεώδες της O , τότε $Irr(j(a)|\mathbb{Q})(x) = H_O(x)$.

<u>ΑΠΟΔΕΙΞΗ</u>

Αν $\{a_t \mid 1\le t\le h\}$ είναι πλήρες σύνολο αντιπροσώπων της C(O) , τότε από την πρόταση 3.3.3.3. έχουμε $H_O(x) = \prod_{1\le t\le h} (x - j(a_t))$. Χωρίς περιορισμό της γενικότητας θεωρούμε ότι η κλάση $a\cdot H(O)$ του a στην C(O) είναι η $a_1\cdot H(O)$, οπότε $j(a_1) = j(a)$. Το $j(a)$ επομένως είναι ρίζα του $H_O(x)$ το οποίο είναι ανάγωγο πάνω από το $\mathbb{Q}$. Επομένως $Irr(j(a)|\mathbb{Q})(x) = H_O(x)$.

Για λόγους πληρότητας αναφέρουμε το παρακάτω θεώρημα που συνδέει την modular εξίσωση με την εξίσωση κλάσεων.

<u>3.3.3.5 ΘΕΩΡΗΜΑ</u> : Έστω $m\in\mathbb{N}$ ελέυθερος τετραγώνου. Για κάθε τάξη O υπάρχει $\tau\in h$ με $O = \mathbb{Z}+\tau\mathbb{Z}$ (βλ. το 2 της πρότασης 2.2.1.10 και θέτουμε $r(O,m) := \#\{ \sigma\in C(m) \mid j(\sigma\cdot\tau)=j(\tau) \}$.

Ισχύει

ότι υπάρχει $c_m \in \mathbf{C}-\{0\}$ ώστε

$$\Phi_m(x,x) = c_m \prod_{O}^{*} H_O(x)^{r(O,m)}$$

όπου το γινόμενο είναι πάνω σε όλες τις τάξεις τετραγωνικών σωμάτων και το "$*$" δηλώνει ότι για τάξεις O,O' τετραγωνικών σωμάτων K,K' αντίστοιχα με $H_O(x) = H_{O'}(x)$, μόνο ένα εκ' των $H_O(x)$, $H_{O'}(x)$ εμφανίζεται στο γινόμενο.
(Βλ. [Cox] θεωρ. 13.4 σελ. 287).

Αναφέρουμε τέλος , χωρίς απόδειξη , το ακόλουθο θεώρημα

3.3.3.6 ΘΕΩΡΗΜΑ : Αν O είναι τάξη σε φανταστικό τετραγωνικό σώμα K , τότε υπάρχει αλγόριθμος υπολογισμού της εξίσωσης κλάσεων $H_O(x)$. (Βλ. [Cox] σελ. 286-298).

§4 ΤΟ ΤΕΛΙΚΟ ΘΕΩΡΗΜΑ

3.4.1 ΤΟ ΤΕΛΙΚΟ ΘΕΩΡΗΜΑ

Σκοπός της παραγράφου 3.4.1 αλλά και ο γενικότερος σκοπός όλης της εργασίας είναι η απόδειξη του θεωρήματος 3.4.1.3. Ξεκινούμε αναφέροντας χωρίς απόδειξη την ακόλουθη πρόταση (Απόδειξη της πρότασης μπορεί να βρεθεί στο [Deuring] και στο [Lang] §13.4.)

<u>3.4.1.1 ΠΡΟΤΑΣΗ</u> : Έστω O_1,O_2 τάξεις σε φανταστικά τετραγωνικά σώματα K_1,K_2 αντίστοιχα και a_1,a_2

proper κλασματικά ιδεώδη των O_1,O_2 αντίστοιχα. Έστω επίσης L ένα σώμα αριθμών που να περιέχει τα $j(a_1)$, $j(a_2)$ και q ένα πρώτο ιδεώδες του R_L . Θέτουμε με p τον μοναδικό πρώτο αριθμό που υπάρχει στο q.
Αν ισχύουν τα ακόλουθα :

1. **$j(a_1)\neq j(a_2)$.**
2. **"$K_1=K_2$" $\rightarrow$ "$p \nmid cond(O_1)$ και $p \nmid cond(O_2)$".**

Τότε ισχύει η παρακάτω συνεπαγωγή :
"$j(a_1)\equiv j(a_2)(mod q_L)$" $\rightarrow p\notin (spl(K_1)\cup spl(K_2))$.

