Θέματα Άλγεβρας και Γεωμετρίας II

Εισαγωγή στην Αλγεβρική Θεωρία Αριθμών και το θεώρημα του Minkowski

Ονομ/νο: Νούλας Δημήτριος
ΑΜ: 1112201800377
email: dimitriosnoulas@gmail.com

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

να βάλω I_n με το *det* στην εξίσωση δακτύλιοι μεταθετικοί με μονάδα!!! η σχέση με adjoint για το τέχνασμα της ορίζουσας ισχύει και για πίνακες $A \in M_n(R)$ για τυχαίο R δακτύλιο μεταθετικό με μονάδα!!! Γνώσεις από θεωρία Galois και μεταθετική άλγεβρα
Έστω $R \subseteq S$ δύο δακτύλιοι και $r \in S$. Θα λέμε ότι το r είναι ακέραιο υπεράνω του R αν υπάρχει μονικό πολυώνυμο με συντελεστές από το R έτσι ώστε

$$r^n + a_{n-1}r^{n-1} + \ldots + a_1 r + a_0 = 0$$

Κάθε $r \in R$ είναι ακέραιο υπεράνω του R. Αν έχουμε επιπλέον ότι το R είναι σώμα και το S επέκτασή του, τότε το $r \in S$ είναι ακέραιο υπεράνω του R αν και μόνο αν είναι αλγεβρικό υπεράνω του R. Ουσιαστικά, θέλουμε να μεταφέρουμε τον ορισμό του αλγεβρικού στοιχείου και σε δακτυλίους και απαιτούμε το πολυώνυμο να είναι μονικό. Αυτό είναι αναγκαίο καθώς και σε πολλά επιχειρήματα στην θεωρία Galois, όπως στην μοναδικότητα του αναγώγου πολυωνύμου, πολλαπλασιάζαμε με τον αντίστροφο συντελεστή του μεγιστοβαθμίου. Σε δακτυλίους φυσικά μπορεί ένας συντελεστής να μην έχει αντίστροφο και για αυτό απαιτούμε το πολυώνυμο να είναι μονικό.

Πρόταση 1. *Έστω $R \subseteq S$ δακτύλιος και $x \in S$. Τα ακόλουθα είναι ισοδύναμα:*

(1) *Το x είναι ακέραιο υπεράνω του R.*

(2) *Το $R[x]$ είναι πεπερασμένα παραγόμενο R-πρότυπο.*

(3) *Το $R[x]$ περιέχεται σε έναν υποδακτύλιο C του S, το οποίο C είναι πεπερασμένα παραγόμενο R-πρότυπο.*

Απόδειξη.

(1) $\implies$ (2) Αν έχουμε ότι

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

με $a_i \in R$ από την υπόθεση, τότε αρκεί να δείξουμε ότι κάθε δύναμη του x παράγετεαι από τα $1, x, x^2, \ldots, x^{n-1}$. Έτσι θα παράγεται από αυτά και κάθε πολυώνυμο του $R[x]$. Πράγματι, από την παραπάνω σχέση έχουμε ότι για κάθε $r \geq 0$ ισχύει η ισότητα:

$$x^{n+r} = -\left(a_{n-1}x^{n+r-1} + \ldots + a_0 x^r\right)$$

και άρα το $R[x]$ παράγεται από τα $1, x, \ldots, x^{n-1}$.

(2) $\implies$ (3) Παίρνουμε $C = R[x]$.

(3) $\implies$ (1) Θα χρησιμοποιήσουμε κάτι που αναφέρεται στην βιβλιογραφία ως το τέχνασμα της ορίζουσας. Έστω ότι $C = (y_1, y_2, \ldots, y_n)$ το πεπερασμένα παραγόμενο R-πρότυπο. Έχουμε ότι $R[x] \subseteq C$ και άρα $xy_i \in C$ για κάθε $i = 1, \ldots, n$. Έτσι, για κάθε $i = 1, \ldots, n$ μπορούμε να γράψουμε ότι:

$$xy_i = \sum_{j=1}^{n} a_{ij}y_j \iff \sum_{j=1}^{n} \left(\delta_{ij}x - a_{ij}\right) y_j = 0$$

όπου δ_{ij} είναι το δέλτα του Kronecker που παίρνει την τιμή 1 αν $i = j$ και 0 διαφορετικά. Αν δούμε τα παραπάνω σε μορφή πίνακα A με στοιχεία $x - a_{ii}$ στην διαγώνιο και $-a_{ij}$ στις άλλες θέσεις, καθώς και $y = (y_1, \ldots, y_n)^T$ θα έχουμε ότι:

$$Ay = 0$$

στην οποία σχέση πολλαπλασιάζουμε από αριστερά με τον προσαρτημένο πίνακα $adj(A)$ και παίρνουμε ότι

$$det(A)y = 0$$

Δηλαδή, το $det(A)$ μηδενίζει όλο το C αφού μηδενίζει κάθε y_i και άρα $det(A) \cdot 1_C = 0$. Άρα $det(A) = 0$ και αν αναπτύξουμε την ορίζουσα θα έχουμε ένα μονικό πολυώνυμο του x να είναι ίσο με το μηδενικό, εφόσον το x^n θα προκύψει μόνο όταν πολλαπλασιαστούν τα στοιχεία της διαγωνίου και θα έχει συντελεστή 1 και οι υπόλοιποι συντελεστές θα είναι πράξεις των a_{ij} δηλαδή στοιχεία του R. □

Πόρισμα 1. *Αν $x_1, \ldots, x_n \in S$ ακέραια υπεράνω του δακτυλίου $R \subseteq S$, τότε το $R[x_1, \ldots, x_n]$ είναι πεπερασμένα παραγόμενο R-πρότυπο.*

Απόδειξη.

Θα το δείξουμε εφαρμόζοντας επαγωγή στο n. Για $n = 1$ έχουμε την απάντηση από το (2) της προηγούμενης πρότασης. Για $n > 1$, έχουμε

$$R[x_1, x_2, \ldots, x_n] = A[x_n]$$

όπου $A = R[x_1, \ldots, x_{n-1}]$ και από την επαγωγική υπόθεση, το A είναι πεπερασμένα παραγόμενο R-πρότυπο. Χρησιμοποιώντας πάλι το (2) της προηγούμενης πρότασης, το $A[x_n]$ είναι πεπερασμένα παραγόμενο A-πρότυπο. Από αυτό έπεται ότι είναι και πεπερασμένα παραγόμενο R-πρότυπο από το γνωστό επιχείρημα πύργων, καθώς αν το $A[x_n]$ παράγεται από τα a_i ως A-πρότυπο και το A παράγεται από τα b_j ως R-πρότυπο, τότε το $A[x_n]$ παράγεται από τα $a_i b_j$ ως R-πρότυπο. □

Πόρισμα 2. *Έστω R, S δακτύλιοι με $R \subseteq S$ και C το σύνολο των $r \in S$ που είναι ακέραια υπεράνω του R, τότε το C είναι υποδακτύλιος του S που περιέχει το R.*

Απόδειξη.

Έστω $x, y \in C$. Τότε από το προηγούμενο πόρισμα έπεται ότι το $R[x, y]$ είναι πεπερασμένα παραγόμενο R-πρότυπο. Τα $R[x + y], R[x - y], R[xy]$ περιέχονται στο $R[x, y]$ που είναι πεπερασμένα παραγόμενο R-πρότυπο και περιέχεται στο S αφού $x, y \in S$. Άρα από το (3) της πρότασης 1 τα $x \pm y, xy$ είναι ακέραια υπεράνω του R.

□

Ορισμός (Ακέραια Θήκη)**.** *Έστω R, S δακτύλιοι με $R \subseteq S$. Τότε ο δακτύλιος C του προηγούμενου πορίσματος ονομάζεται ακέραια θήκη (ή κλειστότητα) του R στο S. Επιπλέον, λέμε ότι το R είναι ακέραια κλειστό στο S αν $C = R$.*

Ορισμός (Σώμα Αριθμών)**.** *Ένα σώμα αριθμών ή αλλιώς αλγεβρικό σώμα αριθμών είναι μια πεπερασμένη επέκταση του $\mathbb{Q}$.*

Αν K είναι ένα σώμα αριθμών, η επέκταση $K/\mathbb{Q}$ εκτός από πεπερασμένη είναι και διαχωρίσιμη εφόσον βρισκόμαστε σε χαρακτηριστική 0. Υπενθυμίζουμε ότι από το θεώρημα πρωταρχικού στοιχείου (Morandi thm 5.6 cor 5.7) η επέκταση $K/\mathbb{Q}$ είναι απλή, δηλαδή υπάρχει $\theta \in K$ τέτοιο ώστε $K = \mathbb{Q}(\theta)$.

Σε ένα σώμα αριθμών K, η ακέραια θήκη του $\mathbb{Z}$ είναι, με βάση το προηγούμενο πόρισμα, ένας δακτύλιος τον οποίο ονομάζουμε δακτύλιο των ακεραίων στο K και τον συμβολίζουμε με $\mathcal{O}_K$. Θα δείξουμε ότι το K είναι το σώμα πηλίκων του $\mathcal{O}_K$.

