Παραγοντοποίηση Ιδεωδών και εφαρμογές σε τετραγωνικά σώματα

Γιαλούρης Γιάννης

Επιβλέπων: Γιάννης Σακελλαρίδης

Τομέας Μαθηματικών
Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών
Εθνικό Μετσοβιο Πολυτεχνείο

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγικές έννοιες

1.1 Δακτύλιοι

Ορισμός: Ορίζουμε δακτύλιο R, ένα σύνολο μαζί με δύο διμελείς πράξεις $(+,\cdot)$ ορισμένες στον R έτσι ώστε

1. το $< R, + >$ είναι αβελιανή ομάδα.
2. ο πολλαπλασιασμός είναι προσεταιριστικός.
3. $\forall a, b, c \epsilon R$, ισχύουν οι επιμεριστικοί νόμοι,
   (α) $a(b+c) = (ab) + (ac)$
   (β) $(a+b)c = (ac) + (bc)$

Για παράδειγμα, τα $< \mathbb{Z}, +, \cdot >, < \mathbb{Q}, +, \cdot >, < \mathbb{R}, +, \cdot >, < \mathbb{Z}/n, +, \cdot >$ είναι δακτύλιοι.

Θεώρημα: Για R δακτύλιο με ταυτοτικό στοιχείο πρόσθεσης το 0, και $a, b \epsilon R$.

1. $0a = a0 = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$.

Απόδειξη:

1. Το $a0 + a0 = a(0+0) = a0 = 0 + a0 \Rightarrow a0 = 0$.
   αντίστοιχα για το $0a = 0$.

2. Τα $-(ab), ab$ είναι προσθετικά αντίθετα, επομένως, $a(-b) + ab = a(-b+b) = a0 = 0$. Αντίστοιχα $(-a)b + ab = (-a+a)b = 0b = 0$

3. $(-a)(-b) = -(a(-b)) = -(-(ab))$, το οποίο είναι το αντίθετο του $-(ab)$, άρα το ab.

1.2 Ομομορφισμοί Δακτυλίων

Ορισμός: Για δύο δακτυλίους R,R', η απεικόνιση $f : R \to R'$ ονομάζεται ομομορφισμός αν ισχύουν οι εξής ιδιότητες:

1. $f(a+b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$

Ορισμός: Ένας $f : R \to R'$, όπου είναι ομομορφισμός , ένα προς ένα και επί, ονομάζεται ισομορφισμός.

1.3 Σώματα και ακέραιες περιοχές

Ορισμός:

1. Έχουμε αντιμεταθετικό δακτύλιο , όταν στον δακτύλιο μας η πράξη του πολλαπλασιασμού είναι αντιμεταθετική.
2. Όταν έχουμε πολλαπλασιαστικά ταυτοτικό στοιχείο ή αλλιώς μοναδιαίο στοιχείο 1 , τέτοιο ώστε $1x = x1 = x$ για κάθε $x \epsilon R$, είμαστε σε δακτύλιο με μοναδιαίο στοιχείο.

Θεώρημα: Το πολλαπλασιαστικό ταυτοτικό στοιχείο του R είναι μοναδικό.

Απόδειξη: Έστω $1, 1'$ μοναδιαία στοιχεία, τότε $(1)(1') = 1', (1)(1') = 1$. Αρα $1 = 1'$.

Ορισμός: Έστω R δακτύλιος με μοναδιαίο στοιχείο.

1. ένα στοιχείο $u \epsilon R$ λέγεται μονάδα αν έχει πολλαπλασιαστικό αντίστροφο στο R.
2. αν κάθε μη μηδενικό στοιχείο του δακτυλίου είναι μονάδα, τότε έχουμε δακτύλιο διαίρεσης.
3. Σώμα, ονομάζεται ένας αντιμεταθετικός δακτύλιος διαίρεσης.

Ορίζεται ο υποδακτύλιος, ως ένα υποσύνολο του δακτυλίου , που κληρονομεί τις πράξεις του δακτυλίου.
Αντίστοιχα ορίζεται και το υπόσωμα.

Ορισμός: Έστω $a, b \epsilon R$ μη μηδενικά στοιχεία , τέτοια ώστε $ab = 0$, τα a, b λέγονται διαιρέτες του μηδενός.
Όταν ένας δακτύλιος δεν έχει διαιρέτες του μηδενός ονομάζεται ακέραια περιοχή.

Θεώρημα:

1. Κάθε σώμα F ειναι ακέραια περιοχή.
2. Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Απόδειξη:

1. Έστω a, b στο F, με $a \neq 0$. Για $ab = 0$, $\frac{1}{a}(ab) = \frac{1}{a}0 = 0$.
   Έτσι έχουμε $0 = \frac{1}{a}(ab) = 1b = b$.

2. Έστω $0, 1, a_1, \ldots, a_n$, τα στοιχεία μιας πεπερασμένης ακέραιας περιοχής D. Θα δείξουμε οτι για κάθε $a \epsilon D$ με $a \neq 0$, υπάρχει κάποιο $b \epsilon D$ τέτοιο ώστε $ab = 1$, δηλαδή οτι το a είναι μονάδα. Παίρνουμε το

$$a1, aa_1, \ldots, aa_n.$$

   Λόγω του νόμου διαγραφής που ισχύει σε ακέραιες περιοχές, τα στοιχεία αυτά είναι διακεκριμένα. Μπορούμε να μετρήσουμε και να δούμε οτι τα στοιχεία $a1, aa_1, \ldots, aa_n$, είναι ίδια με τα $1, a_1, \ldots, a_n$ απλά με διαφορετική διάταξη, επομένως $a1 = 1$ ή $aa_i = 1$ για κάποιο i. Αποδείξαμε οτι υπάρχει πολλαπλασιαστικό αντίστροφο.

1.4 Σώματα πηλίκων

Θα θεωρήσουμε μια ακέραια περιοχή D και θα την επεκτείνουμε σε σώμα F.

Αρχικά θα φτιάξουμε το καρτεσιανό γινόμενο

$$D \times D \supset S = \{(a, b) | a, b \epsilon D, b \neq 0\}$$

το ζεύγος των στοιχείων (a, b) παριστάνει ένα πηλίκο.

Στην συνέχεια θα ορίσουμε την ισοδυναμία $\sim$ για δύο στοιχεία του S

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

1. $(a, b) \sim (a, b)$ γιατί $ab = ba$, λόγω αντιμεταθετικότητας του πολλαπλασιασμού (ανακλαστική)
2. $(a, b) \sim (c, d)$, τότε $ad = bc \Rightarrow cb = da \Rightarrow (c, d) \sim (a, b)$ (συμμετρική)
3. Για $(a, b) \sim (c, d)$ και $(c, d) \sim (r, s)$, έχουμε $ad = bc$ και $cs = dr$.
   Από εκεί κάνοντας πράξεις, $asd = sad = sbc = bcs = bdr = brd, d \neq 0$, και $asd = brd \Rightarrow as = br$, επομένως έχουμε $(a, b) \sim (r, s)$. (μεταβατική)

Μια σχέση ισοδυναμίας, επάγει κλάσεις ισοδυναμίας που θα τις συμβολίσουμε ως $[(a, b)]$ για $(a, b) \epsilon S$.

Θα ορίσουμε την πρόσθεση και τον πολλαπλασιασμό στο σύνολο των κλάσεων ισοδυναμίας F.

1. $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$
2. $[(a, b)][(c, d)] = [(ac, bd)]$

οι οποίες είναι καλά ορισμένες πράξεις στο F.

Προφανώς τα $(ad+bc, bd), (ac, bd)$ ανήκουν στο S. Για να δείξουμε οτι είναι καλά ορισμένες οι πράξεις, πρέπει να επιλέξουμε διαφορετικούς αντιπροσώπους και να δούμε οτι το αποτέλεσμα θα είναι το ίδιο.

Υποθέτουμε οτι $(a_1, b_1)\epsilon[(a, b)]$ και $(c_1, d_1))\epsilon[(c, d)]$.

Τότε $(a_1, b_1) \sim (a, b)$ και $(c_1, d_1) \sim (c, d)$, επομένως $a_1b = b_1a$ και $c_1d = d_1c$.

Πολλαπλασιάζοντας τις σχέσεις με d_1d την μια, και την δεύτερη με b_1b, και στη συνέχεια προσθετοντάς τες, έχουμε :

$$a_1bd_1d+c_1db_1b = b_1ad_1d+d_1cb_1b \Rightarrow (a_1d_1+b_1c_1)bd = b_1d_1(ad+bc) \Rightarrow (a_1d_1+b_1c_1, b_1d_1) \sim (ad+bc, bd)$$

.

Επομένως $(a_1d_1 + b_1c_1, b_1d_1)\epsilon[(ad + bc, bd)]$. Η πρόσθεση είναι καλά ορισμένη.

Για τον πολλαπλασιασμό, έχουμε τις ισότητες $a_1b = b_1a$ και $c_1d = d_1c$, τις πολλαπλασιάζουμε και έχουμε

$$a_1bc_1d = b_1ad_1c \Rightarrow a_1c_1bd = b_1d_1ac \Rightarrow (a_1c_1, b_1d_1) \sim (ac, bd).$$

Επομένως, $(a_1c_1, b_1d_1)\epsilon[(ac, bd)]$

Μας μένει να δείξουμε οτι το F είναι σώμα.

1. Η $< F, + >$ είναι αβελιανή ομάδα.
   (α) Η πρόσθεση είναι αβελιανή
   $[(a, b)] + [(c, d)] = [(ad+bc, bd)]$ $[(c, d)] + [(a, b)] = [(cb_da, db)]$ Όμως ισχύει $(ad+bc, bd) \sim (cb + da, db)$ το οποίο αποδεικνύεται έυκολα με πράξεις
   (β) Η πρόσθεση είναι προσεταιριστική
   (ς) Το $[(0, 1)]$ είναι το ταυτοτικό στοιχείο της πρόσθεσης στο F
   (δ) Το $[(-a, b)]$ είναι το προσθετικό αντίθετο του $[(a, b)]$ στο F
2. Ο πολλαπλασιασμός είναι προσεταιριστικός στο F
3. Ο πολλαπλασιασμός είναι επίσης αντιμεταθετικός στο F
4. Ισχύουν οι επιμεριστικοί νόμοι
5. το $[(1, 1)]$ είναι το ουδέτερο πολλαπλασιαστικό στοιχείο
6. Εαν το $[(a, b)]\epsilon F$ δεν είναι το ταυτοτικό στοιχείο της πρόσθεσης, τότε το $[(b, a)]$ είναι το πολλαπλασιαστικό αντίστροφο του.

Το D περιέχεται στο F, μπορούμε να το δούμε ορίζοντας μια απεικόνιση $i : D \to F$, με $i(a) = [(a, 1)]$, και να δείξουμε οτι είναι ισομορφισμός της D σε μια υποπεριοχή της F.

1.5 Δακτύλιος Πολυωνύμων

Ορισμός: Έστω R ένας δακτύλιος. Ορίζουμε ως πολυώνυμο $f(x)$ με συντελεστές στο R ένα άθροισμα

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots,$$

με $a_i \epsilon R$ και $a_i = 0$ εκτός από πεπερασμένο πλήθος i.
Ορίζουμε τα a_i ως συντελεστές του $f(x)$, και η μεγαλύτερη τιμή του i, για την οποία $a_i > 0$, ορίζεται ως βαθμός του $f(x)$.

Ορισμός: Το σύνολο $R[x]$, είναι τα πολυώνυμα μια απροσδιόριστης x με συντελεστές από τον δακτύλιο R.

Το $R[x]$ είναι δακτύλιος με πράξη την πρόσθεση και τον πολλαπλασιασμό πολυωνύμων.

1. εαν ο R είναι αντιμεταθετικός, τότε επαγωγικά είναι και ο $R[x]$.

2. εαν ο R έχει μοναδιαίο στοιχείο, τότε και ο $R[x]$ είναι δακτύλιος με μοναδιαίο στοιχείο.

Ανάλογα μπορούμε να ορίζουμε και τους δακτυλίους $R[x_1, \ldots, x_n]$

Ορισμός: Έστω F υπόσωμα του σώματος E, και έστω $a \epsilon E$,και x μια απροσδιόριστη.
Ορίζουμε τον ομομορφισμό εκτίμησης $\phi_a : F[x] \to E$, με

$$\phi_a(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1 a + \ldots + a_n a^n$$

για κάθε $(a_0 + a_1 x + \ldots + a_n x^n) \epsilon F[x]$
Ορισμός: Έστω F υπόσωμα, σώματος Ε, και έστω a ένα στοιχείο του Ε.
Για $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ στο $F[x]$ και $\phi_a : F[x] \to E$ ο ομομορφισμός εκτίμησης.

$$\phi_a(f(x)) = a_0 + a_1 a + \ldots + a_n a^n$$

Εαν $f(a) = 0$ τότε το a λέγεται ρίζα του $f(x)$.

Ορισμός: Ένα μη σταθερό πολυώνυμο $f(x) \epsilon F[x]$, ονομάζεται ανάγωγο πάνω από το F, εαν δεν μπρούμε να το γράψουμε ως γινόμενο δύο πολυωνύμων $g(x), h(x)$ στον $F[x]$ μικρότερου βαθμού του $f(x)$.

1.6 Δακτύλιοι Πηλίκα

Θεώρημα: Έστω φ ομομορφισμός δακτυλίου R στο R'.

1. για 0 προσθετικό ουδέτερο , το φ(0)=0$'$, όπου 0$'$ είναι το προσθετικό ουδέτερο του R'

2. εαν $a \epsilon R$, τότε φ(-a)=-φ(a)

3. για S υποδακτύλιο του R, το $\varphi(S)$ είναι υποδακτύλιος του R' , και ανάποδα για S' υποδακτύλιος του R', το $\varphi^{-1}(S')$ είναι υποδακτύλιος του R.

4. εαν το 1 είναι το μοναδιαίο στοιχείο του R , το $\varphi(1)$ είναι μοναδιαίο στοιχείο του $\varphi(R)$.

Αποδείξεις:

1. το πρώτο εξασφαλίζεται από τον ομομορφισμό ομάδων

2. επίσης εξασφαλίζεται από τον ομομορφισμό ομάδων

3. είναι γνωστό οτι διατηρείται η έννοια της υποομάδας, θέλουμε να δούμε τι γίνεται με τον πολλαπλασιασμό, $\phi(s_1)\phi(s_2) = \phi(s_1 s_2)$ και $\phi(s_1 s_2)\epsilon\phi(S)$, οπότε το $\phi(S)$ είναι με τον πολλαπλασιασμό, και ο $\phi(S)$ είναι υποδακτύλιος του R'. Αντίστοιχα και το ανάποδο.

4. $\phi(r) = \phi(1r) = \phi(r1) = \phi(r)\phi(1) = \phi(1)\phi(r)$. Επομένως το $\phi(1)$ είναι πολλαπλασιαστικό ουδέτερο του $\phi(R)$.

Ορισμός: Έστω οτι η απεικόνιση $\phi : R \to R'$ είναι ομομορφισμός δακτυλίων. Ο υποδακτύλιος $\phi^{-1}(\{0'\})$ ονομάζεται πυρήνας του φ, και συμβολίζεται με $ker(\phi)$.

Ενας ομομορφισμός δακτυλίων είναι ένα προς ένα απεικόνιση αν και μόνο αν $ker(\phi) = \{0\}$.

Θεώρημα: Για $\phi : R \to R'$ ομομορφισμό δακτυλίων με πυρήνα H. Τότε, τα προσθετικά σύμπλοκα του H σχηματίζουν ένα δακτύλιο R/H, του οποίου οι διμελείς πράξεις ορίζονται μέσω αντιπροσώπων, δηλαδή

$$(a + H)(b + H) = (a + b) + H$$

και

$$(a + H)(b + H) = (ab) + H$$

.

Η απεικόνιση μ:$R/H \to \phi(R)$, με $\mu(a + H)$=$\varphi(a)$ είναι ισμορφισμός.

Απόδειξη: Ξέρουμε οτι ισχύει για την πρόσθεση απο την θεωρία ομάδων. Θέλουμε να δούμε για τον πολλαπλασιασμό.
Θα δείξουμε οτι ο πολλαπλασιασμός είναι καλά ορισμένος.
Έστω $h_1, h_2 \epsilon H$ και αντιπρόσωποι $a + h_1$ για το $a + H$ και $b + h_2$ για το $b + H$.

$$c = (a + h_1)(b + h_2) = ab + ah_2 + h_1 b + h_1 h_2$$

πρέπει το c να ανήκει στο $ab+H$. Το $ab+H = \phi^{-1}\{\phi(ab)\}$, άρα θέλουμε να δείξουμε οτι $\phi(c) = \phi(ab)$.

$$\phi(c) = \phi(ab + ah_2 + h_1 b + h_1 h_2) = \phi(ab) + \phi(ah_2) + \phi(h_1 b) + \phi(h_1 h_2) =$$
$$\phi(ab) + \phi(a)0' + 0'\phi(b) + 0'0' = \phi(ab) + 0' + 0' + 0' = \phi(ab)$$

Επομένως ο πολλαπλασιασμός είναι καλά ορισμένος.

Η προσεταιριστική ιδιότητα του πολλαπλασιασμού, και οι επιμεριστικοί νόμοι ισχύουν γιατι έπονται από τους αντιπροσώπους των συμπλόκων.

Επίσης για τον ισομορφισμο, μ$((a+H)(b+H))$=μ$(ab+H)$=$\phi(ab)$=$\phi(a)\phi(b)$=μ$(a+H)$μ$(b+H)$. τα υπόλοιπα επάγονται από την θεωρία ομάδων.

Ορισμός: Έστω υποδακτύλιος I ενός δακτυλίου R, και έστω πως ισχύει το εξής:

$$aI \subset I, Ib \subset I, \forall a, b \epsilon R$$

. τότε ο υποδακτύλιος I, ονομάζεται ιδεώδες του R.

Πρόταση: Για N ιδεώδες ενός δακτυλίου R, τα προσθετικά σύμπλοκα του N σχηματίζουν έναν δακτύλιο R/N με τις εξής πράξεις:

$$(a+N)+(b+N)=(a+b)+N$$

$$(a+N)(b+N)=(ab)+N$$

.

Ορισμός: O δακτύλιος R/N ονομάζεται δακτύλιος πηλίκο του R ως προς N.

Θεώρημα: Έστω ιδεώδες N, δακτυλίου R. Η απεικόνιση γ:$R \rightarrow R$/N, με γ(x)=x+N, είναι ομομορφισμός δακτυλίων με πυρήνα N.

Απόδειξη: Το θεώρημα είναι ανάλογο από τη θεωρία ομάδων, και επομένως για τον πολλαπλασιασμό γ(xy)=(xy)+N=$(x$+N$)(y$+N$)$=γ(x)γ(y)

Θεμελιώδες θεώρημα ομομορφισμών: Έστω φ: $R \rightarrow R'$ ομομορφισμός δακτυλίων με πυρήνα N. Το φ(R) είναι δακτύλιος , και η απεικόνιση μ: $R/N \rightarrow$φ(R) ,με μ$(x+N)$ =φ(x), είναι ισομορφισμός.
Αν γ: $R \rightarrow R/N$ είναι ομομορφισμός που ορίζεται ως γ$(x)=x+N$, τότε για κάθε $x \epsilon R$, έχουμε φ(x) =μγ(x).

1.7 Ιδεώδη Δακτυλίων

Θεώρημα: Εαν R είναι δακτύλιος με μοναδιαίο στοιχείο, και N ένα ιδεώδες του R που περιέχει αντιστρέψιμο στοιχείο, τότε $N=R$.

Απόδειξη: Έστω u μονάδα στο N, τότε εξόρισμού u^{-1}N$\subset$ N. Επομένως 1ϵ N, και για κάθε στοιχείο του R , έστω r , $r1 \epsilon N \Rightarrow r \epsilon N$.

Ορισμός:

1. Λέμε ένα ιδεώδες M μέγιστο, με M$\neq R$ αν δεν περιέχεται σε κανένα γνήσιο ιδεώδες του R.

2. Λέμε ένα ιδεώδες N πρώτο, με N$\neq R$ αν για $ab\epsilon N \Rightarrow a\epsilon N$ ή $b\epsilon N$, για κάθε $a, b\epsilon R$.

Θεώρημα: Έστω R ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο,

1. το M είναι μέγιστο ιδεώδες του R, αν και μόνο αν το $R/$M είναι σώμα.
2. το N είναι πρώτο ιδεώδες του R, αν και μόνο αν το $R/$N είναι ακέραια περιοχή.

Απόδειξη:

1. Έστω M μέγιστο ιδεώδες του R.
   Εαν ο R είναι αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο , τότε και ο $R/$M είναι επίσης.
   Έστω $(a+M)\epsilon R/M$, με $a \not\epsilon M$ για να μην ειναι το $a+M$ προσθετικό ουδέτερο.
   Θα δείξουμε οτι το $a+M$ έχει πολλαπλασιαστικό αντίστροφο στον R/M. Θα πάρουμε

   $$N = \{ra + m | r\epsilon R, m\epsilon M\}.$$

   Το N είναι ιδεώδες:

   (α) Το $< N, + >$ ειναι ομάδα. $(r_1a + m_1) + (r_2a + m_2) = (r_1 + r_2)a + (m_1 + m_2)\epsilon N$ και τα $0 = 0a + 0$ και $-(ra + m) = (-r)a + (-m)$ επίσης ανήκουν στο N.

   (β) Ιδιότητα των ιδεωδών: $r_1(ra+m) = (r_1r)a+r_1m$, έχουμε οτι $r_1(ra+m)\epsilon N$ για $r_1\epsilon R$, και λόγω αντιμεταθετικότητας $(ra + m)r_1\epsilon N$.

   Το $a\epsilon N$ γιατι $a = 1a + 0$, και επειδή $m = 0a + m$ έχουμε οτι $M \subset N$. Άρα το $N = R$.
   $1\epsilon N$, επομένως 1=$ba + m$ για $b\epsilon R$ και $m\epsilon M$. Επομένως,

   $$1 + M = ba + M = (b + M)(a + M)$$

   . Δηλαδή το $b + M$ είναι το πολλαπλασιαστικό αντίστροφο του $a + M$.
   Αντίστροφα, έστω πως $R/$M είναι σώμα.
   Εαν N είναι ιδεώδες του R τέτοιο ώστε $M \subset N \subset R$ και γ ο κανονικός ομομορφισμός του R επί του $R/$M, , τότε το $\gamma(N)$ είναι ιδεώδες του $R/$M και $\{(0 + M)\} \subset \gamma(N) \subset R/M$. Άτοπο.

2. Έστω N πρώτο ιδεώδες. Αν $0 = (a + N)(b + N) = ab + N$, τότε $ab\epsilon N$. Επομένως $a\epsilon N$ ή $b\epsilon N$, δηλαδή $a + N = 0$ ή $b + N = 0$. Το αντίστροφο είναι ανάλογο.

Πρόταση: Κάθε μέγιστο ιδεώδες σε αντιμεταθετικό δακτύλιο R με μοναδιαίο στοιχείο, είναι πρώτο ιδεώδες.