<u>3.4.1.2 ΠΟΡΙΣΜΑ</u> : Έστω $D\in Z$ με $D<0$, $D\equiv 0,1(mod4)$ και $D\neq\square$. Έστω επίσης p ένας περιττός πρώτος

αριθμός και O μια τάξη τετραγωνικού φανταστικού σώματος αριθμών K με $d_O = D$. Ισχύουν τα ακόλουθα :

1. **Αν ο p διαιρεί τον σταθερό όρο του $H_O(x)$ και $Q(\sqrt{D})\neq Q(\sqrt{-3})$, τότε ισχύουν τα παρακάτω**
   a. $\left(\frac{D}{p}\right)_2 \neq 1$.
   b. **$p=3$ ή $p\equiv 2(mod3)$.**
2. **Αν ο p διαιρεί την διακρίνουσα του $H_O(x)$, τότε $\left(\frac{D}{p}\right)_2 \neq 1$.**

<u>ΑΠΟΔΕΙΞΗ</u>

Θα θέσουμε κατ' αρχήν $h:=h_O$ και θα θεωρήσουμε $\{a_1,a_{2,\ldots},a_h\}$ ένα πλήρες σύνολο αντιπροσώπων κλάσεων της $C(O)$. Η πρόταση 3.3.3.3 δίνει $H_O(x) = \prod_{1\le t\le h}(x - j(a_t))$. Ο σταθερός όρος του $H_O(x)$ είναι ο $c = (-1)^h \prod_{1\le t\le h} j(a_t)$. Θέτουμε $L:=Q(j(a_1),j(a_2),\ldots,j(a_h))$.

1. Έστω ότι $p|c$. Αν πάρουμε q ένα πρώτο ιδεώδες του L πάνω από το pZ , τότε : $p|c \rightarrow c\in q$. Συνεπώς θα υπάρχει t_o με $1\le t_o\le h$, ώστε $j(a_{t_o})\in q$. Επειδή $j(\omega)=0$ (βλ. το 1 της πρότασης 3.1.2.9) , θα έχουμε : $j(a_{t_o})\equiv j(\omega)(mod q)$ (Σ 3.4.1.2.1)

   Θέτουμε $K_1:=Q(\sqrt{D})$ και $K_2:=Q(\omega)$, ($\omega=e^{2\pi i/3}$). Επειδή $K_2 = Q(\sqrt{-3})$, θα έχουμε από την υπόθεση

ότι $K_1 \neq K_2$. Θα δείξουμε ότι : $j(a_{t_o}) \neq j(\omega)$ (Σ 3.4.1.2.2)

Πράγματι , $j(\omega)=0$ (βλ. το 1 της πρότασης 3.1.2.9) , οπότε αν $j(a_{t_o})=j(\omega)=0$, τότε $c=0$, οπότε το πολυώνυμο $H_O(x)$ θα διαιρείται με το x , πράγμα άτοπο αφού το $H_O(x)$ είναι εξ'ορισμού ανάγωγο.

Θέτουμε $O_1 := O$ και $O_2 := R_{K_1} = Z[\omega]$. Η πρόταση 3.4.1.1 δίνει ότι $p \notin (spl(Q(\omega) \cup spl(Q(\sqrt{D}))$.

Από τον νόμο ανάλυσης στα τετραγωνικά σώματα αριθμών $K_1=Q(\sqrt{D})$ και $K_2= Q(\sqrt{-3})$ (βλ. πρόταση

2.1.1.7) έχουμε τώρα : $\left(\frac{D}{p}\right)_2 \neq 1$ (συνέπεια του ότι $p \notin spl(K_1)$) και "p=3 ή $p \equiv 2(\text{mod}3)$" (συνέπεια

του ότι $p \notin spl(K_2)$).