Πρόταση 2. *Έστω S το σώμα πηλίκων μιας ακέραιας περιοχής R και L ένα σώμα που περιέχει το S. Αν το $a \in L$ είναι αλγεβρικό υπεράνω του S, τότε υπάρχει μη μηδενικό $d \in R$ τέτοιο ώστε το στοιχείο da είναι ακέραιο υπεράνω του R.*

Απόδειξη. β
Το a είναι αλγεβρικό υπεράνω του K, είναι ρίζα του ελαχίστου πολυωνύμου του δηλαδή ικανοποιεί μια εξίσωση της μορφής:

$$a^m + b_{m-1}a^{m-1} + \ldots + b_1 a + b_0 = 0, \quad b_i \in S.$$

Για τα στοιχεία b_i που είναι στο S, δηλαδή είναι κλάσματα με στοιχεία από το R, υπάρχει κοινός παρονομαστής d με $db_i \in R$ για όλα τα i. Έτσι, πολλαπλασιάζοντας με d^m παίρνουμε:

$$d^m a^m + b_{m-1}d^m a^{m-1} + \ldots + d^m b_1 a + d^m b_0 = 0$$

την οποία εξίσωση την ξαναγράφουμε ως:

$$(da)^m + b_{m-1}d(da)^{m-1} + \ldots + b_1 d^{m-1}(da) + b_0 d^m = 0$$

και αφού οι συντελεστές ανήκουν στο R έχουμε ότι το da είναι ακέραιο υπεράνω του R. □

Πόρισμα 3. *Έστω R μια ακέραια περιοχή με σώμα πηλίκων S και έστω C η ακέραια θήκη του R σε ένα σώμα L με $S \subseteq L$. Αν το L είναι αλγεβρικό υπεράνω του S, τότε το L είναι το σώμα πηλίκων του C.*

Απόδειξη.

Από την προηγούμενη πρόταση έχουμε ότι κάθε $a \in L$ γράφεται ως $a = \frac{c}{d}$ με $c \in C, d \in R$.
□

Με το πόρισμα για $R = \mathbb{Z}, S = \mathbb{Q}$ και $L = K$ ένα σώμα αριθμών δείξαμε ότι το K είναι το σώμα πηλίκων του $C = \mathcal{O}_K$.
Στην συνέχεια όπου αναφερόμαστε ότι το R είναι ακέραια κλειστό θα εννοούμε στο σώμα πηλίκων του. Δηλαδή αν S είναι το σώμα πηλίκων του και ισχύει ότι:

$$a \in S, a \text{ ακέραιο υπεράνω του } R \implies a \in R.$$

Πρόταση 3. *Μια περιοχή μοναδικής παραγοντοποίησης είναι ακέραια κλειστή.*

Απόδειξη.

Αν το R είναι σώμα θα ταυτίζεται με το σώμα πηλίκων του άρα δεν έχουμε κάτι να δείξουμε. Έστω ότι το R δεν είναι σώμα και k το σώμα πηλίκων του. Αν $\frac{x}{y} \in k$ είναι ακέραιο πάνω από το R, με $x, y \in R$ θα δείξουμε ότι $\frac{x}{y} \in R$. Εφόσον είμαστε σε περιοχή μοναδικής παραγοντοποίησης μπορούμε να υποθέσουμε ότι δεν υπάρχει ανάγωγο στοιχείο $p \in R$ που να διαιρεί ταυτόχρονα τα x και y, διαφορετικά από την μοναδική παραγοντοποίηση το διαγράφουμε από αριθμητή και παρονομαστή και παίρνουμε νέο κλάσμα χωρίς κοινό ανάγωγο διαιρέτη. Εφόσον το $\frac{x}{y}$ είναι ακέραιο πάνω από το R έχουμε ότι υπάρχουν $a_i \in R$ τέτοια ώστε

$$\left(\frac{x}{y}\right)^n + a_{n-1}\left(\frac{x}{y}\right)^{n-1} + \ldots + a_1\left(\frac{x}{y}\right) + a_0 = 0$$

την οποία σχέση πολλαπλασιάζουμε με το y^n. Έτσι έχουμε

$$x^n + a_{n-1}x^{n-1}y + \ldots + a_1 x y^{n-1} + a_0 y^n = 0$$

Αν τώρα ισχύει ότι $y \notin U(R)$, τότε λόγω μοναδικής παραγοντοποίησης έχουμε ότι υπάρχει ανάγωγο p τέτοιο ώστε $p|y$. Εφόσον το y είναι σε όλους τους όρους εκτός από τον πρώτο και στο δεύτερο μέλος της σχέσης έχουμε 0, έπεται ότι $p|x^n$. Καθώς το p είναι ανάγωγο σε περιοχή μοναδικής παραγοντοποίησης έχουμε ότι $p|x$ εφόσον

$$\text{Αν } x = u q_1^{m_1} \cdots q_s^{m_s}, \quad p|x^n \implies pk = x^n = u^n q_1^{nm_1} \cdots q_s^{nm_s}$$

και λόγω μοναδικής παραγοντοποίησης το ανάγωγο p θα ταυτίζεται με κάποιο από τα q_i και άρα $p|x$. Αυτό είναι άτοπο καθώς έχουμε ότι δεν υπάρχει ανάγωγο p να διαιρεί ταυτόχρονα τα x, y. Συνεπώς $y \in U(R)$ και έτσι έχουμε

$$\frac{x}{y} = \frac{x}{y} \cdot 1 = \frac{x}{y}\frac{y^{-1}}{y^{-1}} = xy^{-1} \in R$$

□

Πρόταση 4. *Έστω k το σώμα πηλίκων του R και K μια πεπερασμένη επέκταση του k. Έστω ότι το R είναι ακέραια κλειστό. Τότε ένα στοιχείο $a \in K$ είναι ακέραιο υπεράνω του R αν και μόνο αν το ελάχιστό του πολυώνυμο υπεράνω του k έχει συντελεστές στο R.*

Απόδειξη.

Έστω $a \in K$. Αν το ελάχιστο πολυώνυμο $Irr(a, k)$ έχει συντελεστές στο R τότε είναι προφανές ότι το a είναι ακέραιο υπεράνω του R.

Αντίστροφα, υποθέτουμε ότι το a είναι ακέραιο υπεράνω του R, δηλαδή ικανοποιεί μια σχέση:

$$g(a) = a^m + b_{m-1}a^{m-1} + \ldots + b_1 a + b_0 = 0, \quad b_i \in R, \quad g(x) \in R[x]$$

Τότε αν δούμε το $g(x)$ ως στοιχείο του $k[x]$, έχουμε $Irr(a, k)|g(x)$ και άρα όλες οι άλλες ρίζες a' του $Irr(a, k)$ είναι ρίζες και του $g(x)$. Συνεπώς, όλες οι ρίζες του $Irr(a, k)$ είναι ακέραιες υπεράνω του R. Ένας άλλος τρόπος να το δούμε είναι με το θεώρημα επέκτασης ισομορφισμών (Morandi thm 3.20) όπου για μια άλλη ρίζα a' του $Irr(a, k)$ παίρνουμε τον k-ισομορφισμό $\sigma : k[a] \to k[a']$ με $\sigma(a) = a'$. Έτσι, εφαρμόζουμε τον σ στην παραπάνω σχέση και παίρνουμε $\sigma(g(a)) = g(\sigma(a)) = 0$, δηλαδή $g(a') = 0$.

Εφόσον οι ρίζες του $Irr(a, k)$ είναι ακέραιες υπεράνω του R και τα ακέραια στοιχεία αποτελούν δακτύλιο, έχουμε ότι οι συντελεστές του $Irr(a, k)$ θα είναι και αυτοί ακέραιοι υπεράνω του R. Αυτό φαίνεται αν θεωρήσουμε μια παραγοντοποίηση του $Irr(a, k)$ σε ένα σώμα ριζών, τότε οι συντελεστές του $Irr(a, k)$ θα είναι πράξεις των ριζών του και έτσι θα ανήκουν στον δακτύλιο των ακέραιων στοιχείων του R στο k. Επειδή το R είναι ακέραια κλειστό έχουμε $Irr(a, k)(x) \in R[x]$. □

Πρόταση 5. *Αν το S είναι ακέραιο υπεράνω του R και πεπερασμένα παραγόμενο ως R-άλγεβρα, τότε είναι πεπερασμένα παραγόμενο ως R-πρότυπο.*

Απόδειξη. □

Λήμμα 1. *Έστω $R_1 \subseteq R_2 \subseteq R_3$ δακτύλιοι. Αν το R_2 είναι πεπερασμένα παραγόμενο ως R_1-πρότυπο και το R_3 είναι πεπερασμένα παραγόμενο ως R_2-πρότυπο, τότε το R_3 είναι πεπερασμένα παραγόμενο R_1-πρότυπο.*

Απόδειξη. □

Πρόταση 6. *Θεωρούμε τις ακέραιες περιοχές $R_1 \subseteq R_2 \subseteq R_3$. Αν το R_2 είναι ακέραιο υπεράνω του R_1 και το R_3 είναι ακέραιο υπεράνω του R_2 τότε το R_3 είναι ακέραιο υπεράνω του R_1.*

Απόδειξη. □

Πόρισμα 4. *Η ακέραια θήκη του R σε μια αλγεβρική επέκταση K/k όπου το k είναι το σώμα πηλίκων του R, είναι ακέραια κλειστή.*

Απόδειξη. □

Τους ακόλουθους ορισμούς της νόρμας και του ίχνους μπορούμε να τους ορίσουμε γενικά για επεκτάσεις δακτυλίων $R \subseteq S$ όπου ο S είναι ελεύθερο R-πρότυπο, αλλά θα τα ορίσουμε κατευθείαν για την περίπτωση που μας ενδιαφέρει, τις πεπερασμένες επεκτάσεις σωμάτων.