Απόδειξη: Εαν το M είναι μέγιστο στον R, το R/M είναι σώμα, επομένως ακέραια περιοχή, και από το προηγούμενο θεώρημα, το M είναι πρώτο ιδεώδες.

Πρόταση: Ενας αντιμεταθετικός δακτύλιος με μοναδιαιο στοιχείο είναι σώμα, αν και μόνο δεν περιέχει γνήσια μη τετριμμένα ιδεώδη.

Απόδειξη: Εαν ο δακτύλιος είναι σώμα, κάθε στοιχείο είναι μονάδα, επάγεται από το προηγούμενο θεώρημα.
Έστω αντιμεταθετικός δακτύλιος R με μοναδιαίο στοιχείο, χωρίς γνήσια μη τετριμμένα ιδεώδη, τότε το $\{0\}$ είναι μέγιστο ιδεώδες και ο $R/\{0\}$ είναι ισόμορφος με τον R και σώμα.

1.8 Ιδεώδη στον $F[x]$

Ορισμός: Εαν έχουμε R αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο $a\epsilon R$, το ιδεώδες $\{ra|r\epsilon R\}$ που παράγεται από το a, λέγεται κύριο. Αυτό το ιδεώδες συμβολίζεται ως N=(a).

Θεώρημα: Έστω F σώμα, κάθε ιδεώδες του $F[x]$ είναι κύριο.

Απόδειξη: Έστω N ιδεώδες του $F[x]$.
Αν N=$\{0\}$, το N=$<0>$.
Έστω N$\neq \{0\}$, και $g(x)\epsilon N$ διάφορο του μηδενός, με τον ελάχιστο δυνατό βαθμό.
Εαν ο βαθμός του $g(x)$ είναι 0, τότε υπάρχει αντίστροφο, αφού $g(x)\epsilon F$, και σε αυτή την περίπτωση, $N = F[x] =< 1 >$.
Έστω ο βαθμός του $g(x)$ μεγαλύτερος από 0, και έστω $f(x)\epsilon N$. Τότε $f(x) = g(x)q(x) + r(x)$ με τον βαθμό του $r(x)$ μικρότερο από το βαθμό του $g(x)$.Τότε $f(x) - g(x)q(x) = r(x)\epsilon N$, επομένως πρέπει $r(x) = 0$. Άρα $f(x) = g(x)q(x)$, και $N =< g(x) >$.

Θεώρημα: Ένα ιδεώδες $< p(x) >$ στον $F[x]$ είναι μέγιστο αν και μόνο αν το $p(x)$ είναι ανάγωγο πάνω από το F.

Απόδειξη: Έστω $< p(x) >\neq 0$ μέγιστο ιδεώδες του $F[x]$. Το $< p(x) >\neq F$, επομένως $p(x) \not\epsilon F$.
Θεωρούμε μια ανάλυση του p, $p(x) = f(x)g(x)$. Εφόσον το $< p(x) >$ είναι μέγιστο ιδεώδες, είναι και πρώτο , άρα $f(x)g(x)\epsilon < p(x) >\Rightarrow f(x)\epsilon < p(x) >$ ή $g(x)\epsilon < p(x) >$. Αυτό σημαίνει οτι οι βαθμοί των $f(x), g(x)$ είναι μεγαλύτεροι από του $p(x)$. Άτοπο.
Αντίστροφα, θεωρούμε το $p(x)$ ανάγωγο πάνω από το F. Εαν το $< p(x) >$ δεν είναι μέγιστο ιδεώδες, υπάρχει N ιδεώδες, τέτοιο ώστε $< p(x) >\subset N \subset F[x]$. Αφού το F είναι σώμα το N είναι κύριο ιδεώδες, έστω $N =< g(x) >$. Όμως το $p(x)$ ανήκει στο N, επομένως $p(x) = g(x)q(x)$ για κάποιο $q(x)\epsilon F[x]$. Αφού το $p(x)$ είναι ανάγωγο, κάποιο $g(x)$ ή $f(x)$ θα έχει βαθμό 0.
Έστω πως το $g(x)$ έχει βαθμό 0, τότε έχει αντίστροφο και το $< g(x) >= N = F[x]$. Έστω πως το $q(x)$ είναι βαθμού 0, τότε $q(x) = c$, και το $g(x) = (1/c)p(x)$ ανήκει στο $< p(x) >$, άρα $N =< p(x) >$. Επομένως δεν γίνεται $< p(x) >\subset N \subset F[x]$.

1.9 Περιοχές μονοσήμαντης ανάλυσης, και κύριων ιδεωδών

Ορισμός: Έστω D ακέραια περιοχή και $a, b\epsilon D$. Αν υπάρχει $c\epsilon D$, τέτοιο ώστε $b = ac$, λέμε οτι το a είναι παράγοντας του b ,και $a|b$.

Ορισμός: Έστω μη μηδενικό στοιχείο p, που δεν είναι μονάδα της ακέραιας περιοχής D, λέγεται ανάγωγο στοιχείο αν για κάθε ανάλυση $p = ab$, ένας από τους παράγοντες του p είναι μονάδα.

Ορισμός: Δύο στοιχεία $a, b\epsilon D$, λέγονται ισοδύναμα αν $a = bu$, όπου το u είναι μονάδα της D.

Ορισμός (Περιοχή Μονοσήμαντης Ανάλυσης): Μια ακέραια περιοχή D είναι περιοχή μονοσήμαντης ανάλυσης (ΠΜΑ), εαν ικανοποιούνται τα εξής:

1. Κάθε στοιχείο της D διάφορο του μηδέν και της μονάδας (αντιστρέψιμο), αναλύεται σε γινόμενο πεπερασμένοου πλήθους ανάγωγων στοιχείων.
2. Για δύο αναλύσεις ενός στοιχείου του D σε γινόμενο ανάγωγων στοιχείων , $p_1, \ldots, p_r$ και $q_1, \ldots, q_s$, τότε $r = s$ και μπορούμε να αριθμήσουμε ξανά το q_i έτσι ώστε να είναι ισοδύναμα με τα p_i.

Για παράδειγμα ο $\mathbb{Z}$ ειναι ΠΜΑ, έχουμε

$$24 = 2 \cdot 2 \cdot 3 \cdot 2 = (-2) \cdot (-3) \cdot 2 \cdot 2$$

όμως τα 2,-2 είναι ισοδύναμα , αφού αν πολλαπλασιασουμε με (-1) είναι ίσα.

Ορισμός (Περιοχή Κύριων Ιδεωδών): Μια ακέραια περιοχή D ονομάζεται περιοχή κύριων ιδεωδών, εαν κάθε ιδεώδες της είναι κύριο.

Θεώρημα: Έστω D μια ΠΚΙ, τότε για $N_1 \subseteq N_2 \subseteq \ldots$ μονότονη αύξουσα αλυσίδα ιδεωδών N_i, θα υπάρχει, θετικός ακέραιος r τέτοιος ώστε $N_r = N_s$, για κάθε $s \geq r$.

Απόδειξη: Έστω $N_1 \subseteq N_2 \subseteq \ldots$ μονότονη αύξουσα αλυσίδα ιδεωδών N_i στην ακέραια περιοχή D.
Θέτουμε $N = \cup_i N_i$.
Προφανώς ισχύει $N \subseteq D$. Το N είναι ιδεώδες της D, επομένως είναι της μορφής $N =< c >$ για $c\epsilon D$.
Το c όμως ανήκει σε ένα N_r, για $r\epsilon\mathbb{Z}_{>0}$.
Εαν $s > r$, τότε

$$< c >\subseteq N_r \subseteq N_s \subseteq N =< c >$$

.
Άρα $N_r = N_s$.

Αργότερα θα ονομάσουμε τους δακτύλιους με αυτη την ιδιότητα, δακτύλιους της $Noether$.

Θεώρημα: Έστω D ΠΚΙ, τότε η D είναι ΠΜΑ.

Απόδειξη: Έστω $a\epsilon D$, και το a δεν είναι ούτε 0 ούτε μονάδα.
Θα δείξουμε οτι το a έχει τουλάχιστον έναν ανάγωγο παράγοντα.
Έστω πως $a = a_1 b_1$, θεωρούμε πως το a δεν είναι ανάγωγο, επομένως κανένα από τα a_1, b_1 δεν είναι μονάδα.
Έχουμε $< a >\subset< a_1 >$.
Εαν είχαμε $< a >=< a_1 >$, τότε τα a και a_1 θα ήταν ισοδύναμα και το b_1 θα ήταν μονάδα .

$< a > \subset < a_1 > \subset < a_2 > \subset \ldots$. Αυτή η αλυσίδα πρέπει να τερματίζει σε κάποιο $< a_r >$, το a_r πρέπει να είναι ανάγωγο.
Επομένως έχουμε αποδείξει οτι για a που δεν είναι ούτε 0 ούτε μονάδα του D, το a είναι ή ανάγωγο ή $a = p_1 c_1$, όπου p_2 ανάγωγο και c_2 όχι μονάδα.
Έτσι παίρνουμε την εξής αλυσίδα

$$< a > \subset < c_1 > \subset < c_2 > \subset \ldots,$$

αυτή η αλυσίδα πρέπει κάποτε να τερματίζει για κάποιο $c_r = q_r$, επομένως $a = p_1 p_2 \ldots p_r q_r$.
Μας μένει να αποδείξουμε οτι η ανάλυση είναι μονοσήμαντη.

Θεώρημα: Ένα ιδεώδες $< p >$ μιας ΠΚΙ είναι μέγιστο αν και μόνο αν το p είναι ανάγωγο.

Απόδειξη: Έστω $< p >$ ένα μέγιστο ιδεώδες στο D, που είναι ΠΚΙ.
Υποθέτουμε οτι $p = ab$, τοτε $< p > \subseteq < a >$.
Έστω πως $< p > = < a >$, τότε τα a και p είναι ισοδύναμα, δηλαδή το b είναι μονάδα.
Αν $< p > \neq < a >$, τότε $< a > = 1 = D$, αφού το p είναι μέγιστο. Όμως τότε τα a και 1 είναι ισοδύναμα, ή το a είναι μονάδα. Άρα το p είναι ανάγωγο στοιχείο της D.
Αντιστρόφως, έστω πως το p είναι ανάγωγο της D. Τότε αν $< p > \subseteq < a >$, έχουμε $p = ab$. Εαν το a είναι μονάδα, τότε $< a > = < 1 > = D$
Εαν το a δεν είναι μονάδα, τότε το b πρέπει να είναι μονάδα, δηλαδή υπάρχει $u \epsilon D$ τέτοιο ώστε $bu = 1$. Τότε $pu = abu = a$, άρα $< a > \subseteq < p >$, και έπεται οτι $< a > = < p >$. Δηλαδή, αν $< p > \subseteq < a >$ έχουμε πως $< a > = D$ ή $< a > = < p >$, και $< p > \neq D$ αλλιώς το p θα ήταν μονάδα. Επομένως το $< p >$ είναι μέγιστο ιδεώδες.

Πρόταση: Σε μια ΠΚΙ, αν κάποιο ανάγωγο στοιχείο p διαιρεί το ab, τότε η p/a ή p/b.

Απόδειξη: Έστω D μια ΠΚΙ, αν p είναι κάποιο ανάγωγο στοιχείο της D έχουμε p/ab. Τότε $(ab) \epsilon < p >$. Αφού κάθε μέγιστο ιδεώδες της D είναι πρώτο ιδεώδες, έχουμε οτι $a \epsilon < p >$ ή $b \epsilon < p >$, άρα p/a ή p/b.

Μπορούμε επαγωγικά να πούμε, οτι για ανάγωγο στοιχείο που διαιρεί το $a_1 a_2 \ldots a_n$ με $a_i \epsilon D$, το p/a_i για τουλάχιστον ένα i.

Ορισμός: Ένα μη μηδενικό και όχι αντιστρέψιμο στοιχείο p, μιας ακέραιας περιοχής D, για τον οποίο ισχύει $p|ab \Rightarrow p|a$ ή $p|b$, λέγεται πρώτος.

Γυρνάμε πίσω στην απόδειξη του θεωρήματος οτι κάθε ΠΚΙ είναι ΠΜΑ, που είχαμε αφήσει τη μοναδικότητα.
Για $a \epsilon D$, αποδείξαμε οτι υπάρχει ανάλυση σε ανάγωγα στοιχεία,

$$a = p_1 p_2 \ldots p_r$$

Έστω πως

$$a = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$$

Τότε $p|(q_1 q_2 \ldots q_s)$ δηλαδή $p_1 | q_{j_1}$ για κάποιο j_1. Χωρις βλάβη της γενικότητας υποθέτουμε πως $j_1 = 1$,

επομένως $p_1|q_1$.Άρα έχουμε $q_1 = p_1u_1$, και εφόσον το p_1 είναι ανάγωγο το u_1 είναι μονάδα, επομένως τα p_1, q_1 είναι ισοδύναμα. Από νόμο διαγραφής στην D, $p_2 \dots p_r = u_1q_2 \dots q_s$.
Συνεχίζοντας την ίδια διαδικασία

$$1 = u_1u_2 \dots u_rq_{r+1} \dots q_s$$

Εφόσον τα q_j είναι ανάγωγα, έχουμε $r = s$.

Πρόταση: Η ακέραια περιοχή $\mathbb{Z}$ είναι ΠΜΑ.

Απόδειξη: Είναι ΠΚΙ.

Επίσης όπως δείξαμε και στην προηγούμενη παράγραφο, για F σώμα, η $F[x]$ είναι επίσης ΠΚΙ.

1.10 Επεκτάσεις σωμάτων

Ορισμός: Ένα σώμα E λέγεται επέκταση, ενός σώματος F, αν $F \leq E$.

Θεώρημα: Έστω F σώμα και $f(x)$ ένα μη σταθερό πολυώνυμο στον $F[x]$. Τότε υπάρχει μια επέκταση σώματος E του F για κάποιο $a \epsilon E$, τέτοιο ώστε $f(a) = 0$.

Απόδειξη: Το $f(x)$ μπορεί να αναλυθεί στον $F[x]$ σε γινόμενο πολυωνύμων, που είναι ανάγωγα πάνω από το F. Έστω $p(x)$ ένα ανάγωγο πολυώνυμο σε μια ανάλυση του f.
Το $< p(x) >$ είναι μέγιστο ιδεώδες στον $F[x]$, επομένως το $F[x]/ < p(x) >$ είναι σώμα.

Θέλουμε να φτιάξουμε μια απεικόνιση ψ:$F \to F[x]/ < p(x) >$ με $\psi(a)$=a+$< p(x) >$. για κάθε $a \epsilon F$.
Αυτή η απεικόνιση είναι 1-1: για $\psi(a)$=$\psi(b) \Rightarrow (a-b) \epsilon < p(x) >$, επομένως το $a - b$ είναι πολλαπλάσιο του πολυωνύμου $p(x)$, το οποίο έχει βαθμό ≥ 1. Το $a - b \epsilon F$ επομένως $a - b = 0 \Rightarrow a = b$.

Μπορούμε να δούμε το E ως το $F[x]/ < p(x) >$ και να ταυτίσουμε το F με το $\{a+ < p(x) > |a \epsilon F\}$.

Τέλος θέλουμε να δείξουμε οτι το E περιέχει μια ρίζα του $p(x)$.
Θέτουμε $a' = x+ < p(x) >$, θεωρούμε τον ομομορφισμό εκτίμησης $\phi_{a'} : F[x] \to E$. Εαν $p(x) = a_0 + a_1x + \ldots + a_nx^n$ με $a_i \epsilon F$, τότε έχουμε

$$\phi_{a'}(p(x)) = a_0 + a_1(x+ < p(x) >) + \ldots + a_n(x+ < p(x) >)^n$$

στο E, επομένως

$$p(a') = (a_0 + a_1x + \ldots + a_nx^n)+ < p(x) >= p(x)+ < p(x) >=< p(x) >= 0$$

. Έχουμε ένα στοιχείο a' στο E με $p(a') = 0$ και $f(a') = 0$.

Ορισμός: Έστω σώμα F και επέκτασή του E. Για $a \epsilon E$, το a λέγεται αλγεβρικό πάνω από το F αν $f(a) = 0$ για κάποιο μη μηδενικό $F[x]$.Εαν δεν είναι αλγεβρικό, τότε το a λέγεται υπερβατικό πάνω από το F.

Ορισμός: Έστω Ε επέκταση σώματος F και $a\epsilon E$ αλγεβρικό στοιχείο πάνω από το F. Το ανάγωγο $p(x)\epsilon F[x]$ για το οποίο $p(a)=0$ το οποίο είναι μονοσήμαντα ορισμένο εκτός από κάποιο σταθερό παράγοντα στο F και για το οποίο ισχύει για $f(x)\epsilon F[x]$ με $f(a)=0$ το $p(x)$ διαιρεί το $f(x)$. Ονομάζεται ανάγωγο πολυώνυμο του a πάνω από το F και το συμβολίζουμε με $irr(a,F)$.

Θα αποδείξουμε την ύπαρξή του: Έστω ϕ_a ομομορφισμός εκτίμησης του $F[x]$ στο E. Ο πυρήνας του ϕ_a είναι ιδεώδες, και μάλιστα πρέπει να είναι κύριο ιδεώδες με γεννήτορα κάποιο $p(x)\epsilon F[x]$. Το $<p(x)>$ αποτελείται από τα πολυώνυμα με ρίζα το a, επομένως το $p(x)$ διαιρεί κάθε πολυώνυμο με ρίζα το a.
Θέλουμε να δείξουμε οτι το $p(x)$ είναι ανάγωγο. Αν $p(x)=r(x)s(x)$ ήταν μια ανάλυση του $p(x)$, τότε $r(a)s(a)=0$ άρα $r(a)=0$ η $s(a)=0$. Άτοπο γιατί το $p(x)$ είναι το πολυώνυμο ελαχίστου βαθμού με $p(a)=0$. Άρα το $p(x)$ είναι ανάγωγο.

Ορισμός: Μια επέκταση E ενός σώματος F λέγεται απλή επέκταση του F αν $E=F(a)$ για κάποιο $a\epsilon E$.

Θεώρημα: Για μια απλή επέκταση E του F, και a αλγεβρικό πάνω από το F, με $deg(a)=n$. Κάθε στοιχείο k του $E=F(a)$ γράφεται μοναδικά ως

$$k=b_0+b_1a+\ldots+b_{n-1}a^{n-1}, b_i\epsilon F.$$

Απόδειξη: Έστω $irr(a,F)=p(x)=x^n+r_{n-1}x^{n-1}+\ldots+r_0$. Ισχύει πως $p(a)=0\Rightarrow a^n=-r_{n-1}a^n-\ldots-r_0$.
Άρα κάθε δύναμη του a, a^m με $m\geq n$ ξέρουμε πως να τη γράψουμε. Επομένως, εαν $k\epsilon F(a)$ μπορούμε να γράψουμε το k ως

$$k=b_0+b_1a+\ldots+b_{n-1}a^{n-1}$$

Για τη μοναδικότητα, έστω

$$b_0+b_1a+\ldots+b_{n-1}a^{n-1}=b'_0+b'_1a+\ldots+b'_{n-1}a^{n-1}, b'_i\epsilon F,$$

τότε

$$(b_0-b'_0)+(b_1-b'_1)x+\ldots+(b_{n-1}-b'_{n-1})x^{n-1}=g(x)$$

. Το $g(x)$ ανήκει στο $F[x]$ και $g(a)=0$, επίσης πρέπει να έχει μικρότερο βαθμό από το $irr(a,F)$, επομένως έχουμε $g(x)=0$ και $b_i=b'_i$.

Ορισμός: Μια επέκταση σώματος E ενός σώματος F λέγεται αλγεβρική επέκταση του F αν κάθε στοιχείο του E είναι αλγεβρικό πάνω από το F.

Ορισμός: Όταν μια επέκταση E ενός σώματος F έχει πεπερασμένη διάσταση n ως διανυσματικός χώρος πάνω από το F, τότε το E λέγεται πεπερασμένη επέκταση βαθμού n πάνω από το F.

Θεώρημα: Κάθε πεπερασμένη επέκταση E ενός σώματος F είναι αλγεβρική επέκταση του F.

Απόδειξη: Έστω $a \epsilon E$. Εαν $[E : F] = n$, τα $1, a, \ldots, a^n$ δεν μπορούν να είναι γραμμικώς ανεξάρτητα, άρα υπάρχουν στοιχεία $c_i \epsilon F$ τέτοια ώστε,

$$c_n a^n + \ldots + c_1 a + c_0 = 0$$

, με κάποια $c_i \neq 0$.Το

$$f(x) = c_n x^n + \ldots + c_1 x + c_0$$

είναι μη μηδενικό πολυώνυμο στο $F[x]$ με $f(a) = 0$.

1.11 R-πρότυπα

Ορισμός: Έστω R δακτύλιος. Ένα (αριστερό) $R-module$ (ή R-πρότυπο) M αποτελείται απο τον R, μια αβελιανή ομάδα $< M, + >$ και μια απεικόνιση $* : RxM \to M$, τέτοια ώστε $\forall a, b \epsilon M$ καί $r, s \epsilon R$ ισχύουν:

1. $(r * a) \epsilon M$
2. $r * (a + b) = r * a + r * b$
3. $(r + s) * a = r * a + r * b$
4. $(rs) * a = r(s * a)$

Αντίστοιχα και το δεξιό $R - module$ (R-πρότυπο).

Παραδείγματα: Κάθε αβελιανή ομάδα G μπορεί να θεωρηθεί ως $\mathbb{Z} - module$. Εαν ορίσουμε $n * a = a^n$ για $a \epsilon G$ και $n \epsilon \mathbb{Z}$, τα αξιώματα βγαίνουν εύκολα.

Παραδείγματα: Για κάθε ιδεώδες N του R, μπορούμε να δούμε τη $< N, + >$ ως ένα $R-module$, όπου για $a \epsilon N$, $r \epsilon R$, παίρνουμε το συνηθισμένο γινόμενο των r και a, βλέποντας τα ως στοιχεία του δακτυλίου.

Εφαρμογή: Να οριστεί ομομορφισμός από το R στο $End(M)$.

Λύση: Αρχικά μπορούμε να ορίσουμε τον ομομορφισμό $f_r : M \longrightarrow M$, με $f_r(x) = r * x$ για κάποιο $r \epsilon R$. Ο f_r είναι ομομορφισμός ομάδων , λόγω του (2), πράγματι, για $a, b \epsilon M : f_r(a + b) = r * (a + b) = r * a + r * b = f_r(a) + f_r(b)$.

Εξ'ορισμού βέβαια,είναι ένα προς ένα και επί, δηλαδή ισομορφισμός. Επομένως έχουμε ένα σύνολο ενδομορφισμών $End(M) = \{f_r : r \epsilon R\}$.