2 Η διακρίνουσα του $H_O(x)$ είναι $d_{H_O} = \prod_{1 \leq i < j \leq h} (j(a_i) - j(a_j))^2$. Παρατηρούμε ότι $j(a_t) \in R_L$, $\forall t \in \{1,2,\ldots,h\}$

(βλ. πρόταση 3.3.2.2) , και συνεπώς επειδή από υπόθεση ισχύει $p \mid d_{H_O}$, θα πρέπει $d_{H_O} \in p \cdot R_L$.

Αναλύοντας το $p \cdot R_L$ σε πρώτα ιδεώδη του R_L , βλέπουμε ότι το d_{H_O} ανήκει σε κάθε πρώτο ιδεώδες του R_L πάνω από το p. Έστω λοιπόν q ένα πρώτο ιδεώδες του R_L πάνω από το p. Επειδή $d_{H_O} \in q$ θα έχουμε ότι υπάρχουν i_o, j_o , με $1 \leq i_o < j_o < h$, ώστε $(j(a_{i_o}) - j(a_{j_o})) \in q$. Συνεπώς $j(a_{i_o}) \equiv j(a_{j_o}) (\text{mod} q)$. Μάλιστα , επειδή $i_o \neq j_o$, θα έχουμε $j(a_{i_o}) \neq j(a_{j_o})$ (βλ. το 1 των παρατηρήεων 3.1.3.10. και την πρόταση 3.1.2.7). Διακρίνουμε τις περιπτώσεις :

<u>1η Περίπτωση</u> : $p \nmid D$.

Στην περίπτωση αυτή , θα ισχύει και $p \nmid con(O)$ (βλ. το 1a της πρότασης 2.2.1.10) , οπότε η πρόταση 3.4.1.1 (που εφαρμόζεται για $O_1=O_2=O$ και $K_1 = K_2 = K$) δίνει ότι

$p \notin spl(Q(\sqrt{D})$ και συνεπώς , από τον νόμο ανάλυσης σε τετραγωνικά σώματα αριθμών

θα ισχύει $\left(\frac{D}{p}\right)_2 \neq 1$ (βλ. πρόταση 2.1.1.7).

<u>2η Περίπτωση</u> : $p \mid D$.

Τότε , εξ' ορισμού $\left(\frac{D}{p}\right)_2 = 0 \neq 1$.

Σε κάθε περίπτωση λοιπόν έχουμε $\left(\frac{D}{p}\right)_2 \neq 1$ και το αποδεικτέο ισχύει.

<u>3.4.1.3 ΘΕΩΡΗΜΑ</u> : Άν n είναι φυσικός αριθμός , τότε υπάρχει μονικό ανάγωγο πολυώνυμο $f_n(x) \in Z[x]$ βαθμού ίσου με h(-4n) , ώστε για κάθε περιττό πρώτο αριθμό p να ισχύει η ακόλουθη ισοδυναμία :

" $\exists x,y \in Z$: $p= x^2+ny^2$ " $\leftrightarrow$ " $\left(\frac{-n}{p}\right)_2 = 1$ και η $f_n(x) \equiv 0(\text{mod}p)$ είναι επιλύσιμη στο Z"

Επιπλέον , υπάρχει αλγόριθμος υπολογισμού του $f_n(x)$.

ΑΠΟΔΕΙΞΗ

Θέτουμε $K:=Q(\sqrt{-n})$. Το σύνολο $O:=Z+\sqrt{-n}\,Z$ είναι μία τάξη του K (βλ. το IV της πρότασης 2.1.1.5

και την πρόταση 2.2.1.4). Ισχύει $d_O=-4n$ (βλ. ορισμό 2.2.1.9). Έχουμε $H_{-4n}(x) = H_O(x) = Irr(j(\sqrt{-n})|Q)(x)$.