Έστω K/F πεπερασμένη αλγεβρική επέκταση. Αν $a \in K$ ορίζουμε την απεικόνιση $L_a : K \to K$ με $L_a(b) = ab \in K$. Φαίνεται ότι η L_a είναι ομομορφισμός F - διανυσματικών χώρων. Καθώς το K είναι είναι F -διανυσματικός χώρος πεπερασμένης διάστασης μπορούμε να δούμε τις F - γραμμικές απεικονίσεις του K ως πίνακες βάσεων. Αν δηλαδή οι F-ενδομορφισμοί του K $End_F(K) = Hom_F(K, K)$ είναι ο δακτύλιος με τις κατά συντεταγμένη πράξεις των ομομορφισμών διανυσματικών χώρων από το K στο K τότε υπάρχει ισομορφισμός $End_F(K) \simeq M_n(F)$ όπου $M_n(F)$ είναι ο δακτύλιος των $n \times n$ πινάκων με στοιχεία από το F

Έστω $\phi : End_F(K) \to M_n(F)$ ένας τέτοιος ισομορφισμός. Χρησιμοποιούμε το ϕ για να ορίσουμε την ορίζουσα και το ίχνος της γραμμικής απεικόνισης. Αν $T \in End_F(K)$ ορίζουμε $det(T) = det(\phi(T))$ και $tr(T) = tr(\phi(T))$ όπου στα δεξιά μέλη είναι οι ορίζουσα και ίχνος με την έννοια πινάκων. Φυσικά αυτοί οι ορισμοί δεν εξαρτώνται από τον ισομορφισμό ϕ που διαλέξαμε. Έστω h ένας άλλος τέτοιος ισομορφισμός. Τότε ο h αντιστοιχεί σε μια διαφορετική βάση του K από αυτήν με την οποία αντιστοιχεί ο ϕ . Δηλαδή οι δύο πίνακες $\phi(T), h(T)$ που αναπαριστούν την γραμμική απεικόνιση T είναι όμοιοι, υπάρχει αντιστρέψιμος πίνακας (πίνακας αλλαγής βάσης) με $h(T) = A^{-1}\phi(T)A$.

Συνεπώς $det(\phi(T)) = det(h(T))$ και $tr(\phi(T)) = tr(h(T))$.

Ορισμός. Έστω K/F πεπερασμένη επέκταση. Η νόρμα και το ίχνος της επέκτασης ορίζονται για όλα τα στοιχεία $a \in K$ ως

$$N_{K/F}(a) = det(L_a)$$

$$T_{K/F}(a) = Tr(L_a)$$

Στην περίπτωση που $F = \mathbb{Q}$, ή δεν υπάρχει σύγχυση για το υπόσωμα θα γράφουμε $N_K(a)$ και $T_K(a)$.

Ένα χρήσιμο παράδειγμα: $d \neq 1$ Έστω η επέκταση K/F με $F = \mathbb{Q}$ και $K = \mathbb{Q}(\sqrt{d})$ με d ακέραιο που δεν είναι τετράγωνο. Μια βολική βάση του K ως F διανυσματικό χώρο είναι η $\{1, \sqrt{d}\}$. Αν $a \in K$ με $a = x + y\sqrt{d}$ τότε

$$L_a(1) = x + y\sqrt{d} = x \cdot 1 + y \cdot \sqrt{d}$$
$$L_a(\sqrt{d}) = \sqrt{d}x + dy = dy \cdot 1 + x \cdot \sqrt{d}$$

Δηλαδή, ο πίνακας που αναπαριστά την απεικόνιση L_a είναι ο:

$$\begin{pmatrix} x & dy \\ y & x \end{pmatrix}$$

Και έτσι παίρνουμε

$$N_K(x + y\sqrt{d}) = x^2 - dy^2$$
$$T_K(x + y\sqrt{d}) = 2x$$

Να δειχθούν:

(1) $T_K(x) = nx$

(2) $T_K(x + y) = T_K(x) + T_K(y)$

(3) $T_K(ax) = aT_K(x)$

(4) $N_K(xy) = N_K(x)N_K(y)$

(5) $N_K(x) = x^n$.

Πρόταση 7. *Έστω K/F μια επέκταση σωμάτων βαθμού n και $x \in K$. Έστω $x_1, \ldots, x_m$ οι ρίζες του $Irr(x, K)$. Τότε:*

$$T_{K/F}(x) = r(x_1 + \ldots + x_m), \quad N_{K/F}(x) = (x_1 \cdots x_m)^r$$

όπου $r = [K : F[x]] = n/m$.

Απόδειξη. □

Πρόταση 8. *Για μια περιοχή R κυρίων ιδεωδών, τα ακόλουθα είναι ισοδύναμα:*

(1) *Η περιοχή R έχει ακριβώς ένα μη μηδενικό πρώτο ιδεώδες.*

(2) *Ως προς συντροφικότητα, η περιοχή R έχει ακριβώς ένα πρώτο στοιχείο.*

(3) *Η περιοχή R είναι τοπικός δακτύλιος και δεν είναι σώμα.*

Απόδειξη. □

Ορισμός. *Ένας δακτύλιος που ικανοποιεί τις παραπάνω συνθήκες ονομάζεται δακτύλιος διακριτής εκτίμησης.*

παράδειγμα $\mathbb{Z}_{(p)}$ διακριτή εκτίμηση να ορίσω τώρα·

Σε έναν δακτύλιο διακριτής εκτίμησης R με πρώτο στοιχείο p, τα μη μηδενικά στοιχεία του R γράφονται μοναδικά ως up^m όπου u είναι αντιστρέψιμο και $m \geq 0$ ($m > 0$ αν το στοιχείο είναι αντιστρέψιμο). Κάθε μη μηδενικό ιδεώδες a είναι της μορφής (p^m) για μοναδικό $m \in \mathbb{N}$. Έτσι, αν το a είναι ιδεώδες του R και το $\mathfrak{p}$ είναι το μοναδικό μέγιστο ιδεώδες του A, τότε $a = \mathfrak{p}^m$ για κάποιον ακέραιο $m \geq 0$.

Για ένα R-πρότυπο M και $m \in M$, ο μηδενιστής του m είναι το σύνολο

$$Ann(m) = \{a \in A| \quad am = 0\}$$

Είναι ιδεώδες του R, το οποίο είναι γνήσιο αν $m \neq 0$. Έστω ότι το R είναι δακτύλιος διακριτής εκτίμησης και c ένα μη μηδενικό στοιχείο του. Έστω $M = A/(c)$. Τότε για ένα στοιχείο $b + (c) \in M$ ο μηδενιστής είναι: p πρώτο στοιχείο του A.

$$Ann(b + (c)) = (p^{m-n})$$

πράγματι

Έτσι, ένα b για το οποίο το ιδεώδες $Ann(b + (c))$ είναι μεγιστικό, είναι της μορφής up^{m-1}, και για αυτήν την επιλογή το $Ann(b + (c))$ είναι πρώτο ιδεώδες που παράγεται από το $\frac{c}{b}$. Θα χρησιμοποιήσουμε αυτές τις παρατηρήσεις στα επόμενα

Πρόταση 9. *Μια ακέραια περιοχή R είναι δακτύλιος διακριτής εκτίμησης αν και μόνο αν:*

(1) *R είναι δακτύλιος της Noether.*

(2) *R είναι ακέραια κλειστός.*

(3) *R έχει ακριβώς ένα μη μηδενικό πρώτο ιδεώδες.*

Απόδειξη. □

Ορισμός. *Μια περιοχή του Dedekind είναι μια ακέραια περιοχή R για την οποία ισχύουν:*

(1) *R είναι δακτύλιος της Noether*

(2) *R είναι ακέραια κλειστός.*

(3) *Κάθε μη μηδενικό πρώτο ιδεώδες είναι μεγιστικό.*

Έτσι, η προηγούμενη πρόταση λέει ότι μια ακέραια περιοχή που είναι τοπικός δακτύλιος είναι περιοχή του Dedekind αν και μόνο αν είναι δακτύλιος διακριτής εκτίμησης.