Ορίζουμε τώρα την $g : R \longrightarrow End(M)$ η οποία θα αποδείξουμε πως είναι ομομορφισμός δακτυλίων. Για $r_1, r_2 \epsilon R$ έχουμε:

$$g(r_1 + r_2) = f_{r_1 + r_2}$$

καί

$$g(r_1) + g(r_2) = f_{r_1} + f_{r_2}$$

$\forall x \epsilon M$ η $f_{r_1+r_2}(x) = (r_1+r_2)x = r_1x + r_2x = f_{r_1}(x) + f_{r_2}(x)$. Άρα η g είναι ομομορφισμός ως προς την πρόσθεση. Θα δείξουμε οτι είναι και ομομορφισμός ως προσ τη σύνθεση συναρτήσεων.

$$g(r_1r_2) = f_{r_1r_2}$$

καί

$$g(r_1)g(r_2) = fr_1 \circ fr_2$$

$\forall x \epsilon M$ η $fr_1r_2(x) = (r_1r_2)x = r_1(r_2x) = fr_1 \circ fr_2(x)$.Άρα η g είναι και ομομορφισμός ως προς τη σύνθεση.

Εαν το R είναι σώμα, τότε το $R - module$ είναι διανυσματικός χώρος.

1.12 Δακτύλιοι της *Noether*

Ορισμός:Έστω δακτύλιος R. Ο R ονομάζεται $Noetherian$, εαν δεν υπάρχει απείρως αυξανόμενη αλυσίδα ιδεωδών του R. Δηλαδή, για κάθε $I_1 \subset I_2 \subset I_3 \subset \ldots$, όπου I_j ιδεώδη του R, $\exists m$ θετικός ακέραιος, τέτοιος ώστε $I_m = I_k$, $\forall k \geq m$.

Πρόταση: Έστω I ιδεώδες ενός $Noetherian$ δακτυλίου R, τότε ο δακτύλιος πηλίκων R/I είναι δακτύλιος της $Noether$.

Απόδειξη: Κάθε άπειρη αλυσίδα ιδεωδών του R/I θα αντιστοιχεί από το τέταρτο θεώρημα ισομορφισμών, σε μια άπειρη αλυσίδα ιδεωδών του R.
Το τέταρτο θεώρημα ισομορφισμών ομάδων, λέει πως εάν έχω μια ομάδα G με κανονική υποομάδα N, τότε υπάρχει ισομορφισμός φ, από τις υποομάδες του G που περιέχουν το N σε υποομάδες του G/N.

Θεώρημα: Τα επόμενα είναι ισοδύναμα:

1. Ο δακτύλιος R είναι $Noetherian$.
2. Κάθε σύνολο ιδεωδών του R περιέχει ένα μέγιστο στοιχείο.
3. Κάθε ιδεώδες του R είναι πεπερασμένα παραγώμενο.

Απόδειξη: (1) $\Rightarrow$ (2) Υποθέτουμε οτι ο R είναι $Noetherian$. Ορίζω Σ το σύνολο ιδεωδών του R. Έστω $I_1 \epsilon\ \Sigma$. Αν I_1 είναι μέγιστο στο Σ, τότε απεδείχθη. Θα θεωρήσουμε πως δεν είναι. Τότε θα υπάρχει $I_2 \epsilon\ \Sigma$ με $I_1 \subset I_2$, αντίστοιχα, εαν το I_2 είναι μέγιστο στο Σ, απεδείχθη. Αντίστοιχα θα θεωρήσουμε πως δεν είναι. Επομένως, υπάρχει $I_3 \epsilon\ \Sigma$, με $I_2 \subset I_3$. Συνεχίζω έτσι , και αν δεν βρίσκω μέγιστο, από αξίωμα επιλογής μπορώ να επιλέξω πάντα μια αλυσίδα στοιχείων, που συνεχώς αυξάνεται , άτοπο απο το (1).
(2) $\Rightarrow$ (3) Έστω N ιδεώδες του R, και Σ το σύνολο των πεπερασμένα παραγώμενων ιδεωδών του N. Παρατηρούμε οτι το Σ δεν είναι κενό αφού $\{0\} \epsilon\ \Sigma$. Το Σ θα περιέχει μέγιστο N′. Εαν το $N' \neq N$, τότε μπορούμε να βρούμε $x \epsilon N - N'$. Επειδή το N′ είναι πεπερασμένα παραγώμενο, το ιδεώδες που παράγεται από το N′ είναι πεπερασμένα παραγώμενο και το x είναι επίσης πεπερασμένα παραγώμενο. Αυτό είναι άτοπο αφού το N′ είναι μέγιστο , άρα $N = N'$.
(3) $\Rightarrow$ (1) Έστω $I_1 \subset I_2 \subset I_3 \subset \ldots$ αλυσίδα ιδεωδών στο R. Έστω επίσης, $N = \cup_{i=1}^{\infty} I_i$.

Προφανώς το N είναι ιδεώδες, ως ένωση ιδεωδών, και επομένως πεπερασμένα παραγώμενο. Έστω λοιπόν $a_1, \dots a_n, a_i \epsilon N$ τα στοιχεια που παράγουν το N. Κάθε a_i ανήκει σε ένα I_{j_i}. Θεωρώ τώρα το $m = max\{j_1, j_2, \dots, j_n\}$. Τότε τα $a_i \epsilon I_m$ για κάθε i, επομένως το ιδεώδες που παράγουν ανήκει στο I_m ή $N \subset I_m$. Επομένως έχουμε $I_m = N = I_k$, $\forall k > m$.

Υπενθύμιση: Αποδείξαμε στο προηγούμενο κεφάλαιο πως οι περιοχές κύριων ιδεωδών είναι της $Noether$, τώρα το γενικεύσαμε για δακτυλίους οπου τα ιδεώδη τους δεν είναι κύρια, αλλά απλά πεπερασμένα παραγώμενα.

Παράδειγμα: Κάθε περιοχή κύριων ιδεωδών ειναι $Noetherian$ δακτύλιος. Εφόσον κάθε ιδεώδες του είναι πεπερασμένα παραγώμενο. Συγκεκριμένα ο $\mathbb{Z}$, ο πολυωνυμικός δακτύλιος $k[x]$ όπου k σώμα, καί οι $Gaussian$ ακέραιοι , δηλαδή το $\mathbb{Z}[i]$.

Κεφάλαιο 2

Παραγοντοποίηση Ιδεωδών σε *Dedekind* Δακτυλίους

Σε αυτό το κεφάλαιο θα θεωρήσουμε πως οι δακτύλιοι μας είναι αντιμεταθετικοί με μοναδιαίο στοιχείο.

2.1 Νόρμα, Ίχνος και Διακρίνουσα

Στη συνέχεια θα χρησιμοποιήσουμε αρκετά την έννοια του σώματος αριθμών. Ένα σώμα αριθμών είναι μια πεπερασμένη επέκταση (επομένως και αλγεβρική) του σώματος των ρητών αριθμών.

Ορισμός: Έστω K σώμα αριθμών, και $\sigma_1, \ldots, \sigma_n$ οι ομομορφισμοί από το K στο $\mathbb{C}$. Για $a \epsilon K$, τα στοιχεία $\sigma_i(a)$ ονομάζονται τα συζυγή στοιχεία του a.

Θεώρημα: Έστω K σώμα αριθμών , $[K : \mathbb{Q}] = n$. Παίρνουμε $a \epsilon K$, και θεωρούμε τον πολλαπλασιασμό με a ώς γραμμική αντιστοίχιση από το $\mathbb{Q}$-διανυσματικό χώρο K στον εαυτό του. Έτσι λοιπόν το $a : K \to K$ ορίζεται ως $b \to ab$. Και τότε το χαρακτηριστικό πολυώνυμο της αντιστοίχισης είναι ίσο με $P_a(x) = \prod_{i=1}^{n}(x - \sigma_i(a))$.

Απόδειξη: Έστω $K = \mathbb{Q}[\theta]$, και η βάση του $1, \theta, \theta^2, \ldots, \theta^{n-1}$. Θεωρούμε M_a τον πίνακα που περιγράφει την γραμμική αντιστοίχιση a σχετικά με αυτή τη βάση.

Αρχικά θεωρούμε $a = \theta$. Έστω $f_0 = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, τότε

$$M_\theta = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -a_{n-1} \end{bmatrix}$$

και υπολογίζουμε το χαρακτηριστικό πολυώνυμο,

$$det(XI_n - M_\theta) = det \begin{bmatrix} x & 0 & \dots & 0 & a_0 \\ -1 & x & \dots & 0 & a_1 \\ 0 & -1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & x + a_{n-1} \end{bmatrix} = \sum a_k x^k$$

Επομένως το χαρακτηριστικό πολυώνυμο του M_θ είναι $f_\theta = \prod_{i=1}^n (x - \sigma_i(\theta))$ όπως θέλαμε.

Επομένως απο γραμμική άλγεβρα ξέρουμε οτι υπάρχει αντιστρέψιμος πίνακας A τέτοιος ώστε:

$$M_\theta = A \begin{bmatrix} \sigma_1(\theta) & 0 & \dots & 0 \\ 0 & \sigma_2(\theta) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_n(\theta) \end{bmatrix} A^{-1}$$

Ισχύει $M_{a \pm b} = M_a \pm M_b$ και $M_{ab} = M_a M_b$. Επομένως εάν έχουμε πολυώνυμο $g \epsilon \mathbb{Q}[x]$ τότε $M_g a = g(M_a)$. Τώρα μπορούμε να γράψουμε κάθε $a \epsilon K$ ως $g(\theta)$ για κάποιο $g \epsilon \mathbb{Q}[x]$. Και έχουμε

$$M_a = g(M_\theta) = A \begin{bmatrix} g(\sigma_1(\theta)) & 0 & \dots & 0 \\ 0 & g(\sigma_2(\theta)) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g(\sigma_n(\theta)) \end{bmatrix} A^{-1} =$$

$$A \begin{bmatrix} \sigma_1(g(\theta)) & 0 & \dots & 0 \\ 0 & \sigma_2(g(\theta)) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_n(g(\theta)) \end{bmatrix} A^{-1} =$$

$$A \begin{bmatrix} \sigma_1(a) & 0 & \dots & 0 \\ 0 & \sigma_2(a) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_n(a) \end{bmatrix} A^{-1}$$

Επομένως το χαρακτηριστικό πολυώνυμο του M_a είναι αυτό που θέλουμε.

Ορισμός: Έστω K σώμα αριθμών, $a \epsilon K$. Ορίζουμε τη νόρμα του a ως

$$N(a) = N_{K/\mathbb{Q}}(a) = \prod_{i=1}^n \sigma_i(a) \epsilon \mathbb{Q}$$

Πρόταση: Ισχύει $N(a) = det(M_a)$ και $N(ab) = N(a)N(b)$

Ορισμός: Έστω K σώμα αριθμών, $a \epsilon K$. Ορίζουμε το ίχνος του a ως

$$Tr(a) = Tr_{K/\mathbb{Q}}(a) = \sum_{i=1}^{n} \sigma_i(a) \epsilon \mathbb{Q}$$

Πρόταση: Ισχύει $Tr(a) = Tr(-a) = Tr(M_a)$ και $Tr(a+b) = Tr(a) + Tr(b)$

Παράδειγμα: Στον $K = \mathbb{Q}[\sqrt{d}]$ που θα ασχολιθούμε στο επόμενο κεφάλαιο, θα έχουμε

1. $Tr(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$
2. $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - \sqrt{d}) = a^2 - db^2$

Στον $K = \mathbb{Q}[\sqrt[3]{2}]$, έχουμε $(x^3 - 2) = (x - \sqrt[3]{2})(x - \zeta_3 \sqrt[3]{2})(x - \zeta_3^2 \sqrt[3]{2})$ όπου $\zeta_3 = e^{(2\pi i)/3}$

1. $Tr(a + b\sqrt[3]{2} + c\sqrt[4]{2}) = (a + b\sqrt[3]{2} + c\sqrt[4]{2}) + (a + \zeta_3 b\sqrt[3]{2} + \zeta_3^2 c\sqrt[4]{2}) + (a + \zeta_3^2 b\sqrt[3]{2} + \zeta_3 c\sqrt[4]{2}) = 3a$
2. $N(a + b\sqrt[3]{2} + c\sqrt[4]{2}) = (a + b\sqrt[3]{2} + c\sqrt[4]{2})(a + \zeta_3 b\sqrt[3]{2} + \zeta_3^2 c\sqrt[4]{2})(a + \zeta_3^2 b\sqrt[3]{2} + \zeta_3 c\sqrt[4]{2}) = a^3 + 2b^2 + 4c^3 + 6abc$

Ορισμός: Έστω K σώμα αριθμών και $a_1, \ldots, a_n$ βάση του K. Έστω $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ όλοι οι ομομορφισμοί. Η διακρίνουσα του $(a_1, \ldots, a_n)$ ορίζεται ως

$$disc(a_1, \ldots, a_n) = \left(det \begin{bmatrix} \sigma_1(a_1) & \sigma_1(a_2) & \ldots & \sigma_1(a_n) \\ \sigma_2(a_1) & \sigma_2(a_2) & \ldots & \sigma_2(a_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(a_1) & \sigma_n(a_2) & \ldots & \sigma_n(a_n) \end{bmatrix} \right)^2$$

Θεώρημα: Έχουμε,

$$disc(a_1, \ldots, a_n) = det \begin{bmatrix} Tr(a_1a_1) & Tr(a_1a_2) & \ldots & Tr(a_1a_n) \\ Tr(a_2a_1) & Tr(a_2a_2) & \ldots & Tr(a_2a_n) \\ \vdots & \vdots & \ddots & \vdots \\ Tr(a_na_1) & Tr(a_na_2) & \ldots & Tr(a_na_n) \end{bmatrix}$$

Απόδειξη: Έστω $M = (\sigma_i(a_j))_{ij}$. Τότε έχουμε $disc(a_1, \ldots, a_n) = det(M)^2 = det(M^2) = det(M_T M)$. Όμως τα στοιχεία του $M_T M$ στα (i,j) είναι $\sum_{k=1}^{n} \sigma_k(a_i)\sigma_k(a_j) = \sum_{k=1}^{n} \sigma_k(a_ia_j) = Tr(a_ia_j)$.

Θεώρημα: Έχουμε οτι $disc(a_1, \ldots, a_n) \neq 0$.

Απόδειξη: Έστω οτι $disc(a_1, \dots, a_n) = 0$, τότε υπάρχουν $c_1, \dots, c_n \epsilon \mathbb{Q}$ με

$$c1 \begin{bmatrix} Tr(a_1 a_1) \\ \vdots \\ Tr(a_n a_1) \end{bmatrix} + \ldots + c_n \begin{bmatrix} Tr(a_n a_1) \\ \vdots \\ Tr(a_n a_n) \end{bmatrix} = 0$$

επομένως,

$$\begin{bmatrix} Tr(a_1 \sum c_j a_j) \\ \vdots \\ Tr(a_n \sum c_j a_j) \end{bmatrix} = 0$$

για $a' = \sum c_j a_j$, έχουμε

$$\begin{bmatrix} Tr(a_1 a') \\ \vdots \\ Tr(a_n a') \end{bmatrix} = 0$$

Δηλαδή $Tr(a_i a') = 0$ για κάθε i.

Όμως ξέρουμε οτι τα a_i είναι βάση για το K πάνω από το $\mathbb{Q}$, επομένως $Tr(ba) = 0, \forall b \epsilon K$,και $a > 0$.
Για $b = a^{-1}$, έχουμε $Tr(ba) = Tr(1) = n = [K : \mathbb{Q}]$, άτοπο.

Παράδειγμα:

1. Έστω $K = \mathbb{Q}[\sqrt{d}]$. Θεωρώντας τη βάση $1, \sqrt{d}$. Υπολογίζουμε τη διακρίνουσα:

$$disc(1, \sqrt{d}) = det \begin{bmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(d) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} = 4d$$

   Αν θεωρήσουμε τη βάση, $1, \frac{1+\sqrt{d}}{2}$, τότε $disc(1, \frac{1+\sqrt{d}}{2}) = (-\sqrt{d})^2 = d$

2. Έστω $K = \mathbb{Q}[\sqrt[3]{d}]$ με βάση $1, \sqrt[3]{d}, \sqrt[3]{d^2}$. Τότε, έχουμε

$$disc(1, \sqrt[3]{d}, \sqrt[3]{d^2}) = det \begin{bmatrix} Tr(1) & Tr(\sqrt[3]{d}) & Tr(\sqrt[3]{d^2}) \\ Tr(\sqrt[3]{d}) & Tr(\sqrt[3]{d^2}) & Tr(d) \\ Tr(\sqrt[3]{d^2}) & Tr(d) & Tr(\sqrt[3]{d}) \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 3d \\ 0 & 3d & 0 \end{bmatrix} = -27d^2$$

2.2 Ακέραιοι αριθμοί

Ορισμός 1: Έστω A δακτύλιος, και $x \epsilon L$, όπου $L \supset A$ σώμα. Το x ονομάζεται ακέραιος πάνω από το A, αν ικανόποιεί μια μονική πολυωνυμική εξίσωση με συντελεστές από το A.

$$x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0, a_i \epsilon A, n \geq 1$$

Θα δώσουμε τώρα κάποιους εναλλακτικούς ορισμούς και ισοδυναμίες.

Πρόταση 1: Έστω A δακτύλιος, και $x\epsilon L$, όπου $L \supset A$ σώμα. Το x είναι ακέραιος πάνω από το A, αν και μόνο αν, υπάρχει πεπερασμένα παραγώμενο $A-module$ $M \subset L$ τέτοιο ώστε $xM \subset M$.

Απόδειξη: Αρχικά, έστω πως ο x είναι ακέραιος πάνω από το A, τότε άμεσα το πεπερασμένα παραγώμενο $module$ M που αναζητάμε, είναι αυτό που παράγεται από τα $1, x, ..., x^{n-1}$, προφανώς ισχύει $xM \subset M$. Αντίστροφα, έστω οτι υπάρχει M πεπερασμένα παραγώμενο από κάποια $< r_1, ..., r_n >$ έτσι ώστε $xM \subset M$. Τότε

$$xr_1 = a_{11}r_1 + ... + a_{1n}r_n$$

$$xr_2 = a_{21}r_1 + ... + a_{2n}r_n$$

$$...$$

$$xr_n = a_{n1}r_1 + ... + a_{nn}r_n$$

περνώντας τα πρώτα μέλη από την άλλη προκύπτει ένας πίνακας όπου η ορίζουσα του μας δίνει την μονική πολυωνυμική εξίσωση που θέλουμε.

$$0 = \begin{vmatrix} (a_{11}-x) & a_{12} & \cdots & a_{1n} \\ a_{21} & (a_{22}-x) & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & (a_{nn}-x) \end{vmatrix}$$

Πρόταση 2: Έστω A δακτύλιος, και $x\epsilon L$, όπου $L \supset A$ σώμα. Το x είναι ακέραιος πάνω από το A, αν και μόνο αν, η A-άλγεβρα που παράγει είναι πεπερασμένα παραγώμενο $A - module$.

Απόδειξη: Έστω πως η A-άλγεβρα που παράγεται από το x, είναι πεπερασμένα παραγώμενο $A - module$.
Τότε υπάρχει πεπερασμένος αριθμός δυνάμεων του x που το παράγουν. Έστω $1, x, \ldots, x^n$. Τότε το $x^{n+1} = \sum_{i=0}^{n} a_i x^i$, και αυτή είναι η πολυωνυμική εξίσωση που ψάχνουμε.
(Μπορούμε να χρησιμοποιήσουμε και το πορηγούμενο θεώρημα , γιατί το $xA[x] \subset A[x]$.)
Αντίστροφα, έστω x ακέραιος πάνω από το A.
Τότε υπάρχει πολυωνυμική εξίσωση που ικανοποιεί , $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \Rightarrow x^n = -a_{n-1}x^{n-1} - \ldots - a_1 x - a_0$. Που σημαίνει οτι κάθε δύναμη του x μεγαλύτερη του n, μπορούμε να την εκφράσουμε με τη βοήθεια της προηγούμενη σχέσης, δηλάδή συναρτήσει των $1, \ldots, x^{n-1}$.

Ορισμός 2: Έστω δακτύλιος B που περιέχει τον A. Θα λέμε οτι είναι ακέραιος πάνω απο τον A, αν κάθε στοιχείο του είναι ακέραιο πάνω απο τον A.

Πρόταση 3: Έστω $A \subset B \subset C$ τρείς δακτύλιοι. Εάν ο B είναι ακέραιος πάνω απο τον A και ο C είναι ακέραιος πάνω απο τον B, τότε ο C είναι ακέραιος πάνω απο τον A.

Απόδειξη: Έστω $x\epsilon C$, το x θα είναι ακέραιο πάνω απο το B, δηλαδή θα υπάρχουν $b_i \epsilon B$ τέτοια ώστε $x^n + b_{n-1}x^{n-1} + ... + b_0 = 0$. Θα θεωρήσουμε τώρα την επέκταση του A, $B_1 = A[b_0, ..., b_{n-1}]$, το B_1 είναι πεπερασμένα παραγώμενο $A-module$, γιατί τα στοιχεία του B είναι ακέραια πάνω από το A (επαγωγικά από Πρόταση 2),καί το $B_1[x]$ είναι πεπερασμένα παραγώμενο $B_1-module$ επομένως και $A-module$. Ισχύει οτι $xB_1[x] \subset B_1[x]$, επομένως από Πρόταση 1 το x είναι ακέραιο πάνω από το A.

Πρόταση 4: Έστω $A \subset B$ δύο δακτύλιοι, και ο B να είναι ακέραιος πάνω από τον A. Έστω επίσης σ ένας ομομορφισμός του B. Τότε σ(B) είναι ακέραιο πάνω από το σ(A).

Απόδειξη: Προκύπτει άμεσα , αφού ο ομομορφισμός διατηρεί τις πράξεις.

Πρόταση 5: Έστω A δακτύλιος, K το σώμα πηλίκων του και x αλγεβρικό πάνω από το K. Τότε υπάρχει ένα στοιχείο του A , $c \neq 0$, τέτοιο ώστε το cx είναι ακέραιο πάνω από το A.

Απόδειξη: Αφού είναι αλγεβρικό πάνω από το K, υπάρχει μια πολυωνυμική εξίσωση

$$a_n x^n + a_{n-1}x^{n-1} + ... + a_0 = 0, a_i \epsilon A$$

. Πολλαπλασιάζωντας με a_n^{n-1} έχουμε,

$$(a_n x)^n + ... + a_0 a_n^{n-1} = 0, a_i \epsilon A$$

. Τότε το $c \epsilon A$ που ψάχνουμε είναι το a_n.

Ορισμός 3: Έστω A δακτύλιος που περιέχεται σε σώμα L, καί έστω B το σύνολο που περιέχει τους ακεραίους πάνω από το A στο L. Τότε ο B είναι δακτύλιος και ονομάζεται ακέραια κλειστότητα του A στο L. Επίσης θα λέμε οτι ένας δακτύλιος A είναι ακέραια κλειστός σε ένα σώμα L αν κάθε στοιχείο του L, που είναι ακέραιο πάνω από το A, βρίσκεται στο A.Τέλος θα λέμε οτι είναι ακέραια κλειστό αν είναι ακέραια κλειστό στο σώμα πηλίκων του.

O B είναι προφανώς δακτύλιος αφού , έστω x, y στο B, εφόσον είναι ακέραιοι πάνω από το A, θα υπάρχουν πεπερασμένα παραγώμενα $A-modules$ M,N τέτοια ώστε $xM \subset M$, $yN \subset N$. Τότε το MN είναι πεπερασμένα παραγώμενο $A-module$ καί $(x \pm y)MN \subset MN$,$xy \subset MN$.