Θέτουμε $f_n(x):= H_{-4n}(x)$ και $\alpha:=j(O)=j(\sqrt{-n})$. Από την πρόταση 3.3.2.2 έχουμε ότι το α είναι πραγματικός αλγεβρικός ακέραιος και από το θεώρημα 3.3.2.5 προκύπτει ότι το σώμα $L:=K(\alpha)$ είναι το ring class field της ταξης O. Το θεώρημα 2.4.2.5 επομένως , θα δώσει ότι για κάθε περιτό πρώτο αριθμό p που δέν διαιρεί την διακρίνουσα του f_n ισχύει η ακόλουθη ισοδυναμία :

$$\text{" } \exists x,y\in Z : \ p= x^2+ny^2 \text{ " } \leftrightarrow \text{ " } \left(\frac{-n}{p}\right)_2 = 1 \quad \text{και η } f_n(x)\equiv 0 (\text{mod} p) \text{ επιλύσιμη στο Z"}$$

Μένει να δειχτεί λοιπόν ότι η παραπάνω ισοδυναμία ισχύει και στην περίπτωση που το p διαιρεί την διακρίνουσα του f_n. Παρατηρούμε ότι για περιττούς πρώτους αριθμούς p που διαιρούν την διακρίνουσα

του f_n ισχύει $\left(\frac{D}{p}\right)_2 \neq 1$ (βλ. το 2 του πορίσματος 3.4.1.2) , οπότε επειδή $D=-4n$, θα ισχύει $\left(\frac{-n}{p}\right)_2 \neq 1$.

Θα δείξουμε ότι σε περιπτώσεις περιττών πρώτων αριθμών που διαιρούν την διακρίνουσα του f_n δεν ισχύει ούτε το αριστερό μέλος, ούτε το δεξιό μέλος της παραπάνω ισοδυναμίας και επομένως η ισοδυναμία θα είναι αληθής.

Πράγματι , αν p είναι περιττός πρώτος που δεν διαιρεί την διακρίνουσα του f_n , τότε

1. Για το αριστερό μέλος : Αν υπήρχαν $x,y\in Z$ με $p=x^2+ny^2$, θα ίσχυε : $x^2\equiv -ny^2 (\text{mod} p) \rightarrow 1 = \left(\frac{x^2}{p}\right)_2 =$

$$= \left(\frac{-ny^2}{p}\right)_2 = \left(\frac{-n}{p}\right)_2 \text{ , πράγμα άτοπο αφού προηγουμένως δείξαμε ότι για}$$

περιττούς πρώτους αριθμούς p που διαιρούν την διακρίνουσα του f_n ισχύει $\left(\frac{-n}{p}\right)_2 \neq 1$.

2. Για το δεξιό μέλος : Το δεξιό μέλος δεν ισχύει γιατί για περιττούς πρώτους αριθμούς p που διαιρούν

$$\text{την διακρίνουσα του } f_n \text{ ισχύει } \left(\frac{-n}{p}\right)_2 \neq 1.$$

Τέλος , το θεώρημα 3.3.3.6 μας δίνει ότι υπάρχει αλγόριθμος υπολογισμού του f_n.

3.4.1.4 ΣΧΟΛΙΑ : 1. Το θεώρημα 3.4.1.3 γενικεύει γνωστά αποτελέσματα. Π.χ. για την έκφραση πρώτων αριθμών από την μορφή x^2+27y^2 το ring class field της τάξης $O=Z[\sqrt{-27}]$ είναι το $K(\sqrt[3]{2})$, οπότε $H_O(x)=x^3-2$ (βλ. πρόταση 1.3.4.4).

2. Τα πολυώνυμα H_O είναι γενικά πολύ δύσκολο να υπολογιστούν λόγω των πολύ μεγάλων συντελεστών τους (π.χ. για τάξη O με διακρίνουσα -56 ισχύει : $H_O(x)=x^4 - (2^8\cdot 19\cdot 937\cdot 3559)x^3 + (2^{20}\cdot 3\cdot 21323)x + (2^8\cdot 11^2\cdot 17\cdot 41)^3$, όπου οι συντελεστές

έχουν αναλυθεί σε γινόμενο πρώτων) και συνεπώς το θεώρημα 3.4.1.3 παρά την

τεράστια θεωρητική αξία του , έχει μειωμένη υπολογιστική σημασία. Πληροφοριακά αναφέρουμε ότι είναι δυνατόν να χαρακτηριστούν τα ring class fields χρησιμοποιώντας την 3^{η} ρίζα της j - αναλλοίωτης καθώς και συναρτήσεις Weber , πράγμα που έχει ως συνέπεια πιο εύχρηστες υπολογιστικά παραλλαγές του θεωρήματος 3.4.1.3. Παραπέμπουμε τον ενδιαφερόμενο στο βιβλίο του Cox : [Cox].