Πρόταση 10. *Έστω R μια περιοχή του Dedekind, και έστω S ενα πολλαπλασιαστικό υποσύνολο του R. Τότε η τοπικοποίηση $S^{-1}A$ είναι περιοχή του Dedekind.*

Απόδειξη. □

Πρόταση 11. *Έστω R μια ακέραια περιοχή και έστω S ένα πολλαπλασιαστικό υποσύνολο του R. Τότε:*

(1) *Αν R είναι δακτύλιος της Noether, τότε είναι και ο $S^{-1}R$.*

(2) *Αν R είναι ακέραια κλειστός, τότε είναι και ο $S^{-1}R$.*

Πρόταση 12. *Μια ακέραια περιοχή R που είναι δακτύλιος της Noether είναι περιοχή του Dedekind αν και μόνο αν, για κάθε μη μηδενικό πρώτο ιδεώδες $\mathfrak{p}$ του R, η τοπικοποίηση $R_{\mathfrak{p}}$ είναι δακτύλιος διακριτής εκτίμησης.*

Απόδειξη. □

Θεώρημα 1. *Έστω R μια περιοχή του Dedekind. Τότε κάθε γνήσιο μη μηδενικό ιδεώδες $\mathfrak{a}$ του R γράφεται στην μορφή:*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

όπου τα $\mathfrak{p}_i$ είναι διακεκριμένα πρώτα ιδεώδη και $r_i > 0$. Τα $\mathfrak{p}_i$ και r_i είναι μοναδικά.

Χρειαζόμαστε τα ακόλουθα λήμματα για την απόδειξη

Λήμμα 2. *Έστω R ένας δακτύλιος της Noether, τότε κάθε ιδεώδες $\mathfrak{a}$ του R περιέχει ένα γινόμενο μη μηδενικών πρώτων ιδεωδών.*

Λήμμα 3. *Έστω R ενας δακτύλιος και $\mathfrak{a}, \mathfrak{b}$ σχετικά πρώτα ιδεώδη του R. Τότε, για κάθε $m, n \in mahtbbN$ τα a^m, b^n είναι σχετικά πρώτα*

Λήμμα 4. *Έστω $\mathfrak{p}$ ένα μεγιστικό ιδεώδες μιας ακέραιας περιοχής R, και έστω $\mathfrak{q}$ το ιδεώδες που παράγεται στην τοπικοποίηση $R_{\mathfrak{p}}$, δηλαδή $\mathfrak{q} = \mathfrak{p}R_{\mathfrak{p}}$. Η απεικόνιση:*

$$a + \mathfrak{p}^m \mapsto a + \mathfrak{q}^m : R/\mathfrak{p}^m \to R_{\mathfrak{p}}/\mathfrak{q}^m$$

είναι ισομορφισμός για κάθε $m \in \mathbb{N}$.

Παρατήρηση:

Στην απόδειξη δείξαμε ότι $\mathfrak{a}^{ec} = \mathfrak{a}$ αν το $\mathfrak{a}$ είναι δύναμη μεγιστικού ιδεωδούς $\mathfrak{p}$ και $S = S \setminus \mathfrak{p}$.

Θα αποδείξουμε τώρα το θεωρήμα ότι κάθε μη μηδενικό ιδεώδες $\mathfrak{a}$ μιας περιοχής του Dedekind R παραγοντοποιείται σε γινόμενο πρώτων ιδεωδών.

Με βάση το πρώτο (από τα 3) λήμματα, το $\mathfrak{a}$ περιέχει ένα γινόμενο μη μηδενικών πρώτων ιδεωδών:

$$\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$$

και υποθέτουμε ότι τα $\mathfrak{p}_i$ είναι διακεκριμένα. Τότε:

$$R/\mathfrak{b} \simeq A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_m^{r_m} \simeq R_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \cdots R_{\mathfrak{p}_m}/\mathfrak{q}_m^{r_m}$$

όπου $\mathfrak{q}_i = \mathfrak{p}_i R_{\mathfrak{p}_i}$ το μέγιστο ιδεώδες στην τοπικοποίηση $R_{\mathfrak{p}_i}$. Ο πρώτος ισομορφισμός είναι από το δεύτερο λήμμα σε συνδυασμό με το κινέζικο θεώρημα υπολοίπων. Ο δεύτερος ισομορφισμός προκύπτει από το τρίτο λήμμα. Με αυτόν τον ισομορφισμό έχουμε ότι το πηλίκο $\mathfrak{a}/\mathfrak{b}$ αντιστοιχεί στο $\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \cdots \times \mathfrak{q}_m^{s_m}/\mathfrak{q}_m^{r_m}$ για κάποια $s_i \leq r_i$. Υπενθυμίζουμε ότι τα $R_{\mathfrak{p}_i}$ είναι όλα δακτύλιοι διακριτής εκτίμησης. Καθώς αυτό το ιδεώδες είναι και η εικόνα του $\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ υπό τον ισομορφισμό, βλέπουμε ότι

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} \quad \text{στο } R/\mathfrak{b}$$

Ωστόσο και τα δύο ιδεώδη αυτά περιέχουν το $\mathfrak{b}$, άρα:

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$$

στο R από το θεώρημα αντιστοιχίας ιδεωδών, υπάρχει 1-1 αντιστοιχία με τα ιδεώδη του $R/\mathfrak{b}$ και τα ιδεώδη του R που περιέχουν το $\mathfrak{b}$.

Για να συμπληρώσουμε την απόδειξη του θεωρήματος, πρέπει να δείξουμε ότι η παραγοντοποίηση είναι μοναδική. Υποθέτουμε ότι έχουμε δύο παραγοντοποιήσεις του ιδεωδούς $\mathfrak{a}$ και αφήνουμε τους εκθέτες να παίρνουν και την τιμή 0 ώστε να έχουμε τα ίδια πρώτα ιδεώδη στις δύο παραγοντοποιήσεις. Έτσι έχουμε:

$$\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} = \mathfrak{a} = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_m^{t_m}$$

Στην πορεία της απόδειξης, παραπάνω δείξαμε ότι:

$$\mathfrak{q}_i^{s_i} = \mathfrak{a}R_{\mathfrak{p}_i} = \mathfrak{q}_i^{t_i}$$

όπου $\mathfrak{q}_i$ το μεγιστικό ιδεώδες του $R_{\mathfrak{p}_i}$. Έπεται ότι $s_i = t_i$ για κάθε $i = 1, \ldots, m$.

Παρατήρηση:

$$s_i > 0 \iff \mathfrak{a}R_{\mathfrak{p}_i} \neq R_{\mathfrak{p}_i} \iff a \subseteq \mathfrak{p}_i$$

Πόρισμα 5. *Έστω $\mathfrak{a}$ και $\mathfrak{b}$ ιδεώδη του R. Τότε*

$$\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{a}R_{\mathfrak{p}} \subseteq \mathfrak{b}R_{\mathfrak{p}}$$

για όλα τα μη μηδενικά πρώτα ιδεώδη $\mathfrak{p}$ του R. Συγκεκριμένα, $\mathfrak{a} = \mathfrak{b}$ αν και μόνο αν $\mathfrak{a}R_{\mathfrak{p}} = \mathfrak{b}R_{\mathfrak{p}}$ για όλα αυτά τα $\mathfrak{p}$.

Απόδειξη. □

Παρατήρηση:
Έστω $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ και $\mathfrak{b} = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_m^{t_m}$ με $s_i, t_i \geq 0$. Τότε:

$$\mathfrak{a}|\mathfrak{b} \iff s_i \leq t_i \quad \forall i \iff \mathfrak{p}_i^{s_i} R_{\mathfrak{p}_i} \supseteq \mathfrak{p}_i^{t_i} R_{\mathfrak{p}_i} \iff \mathfrak{a} \supseteq \mathfrak{b}$$

Πόρισμα 6. *Έστω R μια ακέραια περιοχή με πεπερασμένο αριθμό πρώτων ιδεωδών. Τότε το R είναι περιοχή του Dedekind αν και μόνο αν είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. □

Πόρισμα 7. *Έστω $\mathfrak{a} \supseteq \mathfrak{b} \neq 0$ δύο ιδεώδη σε μια περιοχή R του Dedekind. Τότε $\mathfrak{a} = \mathfrak{b} + (a)$ για κάποιο $a \in R$.*

Πόρισμα 8. *Έστω $\mathfrak{a}$ ένα ιδεώδες σε μια περιοχή R του Dedekind και a ένα μη μηδενικό στοιχείο του $\mathfrak{a}$. Τότε υπάρχει $b \in \mathfrak{a}$ με $\mathfrak{a} = (a, b)$.*

Πόρισμα 9. *Έστω $\mathfrak{a}$ ένα μη μηδενικό ιδεώδες σε μια περιοχή R του Dedekind. Τότε υπάρχει ένα μη μηδενικό ιδεώδες $\mathfrak{a}^*$ τέτοιο ώστε το ιδεώδες $\mathfrak{a}\mathfrak{a}^*$ είναι κύριο. Επιπλέον, το $\mathfrak{a}^*$ μπορεί να επιλεγεί να είναι σχετικά πρώτο με οποιοδήποτε ιδεώδες $\mathfrak{c}$ καθώς και μπορεί να επιλεγεί έτσι ώστε $\mathfrak{a}\mathfrak{a}^* = (a)$ για οποιοδήποτε στοιχείο $a \in \mathfrak{a}$ (αλλά όχι και οι δύο συνθήκες ταυτόχρονα).*