Πρόταση 6: Εάν το A είναι περιοχή μονοσήμαντης ανάλυσης (ΠΜΑ), τότε είναι ακέραια κλειστό.

Απόδειξη: Υποθέτουμε οτι υπάρχει ένα πηλίκο $a/b, a, b \epsilon A$ το οποίο είναι ακέραιο πάνω από το A, και ένα ανάγωγο στοιχείο p του A, το οποίο διαιρεί το b αλλά όχι το a. Προφανώς για κάποια $a_0, ..., a_{n-1} \epsilon A$ θα ισχύει

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + ... + a_0 = 0$$

επομένως

$$a^n + a_{n-1}ba^{n-1} + ... + a_0 b^n = 0$$

εφόσον το p διαιρεί το b θα πρέπει να διαιρεί και το a^n, επομένως καί το a. Άτοπο.

Πρόταση 7: Έστω A υποδακτύλιος ενός δακτυλίου B ακέραιου πάνω από το A. Έστω S πολλαπλασιαστικό υποσύνολο του A. Τότε το $S^{-1}B$ είναι ακέραιο πάνω από το $S^{-1}A$. Και αν το A είναι ακέραια κλειστό , το $S^{-1}A$ είναι επίσης ακέραια κλειστό.

Απόδειξη: Έστω $x\epsilon B$ καί $s\epsilon S$ καί έστω M πεπερασμένα παραγώμενο $A - module$ τέτοιο ώστε $xM \subset M$. Το $S^{-1}M$ είναι πεπερασμένα παραγώμενο $S^{-1}A - module$, και $(s^{-1}x)S^{-1}M \subset S^{-1}M$, επομένως το $s^{-1}x$ είναι ακέραιο πάνω από το $S^{-1}A$. Τώρα έστω x στο σώμα πηλίκων του A, ακέραιο πάνω από το $S^{-1}A$. Έχουμε,

$$x^n + \left(\frac{b_{n-1}}{s_{n-1}}\right)x^{n-1} + ... + \left(\frac{b_0}{s_0}\right) = 0, b_i\epsilon A, s_i\epsilon S$$

επομένως υπάρχει ένα $s\epsilon S$ τέτοιο ώστε το sx να είναι ακέραιο πάνω απο το A, και να βρίσκεται στο A. Επομένως το x βρίσκεται στο $S^{-1}A$.

Θεώρημα: Έστω I μη μηδενικό ιδεώδες του δακτυλίου των ακέραιων O_k, όπου $[K : \mathbb{Q}] = n$. Τότε το I είναι ελεύθερο $\mathbb{Z} - module$ βαθμού n, και παράγεται από μια $\mathbb{Q}$-βάση για το K.

Απόδειξη: Έστω $(a_1, \ldots, a_n)$ μια $\mathbb{Q}$-βάση για το K. Αρχικά ισχυριζόμαστε πως για κάθε i, υπάρχει ένα μη μηδενικό $d_i\epsilon\mathbb{Z}$ τέτοιο ώστε $d_ia_i\epsilon O_k$. Ισχύει αφού είναι αρκέτο να δείξουμε οτι το d_i μπορεί να είναι ο πρώτος όρος κάθε ακέραιου πολυώνυμου που ικανοποιείται από το a_i. Επομένως για κάθε $\beta\epsilon I$, βρίσκουμε οτι $(\beta d_1a_1, \ldots, \beta d_na_n)$ είναι $\mathbb{Q}$-βάση για το K που περιέχεται στο I.
Δείξαμε οτι το I περιέχει μια $\mathbb{Q}$-βάση για το K. Μπορούμε να συνεχίσουμε την απόδειξη με δύο τρόπους.

Το I περιέχεται σε $Noether$ δακτύλιο, επομένως από θεώρημα ταξινόμησης είναι της μορφής $\mathbb{Z}^r\times$(κάτι πεπερασμένο). Όμως το πεπερασμένο δεν μπορεί να υπάρχει διότι είναι υποομάδα σώματος χαρακτηριστικής μηδέν και δεν υπάρχουν στοιχεία στρέψης. Τέλος θα δείξουμε οτι $r = n$. Ξέρουμε ήδη οτι $r \geq n$ γιατι το I περιέχει βάση του διανυσματικού χώρου. Ανάποδα, εαν έχω μη μηδενικό γραμμικό συνδυασμό r στοιχείων πάνω από το $\mathbb{Q}$, μπορούμε να τον μετατρέψουμε σε γραμμική σχέση πάνω από το $\mathbb{Z}$ πολλαπλασιάζοντας με παρονομαστές, άτοπο αφού οι γεννήτορες του $\mathbb{Z}^r$ δεν έχουν σχέση μεταξύ τους.

Αλλιώς, ισχυριζόμαστε οτι από τις βάσεις που περιέχει το I, αυτή με τη μικρότερη διακρίνουσα, είναι Z-βάση για το I. Επειδή η διακρίνουσα των στοιχείων του O_K είναι ακέραιος αριθμός, μπορούμε να βρούμε ελάχιστο.
Έστω $a\epsilon I$, τότε το $a = \sum_{i=1}^{n} b_iq_i$, για $q_i\epsilon\mathbb{Q}$. Θέλουμε να δείξουμε οτι τα $q_i\epsilon\mathbb{Z}$ για κάθε i. Έστω πως αυτό δεν συμβαίνει. Χωρίς βλάβη της γενικότητας, υποθέτουμε οτι $q_1 \not\epsilon\mathbb{Z}$. Τότε το $q_1 = m + \epsilon$, με $0 < \epsilon < 1$ και $m = \lfloor q_1 \rfloor$. Μπορούμε να αλλάξουμε το στοιχείο b_1 με $b_1' = a - mb_1$. Το στοιχείο b_1' ανήκει στο I. Έτσι έχουμε μια καινούργια βάση στο I όπου η ορίζουσα του πίνακα αλλαγής βάσης ειναι ε. Επομένως η καινούργια βάση θα έχει μικρότερη διακρίνουσα.

Παραδείγματα:

1. Τα $n\epsilon\mathbb{Z}$ είναι τα στοιχεία του $\mathbb{Q}$ που είναι ακέραια πάνω από το $\mathbb{Z}$. Αφού η πολυωνυμική εξίσωση που έχει ρίζα το n είναι η $x - n = 0$.

2. Έστω η επέκταση του $\mathbb{Q}$, $\mathbb{Q}[\sqrt{d}]$, με d να είναι ακέραιος, ελεύθερος τετραγώνων. Θα βρούμε τους ακεραίους στο $\mathbb{Q}[\sqrt{d}]$ πάνω από το $\mathbb{Z}$.

   Έστω $(q_1 + q_2\sqrt{d})\epsilon\mathbb{Q}[\sqrt{d}]$, το ανάγωγο πολυώνυμο που έχει ρίζα αυτό το στοιχείο είναι το εξής,

$$\left(\frac{x - q_1}{q_2}\right)^2 - d = 0 \Leftrightarrow$$

$$(x-q_1)^2 - q_2^2 d = 0 \Leftrightarrow$$

$$x^2 + (-2q_1)x + (q_1^2 - q_2^2 d) = 0$$

Θέλουμε τα $(2q_1), (q_1^2 - q_2^2 d) \epsilon \mathbb{Z}$.

(α) $(2q_1)\epsilon\mathbb{Z} \Rightarrow q_1\epsilon\mathbb{Z}$ (ή $q_1 = p_1/2$, όπου p_1 περιττός.) Για $q_1\epsilon\mathbb{Z} \Rightarrow dq_2^2\epsilon\mathbb{Z} \Rightarrow q_2^2\epsilon\mathbb{Z} \Rightarrow q_2\epsilon\mathbb{Z}$.

(β) $q_1 = p_1/2 \Rightarrow p_1^2/4 - dq_2^2\epsilon\mathbb{Z} \Rightarrow p_1^2 - 4dq_2^2\epsilon 4\mathbb{Z}.(1)$
Γενικά θέλω, $4dq_2^2\epsilon\mathbb{Z}$

  ι. $4dq_2^2\epsilon\mathbb{Z} \Rightarrow dq_2^2\epsilon\mathbb{Z} \Rightarrow q_2^2\epsilon\mathbb{Z} \Rightarrow q_2\epsilon\mathbb{Z}$ Όμως σε αυτή την περίπτωση δεν ισχύει η (1) άρα άτοπο.

  ιι. $4dq_2^2\epsilon\mathbb{Z} \Rightarrow q_2 = p_2/2$, όπου p_2 περιττός.
  Θέλω $p_1^2 - dp_2^2 = 0mod4$ επειδή ισχύει από Θεώρημα $Euler$, $p^2 = 1mod4$ αρκεί να δούμε πότε ισχύει $dp_2^2 = 1mod4 \Rightarrow d = 1mod4$.

Άρα η αλγεβρική κλειστότητα $O_k = \mathbb{Z}[\sqrt{d}]$, για $d \neq 1mod4$, ενώ για $d = 1mod4, p_1/2 + p_2/2\sqrt{d} = \frac{p_1 - p_2}{2} + p_2\frac{1+\sqrt{d}}{2}$ έχουμε οτι $O_k = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

2.3 Κλασματικά Ιδεώδη

Ορισμός: Έστω δακτύλιος O και το σώμα πηλίκων του K. Ένα κλασματικό ιδεώδες του O στο K είναι ένα $O-module$ A στο K, τέτοιο ώστε να υπάρχει ένα στοιχείο c στο O για το οποίο $cA \subset O$.

Παρατηρήσεις:

1. Ένα κλασματικό ιδεώδες, δεν είναι απαραίτητα ιδεώδες, αφού δεν είναι πάντα υποσύνολο του O.

2. Εάν το O είναι $Noetherian$ δακτύλιος, τότε το cA και επομένως το A, είναι πεπερασμένα παραγώμενο.

Παράδειγμα:

1. Το $\mathbb{Z}$ είναι περιοχή κύριων ιδεωδών, τα κλασματικά ιδεώδη στο $\mathbb{Q}$ είναι υποσύνολα του $\mathbb{Q}$ της μορφής $r\mathbb{Z}, r\epsilon\mathbb{Q}$. Για παράδειγμα, $\frac{1}{2}\mathbb{Z}$, $\frac{6}{5}\mathbb{Z}$ κλπ.

2. Στο $\mathbb{Q}[\sqrt{-5}]$ το σύνολο $F = \{\frac{(2a_1+a_2-5a_4)+(a_2+2a_3+a_4)\sqrt{-5}}{3+\sqrt{-5}}\}$ είναι κλασματικό ιδεώδες αφού $(3+\sqrt{-5})F \subset \mathbb{Z}[\sqrt{-5}]$.

Λήμμα: Έστω O $Noetherian$ δακτύλιος με σώμα πηλίκων K , και έστω $I \subset K$ ένα $O-module$. Τότε το I είναι πεπερασμένα παραγώμενο αν και μόνο αν, $aI \subset O$ για κάποιο μη μηδενικό $a\epsilon O$.

Απόδειξη: Έστω πως το I είναι πεπερασμένα παραγώμενο $O-module$ από τα στοιχεία $\frac{r_1}{s_1}\frac{r_2}{s_2}\dots\frac{r_n}{s_n}$, τότε το $aI \subset O$, για $a = s_1 \dots s_n$.

Αντίστροφα, έστω $aI \subset O$, τότε το aI είναι ιδεώδες, επομένως πεπερασμένα παραγώμενο (γιατί το O είναι $Noetherian$), και αν τα $a_1, \ldots, a_n$ παράγουν το aI, τότε τα $\frac{a_1}{a}, \ldots, \frac{a_n}{a}$ παράγουν το I.

Επομένως κάθε πεπερασμένα παραγώμενο $O - module$ του K είναι κλασματικό ιδεώδες,και το αντίστροφο ισχύει μόνο αν το O είναι $Noetherian$.

Πόρισμα: Κάθε κλασματικό ιδεώδες ενός $Noetherian$ δακτυλίου O, μπορεί να γραφτεί ως $\frac{1}{a}I$ όπου το $a\epsilon A$ καί το I είναι ιδεώδες.

2.4 *Dedekind* δακτύλιοι

Ορισμός: Ένας $Noetherian$ δακτύλιος O, ακέραια κλειστός, όπου κάθε μη μηδενικό πρώτο ιδεώδες του είναι και μέγιστο, ονομάζεται $Dedekind$ δακτύλιος.

Ένα παράδειγμα $Dedekind$ δακτυλίου, είναι ο δακτύλιος ακεραίων του $\mathbb{Z}$ ενός σώματος αριθμών.

Ορισμός: Για ιδεώδη a, b στο O, το γινόμενο ab είναι το σύνολο όλων των αθροισμάτων

$$\sum_{k=1}^{r} x_k y_k, r \geq 1, x_k \epsilon a, y_k \epsilon b$$

.

Πρόταση: Σε $Dedekind$ δακτυλίους ισχύει η μοναδική παραγοντοποίηση ιδεωδών. Δηλαδή κάθε ιδεώδες γράφεται μοναδικά ως γινόμενο πρώτων ιδεωδών.

Απόδειξη:

1. Αρχικά θα δείξουμε , οτι αν A ιδεώδες ενός δακτυλίου O, τότε υπάρχουν πρώτα ιδεώδη p_i τέτοια ώστε $p_1 \ldots p_n \subset A$.
   Έστω G το σύνολο όλων των ιδεωδών που δεν περιέχουν γινόμενο πρώτων ιδεωδών. Θεώρουμε επίσης οτι το G είναι μη κενό. Επειδή το O είναι της $Noether$,το G έχει μέγιστο στοιχείο , έστω A. Το A δεν μπορεί να ειναι πρώτο, αλλιώς θα περιέχει τον εαυτό του. Επομένως υπάρχουν ιδεώδη $b, c\epsilon O$ τέτοια ώστε $bc\epsilon A, b \not\epsilon A, c \not\epsilon A$.
   Θεωρώ τα $A_1 = A + b, A_2 = A + c$. Τότε $A_1 A_2 \subset A$. Λόγω του οτι το A είναι μέγιστο τα A_1, A_2 δεν ανήκουν στο G. Άρα υπάρχει $p_1, \ldots, p_t, p_{t+1}, \ldots, p_r$ τέτοια ώστε

   $$p_1 \ldots p_t \subset A_1$$

   $$, p_{t+1} \ldots p_r \subset A_2$$

   ή $p_1 \ldots p_r \subset A_1 A_2 \subset A$.
   Τώρα θα ορίσουμε για κάθε ιδεώδες A στο O,

   $$A^{-1} = \{x\epsilon K | xA \subset O\}$$

2. Για q μέγιστο ιδεώδες, $q^{-1} \supset O$.
   Είναι προφανές οτι $O \subset q^{-1}$, θα δείξουμε οτι υπάρχει στοιχείο του q^{-1} που δεν ανήκει στο O. Παίρνουμε ένα $a \epsilon q$ με $a \neq 0$. Έστω r ο μικρότερος αριθμός τέτοιος ώστε $p_1 \dots p_r \subset (a) \subset q$, επειδή τα πρώτα ιδεώδη είναι και μέγιστα, ένα $p_i \subset q$, δηλαδή $p_i = q$. Έστω χωρίς βλάβη της γενικότητας, $p_i = p_1 \Rightarrow p_2 \dots p_r \not\subset (a) \Rightarrow \exists b \epsilon p_2 \dots p_r, b \not\epsilon (a)$. Όμως $bq \subset (a) \Rightarrow ba^{-1}q \subset O \Rightarrow ba^{-1} \epsilon q^{-1}$, και ισχύει $b \not\epsilon aO \Rightarrow ba^{-1} \not\epsilon O$.

3. Κάθε ιδεώδες αντιστρέφεται, από κλασματικό ιδεώδες.
   Θα πάρουμε ένα σύνολο ιδεωδών G, τα οποία δεν αντιστρέφονται, και επειδή είμαστε σε δακτύλιο της $Noether$ θα υπάρχει μέγιστο στοιχείο. Έστω μέγιστο ιδεώδες του G , a. Το a δεν μπορεί να είναι μέγιστο. Επομένως $a \subset p$, $a \neq p$ για p μέγιστο.

   $$a \subset ap^{-1} \subset aa^{-1} \subset O$$

   . Το a είναι πεπερασμένα παραγώμενο , επομένως δεν γίνεται $ap^{-1} = a \Rightarrow ap^{-1} \supset a$, επομένως έχει αντίστροφο, που αν πολλαπλασιαστει με το p δίνει αντίστροφο του a, άτοπο.

4. Μοναδική παραγοντοποίηση
   Έστω ιδεώδη που δεν γράφονται με μοναδική παραγοντοποίηση. Παίρνω a το μέγιστο αυτών. Το a δεν είναι πρώτο $\Rightarrow a \subset p$ όπου p πρώτο , τότε

   $$a \subset ap^{-1} \subset pp^{-1} \subset O$$

   $\exists p_1, \dots, p_r$ τέτοια ώστε $p_1 \dots p_r = ap^{-1} \Rightarrow a = pp_1 \dots p_r$.

   Μοναδικότητα τώρα, έστω $a = p_1 \dots p_r = q_1 \dots q_s$, το p_1 διαιρεί κάποιο παράγοντα q_j, έστω q_1,

   $$p_2 \dots p_r = q_2 \dots q_s$$

   συνεχίζοντας καταλήγουμε στο ζητούμενο.

Πρόταση: Τα μη μηδενικά κλασματικά ιδεώδη με πράξη τον πολλαπλασιασμό αποτελούν ομάδα.

Απόδειξη: Έστω a ιδεώδες διάφορο του μηδενός, και c ένα κλασματικό ιδεώδες τέτοιο ώστε $ac = O$. Τότε $c = a^{-1}$
Ισχύει οτι $c \subset a^{-1}$. Αντίστροφα , αν $xa \subset O$, τότε $xac \subset c$ και επομένως $x \epsilon c$, γιατί $ac = O$. Επομένως τα κλασματικά ιδεώδη αντιστρέφτονται. Εαν a είναι κλασματικό ιδεώδες, τοτε υπάρχει στοιχείο $c \epsilon O$ τέτοιο ώστε $ca \subset O$, και το ca να ειναι αντιστρέψιμο. Εαν $cab = O$ τότε $cb = a^{-1}$. Αυτό αποδεικνύει οτι τα μη μηδενικά κλασματικά ιδεώδη αποτελούν ομάδα.

Ορισμός: Έστω $Dedekind$ δακτύλιος και ένα κλασματικό ιδεώδες a.

$$a = \prod_p p^{r_p}, r_p \epsilon \mathbb{Z}$$

το r_p είναι η τάξη του a στο p.

1. Εαν το $r_p > 0$ το a έχει ένα μηδέν στο p.

2. Εαν το $r_p < 0$ το a έχει ένα πόλο στο p.

Επίσης από ένα $a \epsilon K$ σώμα πηλίκων ενός δακτυλίου A, μπορώ να φτιάξω ένα κλασματικό ιδεώδες,

$$aA = < a >$$

Για κλασματικά ιδεώδη $a \supset b$, έχουμε οτι $ord_p a \leq ord_p b$ για κάθε πρώτο ιδεώδες p.
Σε περίπτωση που $ord_p a = 0$, το a είναι μονάδα στο p, επίσης τότε το a είναι μονάδα και στον τοπικό δακτύλιο A_p.

Πρόταση: Έστω A *Dedekind* δακτύλιος ,και S πολλαπλασιαστικό υποσύνολο του. Ο $S^{-1}A$ είναι *Dedekind* δακτύλιος. Επίσης, η αντιστοίχιση

$$a \to S^{-1}a$$

είναι ένας ομομορφισμός, από την ομάδα κλασματικών ιδεωδών του A, στην ομάδα κλασματικών ιδεωδών του $S^{-1}A$, και ο πυρήνας αυτού του ομομορφισμού είναι τα κλασματικά ιδεώδη του A ,που έχουν κοινά στοιχεία με το S.

Απόδειξη: Έστω a, b ιδεώδη του A, τότε $S^{-1}(ab) = (S^{-1}a)(S^{-1}b)$, επομένως ο πολλαπλασιασμός με S^{-1} είναι ένας ομομορφισμός στην ομάδα τον κλασματικών ιδεωδών.
Επειδή το $a \cap S \neq 0$, $S^{-1}a = S^{-1}A$, μπορούμε να γράψουμε, $1 = a'/s$ για $a' \epsilon a$ καί $s \epsilon S$. Επομένως $a' = s$ καί το a έχει κοινά στοιχεία με το S. Αυτό αποδεικνύει τον ισχυρισμό για τον πυρήνα. Ο ομομορφισμός είναι και επί , γιατι έχουμε οτι κάθε ιδεώδες του $S^{-1}A$ είναι της μορφής $S^{-1}a$ για κάποιο ιδεώδες a του A.

Ορισμός: Ορίζουμε ως κύριο κλασματικό ιδεώδες, το κλασματικό ιδεώδες τύπου aA, δηλαδή αυτό το οποίο παράγεται απο ένα στοιχείο a του σώματος πηλίκων του A.
Εφαρμογή: Ο δακτύλιος ακεραίων O_k του $\mathbb{Z}$ ενός σώματος αριθμών, είναι *Dedekind* δακτύλιος.

Απόδειξη: Θέλω να αποδείξω πρώτα ένα Λήμμα που θα χρησιμοποιήσουμε στη συνέχεια.

Λήμμα: Έστω I μη μηδενικό ιδεώδες στον δακτύλιο ακεραίων O_k. Τότε το O_k/I είναι πεπερασμένο.

Απόδειξη: Θεωρούμε οτι το I περιέχει έναν ακέραιο $m \epsilon \mathbb{Z}$. Τότε το O_k/I είναι ένα πηλίκο του $O_k/(m)$, το οποίο είναι ισομορφικό ως $\mathbb{Z}-module$ με το $(\mathbb{Z}/m\mathbb{Z})^n$, επομένως είναι και τα δύο πεπερασμένα.

1. Έχουμε προαναφέρει οτι το $a \epsilon K$ είναι ακέραιο πάνω από το $\mathbb{Z}$ αν και μόνο αν υπάρχει ενα μη μηδενικό, πεπερασμένα παραγώμενο $\mathbb{Z} - moduleW \subset K$ τέτοιο ώστε $aW \subset W$, και πως όταν το a είναι ακέραιο, τότε το $\mathbb{Z}[a]$ είναι ένα τέτοιο *module*.
   Ας υποθέσουμε λοιπόν ένα $a \epsilon K$ το οποίο ικανοποιεί το πολυώνυμο $x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$

με $a_i \epsilon O_k \forall i$. Και ας πάρουμε το δακτύλιο $W := \mathbb{Z}[\{a_i\}_i, a] \subset K$ ως $\mathbb{Z}-module$. Το $\mathbb{Z}[\{a_i\}_i]$ είναι πεπερασμένα παραγώμενο $\mathbb{Z} - module$ γιατί τα a_i είναι ακέραια πάνω από το $\mathbb{Z}$, και το W είναι πεπερασμένα παραγώμενο $\mathbb{Z}[\{a_i\}_i] - module$ για τον ίδιο λόγο. Εύκολα έπεται οτι το W είναι πεπερασμένα παραγώμενο $\mathbb{Z} - module$ παίρνοντας γινόμενα των γεννητόρων. Αφού $aW \subset W$ έχουμε ότι το a είναι ακέραιο πάνω από το $\mathbb{Z}$, όπως θέλαμε.