ΣΥΜΒΟΛΙΣΜΟΙ

- Με N θα συμβολίζεται το σύνολο των φυσικών αριθμών : 1,2,3,4, …
- Με N_o θα συμβολίζεται το σύνολο $N \cup \{0\}$.
- Με Z θα συμβολίζεται το σύνολο των ακεραίων αριθμών.
- Με Q θα συμβολίζεται το σύνολο των ρητών αριθμών.
- Με R θα συμβολίζεται το σύνολο των πραγματικών αριθμών.
- Με C θα συμβολίζεται το σύνολο των μιγαδικών αριθμών.
- Με P θα συμβολίζεται το σύνολο των πρώτων ακεραίων αριθμών.
- Με P^* θα συμβολίζεται το σύνολο των περιττών πρώτων ακεραίων αριθμών.
- Για δακτύλιο R , θα συμβολίζεται με R^* ή με $E(R)$ το σύνολο των μονάδων (αντιστρέψιμα στοιχεία) του R.

(Προφανώς , αν ο R είναι σώμα τότε $R^*=R-\{0\}$.)

- Για δακτύλιο R και $u \in R$, θα συμβολίζεται με $Ass(u)$ το σύνολο των συνεταιρικών στοιχείων του u. (Των στοιχείων του R δηλαδή της μορφής $\varepsilon \cdot u$, όπου ε μονάδα του R.)
- Για ακέραια περιοχή R , θα συμβολίζεται με $quot(R)$ το σώμα πηλίκων του R.
- Για $m,n \in N$ και S σύνολο , θα συμβολίζεται με $M_{mxn}(S)$ το σύνολο των mxn πινάκων με στοιχεία από το S.
- Με I_n θα συμβολίζεται ο μοναδιαίος πίνακας nxn.
- Για τετραγωνικό πίνακα A θα συμβολίζεται με $det(A)$ ή με $|A|$ η ορίζουσα του A.
- Για G,G' ομάδες (δακτυλίους , σώματα , διανυσματικούς χώρους) θα συμβολίζεται με $Hom(G,G')$ το σύνολο
- των ομομορφισμών $G \to G'$.
- Για G ομάδα (δακτύλιο , σώμα , διανυσματικό χώρο) και H υποομάδα (υποδακτύλιο , υπόσωμα , υπόχωρο

της G θα συμβολίζεται με

  - $End_H(G)$ το σύνολο των ενδομορφισμών της G που αφήνουν τα στοιχεία της H αναλλοίωτα.
  - $Aut_H(G)$ το σύνολο των αυτομορφισμών της G που αφήνουν τα στοιχεία της H αναλλοίωτα.

- Για $n \in N$, θα συμβολίζεται με S_n η ομάδα μεταθέσεων του συνόλου $\{ 1,2,\ldots, n \}$. Επίσης με A_n θα συμβολίζεται

η υποομάδα της S_n των αρτίων μεταθέσεων.

- Για R δακτύλιο και M ένα R-module με $a,b \in M$, θα συμβολίζεται με $<a,b>_R$ το σύνολο των R-γραμμικών συνδιασμών των a και b. Δηλαδή $<a.b>_R = \{\kappa a+\lambda b \mid \kappa,\lambda \in R \}$.
- Για S δακτύλιο και R υποδακτύλιο του S με $x \in S$ θα συμβολίζεται με :

$R[x]$, ο δακτύλιος των πολυωνυμικών εκφράσεων του x με συντελεστές από το R.

$R(x)$, το σώμα πηλίκων του $R[x]$.

$R[[x]]$, ο δακτύλιος των τυπικών δυναμοσειρών του x με συντελεστές από το R.