Στο μάθημα Δακτύλιοι και Πρότυπα δείχνουμε ότι μια περιοχή κυρίων ιδεωδών είναι περιοχή μοναδικής παραγοντοποίησης. Το αντίστροφο δεν ισχύει καθώς, για παράδειγμα το $k[x, y]$ όπου k σώμα είναι περιοχή μοναδικής παραγοντοποίησης ενώ το (x, y) δεν είναι κύριο. Ωστόσο, το αντίστροφο ισχύει για τις περιοχές του Dedekind όπως θα δείξουμε

Πρόταση 13. *Μια περιοχή του Dedekind που είναι περιοχή μοναδικής παραγοντοποίησης είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. □

Ορισμός. *Έστω R μια περιοχή του Dedekind. Ένα κλασματικό ιδεώδες του R είναι ένα μη μηδενικό R-υποπρότυπο $\mathfrak{a}$ του K, όπου $K = Quot(R)$ το σώμα πηλίκων του R, τετοιο ώστε*

$$d\mathfrak{a} = \{da| \quad a \in \mathfrak{a}\}$$

περιέχεται στο R για κάποιο μη μηδενικό $d \in R$ (ή K). Δηλαδή είναι ένα μη μηδενικό R-υποπρότυπο του K του οποίου τα στοιχεία έχουν κοινό παρονομαστή

Για παράδειγμα το $\frac{1}{3}\mathbb{Z}$ είναι κλασματικό ιδεώδες του $\mathbb{Z}$ αφού είναι $\mathbb{Z}$-υποπρότυπο του $\mathbb{Q}$ και $3(\frac{1}{3}\mathbb{Z}) \subseteq \mathbb{Z}$, μάλιστα είναι ίσα.

Όπως φάινεται και στο παράδειγμα, το κλασματικό ιδεώδες δεν είναι ιδεώδες του R με την συνήθη έννοια, εκτός και αν περιέχεται στο R εξ ολοκλήρου. Οπότε θα αναφερόμαστε στα συνήθη ιδεώδη ως ακέραια ιδεώδη.

Πρόταση 14. *Ένα μη μηδενικό $\mathfrak{a}$ R-υποπρότυπο του K είναι πεπερασμένα παραγόμενο αν και μόνο αν είναι κλασματικό ιδεώδες.*

Απόδειξη. □

Κάθε μη μηδενικό στοιχείο b του K ορίζει ένα κλασματικό ιδεώδες:

$$(b) = bR = \{ba : \quad a \in R\}$$

κάθε τέτοιο κλασματικό ιδεώδες το λέμε κύριο όπως στη συνήθη έννοια. Επιπλέον ορίζουμε με τον ίδιο τρόπο το γινόμενο των κλασματικών ιδεωδών, δηλαδή για $\mathfrak{a}, \mathfrak{b}$ δύο κλασματικά ιδεώδη έχουμε:

$$\mathfrak{a} \cdot \mathfrak{b} = \{\sum a_i b_i : \quad a_i \in \mathfrak{a}, \quad b_i \in \mathfrak{b}\}$$

και αυτό είναι πάλι κλασματικό ιδεώδες. Είναι προφανώς R-πρότυπο και αν $d_1\mathfrak{a} \subseteq R, d_2\mathfrak{b} \subseteq R$, τότε $d_1 d_2 \mathfrak{ab} \subseteq R$. Για κύρια κλασματικά ιδεώδη ισχύει $(a)(b) = (ab)$.

Θεώρημα 2. *Έστω R μια περιοχή του Dedekind. Το σύνολο των κλασματικών ιδεωδών $Id(R)$ αποτελεί μια ομάδα με πράξη τον παραπάνω πολλαπλασιασμό. Είναι η ελεύθερη αβελιανή ομάδα με βάση σύνολο των μη μηδενικών πρώτων ιδεωδών.*

Remarks σελίδα 54

Ορισμός (Ομάδα κλάσεως ιδεωδών)**.** *Ορίζουμε την ομάδα κλάσεως ιδεωδών του R να είναι το πηλίκο $Cl(A) = Id(A)/P(A)$ των $Id(A)$ στο πηλίκο των κυρίων ιδεωδών. Ο αριθμός κλάσεως του R είναι η τάξη αυτής της ομάδας (όταν είναι πεπερασμένη).*

Στην περίπτωση που R είναι οι αλγεβρικοί ακέραιοι ενός σωμάτος αριθμών K, ονομάζουμε το $Cl(\mathcal{O}_K)$ την ομάδα κλάσεως ιδεωδών του K και η τάξη της είναι ο αριθμός κλάσεως του K.

Ένα από τα κεντρικά θεωρήματα της αλγεβρικής θεωρίας αριθμών είναι ότι για σώματα αριθμών K ο αριθμός κλάσης h_K του K είναι πεπερασμένος.

Πρόταση 15. *Έστω R μια περιοχή του Dedekind και έστω S ένα πολλαπλασιαστικό υποσύνολο του R. Τότε ή απεικόνιση $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ ορίζει έναν ισομορφισμό από την υποομάδα $Id(R)$ που παράγεται από τα πρώτα ιδεώδη του R που δεν τέμνονται με το S στην ομάδα $Id(S^{-1}R)$.*

Απόδειξη. □

Παρατήρηση: Έστω R μια πεεριοχή του Dedekind με πεπερασμένη ομάδα κλάσεων ιδεωδών. Τότε υπάρχει ένα πεπερασμένο σύνολο ιδεωδών $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ που είναι ένα σύνολο αντιπροσώπων για τις κλάσεις των ιδεωδών. Μπορούμε να πάρουμε το $\mathfrak{a}_i$ να ειναι ακέραιο. Έστω b ένα μη μηδενικό στοιχείο του $\cap \mathfrak{a}_i$ και έστω S το πολλαπλασιαστικό σύνολο που παράγεται από το b, δηλαδή $S = \{1, b, b^2, \ldots\}$. Θα δείξουμε ότι το $S^{-1}R$ είναι περιοχή κυρίων ιδεωδών.

proof σελίδα 55

Παρατήρηση:

Για R μια ακέραια περιοχή της Noether, τα ακόλουθα είναι ισοδύναμα:

(1) R είναι περιοχή του Dedekind.

(2) Για κάθε πρώτο ιδεώδες $\mathfrak{p}$ του R, η τοπικοποίηση $R_\mathfrak{p}$ είναι δακτύλιος διακριτής εκτίμησης.

(3) Τα κλασματικά ιδεώδη του R αποτελούν ομάδα.

(4) Για κάθε κλασματικό ιδεώδες $\mathfrak{a}$ του R, υπάρχει ιδεώδες $\mathfrak{b}$ με $\mathfrak{ab} = R$.

σχεδόν απόδειξη σελ 55

Ορισμός (Διακριτή Εκτίμηση)**.** *Έστω K ένα σώμα. Μια διακριτή εκτίμηση του K είναι ένας μη μηδενικός ομομορφισμός $\nu : K^\times \to \mathbb{Z}$ τέτοιος ώστε:*

$$\nu(a+b) \geq \min(\nu(a), \nu(b))$$

Καθώς το ν δεν είναι ο μηδενικός ομομορφισμός, η εικόνα του είναι μη μηδενική υποομάδα του $\mathbb{Z}$ και άρα είναι της μορφής $m\mathbb{Z}$ για κάποιο $m \in \mathbb{Z}$. Αν $m = 1$, τότε το ν είναι επιμορφισμός και θα λέγεται κανονικοποιημένο. Διαφορετικά, η απεικόνιση $x \mapsto m^{-1}\nu(x)$ θα είναι μια κανονικοποιημένη διακριτή εκτίμηση. Επεκτείνουμε το ν σε μια απεικόνιση $K \mapsto \mathbb{Z} \cup \{\infty\}$ θέτοντας $\nu(0) = \infty$, όπου το ∞ είναι ένα σύμβολο μεγαλύτο του n για κάθε $n \in \mathbb{Z}$.

Για μια διακριτή εκτίμηση ν

$$\nu(a_1 + \ldots + a_m) \geq \min(\nu(a_1), \nu(a_2 + \ldots + a_m)) \geq \cdots \geq \min(\nu(a_i))$$

Παραδείγματα σελ 56

Πρόταση 16. *Έστω ν μια διακριτή εκτίμηση στο σώμα K. Τότε:*

$$\{a \in K : \quad \nu(a) \geq 0\}$$

είναι μια περιοχή κυρίων ιδεωδών με μεγιστικό ιδεώδες:

$$\{a \in K : \quad \nu(a) > 0\}$$

Αν $\nu(K^\times) = m\mathbb{Z}$, τότε το παραπάνω μεγιστικό ιδεώδες παράγεται από κάθε στοιχείο x τέτοιο ώστε $\nu(x) = m$.