2. Κάθε πρώτο ιδεώδες είναι μέγιστο.
   Έστω p πρώτο ιδεώδες του O_K, τότε το O_K/p είναι πεπερασμένη ακέραια περιοχή. Επομένως σώμα, και το p είναι μέγιστο.

3. Μένει να δείξουμε πως είναι δακτύλιος της $Noether$.
   Έστω I μη μηδενικό ιδεώδες, τότε το O_K/I είναι πεπερασμένο από το Λήμμα, και τα ιδεώδη που περιέχουν το I στο O_K είναι ισομορφικά με τα ιδεώδη του O_K/I, επομένως είναι και αυτά πεπερασμένα , άρα η αλυσίδα ιδεωδών σταματάει και ο δακτύλιος είναι της $Noether$.

Απόδειξη πως υπάρχει ο προηγούμενος ισομορφισμός: Έστω R δακτύλιος, και I ιδεώδες του R. Υπάρχει ισομορφισμός ανάμεσα στο $A = \{J|J$ ιδεώδες του R με $J \geq I\}$ και $B = \{J'|J'$ ιδεώδες του $R/I\}$.
Ορίζουμε λοιπόν φ:A→B και

$$j\epsilon A : \phi(J) = J' = \{j + I|j\epsilon J\}.$$

1. Αρχικά θα δείξουμε οτι η φ είναι καλά ορισμένη. Παίρνουμε J' ιδεώδες του R/I τέτοιο ώστε $J'\epsilon B$.
   (α) το J' δεν είναι κενό: $0 + I\epsilon J'$
   (β) το J' είναι κλειστό στην αφαίρεση: $a + I\epsilon J', b + I\epsilon J', a, b\epsilon J$ τότε $(a + I) - (b + I) = (a - b) + I, a - b\epsilon J : (a - b) + I\epsilon J'$

2. Η φ είναι ¨1-1¨.
   $J_1, J_2\epsilon A$ με $J_1 \cap J_2 = \{\oslash\} \Rightarrow j_1\epsilon J_1, j_1 \ /\epsilon J_2$, Θα δείξω οτι $J_1' \neq J_2'$. Έστω $J_1' = J_2' \Rightarrow (j_1 + I)\epsilon J_1' = J_2'$ τότε $\exists j_2\epsilon J_2 : j_1 + I = j_2 + I \Rightarrow j_1 - j_2\epsilon I \subset J_2$ άτοπο γιατί $j_1 = j_1 + j_2 - j_2\epsilon J_2$ καί $j_1 \not\epsilon J_2$. Επομένως, εαν $J_1 \neq J_2$ τότε $J_1' \neq J_2$.

3. η φ είναι επί.
   Έστω J_2 ιδεώδες του R/I. Ορίζουμε το $J = \{j\epsilon R|j + I\epsilon J_2\}$ πρέπει να δείξουμε οτι το J είναι ιδεώδες και φ(J)=J'=J_2.
   (α) το J είναι μη κενό: $0 + I\epsilon J_2$ και $0\epsilon J$
   (β) $a, b\epsilon J : a + I\epsilon J_2$ και $b + I\epsilon J_2$, αφού το J_2 είναι ιδεώδες του R/I

$$(a + I) - (b + I) = a - b + I\epsilon J \Rightarrow a - b\epsilon R, a - b\epsilon J$$

   (ς) $a\epsilon J_2, r\epsilon R \Rightarrow a + I\epsilon J$ και $r + J\epsilon R/I \Rightarrow J_2$ ιδεώδες του R/I

$$(a + J)(r + I) = ar + I\epsilon J_2 \Rightarrow ar\epsilon J$$

   Άρα είναι ιδεώδες, θα δείξουμε οτι $\phi(J) = J' = J_2$
   Από τη μια πλευρά $x\epsilon\phi(J) \Leftrightarrow x = j + I\epsilon J_2$ και $\phi(J) \subset J_2$
   Αντίστροφα, $x\epsilon J_2 \Rightarrow x = j + I$ για $j\epsilon R \Rightarrow x\epsilon\phi(J)$.

2.5 Ομάδα κλάσεων ιδεωδών

Ορισμός: Έστω A *Dedekind* δακτύλιος. Η ομάδα των κλασματικών ιδεωδών *modulo* την ομάδα τον κύριων ιδεωδών ονομάζεται ομάδα κλάσης ιδεωδών του A.

Η τάξη της ομάδας κλάσης ιδεωδών ονομάζεται αριθμός κλάσης.

Βασικά η ομάδα κλάσης ιδεωδών μετράει πόσο απέχει ένας *Dedekind* δακτύλιος από το να είναι περιοχή κύριων ιδεωδών.

Πρόταση: Έστω A *Dedekind* δακτύλιος, με πεπερασμένη ομάδα κλάσεων ιδεωδών. Έστω $a_1, \ldots a_r$ αντιπρόσωποι των κλασματικών ιδεωδών της ομάδας κλάσεων ιδεωδών, και b ένα μη μηδενικό στοιχείο του A που βρίσκεται σε κάθε a_i. Έστω S το πολλαπλασιαστικό υποσύνολο του A που παράγεται από τις δυνάμεις του b. Τότε κάθε ιδεώδες του $S^{-1}A$ είναι κύριο.

Απόδειξη: Όλα τα ιδεώδη $S^{-1}a_1, \ldots, S^{-1}a_r$ αντιστοιχούν στο μοναδιαίο ιδεώδες , μέσω τον ομομορφισμό της προηγούμενης πρότασης. Εφόσον κάθε ιδεώδες του A αντιστοιχεί σε ένα a_i πολλαπλασιασμένο με ένα κύριο ιδεώδες, η πρόταση έπεται από το γεγονός οτι η αντιστοίχηση είναι επί , που αποδειξαμε πριν.

Θέλουμε να αποδείξουμε οτι η ομάδα κλάσεων ιδεωδών είναι πεπερασμένη.
Ορισμός: Έστω $e_1, \ldots, e_n \epsilon \mathbb{R}^n$, με e_i γραμμικά ανεξάρτητα πάνω από το $\mathbb{R}$. Επομένως τα e_i είναι βάση του $\mathbb{R}^n$ ως διανυσματικός χώρος πάνω από το $\mathbb{R}$. Τα e_i δημιουργούν επίσης βάση για ένα ελεύθερο $\mathbb{Z}-module$ βαθμού n,

$$H = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n.$$

Το σύνολο H που είναι φτιαγμένο με αυτό τον τρόπο λέγεται πλέγμα στον $\mathbb{R}^n$.
Ο στοιχειώδης χώρος του H, για κάποια βάση $e_1, \ldots, e_n$, δίνεται από το

$$T = \{x \epsilon \mathbb{R}^n : x = \sum_{i=1}^{n} a_i e_i, 0 \leq a_i \leq 1\}.$$

Στην πιο κοινή περίπτωση, τα e_1, e_2 είναι γραμμικά ανεξάρτητα διανύσματα, και T είναι το παραλληλόγραμμο που παράγεται από τα e_i. Γενικά, κάθε σημείο του $\mathbb{R}^n$ είναι ισοδύναμο $moduloH$ σε ένα μοναδικό σημείο του T, επομένως το $\mathbb{R}^n$ είναι η ένωση των ξένων συνόλων $h + T, h \epsilon H$. Εαν το μ είναι το μέτρο *Lebesgue*, τότε ο όγκος μ(T) του στοιχειώδες χώρου T θα συμβολίζεται με $u(H)$. Αν παράξουμε το H με διαφορετική $\mathbb{Z}-$βάση , ο όγκος του στοιχειώδους χώρου παραμένει σταθερός.

Λήμμα: Έστω S *Lebegue* μετρήσιμο υποσύνολο του $\mathbb{R}^n$ με μ$(S) > u(H)$. Τότε υπάρχουν διαφορετικά $x, y \epsilon S$ τέτοια ώστε $x - y \epsilon H$.

Απόδειξη: Όπως είδαμε τα $\{h + T\}, h \epsilon H$ είναι ξένα ανα δύο και καλύπτουν τον $\mathbb{R}^n$. Επομένως τα $S \cap (h + T), h \epsilon H$ είναι ξένα και καλύπτουν το S δηλαδή

$$\mu(S) = \sum_{h \epsilon H} \mu(S \cap (h + T))$$

και ισχύει οτι $\mu(S \cap (h+T)) = \mu((-h+S)\cap T)$.
Εαν τα $S\cap(h_1+T)$ και $S\cap(h_2+T)$ είναι ξένα, δεν ισχύει οτι τα $(-h_1+S)\cap T$ και $(-h_2+S)\cap T$ είναι ξένα. Εαν υποθέταμε οτι ήταν ξένα θα είχαμε

$$u(H) = \mu(T) \geq \sum_{h\epsilon H} \mu((-h+S)\cap T) = \mu(S).$$

άτοπο. Επομένως υπάρχουν $h_1, h_2 \epsilon H$ τέτοια ώστε $(-h_1+S)\cap(-h_2+S)\cap T \neq 0$. Διαλέγουμε $x, y\epsilon S : -h_1 + x = -h_2 + y \Rightarrow x - y = h_1 - h_2 \epsilon H$.

Θεώρημα: Έστω H πλέγμα του $\mathbb{R}^n$ και S να είναι *Lebesgue* μετρήσιμο υποσύνολο του $\mathbb{R}^n$ το οποίο είναι συμμετρικό και κυρτό.
Εαν

1. $\mu(S) > 2^n u(H)$ ή
2. $\mu(S) \geq 2^n u(H)$ και S συμπαγές

Τότε, $S \cap (H\setminus\{0\}) \neq 0$

Απόδειξη:

1. Έστω $S' = 1/2S$, τότε $\mu(S') = 2^{-n}\mu(S) > u(H) \Rightarrow \exists y, z\epsilon S'$ τέτοια ώστε $y - z\epsilon H$. Το $y - z = 1/2(2y + (-2z))$ είναι κυρτός συνδυασμός των $2y, 2z$.
   $y\epsilon S' \Rightarrow 2y\epsilon S$ και $z\epsilon S' \Rightarrow -2z\epsilon S$, άρα $y - z\epsilon S$ και $y - z\epsilon H\setminus\{0\}$.

2. Εφαρμόζουμε το (1) στο $(1+1/m)S, m = 1, 2, \ldots$. Εφόσον το S είναι φραγμένο, το $(1+1/m)S$ είναι φραγμένο σύνολο, και περιέχει πεπερασμένο αριθμό στοιχείων του πλέγματος H. Άρα για κάθε θετικό ακέραιο m, $S_m = (1+1/m)S \cap (H\setminus\{0\})$ είναι διάφορο του κενού πεπερασμένο, επομένως συμπαγές υποσύνολο του $\mathbb{R}^n$. Εφόσον $S_{m+1} \subseteq S_m$ για κάθε m, τα σύνολα S_m δημιουργούν μια συγκλίνουσα ακολουθία, και επομένως $\cap_{m=1}^{\infty} S_m \neq \emptyset$. Εαν το $x\epsilon \cap_{m=1}^{\infty} S_m$, τότε $x\epsilon H\setminus\emptyset$ και $x\setminus(1+1/m)\epsilon S$ για κάθε m. Επειδή το S είναι κλειστό, αφήνουμε το $m\to\infty$ και παίρνουμε οτι $x\epsilon S$.

Θα δουλέψουμε στον $\mathbb{R}^n$, τα στοιχεία με δείκτες έως r_1 είναι στοιχεία στον $\mathbb{R}$, ενώ τα υπόλοιπα είναι στον $\mathbb{C}$, επίσης προφανώς $r_1 + 2r_2 = n$.
Το ενδιαφέρον μας είναι στο σύνολο

$$B_t = \{(y_1,\ldots,y_{r_1}, z_1,\ldots,z_{r_2})\epsilon\mathbb{R}^{r_1}\times\mathbb{C}^{r_2} : \sum_{i=1}^{r_1}|y_i| + 2\sum_{j=1}^{r_2}|z_j| \leq t\}, t\geq 0$$

.

Θα δείξουμε οτι ο όγκος του B_t δίνεται από το

$$V(r_1, r_2, t) = 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{t^n}{n!}$$

Απόδειξη: Με διπλή επαγωγή στα r_1, r_2.
Εαν τα $r_1 = 1$ και $r_2 = 0$, έχουμε $n = 1$, θα υπολογίσουμε το μήκος του $[-t, t]$, το οποίο είναι $2t$ όπως θέλουμε.
Εαν τα $r_1 = 0$ και $r_2 = 1$, έχουμε $n = 2$, θα υπολογίσουμε τον εμβαδόν του $\{z_1 : 2|z_1| \leq t\}$, ένας δίσκος με ακτίνα $t/2$. Το αποτέλεσμα είναι $\pi t^2/4$, όπως θέλουμε.
Υποθέτουμε οτι ο τύπος ισχύει για r_1, r_2 για κάθε t. Τότε $V(r_1 + 1, r_2, t)$ είναι ο όγκος του συνόλου με

$$|y| + \sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq t$$

ή ισοδύναμα,

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq t - |y|$$

Επομένως εαν $|y| > t$, τότε το B_t είναι κενό. Για μικρότερα $|y|$, εαν αλλάξουμε το $|y|$ σε $|y| + dy$, έχουμε ένα κουτί στο $(n + 1)$-διάστατο χώρο με dy μια από τις διαστάσεις του. Ο όγκος του κουτιού είναι $V(r_1, r_2, t - |y|)dy$. Επομένως, έχουμε

$$V(r_1 + 1, r_2, t) = \int_{-t}^{t} V(r_1, r_2, t - |y|)dy$$

το οποίο απο την υπόθεση επαγωγής είναι $2\int_0^t 2^{r_1}(\pi/2)^{r_2}[(t-y)^n/n!]dy = 2^{r_1+1}(\pi/2)^{r_2}t^{n+1}/(n+1)!$, όπως θέλουμε.
Τέλος, $V(r_1, r_2 + 1, t)$ είναι ο όγκος του

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| + 2|z| \leq t.$$

Αντίστοιχα,

$$V(r_1, r_2 + 1, t) = \int_{|z| \leq t/2} V(r_1, r_2, t - 2|z|)d\mu(z)$$

όπου μ είναι το μέτρο *Lebesgue* στον $\mathbb{C}$. Σε πολικές συντεταγμένες, το ολοκλήρωμα γίνεται

$$\int_{\theta=0}^{2\pi} \int_{r=0}^{t/2} 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{(t-2r)^n}{n!} r dr d\theta$$

το οποίο είναι $2^{r_1}(\pi/2)^{r_2}(2\pi/n!)\int_{r=0}^{t/2}(t-2r)^n r dr$ Με ολοκλήρωση κατά παράγοντες, έχουμε $V(r_1, r_2 + 1, t) = 2^{r_1}(\pi/2)^{r_2}(2\pi/n!)t^{n+2}/4(n + 1)(n + 2) = 2^{r_1}(\pi/2)^{r_2+1}t^{n+2}/(n + 2)!$. Το $n + 2$ είναι σωστό αφού $r_1 + 2(r_2 + 1) = r_1 + 2r_2 + 2 = n + 2$.

Ορισμός: Έστω L σώμα αριθμών βαθμού n πάνω από το $\mathbb{Q}$, και έστω $\sigma_1, \ldots, \sigma_n$ οι $\mathbb{Q}$-μονομορφισμοί του L στο $\mathbb{C}$. Εαν τα σ_i έχοθν σύνολο τιμών εξόλοκλήρου στο $\mathbb{R}$ λέμε οτι τα σ_i πραγματικούς αυτομορφισμούς, αλλιώς φανταστικούς. Εφόσον ο συζυγής ενός $\mathbb{Q}-$μονομορφισμού είναι $\mathbb{Q}-$μονομορφισμός, μπορούμε να απαριθμήσουμε τα σ_i έτσι ώστε οι πραγματικοί αυτομορφισμοί να είναι $\sigma_1, \ldots, \sigma_{r_1}$, και οι φανταστικοί αυτομορφισμοί να είναι $\sigma_{r_1+1}, \ldots, \sigma_n$, με σ_{r_1+j} να είναι ζευγαρωμένο με το συζυγές του

$\sigma_{r_1+r_2+j}, j = 1, \ldots, r_2$. Επομένως υπάρχουν $2r_2$ φανταστικοί αυτομορφισμοί και $r_1 + 2r_2 = n$.

Ο κανονικός αυτομορφισμός $\sigma : L \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \mathbb{R}^n$ δίνεται από το

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x))$$

.

Κάποιες πράξεις πινάκων που θα χρησιμεύσουν: Έστω $x_1, \ldots, x_n \epsilon L$ γραμμικά εξαρτημένα στον $\mathbb{Z}$, και έστω C ο πίνακας του οποίου η k-οστή στήλη είναι

$$\sigma_1(x_k), \ldots, \sigma_{r_1}(x_k), Re\sigma_{r_1+1}(x_k), Im\sigma_{r_1+1}(x_k), \ldots, Re\sigma_{r_1+r_2}(x_k), Im\sigma_{r_1+r_2}(x_k).$$

Θεωρούμε οτι

$$\begin{bmatrix} \sigma_j(x_k) \\ \overline{\sigma_j}(x_k) \end{bmatrix} = \begin{bmatrix} x + yi \\ x - yi \end{bmatrix}$$

Κρατάμε το j και αφήνουμε το k να κινείται από το 1 στο n.

Προσθέτουμε την δεύτερη σειρά στην πρώτη , και στη συνέχεια προσθέτουμε την πολλαπλασιασμένη με (-1/2) πρώτη σειρά στη δεύτερη και βγάζουμε κοινό παράγοντα το (-2i)

$$-2i \begin{bmatrix} x \\ y \end{bmatrix} = -2i \begin{bmatrix} Re\sigma_j(x_k) \\ Im\sigma_j(x_k) \end{bmatrix}$$

το κάνουμε αυτό για $j = 1, \ldots, r_2$.

επομένως έχουμε

$$detC = (2i)^{-r_2} det(\sigma_j(x_k))$$

Εαν το M είναι ελεύθερο $\mathbb{Z}-module$ που παράγεται απο τα x_i, έτσι ώστε το $\sigma(M)$ να ειναι ελεύθερο $\mathbb{Z}-module$ με βάση $\sigma(x_i), i = 1, \ldots, n$, δηλαδή πλέγμα στον $\mathbb{R}^n$, ο χώρος ειναι ένα παραλληλόγραμμο που οι πλευρές του ειναι $\sigma(x_i)$, και ο όγκος του ειναι η απόλυτη τιμή της διακρίνουσας της οποίας οι γραμμές ή οι στήλες είναι τα $\sigma(x_i)$. Επομένως

$$v(\sigma(M)) = |detC| = 2^{-r_2} |det\sigma_j(x_k)|.$$

Θα εφαρμόσουμε αυτό το αποτέλεσμα.

Πρόταση: Έστω B ο δακτύλιος ακεραίων ενός σώματος αριθμών L, και έστω I ένα μη μηδενικό ιδεώδες μη τετριμμένο του B, τέτοιο ώστε, το σ(I) να είναι πλέγμα στον $\mathbb{R}^n$. Τότε ο όγκος ενός στοιχειώδη χώρου στο πλέγμα είναι

$$u(\sigma(I)) = 2^{-r_2} |d|^{1/2} N(I)$$

συγκεκριμένα $u(\sigma(B)) = 2^{-r_2} |d|^{1/2}$, όπου d είναι η διακρίνουσα του σώματος.

Απόδειξη: Το αποτέλεσμα για $I = B$, βγαίνει από την προηγούμενη εφαρμογή, έχοντας τα x_k για βάση του B. Για το γενικό αποτέλεσμα, παρατηρούμε οτι ο στοιχειώδης χώρος του σ(I) μπορεί να γραφτεί ως ξένων N(I) ενώσεων του στοιχειώδη χώρου του σ(B).Για παράδειγμα, έστω e_1,e_2 τα διανύσματα βάσης, τότε το πλέγμα H′ παράγεται από τα $2e_1$,$3e_2$ είναι υποομάδα του H που παράγεται από τα e_1,e_2, αλλά ο στοιχειώδης χώρος T′ του H′ είναι μεγαλύτερος απο τον T του H. Συγκεκριμένα υπάρχουν ακριβώς 6 αντίγραφα του T που χωράνε μέσα στο T′.

Θεώρημα: Εαν το I ειναι μη τετριμμένο ιδεώδες του B, τότε το I περιέχει ένα μη μηδενικό στοιχείο x τέτοιο ώστε

$$|N_{L\setminus\mathbb{Q}}(x)| \leq (4/\pi)^{r_2}(n!/n^n)|d|^{1/2}N(I)$$

Απόδειξη: Το σύνολο B_t από πριν είναι συμπαγές κυρτό και συμμετρικό. Ο όγκος του είναι $\mu(B_t) = 2^{r_1}(\pi/2)^{r_2}t^n/n!$, με μ το μέτρο *Lebesgue*. Διαλέγουμε t έτσι ώστε $\mu(B_t) = 2^n u(\sigma(I))$, το οποίο είναι ίσο με $2^{n-r_2}|d|^{1/2}N(I)$, από την ισότητα των δύο εκφράσεων έχουμε

$$t^n = 2^{n-r_1}\pi^{-r_2}n!|d|^{1/2}N(I).$$

Εφαρμόζουμε τη σχέση $\mu(S) \geq 2^n u(H)$ και S συμπαγές τότε, $S \cap (H \setminus \{0\}) \neq 0$
. Για $H = \sigma(I)$ και $S = B_t$. Από την υποθεσή μας για το t η συνθήκη της σχέσης ικανοποιείται και έχουμε $S \cap (H \setminus \{0\}) \neq 0$. Επομένως υπάρχει μη μηδενικό στοιχειο $x\epsilon I$ τέτοιο ώστε $\sigma(x)\epsilon B_t$.
Η απόλυτη τιμή της νόρμας του x, είναι το γινόμενο των θετικών αριθμών $a_i = |\sigma_i(x)|, i = 1, \ldots, n$. Για να προσεγγίσουμε το $N(x)$, θα επικαλέσουμε την ανισότητα των αριθμητικών και γεωμετρικών μέσων, δηλαδή $(a_1 \ldots a_n)^{1/n} \leq (a_1 + \ldots + a_n)/n \Rightarrow a_1 \ldots a_n \leq \big(\sum_{i=1}^n a_i/n\big)^n$
Για τα δικά μας a_i έχουμε

$$|N(x)| \leq \Big(\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(x)| + \frac{2}{n}\sum_{i=r_1+1}^{r_1+r_2}|\sigma_i(x)|\Big)^n$$

Αφού $\sigma(x)\epsilon B_t$, έχουμε $|N(x)| \leq t^n/n^n$. Με επιλογή t,

$$|N(x)| \leq (1/n^n)2^{n-r_1}\pi^{-r_2}n!|d|^{1/2}N(I).$$

Όμως $n - r_1 = 2r_2$, τότε $2^{n-r_1}\pi^{-r_2} = 2^{2r_2}\pi^{-r_2} = (4/\pi)^{r_2}$.