$R((x))$, το σώμα πηλίκων του $R[[x]]$.

$R<x>$, ο δακτύλιος των τυπικών μερόμορφων δυναμοσειρών του x (σειρών Laurent) με συντελεστές από το R.

$R<<x>>$, το σώμα πηλίκων του $R<x>$.

- Ένας ακέραιος αριθμός με την ιδιότητα να μη διαιρείται από κανένα τετράγωνο ακεραίου αριθμού θα ονομάζεται "ελεύθερος τετραγώνου".

- Για ρητό αριθμό m ο συμβολισμός $m=\square$ θα σημαίνει ότι ο m είναι τετράγωνο ρητού αριθμού.
- Για ρητό αριθμό m ο συμβολισμός $m\neq\square$ θα σημαίνει ότι ο m δεν είναι τετράγωνο ρητού αριθμού.
- Με 0 θα συμβολίζεται το μηδενικό στοιχείο μιας ομάδας.(Πχ το 0 για συναρτήσεις είναι η μηδενική συνάρτηση , το 0 για ιδεώδη είναι ο μηδενικό ιδεώδες , κ.ο.κ.)
- Αν K σώμα και u ένα στοιχείο αλγεβρικό του K , τότε με Irr(u|K) θα συμβολίζεται το ελάχιστο πολυώνυμο του

u πάνω από το K. Ειδικά , αν K=Q τότε με Irr(u|Z) θα συμβολίζεται το ανάγωγο πολυώνυμο του Z[x] με μεγιστοβάθμιο συντελεστή θετικό , που προκύπτει από τον πολλαπλασιασμό του Irr(u|Q) με το ελάχιστο κοινό πολλαπλάσιο των παρανομαστών των συντελεστών του (οι συντελεστές του Irr(u|Q) θεωρούνται κλάσματα σε

ανάγωγη μορφή). Είναι εύκολο να δεί κανείς ότι το u είναι ρίζα του Irr(u|Z) και ότι οι συντελεστές του Irr(u|Z) έχουν μέγιστο κοινό διαιρέτη 1
- Για μιγαδικό αριθμό z , θα συμβολίζουμε με $\bar{z}$ τον μιγαδικό συζυγή του και με ||z|| ή |z| το μέτρο του , εκτός και αν ο $\bar{z}$ ή οι ||z|| , |z| έχουν οριστεί προηγουμένως ως κάτι διαφορετικό.

Με Rez θα συμβολίζεται το πραγματικό μέρος του z και με Imz , το φανταστικό μέρος του z.
Πολλές φορές θα χρησιμοποιηθεί και ο συμβολισμός z' για τον $\bar{z}$. Επίσης πολλές φορές στο κείμενο το γράμμα

"σ" θα συμβολίζει την μιγαδική συζυγία.
- Για n,m∈N και πίνακα nxm $A=[\alpha_{i,j}]_{i,j=1\ldots n}$, με στοιχεία από κάποιο σύνολο S , θα συμβολίζεται με A^T ο

ανάστροφος πίνακας του A , δηλαδή ο $[\alpha_{j,i}]_{i,j=1\ldots n}$. Επίσης για S=C , θα συμβολίζεται με $\bar{A}$ ο πίνακας $[\overline{\alpha_{i,j}}]_{i,j=1\ldots n}$.
- Για σώματα L και K , τα σύμβολα L/K , $\frac{L}{K}$ και $L\diagup K$ θα σημαίνουν ότι K⊆L.
- Για επέκταση σωμάτων L/K , θα συμβολίζεται με (L : K) ή με [L : K] ο βαθμός της επέκτασης και με G(L|K) η ομάδα Galois της επέκτασης.
- Για οποιοδήποτε σύνολο S , θα συμβολίζεται με #S ή με |S| ή με card(S) , ο πληθάριθμος του S.
- Κάθε υπόσωμα του C θα λέγεται μιγαδικό σώμα και κάθε υπόσωμα του R θα λέγεται πραγματικό σώμα