Απόδειξη. □

Πρόταση 17. *Έστω $x_1, \ldots, x_m$ στοιχεία μιας περιοχής R του Dedekind και έστω $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ να είναι διακεκριμένα πρώτα ιδεώδη του R. Για κάθε ακέραιο n, υπάρχει $x \in R$ τέτοιο ώστε:*

$$ord_{\mathfrak{p}_i}(x - x_i) > n, \quad i = 1, 2, \ldots, m.$$

Απόδειξη. □

Θεώρημα 3. *Έστω R μια περιοχή του Dedekind με σώμα πηλίκων K. Έστω B η ακέραια θήκη του R σε μια πεπερασμένη διαχωρίσιμη επέκταση L του K. Τότε το B είναι περιοχή του Dedekind.*

Απόδειξη. □

Λήμμα 5. *Κάθε ακέραια περιοχή B που περιέχει ένα σώμα k και είναι αλγεβρική υπεράνω του k είναι σώμα.*

Απόδειξη. □

in fact σελ 57

Έστω R μια περιοχή του Dedekind με σώμα πηλίκων K και έστω B η ακέραια θήκη του R σε μια πεπερασμένη διαχωρίσιμη επέκταση L του K.

Ένα πρώτο ιδεώδες $\mathfrak{p}$ θα παραγοντοποιείται στο B ως:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \quad e_i \geq 1$$

Αν κάποιος από τους εκθέτες είναι > 1 λέμε ότι το $\mathfrak{p}$ διακλαδίζεται στο B (ή L). Ο αριθμός e_i λέγεται δείκτης διακλάδωσης.

Θα λέμε ότι το $\mathfrak{P}$ διαιρεί το $\mathfrak{p}$ και θα χρησιμοποιούμε τον συνήθη συμβολισμό $\mathfrak{P}|\mathfrak{p}$ αν το $\mathfrak{P}$ εμφανίζεται στην παραγοντοποίηση του $\mathfrak{p}$. Γράφουμε $e(\mathfrak{P}/\mathfrak{p})$ για τον δείκτη διακλάδωσης και $f(\mathfrak{P}/\mathfrak{p})$ για τον βαθμό της επέκτασης σωμάτων $[B/\mathfrak{P} : R/\mathfrak{p}]$ (το οποίο ονομάζεται βαθμός κλάσεως υπολοίπων).

Ένα πρώτο ιδεώδες $\mathfrak{p}$ του R θα λέμε ότι διασπάται (ή διασπάται πλήρως) στο L αν $e_i = f_i = 1$ για όλα τα i, και λέμε ότι είναι αδρανές στο L αν το $\mathfrak{p}B$ είναι πρώτο ιδεώδες (δηλαδή $g = 1 = e$).

Για παράδειγμα σελίδα 59

Λήμμα 6. *Ένα πρώτο ιδεώδες $\mathfrak{P}$ του B διαιρεί το $\mathfrak{p}$ αν και μόνο αν $\mathfrak{p} = \mathfrak{P} \cap K$.*

Απόδειξη. □

Θεώρημα 4. *Έστω m ο βαθμός της επέκτασης L υπεράνω του K και $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ τα πρώτα ιδεώδη που διαιρούν το $\mathfrak{p}$. Τότε:*

$$\sum_{i=1}^{g} e_i f_i = m$$

όπου $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ και $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Αν η επέκταση L/K είναι Galois, τότε όλοι οι δείκτες διακλάδωσης είναι ίσοι, καθώς και οι βαθμοί κλάσεων υπολοίπων. Άρα σε αυτή τη περίπτωση ισχύει:

$$efg = m$$

Απόδειξη. □

Θεώρημα 5. *Έστω L μια πεπερασμένη επέκταση ενός σωμάτος αριθμών K και έστω R μια περιοχή του Dedekind που περιέχεται στο K και έχει το K ως σώμα πηλίκων (π.χ. $R = \mathcal{O}_K$). Έστω B η ακέραια θήκη του R στο L. Υποθέτουμε ότι το B είναι ελεύθερο R-πρότυπο (αυτό ισχύει για παράδειγμα όταν R είναι περιοχή κυρίων ιδεωδών). Τότε ένα πρώτο ιδεώδες $\mathfrak{p}$ διακλαδίζεται στο L αν και μόνο αν $\mathfrak{p}|disc(B/A)$. Συγκεκριμένα, μόνο πεπερασμένο πλήθος πρώτων ιδεωδών διακλαδίζονται.*

Η απόδειξη του θεωρήματος βασίζεται στα ακόλουθα λήμματα

Λήμμα 7. *Έστω R δακτύλιος και B ένας δακτύλιος που περιέχει το A και έχει μια πεπερασμένη βάση $\{e_1, \ldots, e_m\}$ ως R-πρότυπο. Τότε για κάθε ιδεώδες $\mathfrak{a}$ του R, τα στοιχεία $\overline{e}_i = e_i + \mathfrak{a}$ αποτελούν βάση του $R/\mathfrak{a}$-προτύπου $B/\mathfrak{a}B$ και:*

$$D(\overline{e}_1, \ldots, \overline{e}_m) = D(e_1, \ldots, e_m) \quad mod\mathfrak{a}$$

Απόδειξη. □

Λήμμα 8. *Έστω R δακτύλιος και $B_1, \ldots, B_g$ δακτύλιοι που περιέχουν το R και είναι ελεύθερα με πεπερασμένο βαθμό σαν R-πρότυπα. Τότε:*

$$disc((\prod B_i)/R) = \prod disc(B_i/A).$$

Υπενθυμίζουμε ένα στοιχείο a ενός δακτυλίου λέγεται μηδενοδύναμο αν $a^m = 0$ για κάποιον ακέραιο $m > 1$. Ένας δακτύλιος λέγεται reduced αν δεν έχει μη μηδενικά μηδενοδύναμα στοιχεία.

Επιπλέον ένα σώμα k λέγεται τέλειο αν κάθε πεπερασμένη επέκταση K/k είναι διαχωρίσιμη και ένα σώμα k χαρακτηριστικής $p \neq 0$ είναι τέλειο αν κάθε στοιχείο του είναι μια p-οστή δύναμη. (Να δω από Morandi). Ένα πεπερασμένο σώμα k χαρακτηριστικής p είναι τέλειο καθώς η απεικόνιση $k \to k, x \mapsto x^p$ είναι μονομορφισμός και άρα και επιμορφισμός.

Λήμμα 9. *Έστω k ένα τέλειο σώμα και έστω B μια k-άλγεβρα πεπερασμένης διάστασης. Τότε το B είναι reduced αν και μόνο αν $disc(B/k) \neq 0$.*

Απόδειξη. □

Απόδειξη Θεωρήματος σελίδα 62

Βρίσκοντας παραγοντοποιήσεις

Θεώρημα 6. *Έστω $B = R[a]$ και $f(x)$ το ελάχιστο πολυώνυμο του a υπεράνω του $K = Quot(R)$. Έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες του R. Διαλέγουμε μονικά πολυώνυμα $g_1(x), \ldots, g_r(x)$ στο $R[x]$ τα οποία είναι διακεκριμένα και ανάγωγα modulo $\mathfrak{p}$, τέτοια ώστε*

$$f(x) = \prod g_i(x)^{e_i} \quad mod \mathfrak{p}$$

. Τότε:

$$\mathfrak{p}B = \prod (\mathfrak{p}, g_i(a))^{e_i}$$

είναι η παραγοντοποίηση του $\mathfrak{p}B$ σε ένα γινόμενο δυνάμεων διακεκριμένων πρώτων ιδεωδών. Επιπλέον, το σώμα υπολοίπων $B/(\mathfrak{p}, g_i(a)) \simeq (A/\mathfrak{p})[x]/(\overline{g}_i)$ και έτσι το f_i είναι ίσο με τον βαθμό του πολυωνύμου g_i.

Απόδειξη. □

μετά examples

Έστω A μια περιοχή του Dedekind με σωμα πηλίκων K και έστω B η ακέραια θήκη του A σε μια πεπερασμένη διαχωρίσιμη επέκταση L/K. Θέλουμε να επεκτείνουμε τον ορισμό της νόρμας στοιχείως σε έναν ομομορφισμό $N : Id(B) \to id(A)$, δηλαδή το παρακάτω διάγραμμα να είναι μεταθετικό

$$\begin{array}{ccc} L^\times & \xrightarrow{b\mapsto(b)} & Id(B) \\ {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle N} \\ K^\times & \xrightarrow{a\mapsto(a)} & Id(A) \end{array}$$

Καθώς το $Id(B)$ είναι ελεύθερη αβελιανή ομάδα με βάση τα πρώτα ιδεώδη, έχουμε να ορίσουμε το $N(\mathfrak{p})$ για $\mathfrak{p}$ πρώτο.

Έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες του A και η παραγοντοποίηση $\mathfrak{p}B = \prod_i \mathfrak{P}_i^{e_i}$. Αν το $\mathfrak{p}$ είναι κύριο, έστω $\mathfrak{p} = (\pi)$, τότε θα θέλουμε να έχουμε:

$$N(\mathfrak{p}B) = N(\pi B) = N(\pi)A = (\pi^m) = \mathfrak{p}^m, \quad m = [L : K]$$

και καθώς το N είναι ομομορφισμός θα θέλουμε

$$N(\mathfrak{p}B) = N(\prod \mathfrak{P}_i^{e_i}) = \prod N(\mathfrak{P}_i^{e_i})$$

Συγκρίνουμε τα παραπάνω καθώς και από τα προηγούμενα έχουμε $m = \sum e_i f_i$, άρα βλέπουμε ότι πρέπει να ορίσουμε $N(\mathfrak{P}_i) = \mathfrak{p}^{f_i}$. Άρα ορίζουμε:

Ορισμός (Νόρμα Ιδεωδούς)**.** *Για $\mathfrak{p}B = \prod_i \mathfrak{P}_i^{e_i}$ όπως παραπάνω, Θέτουμε*

$$N(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$$

όπου $\mathfrak{p} = \mathfrak{P} \cap A$ και $f(\mathfrak{P}/\mathfrak{p}) = [B/\mathfrak{P} : A/\mathfrak{p}]$. Θα συμβολίζουμε την νόρμα ιδεωδών με $\mathcal{N}$

Για διαδοχικές επεκτάσεις σωμάτων $K \subseteq L \subseteq M$ ισχύει ότι:

$$\mathcal{N}_{L/K}(\mathcal{N}_{M/L}(\mathfrak{a})) = \mathcal{N}_{M/K}(\mathfrak{a})$$

καθώς $f(\mathfrak{Q}/\mathfrak{P}) \cdot f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{p})$, δηλαδή $[C/\mathfrak{Q} : B/\mathfrak{P}] \cdot [B/\mathfrak{P} : A/\mathfrak{p}] = [C : \mathfrak{Q} : A/\mathfrak{p}]$ όπου $C \supseteq B \supseteq A$ είναι ακέραιες θήκες του A στα M, L, K αντίστοιχα.

Πρόταση 18. *Έστω $A \subseteq B$ και $K \subseteq L$ όπως παραπάνω. Τότε:*

(1) *Για κάθε μη μηδενικό ιδεώδες $\mathfrak{a} \subseteq A$, $\mathcal{N}_{K/L}(\mathfrak{a}B) = a^m$, όπου $m = [L : K]$.*

(2) *Υποθέτουμε ότι η επέκταση L/K είναι Galois. Έστω $\mathfrak{P}$ ένα μη μηδενικό πρώτο ιδεώδες του B και έστω $\mathfrak{p} = \mathfrak{P} \cap A$. Γράφουμε $\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ (από πρόταση τάδε, galois). Τότε*

$$\mathcal{N}(\mathfrak{B}) \cdot B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{ef} = \prod_{\sigma \in Gal(L/K)} \sigma\mathfrak{P}$$

.

(3) *Για κάθε μη μηδενικό $b \in B, N(b) \cdot A = N(b \cdot B)$.*

Απόδειξη. □

Πρόταση 19. *Έστω $\mathfrak{a}$ ένα μη μηδενικό ιδεώδες στον δακτύλιο ακεραίων $\mathcal{O}_K$ ενός σώματος αριθμών K. Τότε το $\mathfrak{a}$ είναι πεπερασμένου δείκτη, δηλαδή $[\mathcal{O}_K : \mathfrak{a}] < \infty$.*

Απόδειξη. □

Ορισμός. *Έστω* $\mathfrak{a}$ *όπως στην προηγούμενη πρόταση. Ορίζουμε την αριθμητική νόρμα* $\mathbb{N}\mathfrak{a}$ *του* $\mathfrak{a}$ *να είναι ο πεπερασμένος δείκτης:*

$$\mathbb{N}\mathfrak{a} = (\mathcal{O}_K : \mathfrak{a})$$

Πρόταση 20. *Έστω* $\mathcal{O}_K$ *ο δακτύλιος των ακεραίων σε ένα σώμα αριθμών* K*. Τότε:*

(1) *Για κάθε ιδεώδες* $\mathfrak{a}$ *του* $\mathcal{O}_K$*, έχουμε* $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) = (\mathbb{N}(a))$ *και άρα ισχύει* $\mathbb{N}(\mathfrak{ab}) = \mathbb{N}(\mathfrak{a})\mathbb{N}(\mathfrak{b})$*.*

(2) *Έστω* $\mathfrak{b} \subseteq \mathfrak{a}$ *κλασματικά ιδεώδη στο* K*. Τότε:*

$$(\mathfrak{a} : \mathfrak{b}) = \mathbb{N}(\mathfrak{a}^{-1}\mathfrak{b})$$

.

Απόδειξη. □

κεντρικό θεώρημα:

Θεώρημα 7. *Έστω* K *μια επέκταση βαθμού* n *του* $\mathbb{Q}$ *και* Δ_K *η διακρίνουσα του* $K/\mathbb{Q}$*. Έστω* $2s$ *ο αριθμός των μη πραγματικών εμφυτεύσεων του* K *στο* $\mathbb{C}$*. Τότε υπάρχει ένα σύνολο αντιπροσώπων για την ομάδα κλάσεως ιδεωδών του* K *που αποτελείται από (ακέραια) ιδεώδη* $\mathfrak{a}$ *με*

$$\mathbb{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |Delta_K|^{\frac{1}{2}}$$

Ο αριθμός αριστερά καλείται το φράγμα του Minkowski και ο όρος $C_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s$ η σταθερά του Minkowski.

Θεώρημα 8. *Ο αριθμός κλάσης ενός σώματος αριθμών* K *είναι πεπερασμένος*

Απόδειξη. □

παραδείγματα

Ορισμός. *Μια επέκταση* L/K *ενός σώματος αριθμών ονομάζεται αδιακλάδωτη υπεράνω του* K *αν δεν υπάρχει πρώτο ιδεώδες του* $\mathcal{O}_K$ *που να διακλαδίζεται στο* $\mathcal{O}_L$*.*

Θεώρημα 9. *Δεν υπάρχει αδιακλάδωτη επέκταση του* $\mathbb{Q}$*.*

Απόδειξη. □

Δικτυωτά

Έστω V ένας διανυσματικός χώρος διάστασης n υπεράνω του $\mathbb{R}$. Ένα δικτυωτό Λ στο V είναι μια υποομάδα της μορφής:

$$\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$$

με $e_1, \ldots, e_r$ γραμμικά ανεξάρτητα στοιχεία του V. Συνεπώς, ένα δικτυωτό είναι μια ελεύθερη αβελιανή υποομάδα του V που παράγεται από τα στοιχεία του V που είναι γραμμικά ανεξάρτητα υπεράνω του $\mathbb{R}$. Όταν $r = n$, λέμε το δικτυωτό ότι είναι πλήρες. Αντίθετα, $\Lambda = \{0\}$ είναι ένα δικτυωτό που παράγεται από το κενό σύνολο.

Χρειαζόμαστε κριτήρια για το πότε υποομάδες Λ του V είναι δικτυωτά. Η επιλογή μιας βάσης του V καθορίζει έναν ισομορφισμό του V με το $\mathbb{R}^n$, και άρα μια τοπολογία στο V. Η τοπολογία αυτή είναι ανεξάρτητη της βάσης που διαλέξαμε καθώς κάθε γραμμικός αυτομορφισμός του $\mathbb{R}^n$ είναι ομοιομορφισμός. Μια υποομάδα Λ του V λέγεται διακριτή, αν είναι διακριτή με την τοπολογία που προκύπτει. Ένας τοπολογικός χώρος λέγεται διακριτός αν όλα του τα σημεία (και άρα όλα τα υποσύνολα) είναι ανοιχτά. Άρα το ότι το Λ είναι διακριτό σημαίνει ότι κάθε στοιχείο του a στο Λ έχει μια περιοχή U στο V τέτοια ώστε $U \cap \Lambda = \{a\}$.

Λήμμα 10. *Για μια υποομάδα Λ ενός πεπερασμένης διάστασης πραγματικού διανυσματικού χώρου V, τα ακόλουθα είναι ισοδύναμα:*

(1) *Λ είναι διακριτή υποομάδα.*

(2) *Υπάρχει ανοιχτό υποσύνολο U του V με $U \cap \Lambda = \{0\}$.*

(3) *Κάθε συμπαγές υποσύνολο του V τέμνει το Λ και η τομή τους είναι πεπερασμένο σύνολο.*

(4) *Κάθε φραγμένο υποσύνολο του V τέμνει το Λ και η τομή τους είναι πεπερασμένο σύνολο*

Απόδειξη. □

Πρόταση 21. *Μια υποομάδα Λ του V είναι δικτυωτό αν και μόνο αν είναι διακριτή.*

Απόδειξη. □

Ορισμός. *Έστω V ένας πραγματικός διανυσματικός χώρος διάστασης n και έστω Λ ένα πλήρες δικτυωτό στο V, $\Lambda = \sum \mathbb{Z}e_i$. Για ένα $\lambda_0 \in \Lambda$, ορίζουμε*

$$D = \{\lambda_0 + \sum a_i e_i : \quad 0 \leq a_i < 1\}$$

Ένα τέτοιο σύνολο θα λέγεται θεμελιώδες παραλληλεπίπεδο στο Λ.