Θεώρημα(Φράγμα *Minkowski* για νόρμες ιδεωδών): Κάθε κλάση ιδεωδών του L περιέχει ένα μη τετριμμένο ιδεώδες I τέτοιο ώστε

$$N(I) \leq (4/\pi)^{r_2}(n!/n^n)|d|^{1/2}.$$

Απόδειξη: Έστω J' κλασματικό ιδεώδες στη κλάση μας. Μπορούμε να πολλαπλασιάσουμε με ενα κύριο ιδεώδες του B, χωρίς να αλλάξουμε την κλάση ιδεωδών, επομένως μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας οτι το $J = (J')^{-1}$ είναι μη τετριμμένο ιδεώδες. Διαλέγουμε ένα μη μηδενικό στοιχείο $x\epsilon J$ τέτοιο ώστε το x να ικανοποιεί την προηγούμενη ανισότητα της νόρμας. Θέλουμε το $I = xJ'$.

Αρχικά το J είναι μη τετριμμένο αφού $x\epsilon J$ και $JJ' = B$. Το $(x) = IJ$, επομένως

$$N(I)N(J) = N(x) \leq (4/\pi)^{r_2}(n!/n^n)|d|^{1/2}N(J).$$

Διαγράφουμε το $N(J)$ και καταλήγουμε εκεί που θέλουμε.

Και τώρα στο ζητούμενο.

Θεώρημα: Η ομάδα κλάσης ιδεωδών ενός σώματος αριθμών είναι πεπερασμένη.

Απόδειξη: Υπάρχουν μόνο πεπερασμένα μη τετριμμένα ιδεώδη με μια συγκεκριμένη νόρμα. Και από το νόμο του $Minkowski$ μπορούμε να συσχετίσουμε κάθε κλάση ιδεωδών ως ένα μη τετριμμένο ιδεώδες όπου η νόρμα του είναι φραγμένη από μια σταθερά. Εαν η ομάδα κλάσης ιδεωδών είναι άπειρη, θα χρησιμοποιούσαμε εν τέλει το ίδιο μη τετριμμένο ιδεώδες σε δύο διαφορετικές κλάσεις , το οποίο είναι άτοπο.

Έστω οτι το φράγμα $Minkowski$, M_K είναι μικρότερο από 2. Εφόσον το μόνο ιδεώδες νόρμας 1 είναι το τετριμμένο (1)=B, κάθε κλάση ιδεωδών πρέπει να περιέχει το (1). Έτσι υπάρχει μόνο μια κλάση ιδεωδών. Θα αποδείξουμε οτι αυτό σημαίνει οτι είμαστε σε περιοχή κυρίων ιδεωδών

Εαν η ομάδα κλάσης ιδεωδών $C(R)$ είναι τετριμμένη , τότε κάθε μη τετριμμένο ιδεώδες I στον δακτύλιο R ειναι κύριο κλασματικό ιδεώδες Rx για $x \epsilon K$, με K σώμα πηλίκων . Όμως το $I \subseteq R$, επομένως το $x = 1x$ πρέπει να ανήκει στο R, το οποίο αποδεικνύει οτι το R είναι περιοχή κύριων ιδεωδών.
Αντίστροφα, εαν το R είναι περιοχή κύριων ιδεωδών και I είναι μη μηδενικό κλασματικό ιδεώδες, τότε $rI \subseteq R, r \epsilon R$. Από υπόθεση, το μη τετριμμένο ιδεώδες rI πρέπει να είναι κύριο, επομένως $rI = Ra, a \epsilon R$. Και έτσι $I = R(a/r), (a/r) \epsilon K$, καταλήγουμε οτι κάθε μη μηδενικό κλασματικό ιδεώδες του R είναι κύριο κλασματικό ιδεώδες.

Εφαρμογή: για πραγματικά τετραγωνικά σώματα $n = 2, r_2 = 0 \Rightarrow M_K = \frac{1}{2}\sqrt{|D|}$
για φανταστικά τετραγωνικά σώματα $n = 2, r_2 = 1 \Rightarrow M_K = \frac{2}{\pi}\sqrt{|D|}$

Εαν το $M_K < 2 \Rightarrow$ η ομάδα κλάσεων είναι τετριμμένη, δηλάδη είμαστε σε περιοχή κύριων ιδεωδών.

1. για πραγματικα τετραγωνικά σώματα $M_K < 2 \Rightarrow |D| < 16$
2. για φανταστικά τετραγωνικά σώματα $M_K < 2 \Rightarrow |D| < \pi^2$

Σε τετραγωνικά σώματα $K = \mathbb{Q}[\sqrt{d}]$ η διακρίνουσα είναι η εξής $D = d$ αν $d = 1mod4$, ή $D = 4d$ αλλιώς.
άρα τα επόμενα τετραγωνικά σώματα έχουν αριθμό κλάσης 1:

$$\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}], \mathbb{Q}[\sqrt{5}], \mathbb{Q}[\sqrt{13}], \mathbb{Q}[\sqrt{i}], \mathbb{Q}[\sqrt{-2}], \mathbb{Q}[\sqrt{-3}], \mathbb{Q}[\sqrt{-7}]$$

.

Κεφάλαιο 3

Εφαρμογή σε τετραγωνικά σώματα

Για έναν ακέραιο ελεύθερο τετραγώνων $d \neq 1$, θεωρούμε

$$K = \mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y\epsilon\mathbb{Q}\}$$

.
Το K είναι τετραγωνικό σώμα και έχει βαθμό 2 πάνω από το $\mathbb{Q}$.

3.1 Νόρμα, ίχνος και συζυγία

Μαζί με τις υπόλοιπες βασικές πράξεις που υπάρχουν σε ένα τετραγωνικό σώμα, υπάρχει και η συζυγία. Μιλάμε για τη γενίκευση της μιγαδικής συζυγίας. Για $a = x + y\sqrt{d}\epsilon K$, θεωρούμε το συζυγές του

$$\overline{a} = x - y\sqrt{d}$$

Είναι εύκολο να αποδειχθούν τα εξής:

$$\overline{a+b} = \overline{a} + \overline{b}, \overline{ab} = \overline{a}\overline{b}, \overline{\overline{a}} = a$$

.

Επίσης είναι προφανές πως $\overline{a} = a \Leftrightarrow a\epsilon\mathbb{Q}$.

Ορισμός: Για $a\epsilon K$, ορίζουμε το ίχνος $Tr(a) = a + \overline{a}$ και τη νόρμα $N(a) = a\overline{a}$.

Άμμεσο είναι πως το ίχνος διατηρεί την πρόσθεση και η νόρμα τον πολλαπλασιασμό. $Tr(a+b) = Tr(a) + Tr(b), N(ab) = N(a)N(b)$.

Επομένως κάθε $a\epsilon K$ είναι η ρίζα μονικού πολυωνύμου βαθμού 2 , με ρητούς συντελεστές

$$(x-a)(x-\overline{a}) = x^2 - (a+\overline{a})x + a\overline{a} = x^2 - Tr(a)x + N(a)$$

.

Άρα εάν τα $Tr(a)$, $N(a)$ ανήκουν στο $\mathbb{Z}$ τότε το a είναι ακέραιος πάνω από το $\mathbb{Z}$.

Είχαμε ορίσει τους δακτύλιους ακεραίων για τετραγωνικές επεκτάσεις στο προηγούμενο κεφάλαιο. Ο δακτύλιος ακεραίων του Κ ήταν ο εξής: $O_K = \mathbb{Z}[\sqrt{d}]$, για $d \neq 1 mod 4$, ενώ για $d = 1 mod 4$ έχουμε $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Θεώρημα: Εάν το $a \epsilon O_K$, τότε το $\overline{a} \epsilon O_K$.

Απόδειξη: Είναι άμμεσο αφού έχουν το ίδιο ίχνος και νόρμα.

3.2 Παραγοντοποίηση στοιχείων τετραγωνικών σωμάτων

Θεώρημα: Έστω $O_K^x = \{a \epsilon O_K | N(a) = \pm 1\}$ και $O_K^x \cap \mathbb{Q} = \{\pm 1\}$

Απόδειξη: Έστω $a \epsilon O_K$.
Εαν το a είναι μονάδα (έχει αντίστροφο), τότε $ab = 1$ για κάποιο $b \epsilon O_K$. Παίρνουμε νόρμες και έχουμε $N(a)N(b) = N(1) = 1$ στο $\mathbb{Z}$, επομένως $N(a) = \pm 1$.
Αντίστροφα, θεωρούμε πως $N(a) = \pm 1$, εφόσον έχουμε $N(a) = a\overline{a} \Rightarrow a\overline{a} = \pm 1$. Άρα το $\pm \overline{a}$ είναι αντίστροφο του a, και βρισκεται στο O_K.
Για να δείξουμε οτι $O_K^x \cap \mathbb{Q} = \{\pm 1\}$ η πλευρά $\supset$ είναι προφανής. Για την άλλη πλευρά, έστω $q \epsilon O_K^x \cap \mathbb{Q}$. Τότε $N(q) = \pm 1$, αφού το $q \epsilon O_K^x$, επομένως $q^2 = \pm 1$ γιατί το q είναι ρητός, επομένως $q = \pm 1$.

Θεώρημα: Εαν η νόρμα του $a \epsilon O_K$ είναι πρώτος στο $\mathbb{Z}$ τότε το a δεν αναλύεται στο O_K.

Απόδειξη: Έστω $a = bc$ με $b, c \epsilon O_K$. Τότε παίρνοντας τις νόρμες $N(a) = N(b)N(c)$ στο $\mathbb{Z}$. Το $N(a)$ είναι πρώτος, επομένως ή το $N(b)$ ή το $N(c)$ είναι ± 1. Επομένως ένα από τα δύο είναι μονάδα στο O_k. Επομένως το a δεν έχει μη τετριμμένη ανάλυση στο O_k.

Βέβαια το αντίστροφο δεν ισχύει , ας δούμε ένα παράδειγμα.

Παράδειγμα: Στο $\mathbb{Z}[\sqrt{-14}], N(3) = 9$ δεν ειναι πρώτος στο $\mathbb{Z}$. Το 3 όμως δεν αναλύεται στο $\mathbb{Z}[\sqrt{-14}]$. Έστω οτι $3 = ab$ στο $\mathbb{Z}[\sqrt{-14}]$. Τότε $9 = N(a)N(b)$ στο $\mathbb{Z}$.Οι νόρμες των a, b πρέπει να είναι 3 γιατί αν ήταν 1 ,θα ήταν μονάδες. Το $3 = a^2 + 14b^2$ δεν έχει λύση όμως στο $\mathbb{Z}$, επομένως δεν ύπάρχουν στοιχεία με νόρμα 3.

Παράδειγμα: Η νόρμα του $1 + \sqrt{-14}$ είναι 15, που δεν είναι πρώτος στο $\mathbb{Z}$. Όμως το $1 + \sqrt{-14}$ δεν αναλύεται στο $\mathbb{Z}[\sqrt{-14}]$. Αν γράψουμε το $1 + \sqrt{-14} = ab$ και πάρουμε νόρμες $15 = N(a)N(b)$ στο $\mathbb{Z}$. Όμως τα 3,5 δεν είναι νόρμες στο $\mathbb{Z}[\sqrt{-14}]$,ένα πρέπει να έχει νόρμα ± 1, άρα ένα από τα a, b είναι μονάδα.

Θεώρημα: Κάθε μη μηδενικό, που δεν είναι μονάδα στοιχείο του O_k είναι γινόμενο ανάγωγων στοιχειων του O_k.

Απόδειξη: Έστω a στο O_k θα χρησιμοποιήσουμε επαγωγή.

1. Για $|N(a)| = 2$ το a έχει νόρμα πρώτο επομένως δεν αναλύεται και επομένως η ελάχιστη παραγοντοποίηση του είναι ο εαυτός του.

2. Για $N(a) = n \geq 3$ και για κάθε στοιχείο με νόρμα από 2 έως $n-1$, υποθέτουμε πως ισχύει οτι αναλύεται.
Εαν το a αναλύεται τότε μπορούμε να γράψουμε $a = bc$ όπου b, c δεν είναι μονάδες. Επομένως τα $|N(b)|, |N(c)|$, είναι μικρότερα από το $|N(a)|$, από την υπόθεση της επαγωγής έχουμε
$$b = p_1 \dots p_r, c = p_1', \dots, p_{r'}'$$
με p_i, p_j' δεν αναλύονται στο O_k. Επομένως και το a γράφεται ως γινόμενο στοιχείων που δεν αναλύονται.

Το πρόβλημα της διπλωματικής εστιάζεται εδώ, πως όταν φεύγουμε από τον $\mathbb{Z}$ χάνουμε την μοναδική ανάλυση σε πρώτους, ένα στοιχείο στον O_k μπορεί να αναλύεται μοναδικά μπορεί και όχι.

Παράδειγμα: Στον $\mathbb{Z}[\sqrt{-14}]$,

1. το 15 αναλύεται με δύο διαφορετικούς τρόπους
$$3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$$

2. σε αυτό το παράδειγμα βλέπουμε οτι 4 αναλλοίωτοι όροι αντιστοιχούν σε 2 αναλλοίωτους όρους
$$3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$$

Είναι εύκολο να ελένξουμε οτι οι όροι $5 \pm 2\sqrt{-14}$ δεν αναλύωνται. $N(5+2\sqrt{-14} = 81$ γράφεται ως κάποιο γινόμενο των 3,9,27. Δεν υπάρχει όμως στοιχείο με νόρμα 3 ή 27, και τα στοιχεία με νόρμα 9 είναι τα ± 3 τα οποία δεν είναι παράγοντες του $5+2\sqrt{-14}$. Αντίστοιχα για το $5-2\sqrt{-14}$.

Θα επιδιώξουμε λοιπόν να αντικαταστήσουμε την μη μοναδική παραγοντοποίηση στοιχείων, με μοναδική παραγοντοποίηση ιδεωδών.

3.3 Ιδεώδη σε τετραγωνικά σώματα

Όπως ξέρουμε από το προηγούμενο κεφάλαιο, σε ένα *Dedekind* δακτύλιο, επειδή είναι της *Noether*, τα ιδεώδη του είναι πεπερασμένα παραγώμενα.

Θεώρημα: Στη συγκεκριμένη περίπτωση, κάθε ιδεώδες του O_k είναι πεπερασμένα παραγώμενο, με το πολύ δύο γεννήτορες.

Απόδειξη: Ένα ιδεώδες του O_k είναι υποομάδα του O_k. Ως προσθετική ομάδα $O_k \cong \mathbb{Z}^2$.Επομένως από ταξινόμηση πεπερασμένα παραγώμενων αβελιανών ομάδων, κάθε υποομάδα του O_k είναι 0 ή ισόμορφη με το $\mathbb{Z}$ ή με το $\mathbb{Z}^2$. Αυτό δείχνει οτι ένα ιδεώδες του O_k στη συγκεκριμένη περίπτωση τετραγωνικών σωμάτων, έχει το πολύ 2 γεννήτορες ως $\mathbb{Z} - module$.

Για ένα πεπερασμένο σύνολο στοιχείων του O_k, $a_1, \ldots, a_m$, το ιδεώδες που παράγεται συμβολίζεται με $(a_1, \ldots, a_m)$

Παράδειγμα: Στον $\mathbb{Z}[\sqrt{-14}]$, ϑα δείξουμε οτι

$$(17 + 2\sqrt{-14}, 20 + \sqrt{-14}) = (3 - \sqrt{-14})$$

Στον $\mathbb{Z}[\sqrt{-14}]/(3-\sqrt{-14})$, $\sqrt{-14} = 3$, επομένως $-14 = 9$ καί $23 = 0$. Άρα έχουμε $17+2\sqrt{-14} = 17+6 = 0, 20+\sqrt{-14} = 23 = 0$. Το $(3-\sqrt{-14})$ διαιρεί τα $(17+2\sqrt{-14}), (20+\sqrt{-14})$. Και επομένως το ίδεωδες στα δεξιά περιέχεται σε αυτο στα αριστερά.
Αντίστοιχα, στο $\mathbb{Z}[\sqrt{-14}]/(17 + 2\sqrt{-14}, 20 + \sqrt{-14})$ έχουμε $\sqrt{-14} = -20, 17 = -2\sqrt{-14}$ δηλαδή $17 = 40, 23 = 0$. Το $3 - \sqrt{-14} = 23 = 0$. Επομένως αποδείξαμε το ζητούμενο.

Παράδειγμα: Μια άλλη εφαρμογή είναι να δείξουμε οτι το $(2, \sqrt{-14})$ δεν είναι κύριο.

Έστω πως $(2, \sqrt{-14}) = (a)$. Τότε, αφού το $2\epsilon(2, \sqrt{-14})$, έχουμε οτι $2\epsilon(a)$, άρα $a|2$ στο $\mathbb{Z}[\sqrt{-14}]$. Γράφοντας $2 = ab$ και παίρνοντας νόρμες $4 = N(a)N(b)$ στο $\mathbb{Z}$, επομένως $N(a)|4$. Αντίστοιχα $\sqrt{-14}\epsilon(a)$, και επομένως $N(a)|14$ στο $\mathbb{Z}$.
Εφόσον το $N(a)$ διαιρεί τα 2 και 14, $N(a) = 1$ ή 2. Όμως $N(a) = x^2 + 14y^2$ δεν είναι ποτέ 2. Άρα $N(a) = 1$, και $(a) = 1$, ή $1\epsilon(2, \sqrt{-14})$ άτοπο.

Θεώρημα: Έστω $a = (a_1, \ldots, a_m)$ καί $b = (b_1, \ldots, b_n)$ δύο ιδεώδη του O_k. Τότε τα επόμενα είναι ισοδύναμα:

1. $a \subset b$,
2. κάθε a_i βρίσκεται στο b,
3. κάθε a_i είναι ένας O_k-γραμμικός συνδυασμός των b_j.

Απόδειξη: Τα $(1) \Rightarrow (2) \Rightarrow (3)$ επάγονται άμμεσα.
Εαν κάθε a_i είναι ένας O_k-γραμμικός συνδυασμός των b_j, τότε κάθε a_i βρίσκεται μέσα στο b, επομένως κάθε O_k-γραμμικός συνδυασμός των a_i βρίσκεται μέσα στο b.

Πρόταση: Επομένως, έπεται άμμεσα οτι $a = b$ αν και μόνο αν κάθε a_i είναι O_k-γραμμικός συνδυασμός των b_j, καί κάθε b_j είναι O_k-γραμμικός συνδυασμός των a_i

Παραδείγματα:

1. για a_1, a_2 στο O_k, $(a_1, a_2) = (a_1, a_2 + ca_1)$ για κάθε c στο O_k.
2. στο $\mathbb{Z}[\sqrt{-14}]$,
   (α) $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14})$
   Αντίστοιχα όπως πρίν στο $\mathbb{Z}[\sqrt{-14}]/(2 + \sqrt{-14}, 7 + 2\sqrt{-14})$ έχουμε $\sqrt{-14} = -2$ καί $0 = 7 + 2\sqrt{-14} = 3$.
   Άρα $1 - \sqrt{-14} = 1 - (-2) = 3 = 0$. Και επομένως το $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) \supset (3, 1 - \sqrt{-14})$. Ανάλογα δουλέυουμε για το ανάποδο.

(β) $(2, 1+\sqrt{-14}) = (1)$.
στον $\mathbb{Z}[\sqrt{-14}]/(2, 1+\sqrt{-14})$ έχουμε $2 = 1+\sqrt{-14} \Rightarrow \sqrt{-14} = 1 \Rightarrow 15 = 0$. Επίσης $2 = 0 \Rightarrow 14 = 0 \Rightarrow 15 - 14 = 1 = 0$. Άρα $(2, 1+\sqrt{-14}) = \mathbb{Z}[\sqrt{-14}] = (1)$.

Θεώρημα: Εαν ένα ιδεώδες στο O_k περιέχει δύο στοιχεία του $\mathbb{Z}$ τα οποία είναι σχετικά πρώτα τότε το ιδεώδες είναι το τετριμμένο O_k. Συγκεκριμένα, ένα ιδεώδες είναι το τετριμμένο ιδεώδες εαν περιέχει δύο στοιχεία των οποίων η νόρμες είναι πρώτες μεταξύ τους.

Απόδειξη: Έστω A ένα ιδεώδες και a, b στοιχεία του A τα οποία είναι στον $\mathbb{Z}$ καί είναι σχετικά πρώτα. Μπορούμε να γράψουμε $1 = ax + by$ για κάποια $x, y \epsilon \mathbb{Z}$. Η δεξιά πλευρά ανήκει στο A επομένως μπορούμε να γράψουμε $1 \epsilon A$ άρα $A = (1)$.
Αφού η νόρμα κάθε $a \epsilon A$ είναι και αυ'τη στο A, δυο σχετικά πρώτες νόρμες στοιχείων του A είναι οι ίδιες στοιχεία του A. Άρα $A = (1)$.

Θεώρημα: Κάθε ιδεώδες στο O_k που έχει σύνολο γεννητόρων από το $\mathbb{Z}$, είναι κύριο ιδεώδες.

Απόδειξη: Έστω $a = (a_1, \ldots, a_m)$ με $a_i \epsilon \mathbb{Z}$. Έστω d ο μέγιστος κοινός διαιρέτης των a_i, τότε κάθε στοιχείο του a διαιρείται από το d στο O_k. Επομένως $a \subset (d)$. Αντίστροφα, ο $\mathbb{Z}$ όπως ξέρουμε είναι περιοχή κύριων ιδεωδών, επομένως μπορούμε να γράψουμε $d = c_1 a_1 + \ldots + c_m a_m$ για κάποια $c_i \epsilon \mathbb{Z}$. Επομένως οποιοδήποτε O_k-πολλαπλάσιο του d είναι O_k-γραμμικός συνδιασμός των a_i. Άρα $(d) \subset a \Rightarrow (d) = a$.

Θεώρημα: Για a, b στο O_k, τα $(a) = (b)$ αν και μόνο αν, τα a, b είναι ίσα πολλαπλάσιάζοντας τα με κάποια μονάδα στο O_k.

Απόδειξη: $(a) = (b) \Rightarrow a|b$ και $b|a$, από το οποίο έπεται άμμεσα αυτό που θέλουμε.

Τώρα θα ορίσουμε πράξεις ιδεωδών,

Υπενθύμιση: Για ιδεώδη a, b στο O_K, το γινόμενο ab είναι το σύνολο όλων των αθροισμάτων

$$\sum_{k=1}^{r} x_k y_k, r \geq 1, x_k \epsilon a, y_k \epsilon b$$

.

Θεώρημα: Για $a = (a_1, \ldots, a_m)$ και $b = (b_1, \ldots, b_n)$, τότε $ab = (a_1 b_1, \ldots, a_i b_j, \ldots, a_m b_n)$. Συγκεκριμένα $(a)(b) = (ab)$.