Φανταστικό σώμα θα λέγεται κάθε μιγαδικό σώμα που δεν είναι πραγματικό.
- Για m∈Z θα συμβολίζεται με Z_m ο δακτύλιος $\frac{Z}{mZ}$.
- Για n∈N και R δακτύλιο θα συμβολίζεται με sl(n,R) το σύνολο $\{ A\in M_{nxn}(R) \mid detA=\pm 1 \}$.
- Με **h** θα συμβολίζεται το άνω μιγαδικό επίπεδο : {z∈C| Im(z)>0}.
- Για α,β∈C και m∈Z, το σύμβολο α≡β(modm) θα σημαίνει ότι υπάρχει k∈Z με α=β+km.
- Για ομάδα (G,∗) με g∈G και κανονική υποομάδα H της G , θα συμβολίζεται με [g] (ή με $[g]_H$ για ακρίβεια) το coset g∗H της g στην G.
- Για $\alpha_1,\alpha_2,\ldots,\alpha_v\in Z$, θα συμβολίζεται με ΜΚΔ$(\alpha_1,\alpha_2,\ldots,\alpha_v)$ τον μέγιστο κοινό διαιρέτη των $\alpha_1,\alpha_2,\ldots,\alpha_v\in Z$ και με

ΕΚΠ$(\alpha_1,\alpha_2,\ldots,\alpha_v)$ το ελάχιστο κοινό τους πολλαπλάσιο. Όταν δεν υπάρχει κίνδυνος παρερμηνίας θα συμβολίζεται

με $(\alpha_1,\alpha_2,\ldots,\alpha_v)$ ο ΜΚΔ$(\alpha_1,\alpha_2,\ldots,\alpha_v)$ και με $[\alpha_1,\alpha_2,\ldots,\alpha_v]$ το ΕΚΠ$(\alpha_1,\alpha_2,\ldots,\alpha_v)$.
- Για z∈C-{0} , το $e^{2\pi i/z}$ θα συμβολίζεται με ζ_z. Επίσης το ω θα συμβολίζει το ζ_3 αν δεν έχει καθοριστεί προηγουμένως ως κάτι διαφορετικό.
- Για αλγεβρικό σώμα αριθμών K , το $P_o(K)$ θα συμβολίζει το σύνολο των πεπερασμένων πρώτων και το $P_\infty(K)$, θα συμβολίζει το σύνολο των απείρων πρώτων του K. Το P(K) θα συμβολίζει το σύνολο όλων των πρώτων του K.

(Δηλαδή $P(K)=P_o(K)\cup P_\infty(K)$).

- Για επέκταση αλγεβρικών σωμάτων αριθμών L/K , θα συμβολίζεται με $spl(L/K)$ ή $spl(\frac{L}{K})$ ή $spl(L/K)$ το σύνολο
των πεπερασμένων πρώτων του K που αναλύονται πλήρως στο L. Επίσης το $spl(K/Q)$ θα συμβολίζεται και $spl(K)$.
- Αν L/K είναι επέκταση αλγεβρικών σωμάτων αριθμών , τότε με $\tilde{spl}(L/K)$ ή με $\tilde{spl}(L/K)$ ή με $\tilde{spl}(\frac{L}{K})$, θα συμβολίζεται το σύνολο :
$$\{ p\in P_o(K) \mid \text{ο } p \text{ δεν διακλαδίζεται στο } L \text{ και υπάρχει } q\in P_o(L) \text{ πάνω από το } p, \text{ με } f\left(\frac{q}{p}\right)=1 \}.$$
Επίσης με $\tilde{spl}(L)$ θα συμβολίζεται το σύνολο $\tilde{spl}(L/Q)$.
- Αν S,T είναι δύο σύνολα , τότε ο συμβολισμός $S\overset{\bullet}{\subseteq}T$ θα σημαίνει ότι υπάρχει πεπερασμένο σύνολο E, ώστε
$S\subseteq T\cup E$. Επίσης , ο συμβολισμός $S\overset{\bullet}{=}T$ θα σημαίνει ότι $S\overset{\bullet}{\subseteq}T$ και $T\overset{\bullet}{\subseteq}S$. (Όπως φαίνεται από τους ορισμούς ,
ο συμβολισμός $S\overset{\bullet}{=}T$ σημαίνει ότι τα S,T διαφέρουν κατά πεπερασμένο πλήθος στοιχείων.)

- Αν R είναι δακτύλιος και S είναι υπερδακτύλιος του R τότε για $X\subseteq S$ θα συμβολίζεται με $R[X]$ ο δακτύλιος των πολυωνυμικών εκφράσεων των στοιχείων του X με συντελεστες από το R και με $R(X)$ το $quot(R[X])$.
- Αν R είναι δακτύλιος , και $f(x)$ είναι στοιχείο του δακτυλίου πολυωνύμων $R[x]$, τότε ο βαθμός του πολυωνύμου
$f(x)$ θα συμβολίζεται με $deg(f)$ ή $deg(f(x))$.
- Για σύνολα A,B,Γ με $A\subseteq B$ και συνάρτηση $f : A \to \Gamma$ θα συμβολίζεται με $f_{|B}$ ο περιορισμός της f στο σύνολο B.
- Για L/K Galois επέκταση αλγεβρικών σωμάτων αριθμών και q πρώτο μη διακλαδιζόμενο ιδεώδες του L θα
συμβολίζεται με $\left[\frac{L\mid K}{q}\right]$ το σύμβολο του Frobenius. (Δηλαδή το $\left[\frac{L\mid K}{q}\right]$ είναι το μοναδικό στοιχείο της $G(L|K)$
με την ιδιότητα $\left[\frac{L\mid K}{q}\right](x)\equiv x^{N(p)}(\mathrm{mod} q)$, $\forall x\in R_L$ όπου $p=K\cap R_L$). Επίσης στην περίπτωση που η L/K είναι
αβελιανή , με $\left[\frac{L\mid K}{p}\right]$ θα συμβολίζεται το σύμβολο του Artin για πρώτο p του K μη διακλαδιζόμενο στο L.

- Για επέκταση αλγεβρικών σωμάτων αριθμών L/K και p,q πρώτα ιδεώδη των K,L αντίστοιχα ώστε το q να είναι

πάνω από το p , θα συμβολίζονται με $f\left(\frac{q}{p}\right)$,$e\left(\frac{q}{p}\right)$ ο βαθμός αδρανείας και ο δείκτης διακλάδωσης του q πάνω

από το p αντίστοιχα. Επίσης με $r\left(\frac{q}{p}\right)$ θα συμβολίζεται το $\frac{[L : K]}{f\left(\frac{q}{p}\right) \cdot e\left(\frac{q}{p}\right)}$.

- Για τυχαία υποσύνολα S,T του C , ώστε το T να είναι ανοιχτό , το σύμβολο $H(T ; S)$ θα συμβολίζει το σύνολο των ολόμορφων συναρτήσεων $T \to S$. (Το $H(T ; S)$ είναι αντιμεταθετικός δακτύλιος χωρίς μηδενοδιαιρέτες).

ΒΙΒΛΙΟΓΡΑΦΙΑ

[Αντων] Αντωνιάδη Α. Γιάννη , *Αλγεβρική Θεωρία Αριθμών Ι ,* Σημειώσεις, Ηράκλειο 1988.

[Apost] T. M. Apostol , *Modular Functions and Dirichlet Series in Number Theory* , Springer-Verlag , New York 1976.

[Cox] David A. Cox , *Primes of the Form* x^2+ny^2 , John Wiley and Sons , New York 1989.

[Deuring] M. Deuring *Teilbarkeitseigenschaften der singulaeren Moduln der elliptischen Funktionen und die Discriminante der Klassengleichung* , Commentarii Math. Helv. 19(1946) , 74-82.

[Gauss] C. F. Gauss , *Disquisitiones Arithmeticae* , Leipzig 1810.

[Ir.Ro] K. Ireland and M. Rosen , *A Classical Introduction to Modern Number Theory* , Springer-Verlag , New York 1990.

[Janusz] G. Janusz , *Algebraic Number Fields ,* Academic Press , New York 1973.

[Lang] Serge Lang , *Elliptic Functions ,* 2nd edition , Springer-Verlag , New York 1978.