Απόδειξη: Κάθε στοιχείο του ab έχει μορφή $x_1 y_1 + \ldots + x_r y_r$ με $x_k \epsilon a, y_k \epsilon b$. Μπορούμε να γράψουμε κάθε x_k ως O_k-γραμμικό συνδυασμό των a_i και αντίστοιχα τα y_k ως O_k-γραμμικό συνδυασμό των b_j. Επομένως το $x_k y_k$ είναι O_k-γραμμικός συνδυασμός των $a_i b_j$. Και το άθροισμα τους είναι επίσης O_k-γραμμικός συνδυασμός των $a_i b_j$, άρα $ab \subset (a_1 b_1, \ldots, a_i b_j, \ldots, a_m b_n)$.
Αντίστροφα, κάθε στοιχείο αυτού του ιδεωδώς είναι ένας O_k-γραμμικός συνδυασμός των $a_i b_j$, δηλαδή

ένα άθροισμα της μορφής

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}a_ib_j$$

. Με $c_{ij}\epsilon O_k$. Αφού τα $c_{ij}a_i\epsilon a$ και $b_j\epsilon b$ το προηγούμενο άθροισμα είναι της μορφής $\sum_{k=1}^{r} x_ky_k, r \geq 1, x_k\epsilon a, y_k\epsilon b$.

Παράδειγμα: Στον $\mathbb{Z}[\sqrt{-14}]$. Έστω $a = (5+\sqrt{-14}, 2+\sqrt{-14})$ και $b = (4+\sqrt{-14}, 2-\sqrt{-14})$. Το $ab = (5+\sqrt{-14}, 2+\sqrt{-14})(4+\sqrt{-14}, 2-\sqrt{-14}) = (6+9\sqrt{-14}, -6+6\sqrt{-14}, 24-3\sqrt{-14}, 18)$

Πρόταση: Για ιδεώδη a, b το $ab = (0)$, αν και μόνο αν $a = (0)$ ή $b = (0)$.

Απόδειξη: Εαν $(a) = 0(b) = 0$ τότε $(ab) = 0$, από το προηγούμενο θεώρημα. Εαν $(a) \neq 0$ καί $(b) \neq 0$, τότε το a έχει μη μηδενικό στοιχείο x και το b έχει μη μηδενικό y αντίστοιχα. Τότε το ab περιέχει το xy άρα $ab \neq 0$.

Στον πολλαπλασιασμό ιδεωδών ισχύουν η αντιμεταθετικότητα και η προσεταιριστικότητα της πρόσθεσης.

Πρόταση: Για ιδεώδες $a = (a_1, \ldots, a_m)$ και κύριο ιδεώδες (c) , τότε επάγεται έυκολα οτι

$$(c)a = (ca_1, ca_2, \ldots, ca_m)$$

.

Παράδειγμα: Είχαμε δείξει προηγουμένος οτι το $(2, \sqrt{-14})$ στο $\mathbb{Z}[\sqrt{-14}]$ δεν είναι κύριο. Θα το δειξουμε με διαφορετικό τρόπο τώρα,

$$(2, \sqrt{-14})^2 = (2, \sqrt{-14})(2, \sqrt{-14}) = (4, 2\sqrt{-14}, -14) = (2)(2, \sqrt{-14}, -7)$$

.
Όμως τα 2 και 7 είναι σχετικά πρώτα στο $\mathbb{Z}$, επομένως άμμεσα

$$(2, \sqrt{-14})^2 = (2)(1) = (2)$$

.
Εαν $(2, \sqrt{-14}) = (a)$ τότε $(2) = (a)^2 = (a^2) \Rightarrow a = \pm 2$. Παίρνουμε νόρμες $N(a)^2 = 4 \Rightarrow N(a) = 2$. Δεν υπάρχει στοιχείο στον $\mathbb{Z}[\sqrt{-14}]$ με νόρμα 2, επομένως άτοπο.

Ορισμός: Για ένα ιδεώδες A, το συζυγές του ιδεώδες είναι το $\overline{A} := \{\overline{a} : a\epsilon A\}$.

Θεώρημα: Εαν $a = (a_1, \ldots, a_m)$ τότε $\overline{a} = (\overline{a_1}, \ldots, \overline{a_m})$. Συγκεκριμένα, αν το $c = (k)$ είναι κύριο ιδεώδες, το $\overline{c} = (\overline{k})$ είναι επίσης κύριο.
Για κάθε ιδεώδη a, b ισχύει το εξής $\overline{ab} = \overline{a}\overline{b}$ και $\overline{\overline{a}} = a$.
οι αποδείξεις επάγονται άμμεσα απο τους ορισμούς.

Παραδείγματα:

1. Οταν ένας στοιχείο του O_k είναι ίσο με το συζυγές του , ανήκει στο $\mathbb{Z}$, αλλά αυτό δεν επεκτείνεται στα ιδεώδη. Όταν ένα ιδεώδες είναι ίσο με το συζυγές του δεν σημαίνει απαραίτητα οτι οι γεννήτορες του είναι από το $\mathbb{Z}$.
   Στον $\mathbb{Z}[\sqrt{-14}]$,το $\overline{(2, \sqrt{-14})} = (2, -\sqrt{-14}) = (2, \sqrt{-14})$. το ιδεώδες είναι ίσο με το συζυγές του αλλά δεν έχει γεννήτορες από το $\mathbb{Z}$ αλλώστε αν είχε θα ήταν κύριο όπως είχαμε αποδείξει.

2. Θα δείξουμε οτι το $(3, 1+\sqrt{-14})$ στο $\mathbb{Z}[\sqrt{-14}]$ δεν είναι κύριο και δεν είναι και ίσο με το συζυγές του.
   Αρχικά παρατηρούμε οτι

   $$(3, 1+\sqrt{-14})(3, 1-\sqrt{-14}) = (9, 3-3\sqrt{-14}, 3+3\sqrt{-14}, 15) = (3)(3, 1-\sqrt{-14}, 1+\sqrt{-14}, 5).$$

   Το 3 και 5 είναι σχετικά πρώτα μεταξύ τους επομένως

   $$(3, 1+\sqrt{-14})(3, 1-\sqrt{-14}) = (3)$$

   Εαν το ιδεώδες μας είναι κύριο , έχουμε

   $$(a)(\overline{a}) = (3)) \Rightarrow (a\overline{a}) = (N(a)) = (3) \Rightarrow N(a) = \pm 3$$

   . Όμως στο $\mathbb{Z}[\sqrt{-14}]$ δεν υπάρχει στοιχείο με νόρμα 3. Άρα το ιδεώδες μας δεν μπορεί να είναι κύριο.

   Για να δέιξουμε οτι το $(3, 1+\sqrt{-14})$ δεν είναι ίσο με το συζυγές του , υποθέτουμε πως είναι τότε

   $$(3, 1+\sqrt{-14})^2 = (3)$$

   .
   Όμως $(3, 1+\sqrt{-14})^2 = (9, 3+3\sqrt{-14}, -13+2\sqrt{-14})$ Αυτό δεν μπορεί να είναι (3) αφού το $-13+2\sqrt{-14} \not\in (3)$

Τέλος θα μιλήσουμε λίγο για τη διαιρετότητα ιδεώδων.

Ορισμός: Θέτουμε $a|b$ εαν $b = ac$ για κάποιο ιδεώδες c.

Θεώρημα: Για a, b στο O_k, έχουμε $(a)|(b)$ αν και μόνο αν $a|b$.

Απόδειξη: Υποθέτουμε $a|b$ στο O_k. Εξ' ορισμού $b = ac$ για κάποιο $c \epsilon O_k$, επομένως $(b) = (ac) = (a)(c) \Rightarrow (a)|(b)$.
Αντίστροφα, εαν $(a)|(b)$ τότε $(b) = (a)C$ για κάποιο ιδεώδες C. Γράφουμε $C = (c_1, \ldots, c_r)$, επομένως

$$(b) = (ac_1, \ldots, ac_r)$$

τότε το b είναι O_k-γραμμικός συνδυασμός των γινομένων ac_k:

$$b = \sum_{k=1}^{r} d_k a c_k = a \sum_{k=1}^{r} d_k c_k,$$

άρα $a|b$ στο O_k.

Θεώρημα: Για $a \epsilon O_k$ και ιδεώδες $b = (b_1, \ldots, b_m)$ στο O_k, τα επόμενα είναι ισοδύναμα:

1. $(a)|b$
2. $a|b_j$ για κάθε j
3. $(a) \supset b$

Απόδειξη: Εαν $(a)|b$ τότε $b = (a)c$ για κάποιο ιδεώδες c. Άρα $b = (ac_1, \ldots, ac_n)$. Κάθε στοιχείο του b διαιρείται από το a. Επομένως $b_j \epsilon (a)$ για κάθε j, άρα $b \supset (a)$. Μπορούμε να γράψουμε κάθε b_j σαν πολλαπλάσιο του a άρα το b έχει το ιδεώδες (a) ως παράγοντα.

Θεώρημα: Για ιδεώδη a, b, εαν $a|b$ τότε $a \supset b$. Συγκεκριμένα, εαν $a|b$ και το $b|a$ τότε $a = b$.

Απόδειξη: Υποθέτουμε οτι $a|b$, τότε $b = ac$. Τα ιδεώδη είναι $O_k - modules$, άρα $ac \subset a$.

Επομένως, σε αυτή την παράγραφο με τα ιδεώδη έχουμε αντικαταστίσει τον πολλαπλασιασμό και την διαίρεση στοιχείων του O_k, σε πολλαπλασιασμό και διαίρεση ιδεωδών στο O_k. Αυτές οι πράξεις των ιδεωδών μέχρι τώρα αντικατοπτρίζονται στις πράξεις των γεννητόρων. Προσπαθούμε λοιπόν να αντικαταστήσουμε τα στοιχεία με ιδεώδη για να διατηρήσουμε τη μοναδική παραγοντοποίηση τών στοιχείων που χάνεται.

Παραδείγματα:

1. Έστω $p = (3, 1 + \sqrt{-14})$ και $q = (5, 1 + \sqrt{-14})$. Στα προηγούμενα παραδείγματα είδαμε οτι $(3) = p\overline{p}$, με τον ίδιο τρόπο μπορούμε να δούμε οτι $(5) = q\overline{q}$, $pq = (1 + \sqrt{-14})$, και, $\overline{pq} = (1 - \sqrt{-14})$
   Τότε το κύριο ιδεώδες (15) μπορεί να αναλυθεί σε

   $$(15) = (3)(5) = p\overline{p}q\overline{q}$$

   και επίσης ως

   $$(15) = (1 + \sqrt{-14})(1 - \sqrt{-14}) = pq\overline{pq}$$

   Όσο μιλάμε για το στοιχείο 15, βλέπουμε οτι δεν αναλύεται μοναδικά. Αν αντικαταστήσουμε όμως τα στοιχεία από τα κύρια ιδεώδη, τα $(3), (5), (1 \pm \sqrt{-14})$ αναλύονται σε ιδεώδη p, q.

2. Στο $\mathbb{Z}[\sqrt{-14}]$, το $2 \cdot (-7) = \sqrt{-14}^2$, είναι τέλειο τετράγωνο ένω τα 2,-7 δεν έχουν κοινό διαιρέτη.
   Αυτό αν περάσουμε σε ιδεωδη εξηγείται, $a = (2, \sqrt{-14}), b = (7, \sqrt{-14})$, τότε $(2) = a^2$ και $(-7) = (7) = b^2$ και
   $$ab = (14, 2\sqrt{-14}, 7\sqrt{-14}, -14) = (\sqrt{-14})(\sqrt{-14}, 2, 7, \sqrt{-14}) = (\sqrt{-14})$$
   .

Ο κύριος μας στόχος είναι να παραγοντοποιήσουμε μοναδικά τα ιδεώδη του O_k σε πρώτα ιδεώδη, το επόμενο μας βήμα θα είναι να βρούμε την αναλογία του νόμου διαγραφής τον μη μηδενικών ακεραίων με τα ιδεώδη.

3.4 Απαλείφοντας Ιδεώδη

Ορισμός: Ένα ιδεώδες c στο O_k ονομάζεται απαλείψιμο αν όποτε $ac = bc$ για ιδεώδη a, b στο O_k έχουμε $a = b$.

Θεώρημα: Μη μηδενικά κύρια ιδεώδη είναι απαλείψιμα. Δηλαδή για μη μηδενικό c στο O_k και ιδεώδη a, b, εαν $a(c) = b(c)$ τότε $a = b$.

Απόδειξη: Θα δειξουμε οτι $a \subset b$. Το ανάποδο το χειριζόμαστε παρόμοια.
Δεν είναι δύσκολο να δούμε οτι το $a(c) = ca$ είναι το σύνολο των πολλαπλάσιων των a με το c. Αφού μπορούμε να απλοποιήσουμε το c ως κοινό παράγοντα, οι σχέσεις $ca = cb$ και $a = b$ είναι ισοδύναμες.

Πρόταση: Κάθε ιδεώδες στο O_k με μη μηδενικό κύριο πολλαπλάσιο είναι απαλείψιμο.

Απόδειξη: Έστω c ένα ιδεώδες με μη μηδενικό κύριο πολλαπλάσιο, δηλαδή $cc' = (\gamma)$ με $\gamma \neq 0$. Τότε εαν $ac = bc$, πολλαπλασιάζοντας και τις δύο πλευρές με c' για να πάρουμε $a(\gamma) = b(\gamma)$, τότε $a = b$

Αποδεικνύεται οτι κάθε μη μηδενικό ιδεώδες στο O_k έχει μη μηδενικό κύριο πολλαπλάσιο, επομένως στο O_k κάθε μη μηδενικό ιδεώδες είναι απαλείψιμο.

Θεώρημα: Για κάθε ιδεώδες a στο O_k, το γινόμενο $a\overline{a}$ είναι κύριο ιδεώδες.
Θα το αποδείξουμε στη συνέχεια (*)

Παράδειγμα: Έχουμε δειξει οτι όταν $d = 1 mod 4$, τότε $O_k \neq \mathbb{Z}[\sqrt{d}]$, έχουμε την ισότητα των ιδεωδών στο $\mathbb{Z}[\sqrt{d}]$:
$$(2, 1 + \sqrt{d})(2, 1 + \sqrt{d}) = (4, 2(1 + \sqrt{d})) = (2)(2, 1 + \sqrt{d})$$

Από το προηγούμενο θεώρημα και το λήμμα, έχουμε οτι το $(2, 1 + \sqrt{d})$ ειναι απαλείψιμο. Αλλά τότε θα είχαμε
$$(2, 1 + \sqrt{d}) = (2)$$

, το οποίο δεν ισχύει αφού $1+\sqrt{d}\epsilon 2\mathbb{Z}[\sqrt{d}]$.
Αν δουλέψουμε στο $O_k = \mathbb{Z}[(1+\sqrt{d})/2]$, τότε η μη απαλειψιμότητα εξαφανίζεται αφού $(2, 1+\sqrt{d}) = (2)(1, (1+\sqrt{d})/2) = (2)$.

Θεώρημα: Έστω $A = (a, b)$ ένα ιδεώδες του O_k με δύο γεννήτορες. Τότε

$$A\overline{A} = (N(a), Tr(a\bar{b}), N(b))$$

Απόδειξη: Εαν το a ή το b είναι 0 το θεώρημα αποδεικνύεται εύκολα. Μπορούμε να θεωρήσουμε τα a και b είναι μη μηδενικά.
$A\overline{A} = (a, b)(\overline{a}\overline{b}) = (a\overline{a}, a\bar{b}, b\overline{a}, b\bar{b}) = (N(a), a\bar{b}, \overline{a}b, N(b))$.
θέλουμε να δείξουμε οτι

$$(N(a), a\bar{b}, \overline{a}b, N(b)) = (N(a), Tr(a\bar{b}), N(b))$$

Αφού $Tr(a\bar{b}) = a\bar{b} + \overline{a}b$, το ιδεώδες στα δεξιά περιέχεται στο ιδεώδες στα αριστερά. Για τον ανάποδο, πρέπει να δείξουμε οτι τα $a\bar{b}, \overline{a}b$ περιέχονται στα δεξιά.

Θα δείξουμε οτι $a\bar{b}\epsilon(N(a), Tr(a\bar{b}), N(b))$. Έστω γ$=a/b\epsilon K = \mathbb{Q}[\sqrt{d}]$. Είναι ρίζα του

$$(X-\gamma)(X-\overline{\gamma}) = X^2 - \frac{Tr(a\bar{b})}{N(b)}X + \frac{N(a)}{N(b)}.$$

Και έστω c το ΕΚΠ των $\frac{Tr(a\bar{b})}{N(b)}$ και $\frac{N(a)}{N(b)}$. Τότε

$$\frac{N(a)}{N(b)} = \frac{\alpha}{c}, \frac{Tr(a\bar{b})}{N(b)} = \frac{\beta}{c}$$

όπου $\alpha, \beta, c\epsilon\mathbb{Z}$ δεν έχουν κοινό παράγοντα μεγαλύτερο του 1. Τότε

$$N(a) = k\alpha, Tr(a\bar{b}) = k\beta, N(b) = kc$$

για κάποιο ακέραιο k, επομένως

$$(N(a), Tr(a\bar{b}), N(b)) = (k\alpha, k\beta, kc) = (k)(\alpha, \beta, c) = (k)(1) = (k).$$

Αφού

$$\gamma^2 - \frac{\beta}{c}\gamma + \frac{\alpha}{c} = 0 \Rightarrow (c\gamma)^2 - \beta(c\gamma) + \alpha c = 0,$$

Το $c\gamma = ca/b\epsilon O_K$. Όμως $ca/b = ca\bar{b}/N(b) = a\bar{b}/k$, άρα τέλος το $a\bar{b}\epsilon kO_K = (k)$ ή $a\bar{b}\epsilon(N(a), Tr(a\bar{b}), N(b))$.

(*) Η απόδειξη που αφήσαμε προκύπτει εύκολα τώρα αφού το $A\overline{A}$ έχει γεννήτορες του $\mathbb{Z}$. Επομένως είναι κύριο ιδεώδες.

Θεώρημα: Για ιδεώδη a,b στο O_k, $a|b$ αν και μόνο αν $a \supset b$.

Απόδειξη: Όταν $a = (0)$ έχουμε $(0)|b \Leftrightarrow b = (0) \Leftrightarrow (0) \supset b$.
Υποθέτουμε οτι $a \neq (0)$. Εαν $a|b \Rightarrow a \supset b$. Υποθέτουμε οτι $a \supset b$, τότε $a\overline{a} \supset b\overline{a}$. Γράφουμε $a\overline{a} = (k)$ επομένως $(k) \supset b\overline{a}$. Άρα $(k)|b\overline{a} \Rightarrow (k)c = b\overline{a}$. Πολλαπλασιάζοντας επί a έχουμε $(k)ca = b(k)$. Και επομένως απαλείφοντας το (k) δίνει $ac = b \Rightarrow a|b$.

Θεώρημα: Ορίζουμε την πρόσθεση ιδεωδών. Εαν $A = (a_1, \ldots, a_m)$ καί $B = (b_1, \ldots, b_n)$, τότε

$$A + B = (a_1, \ldots, a_m, b_1, \ldots, b_n)$$

.

Θεώρημα: Για ιδεώδη a και b, το ιδεώδες $a + b$ είναι ο μέγιστος κοινός διαιρέτης των a,b

Απόδειξη: Αφού $a \subset a + b$ και $b \subset a + b$, το $a + b$ είναι κοινός διαιρέτης των a και b, γιατί αν το περιέχει το διαιρεί. Για κάθε ιδεώδες d που διαιρεί και τα a, b έχουμε $a \subset d, b \subset d$. Επειδή το d είναι κλειστό ως προς την πρόσθεση όμως $a + b \subset d$. Επομένως είναι ο μέγιστος κοινός διαιρέτης.

Παρατηρούμε οτι κάθε ιδεώδες $(a_1, \ldots, a_m)$ του O_k. Είναι ο μέγιστος κοινός διαιρέτης των κύριων ιδεωδών.

$$(a_1, \ldots, a_m) = (a_1) + \ldots + (a_m)$$

.

3.5 Νόρμα Ιδεωδών

Ορισμός: Για μη μηδενικό ιδεώδες a στο O_k, θέτουμε Na να είναι ο θετικός ακέραιος που παράγει το $a\overline{a}$. Το Na λέγεται νόρμα του a.

Παρατηρούμε οτι σε κύρια ιδεώδη $A = (a)$ η νόρμα τους είναι ίση με την απόλυτη τιμή της νόρμα τους γεννήτορα.

Παράδειγμα: Στον $\mathbb{Z}[\sqrt{-14}]$ το ιδεώδες $(3, 1 + \sqrt{-14})$ έχει νόρμα 3.

Θεώρημα: Για μη μηδενικά ιδεώδη a, b, $N(ab) = NaNb$.

Απόδειξη: $(N(ab)) = ab\overline{ab} = ab\overline{a}\overline{b} = a\overline{a}b\overline{b} = (Na)(Nb) = (NaNb)$.

Λήμμα: Για μη μηδενικά ιδεώδη a, b, εαν $a|b$ τότε $Na|Nb$ στο $\mathbb{Z}$.
(Το αντίστροφο γενικά δεν ισχύει. Για παράδειγμα $a = (1 + \sqrt{-14})$ και $b = (1 - \sqrt{-14})$).

Απόδειξη: Γράφοντας το $b = ac$ παίρνουμε νόρμες σε κάθε πλευρά.

Πρόταση: Έστω μη μηδενικό ιδεώδες a, κάθε παράγοντας ιδεώδες του a εκτός του εαυτού του, έχει νόρμα μικρότερη από Na.

Απόδειξη: Έστω b παράγοντας του a , τότε $a = bc$ και $c \neq (1)$. Εφόσον $Na = NbNc$ με $Na \neq (0)$ και $Nc > 1, Nb < Na$.

θα προσπαθήσουμε να υπολογίσουμε κάποιες νόρμες τώρα.

Παραδείγματα:

1. Έστω $a = (3, 1 + \sqrt{-14})$. Το ιδεώδες $a\overline{a}$ παράγεται από τα $N(3), Tr(3(1 - \sqrt{-14}))$ και $N(1 + \sqrt{-14})$, δηλαδή από τα 9,6 και 15. Ο μέγιστος κοινός διαιρέτης τους ειναι το 3, αρα $Na = 3$.

2. Έστω $a = (1+\sqrt{-14}, 1-\sqrt{-14})$. Η νόρμα είναι ο μέγιστος κοινός διαιρέτης των $N(1 \pm \sqrt{-14}) = 15$ και $Tr((1+\sqrt{-14})^2) = -26$. Αφού τα 15 και 26 είναι πρώτα μεταξύ τους $Na = 1$. Επομένως $a = (1)$.

3. Έστω $a = (4+\sqrt{-14}, 2-\sqrt{-14})$. Αφού $N(4+\sqrt{-14}) = 30, Tr((4+\sqrt{-14})(2+\sqrt{-14})) = -12$, και $N(2 - \sqrt{-14}) = 18$, $Na = 6$.

θα πούμε κάποια πράγματα τώρα που αφορούν την μοναδική παραγοντοποίηση των ιδεωδών, την οποία έχουμε αποδειξει στο προηγούμενο κεφάλαιο.

Θεώρημα: Εαν ένα ιδεώδες είναι πρώτο, τότε το συζυγές του ιδεώδες είναι επίσης πρώτο.

Απόδειξη: Οι δακτύλιοι O_k/p και $O_k/\overline{p}$ είναι ισόμορφοι, επομένως ο ένα δακτύλιος είναι ακέραια περιοχή αν και μόνο αν είναι και ο άλλος.

Πρόταση: Ισχύει οτι $Na = 1$ αν και μόνο αν $a = (1)$.

Απόδειξη: Η μια πλευρά είναι προφανής.
Εαν $N(a) = 1$ τότε $a\overline{a} = (1)$, επομένως $a|(1)$. Στα ιδεώδη το διαιρώ είναι περιέχομαι , οπότε $a \supset (1) = O_K$, επομένως $a = (1)$.

Θεώρημα: Κάθε ιδεώδες που η νόρμα του είναι πρώτος, είναι πρώτο ιδεώδες.

Το αντίστροφο δεν ισχύει.

Απόδειξη: Έστω $Na = p$ πρώτος. Εαν $a = bc$, παίρνοντας νόρμες έχουμε οτι το $p = NbNc$. Επομένως αφου το p είναι πρώτος, το b ή το c έχουν νόρμα 1, επομένως ένα από τα δύο είναι το (1).

Παραδείγματα:Στον $\mathbb{Z}[\sqrt{-14}]$

1. Το ιδεώδες $(3, 1 + \sqrt{-14})$ έχει νόρμα 3, επομένως είναι πρώτο ιδεώδες.

2. Θα δείξουμε το ιδεώδες (11), του οποίου η νόρμα είναι 121, είναι πρώτο.
Υποθέτουμε οτι $(11) = ab, a \neq (1), b \neq (1)$. Τότε παίρνοντας νόρμες έχουμε $121 = NaNb$. Άρα $Na = 11$. Γράφοντας το $a = (a_1, \ldots, a_m)$, έχουμε οτι $a|(a_i)$ παίρνοντας νόρμες $11|N(a_i)$.

Επομένως πρέπει να δούμε ποια στοιχεία του $\mathbb{Z}[\sqrt{-14}]$ έχουν νόρμα που διαιρείται με το 11.

Εαν το $x+y\sqrt{-14}$ ικανοποιεί την $x^2+y^2 14 = 0 mod 11$ τότε $x^2 = -3y^2 mod 11$. Το $-3 mod 11$ δεν είναι τετράγωνο, επομένως πρέπει να έχουμε $y = 0 mod 11$ και $x = 0 mod 11$. Αυτο υπονοεί οτι το $x+y\sqrt{-14}$ διαιρείται από το 11 στον $\mathbb{Z}[\sqrt{-14}]$.
Γυρνώντας πίσω, $(11) = ab$, το a είναι πολλαπλάσιο του 11. Το $a = (11)c$ για κάποιο ιδεώδες c. Τότε το Na διαιρείται από το 121, με $Na = 11$. Άτοπο, άρα το (11) είναι πρώτο ιδεώδες στο $\mathbb{Z}[\sqrt{-14}]$.

Θεώρημα: Εαν το p είναι πρώτο ιδεώδες και $p|ab$, τότε $p|a$ ή $p|b$.

Απόδειξη: Θεωρούμε οτι το p δεν διαιρεί το a και αποδεικνύουμε οτι $p|b$. Το ιδεώδες $p+a$ είναι κοινός διαιρέτης των p και a. Οι μόνοι διαιρέτες του p είναι το p και το (1), εφόσον το p είναι πρώτο. Επειδή το p δεν διαιρεί το a , $p+a \neq p$. Επομένως $p+a = (1)$,άρα το $1 = x+\alpha$ για κάποιο $x\epsilon p, \alpha\epsilon a$. Τότε για κάθε $\beta\epsilon b$,

$$\beta = 1\cdot\beta = x\beta + \alpha\beta\epsilon p + ab \subset p,$$

το οποίο δείχνει οτι $b \subset p$. Επομένως $p|b$.

Εαν το p είναι πρώτο ιδεώδες και $p|a_1,\dots,a_r$, τότε $p|a_i$ για κάποιο i.

3.6 Δημιουργία πρώτων ιδεωδών.

Θεώρημα: Κάθε μη μηδενικό πρώτο ιδεώδες στον O_k διαιρεί ένα μοναδικό πρώτο αριθμό.
Εαν το P είναι μη μηδενικό πρώτο ιδεώδες τότε $P|(p)$ για ένα πρώτο p στο $\mathbb{Z}$.

Απόδειξη: Το ιδεώδες $P\overline{P} = (NP)$ διαιρείται από το P και έχει έναν γεννήτορα στο $\mathbb{Z}_{>0}$. Αφού $P \neq (1), NP > 1$. Αναλύουμε το NP σε πρώτους στο $\mathbb{Z}_{>0}$,

$$NP = p_1p_2\dots p_r.$$

Τότε $P\overline{P} = (p_1p_2\dots p_r) = (p_1)\dots(p_r)$ άρα το P διαιρεί κάποιο (p_i).
Για την μοναδικότητα, θεωρούμε $P|(p)$ και $P|(q)$ για δύο διαφορετικούς πρώτους p, q. Τότε $p\epsilon P, q\epsilon P$. Αφού τα p, q είναι πρώτα μεταξύ τους, το p περιέχει ένα ζευγάρι πρώτων μεταξύ τους ακεραίων και $P = (1)$. Ατοπο.

Πρόταση: Κάθε μη μηδενικό πρώτο ιδεώδες στον O_k έχει νόρμα p ή p^2 για κάποιο πρώτο αριθμό p.

Απόδειξη: Έστω P μη μηδενικό πρώτο ιδεώδες στον O_k. Τότε υπάρχει πρώτος αριθμός με $P|(p)$. Παίρνοντας νόρμες $NP|N((p))$. Επομένως $N((p)) = |N(p)| = p^2$, το NP είναι p ή p^2.

Άρα μπορούμε να βρούμε κάθε μη μηδενικό πρώτο ιδεώδες στον O_k, παραγοντοποιώντας πρώτους αριθμούς στον O_k.
Για παράδειγμα, στον $\mathbb{Z}[\sqrt{-14}]$, ξέρουμε οτι $(2) = (2,\sqrt{-14})^2$ και $(3) = (3, 1+\sqrt{-14})(3, 1-\sqrt{-14})$.

Επομένως το $(2, \sqrt{-14})$ είναι το μόνο πρώτο ιδεώδες με νόρμα 2, και τα $(3, 1+\sqrt{-14}), (3, 1-\sqrt{-14})$, τα μόνα με πρώτα ιδεώδη με νόρμα 3.

Θεώρημα: Έστω $K = \mathbb{Q}[\sqrt{d}]$ τετραγωνικό σώμα, με d ελεύθερο τετραγώνων και $O_k = \mathbb{Z}[\omega]$, με $f(X)$ το τετραγωνικό πολυώνυμο που έχει τα $\omega, \overline{\omega}$ ως ρίζες:

$$f(X) = \begin{cases} X^2 - d & \text{για } d \neq 1 mod 4, \\ X^2 - X + \frac{1-d}{4} & \text{για } d = 1 mod 4. \end{cases}$$

Για κάθε πρώτο αριθμό p, ο τρόπος με τον οποίο το (p) παραγοντοποιείται στο O_k ταιριάζει με τον τρόπο η $f(X)$ παραγοντοποιείται $modulo p$:

1. Εαν $f(X) mod p$ είναι ανάγωγο τότε το (p) είναι πρώτο στο O_k με νόρμα p^2.
2. Εαν $f(X) = (X-c)(X-c') mod p$ και $c \neq c' mod p$ τότε $(p) = P\overline{P}$ όπου $P \neq \overline{P}$ και τα $P, \overline{P}$ έχουν νόρμα p.
3. Εαν $f(X) = (X-c)^2 mod p$ τότε $(p) = P^2$ και $NP = p$.

Συγκεκριμένα, τα πρώτα ιδεώδη στον O_k έχουν νόρμα πρώτο, εκτός των κύριων ιδεωδών (p) όπου p είναι πρώτος αριθμός τέτοιος ώστε το $f(X) mod p$ να είναι ανάγωγο.

Απόδειξη: Αφού $O_k = \mathbb{Z}[\omega] \cong \mathbb{Z}[X]/(f(X)), O_k/(p) \cong \mathbb{Z}[X]/(p, f(X)) \cong (\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$. Θα συγκρίνουμε τους δακτυλίους $O_k/(p)$ και $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$, για να βρούμε την αντιστοιχία παραγοντοποίησης του (p) στον O_k με την παραγοντοποίηση του $f(X)$ στον $(\mathbb{Z}/p\mathbb{Z})[X]$.

Εαν το $f(X) mod p$ είναι ανάγωγο τότε το $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$ είναι σώμα. Εαν το $f(X) = (X - c)(X-c') mod p$ και $c \neq c' mod p$ τότε

$$(\mathbb{Z}/p\mathbb{Z})[X]/(f(X)) \cong (\mathbb{Z}/p\mathbb{Z})[X]/(X-c) \times (\mathbb{Z}/p\mathbb{Z})[X]/(X-c') \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$$

είναι καρτεσιανό γινόμενο δύο σωμάτων , δεν είναι σώμα και δεν έχει μη μηδενικά μηδενοδύναμα στοιχεία. Εαν $f(X) = (X-c)^2 mod p$ τότε το $(\mathbb{Z}/p\mathbb{Z})[X]/(X-c)^2$ έχει μη μηδενικό μηδενοδύναμο στοιχείο: $X - c mod (X-c)^2$. Επομένως ο τρόπος με τον οποίο η $f(X)$ αναλύεται στον $(\mathbb{Z}/p\mathbb{Z})[X]$ ανταναλκά στην δομή του δακτυλίου $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$.

Ο δακτύλιος $O_k/(p)$ είναι σώμα αν και μόνο αν το (p) είναι μέγιστο ιδεώδες ή επομένως πρώτο ιδεώδες. Άρα, το $f(X) mod p$ είναι ανάγωγο αν και μόνο αν το (p) είναι πρώτο στον O_k.
Αν το (p) δεν είναι πρώτο τότε , $(p) = ab$ με $a, b \neq (1)$. Παίρνοντας νόρμες $p^2 = NaNb$, άρα $Na = Nb = p$ και επομένως είναι πρώτα ιδεώδη. Συγκεκριμένα αφού $Na = p$ έχουμε $(p) = (Na) = a\overline{a}$, και από μοναδική παραγοντοποίηση σε πρώτα ιδεώδη έχουμε $b = \overline{a}$. Γράφουμε το a ώς P αφού είναι πρώτο ιδεώδες. Η παραγώγηση του (p) είναι $P\overline{P}$. Εαν $P = \overline{P}$ τότε το $O_k/(p) = O_k/P^2$ έχει ένα μη μηδενικό μηδενοδύναμο στοιχείο , επομένως $f(X) = (X-c)^2 mod p$ για κάποιο c.
Εαν $P \neq \overline{P}$ τότε το $O_k/(p) = O_k/P\overline{P}$ δεν είναι σώμα και δεν έχει μη μηδενικό μηδενοδύναμο στοιχείο , διοτι εαν $x^m = 0 mod P\overline{P}$ τότε τα P και $\overline{P}$ διαιρούνται με το $(x^m) = (x)^m$, δηλαδή με το (x), $P\overline{P}|(x)$ γιατι $P \neq \overline{P}$. Επομένως $x = 0 mod P\overline{P}$, και πρέπει να έχουμε $f(X) = (X-c)(X-c') mod p$ με

$c \neq c' mod p$.

Πρόταση: Εαν το (p) δεν είναι πρώτο στο O_k τότε το $f(X) mod p$ έχει ρίζα . Για κάθε ρίζα $c mod p$,το $(p, \omega - c)$ είναι ένα από τα πρώτα ιδεώδη που διαιρεί το (p).

Απόδειξη: Δείξαμε οτι $(p) = P\overline{P}$ για πρώτο ιδεώδες P. Θέτουμε $a = (p, \omega - c)$. Αφού $p \epsilon a, a|(p)$. Όμως $\omega - c \not\epsilon (p), a \neq (p)$ άρα ή το a είναι ένα από τα πρώτα ιδεώδη που διαιρεί το (p) ή το $a = (1)$. Θέλουμε να δείξουμε οτι $a \neq (1)$. Η νόρμα του a είναι ο μέγιστος κοινός διαιρέτης των $N(p) = p^2, Tr(p(\overline{\omega} - c)) = pTr(\overline{\omega} - c)$, και $N(\omega - c) = f(c) = 0 mod p$. Αυτά διαιρούνται από το p επομένως $p|Na$. Και $a \neq (1)$, επομένως το a είναι P ή $\overline{P}$. Οι ρόλοι των P και $\overline{P}$ μέχρι τώρα ήταν συμμετρικοί, άρα μπορούμε να θέσουμε $P = a = (p, \omega - c)$.

Παράδειγμα: Πως το (2) παραγοντοποιείται σε ακεραίους του $\mathbb{Q}[\sqrt{-39}]$;
Το $d = 1 mod 4$ επομένως $f(X) = X^2 - x + 10$.

$$X^2 - X + 10 = X(X - 1) mod 2$$

Η παραγοντοποίηση του (2) είναι $P\overline{P}$.

Όταν το $p \neq 2$ ο τρόπος με τον οποίο το $f(X)$ παραγοντοποιείται $modulo p$ καθορίζεται από την διακρίνουσα του.
Υπάρχουν δύο διαφορετικές ρίζες, εαν η διακρίνουσα είναι μη μηδενική τετράγωνο $mod p$,
Καμία ρίζα εαν η διακρίνουσα δεν είναι τετράγωνο $mod p$,
Και επαναλαμβανόμενη ρίζα εαν η διακρίνουσα είναι $0 mod p$.

Εαν η $f(X)$ είναι $X^2 - d$ η διακρίνουσα είναι $4d$ αλλιώς d, επομένως ο τρόπος με τον οποίο παραγοντοποιείται η εξαρτάται από το σύμβολο $Legendre \left(\frac{d}{p}\right)$.

Θα μαζέψω τα αποτελέσματα και θα προχωρήσω σε παράδειγμα.

Έστω οτι βρισκόμαστε σε $\mathbb{Q}[\sqrt{d}]$. Οι ακέραιοι μας είναι οι $\mathbb{Z}[\omega]$, το πολυώνυμο $f(x)$ και η διακρίνουσα D.

$$f(X) = \begin{cases} X^2 - d & \text{για } d \neq 1mod4, \\ X^2 - X + \frac{1-d}{4} & \text{για } d = 1mod4. \end{cases}$$

$$D = \begin{cases} 4d & \text{για } d \neq 1mod4, \\ d & \text{για } d = 1mod4. \end{cases}$$

$$\omega = \begin{cases} \sqrt{d} & \text{για } d \neq 1mod4, \\ \frac{1+\sqrt{d}}{2} & \text{για } d = 1mod4. \end{cases}$$

1. $\left(\frac{D}{p}\right) = 1 \Rightarrow f(X) = (X-c)(X-c')modp \Rightarrow (p) = P\overline{P}, P \neq \overline{P}, NP = N\overline{P} = p$
2. $\left(\frac{D}{p}\right) = -1 \Rightarrow f(X)$ ανάγωγο $modp \Rightarrow (p)$ είναι πρώτο , $N(p) = p^2$
3. $\left(\frac{D}{p}\right) = 0 \Rightarrow f(X) = (X-c)^2 modp \Rightarrow (p) = P^2, NP = p$

Για ρίζα $modp$ του $f(X)$, c, έχουμε $P = (p, \omega - c)$

3.7 Τελική εφαρμογή

Θα συνεχίσουμε να δουλεύουμε στον $\mathbb{Z}[\sqrt{-14}]$. Θα βρούμε αρχικά μικρούς πρώτους.

Ο τρόπος με τον οποίο ένα (p) παραγοντοποιείται στον $\mathbb{Z}[\sqrt{-14}]$ εξαρτάται απο το πως παραγοντοποιείται το $X^2 + 14\ modp$.

1. Για $p = 2$, $f(X) = x^2 mod2 \Rightarrow c = 0mod2$ επομένως $(2) = P^2$, όπου $P = (2, \sqrt{-14})$.
2. Για $p = 3$, $f(X) = (x^2+2)mod3 = (x+1)(x+2)mod3 \Rightarrow c = -1mod3, c' = -2mod3$ επομένως $(3) = P\overline{P}$, όπου $P = (3, \sqrt{-14}+1)$. Δεν παίρνουμε το $P = (3, \sqrt{-14}+2)$, διότι τότε $N(3, \sqrt{-14}+2) \neq 3$.
3. Για $p = 5$, $f(X) = (x^2-1)mod5 = (x+1)(x+4)mod5 \Rightarrow c = -1mod5, c' = -4mod5$ επομένως $(5) = P\overline{P}$, όπου $P = (5, \sqrt{-14}+1)$. Δεν παίρνουμε το $P = (5, \sqrt{-14}+4)$, διότι τότε $N(3, \sqrt{-14}+2) \neq 5$.
4. Για $p = 7$, $f(X) = x^2 mod7 \Rightarrow c = 0mod7$ επομένως $(7) = P^2$, όπου $P = (7, \sqrt{-14})$.
5. Για $p = 11$, $f(X) = x^2 + 3mod11$ το οποίο είναι ανάγωγο, επομένως το (11) είναι πρώτο.

Αν συνεχίσουμε ανάλογα,

p	(p)	P
2	P^2	$(2, \sqrt{-14})$
3	$P\overline{P}$	$(3, \sqrt{-14}+1)$
5	$P\overline{P}$	$(5, \sqrt{-14}+1)$
7	P^2	$(7, \sqrt{-14})$
11	(11)	(11)
13	$P\overline{P}$	$(13, \sqrt{-14}+5)$
17	(17)	(17)
19	$P\overline{P}$	$(19, \sqrt{-14}+9)$
23	$P\overline{P}$	$(\sqrt{-14}+3)$

Με γνώση αυτού θα προχωρήσουμε σε παραγοντοποίηση ιδεωδών που δεν έχουν γεννήτορες από το $\mathbb{Z}$

Παράδειγμα 1: Το $(1+\sqrt{-14})$. Το ιδεώδες έχει νόρμα 15, και γράφοντας το ως γινόμενο πρώτων ιδεωδών, το γινόμενο των νόρμων τους είναι 15, άρα πρέπει να έχουν νόρμες 3 και 5. Εφόσον το $(1+\sqrt{-14})\epsilon(3, \sqrt{-14}+1)$ καί $(1+\sqrt{-14})\epsilon(5, \sqrt{-14}+1)$, το $(1+\sqrt{-14})$ διαιρείται από τα $(3, \sqrt{-14}+1), (5, \sqrt{-14}+1)$. Επομένως έχουμε

$$(1+\sqrt{-14}) = (3, \sqrt{-14}+1)(5, \sqrt{-14}+1)$$

Παράδειγμα 2: Το $(5+2\sqrt{-14})$. Το ιδεώδες έχει νόρμα 81. Οι πιθανοί παράγοντες πρώτα ιδεώδη του $(5+2\sqrt{-14})$, είναι τα $(3, \sqrt{-14}+1)$ και $(3, -\sqrt{-14}+1)$. Όμως δεν μπορεί να διαιρεθεί από κανένα , επομένως διαιρείται από το $(3, \sqrt{-14}+1)(3, -\sqrt{-14}) = (3)$. Όμως ξέρουμε οτι το (3) δεν διαιρεί το $5+2\sqrt{-14}$ στον $\mathbb{Z}[\sqrt{-14}]$, και επομένως το $(5+2\sqrt{-14})$ είναι δύναμη του $(3, \sqrt{-14}+1)$ ή του $(3, -\sqrt{-14}+1)$. Λόγω νόρμας είναι $(3, \sqrt{-14}+1)^4$ ή $(3, -\sqrt{-14}+1)^4$.
Στον $\mathbb{Z}[\sqrt{-14}]/(3, \sqrt{-14}+1) \cong \mathbb{Z}/3\mathbb{Z}$, αφού $1+\sqrt{-14} = 0$, $5+2\sqrt{-14} = 3 = 0$ και επομένως $(3, \sqrt{-14}+1)|(5+2\sqrt{-14})$, άρα

$$(5+2\sqrt{-14}) = (3, \sqrt{-14}+1)^4$$

Παράδειγμα 3: Το ιδεώδες $a = (2+3\sqrt{-14})$ έχει νόρμα $130 = 2\cdot 5\cdot 13$. Επομένως $(2, \sqrt{-14})|a$, θέλουμε να δούμε εαν το $(5, \sqrt{-14}+1)$ διαιρεί το a ή το συζυγές του.
Το ιδεώδες $(1+\sqrt{-14})$ διαιρείται απο το $(5, \sqrt{-14}+1)$ και όχι από το συζυγές του, ο μέγιστος κοινός διαιρέτης του a και τού $(1+\sqrt{-14})$, είναι ο $(1+\sqrt{-14}, 2+3\sqrt{-14})$. Η νόρμα του είναι 1, επομένως πρέπει το συζυγές του να διαιρεί το a.
Και θέλουμε να αποφασίσουμε τελικά εαν το $(13, \sqrt{-14}+5)$ διαιρεί το a ή το συζυγές του. Αντίστοιχα κοιτάμε $(2+3\sqrt{-14}, \sqrt{-14}+5)$, είναι είτε $(13, \sqrt{-14}+5)$, είτε (1). Η νόρμα του είναι 13 επομένως το $(13, \sqrt{-14}+5)$ διαιρεί το a και έχουμε,

$$a = (2, \sqrt{-14})(5, -\sqrt{-14}+1)(13, \sqrt{-14}+5)$$

Παράδειγμα 4: Το ιδεώδες $a = (7+3\sqrt{-14})$, έχει νόρμα $175 = 5^2\cdot 7$. Επομένως $(7, \sqrt{-14})|a$. Ξανά θέλουμε να δούμε εαν το $(5, \sqrt{-14}+1)$ διαιρεί το a ή το συζυγές του. Το ιδεώδες $(7+3\sqrt{-14}, 1+$

$\sqrt{-14})$ έχει νόρμα 1, άρα το a διαιρείται απο το συζυγές του, και

$$a = (7, \sqrt{-14})(5, \sqrt{-14} + 1)^2$$

Βιβλιογραφία

1. *John B. Fraleigh* 2012: ¨Εισαγωγή στην Άλγεβρα' , Πανεπιστημιακές Εκδόσεις Κρήτης
2. *Joseph Rotman* 2000: ¨Θεωρία *Galois*' , Εκδόσεις *Leader Books*
3. *David S. Dummit* καί *Richard M. Foote* , "*Abstract Algebra*" *Third Edition* , *John Wiley and Sons*, *Inc.*
4. *Keith Conrad* , *Algebraic Number Theory* , *thtp* : *//www.math.uconn.edu/ kconrad/blurbs/*
5. *Allen Hatcher* , *Quadratic Fields* , *http* : *//www.math.cornell.edu/ hatcher/*3320*/TNch*3*.pdf*
6. *Brian Osserman* , *Ring of Integers and Dedekind Domains* , *https* : *//www.math.ucdavis.edu/ osserman*
7. *Johan Bosman* , *Algebraic Number Theory* , *http* : *//www*2*.warwick.ac.uk/fac/sci/maths/people/staff/*
8. *Robert B. Ash* , "*A Course In Algebraic Number Theory*" , *http* : *//www.math.uiuc.edu/ r−ash/ANT.html*