το σχήμα του παραλληλεπίπεδου εξαρτάται από την βάση (e_i), αλλά αν θεωρήσουμε μια σταθερή βάση, τότε για τα διάφορα $\lambda_0 \in \Lambda$ τα παραλληλεπίπεδα καλύπτουν τον χώρο $\mathbb{R}^n$ χωρίς επικαλύψεις.

Παρατήρηση: (από ανάλυση)

$\Lambda = \mathbb{Z}f_1 + \ldots + \mathbb{Z}f_n$ στο $\mathbb{R}^n$, τότε ο όγκος του D είναι:

$$\mu(D) = |det(f_1, \ldots, f_n)|$$

όπου μ είναι το μέτρο Lebesgue

Θεώρημα 10. *Έστω D_0 ένα θεμελιώδες παραλληλεπίπεδο για ένα πλήρες δικτυωτό στο V και έστω S ένα μετρήσιμο υποσύνολο στο V. Αν $\mu(S) > \mu(D_0)$, τότε το S περιέχει διακεκριμένα σημεία a και b τέτοια ώστε $b - a \in \Lambda$.*

Απόδειξη. □

Υπενθυμίζουμε ένα σύνολο λέγεται κυρτό, αν μεταξύ δύο σημείων τραβώντας μια ευθεία που ενώνει τα σημεία η ευθεία παραμένει μέσα στο σύνολο. Επιπλέον λέμε ότι ένα σύνολο T είναι συμμετρικό στο $0 \in \mathbb{R}^n$ αν από την σχέση $a \in T$ συνεπάγεται $-a \in T$.

Θεώρημα 11 (Miknowski)**.** *Έστω T ένα υποσύνολο του V που είναι συμπαγές, κυρτό και συμμετρικό στο* 0*. Αν ισχύει ότι:*

$$\mu(T) \geq 2^n \mu(D)$$

τότε το T περιέχει και άλλο σημείο εκτός από το 0*.*

Απόδειξη. □

some calculus

Έστω K ένα σώμα αριθμών βαθμού n υπεράνω του $\mathbb{Q}$. Υποθέτουμε ότι το K έχει r πραγματικές εμφυτεύσεις $\{\sigma_1, \ldots, \sigma_r\}$ και $2s$ μιγαδικές $\{\sigma_{r+1}, \overline{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma}_{r+s}\}$. Έτσι $n = r + 2s$. Έχουμε την εμφύτευση

$$\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s, \quad a \mapsto (\sigma_1 a, \ldots, \sigma_{r+s} a)$$

.

Θα αναγνωρίζουμε το $V = \mathbb{R}^r \times \mathbb{C}^s$ ως το $\mathbb{R}^n$ χρησιμοποιώντας την βάση $\{1, i\}$ για το $\mathbb{C}$.

Πρόταση 22. *Έστω $\mathfrak{a}$ ένα μη μηδενικό ιδεώδες του $\mathcal{O}_K$, τότε $\sigma(\mathfrak{a})$ είναι ένα πλήρες δικτυωτό στο V, και ο όγκος ενός θεμελιώδους παραλληλεπιπέδου του $\sigma(\mathfrak{a})$ είναι $2^{-s} \cdot \mathbb{N}(\mathfrak{a})|\Delta_K|^{\frac{1}{2}}$.*

Απόδειξη. □

Πρόταση 23. *Έστω $\mathfrak{a}$ ένα μη μηδενικό ιδεώδες στο $\mathcal{O}_K$. Τότε το $\mathfrak{a}$ περιέχει ένα μη μηδενικό στοιχείο a του K με*

$$|N(a)| \leq B_K \cdot \mathbb{N}(\mathfrak{a}) = \left(\frac{4}{\pi}\right) \frac{n!}{n^n} \mathbb{N}(\mathfrak{a})|\Delta_K|^{\frac{1}{2}}$$

.

Απόδειξη. □

και απόδειξη θεωρήματος πιο πριν και τέλος

Ορισμός (Περιοχή Dedekind)**.** *Μια ακέραια περιοχή R την ονομάζουμε περιοχή του Dedekind αν:*

(1) *Κάθε ιδεώδες είναι πεπερασμένα παραγόμενο.*

(2) *Κάθε πρώτο ιδεώδες είναι και μεγιστικό.*

(3) *Το R είναι ακέραια κλειστό στο σώμα πηλίκων του. Δηλαδή, αν K είναι το σώμα πηλίκων του και $a/b \in K$ είναι μια ρίζα ενός μονικού πολυωνύμου με συντελεστές από το R, τότε $a/b \in R$ και έτσι $b|a$ στο R.*

Έστω ένα σώμα αριθμών $K = \mathbb{Q}(\theta)$ βαθμού $n = [K : \mathbb{Q}]$. Μπορούμε να δούμε το K μέσω ισομορφισμού ως $\mathbb{Q}[x]/(f)$ όπου f είναι το ελάχιστο πολυώνυμο του $\theta \in K$. Καθώς το $\mathbb{C}$ είναι αλγεβρικά κλειστό και το f είναι ανάγωγο, αυτό έχει n διακεκριμένες μιγαδικές ρίζες. Κάθε τέτοια ρίζα $z_i \in \mathbb{C}$ επάγει έναν ομομορφισμό $\mathbb{Q}[x] \to \mathbb{C}$ με $g(x) \mapsto g(z_i)$ με πυρήνα το ιδεώδες που παράγεται από το f. Έτσι έχουμε n μονομορφισμούς του $K \simeq \mathbb{Q}[x]/(f) \hookrightarrow \mathbb{C}$. Αυτοί είναι και όλοι οι μονομορφισμοί $K \hookrightarrow \mathbb{C}$, εφόσον κάθε τέτοιος μονομορφισμός θα κρατάει σταθερό το $\mathbb{Q}$ και στην ουσία μιλάμε για τα n στοιχεία της ομάδας $Gal(K/\mathbb{Q})$ με την μόνη διαφορά ότι δεν τα βλέπουμε πλέον σαν $\mathbb{Q}$-αυτομορφισμούς του K και αλλάζουμε το πεδίο τιμών να είναι το $\mathbb{C}$.
Με βάση τους παραπάνω μονομορφισμούς, θα ορίσουμε την διακρίνουσα βάσης ενός σώματος αριθμών.

Ορισμός (Διακρίνουσα Βάσης)**.** *Έστω $K = \mathbb{Q}(\theta)$ και $a_1, \ldots, a_n$ μια βάση του ως $\mathbb{Q}$-διανυσματικός χώρος. Θεωρούμε τους μονομορφισμούς $\sigma_i : K \hookrightarrow \mathbb{C}$ για $i = 1, \ldots, n$. Ορίζουμε τον πίνακα:*

$$(\sigma_i(a_j)) = \begin{pmatrix} \sigma_1(a_1) & \sigma_1(a_2) & \cdots & \sigma_1(a_n) \\ & \cdots & & \\ \sigma_n(a_1) & \sigma_n(a_2) & \cdots & \sigma_n(a_n) \end{pmatrix}$$

και η διακρίνουσα της βάσης θα ονομάζεται ο μιγαδικός αριθμός $\Delta(a_1, \ldots, a_n) = (det(\sigma_i(a_j)))^2$.

Πρόταση 24. *Κάθε διακρίνουσα βάσης αριθμητικού σώματος είναι μη μηδενικός ρητός αριθμός.*

Απόδειξη. Έστω $K = \mathbb{Q}(\theta)$ σώμα αριθμών και $\theta_1, \ldots, \theta_n$ οι μιγαδικές ρίζες του ελαχίστου πολυωνύμου $Irr(\theta, \mathbb{Q})$. Δεν έχουμε κάποια πολλαπλή ρίζα καθώς τα ανάγωγα πολυώνυμα με συντελεστές υποσώματα του $\mathbb{C}$ έχουν μόνο απλές ρίζες αν χρησιμοποιήσουμε το κριτήριο της παραγώγου και την χαρακτηριστική 0. Υπενθυμίζουμε ότι μια βάση του K ως $\mathbb{Q}$-διανυσματικού χώρου είναι η $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$. Έχουμε την διακρίνουσα αυτής της βάσης να είναι

$$\Delta(1, \theta, \ldots, \theta^{n-1}) = det(\theta_i^j)^2, \quad i = 1, \ldots, n, \quad j = 1, \ldots, n-1$$

και η ορίζουσα

$$det(\theta_i^j) = det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ & & \cdots & & \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{pmatrix}$$

είναι γνωστή ως ορίζουσα Vandermode. Άρα

$$\Delta(1, \theta, \ldots, \theta^{n-1}) = \prod_{r<s} (\theta_r - \theta_s)^2$$

Το δεξί μέλος είναι συμμετρικό ως προς τα θ_i και άρα από το θεμελιώδες θεώρημα συμμετρικών πολυωνύμων είναι πολυώνυμο στα στοιχειώδη συμμετρικά πολυώνυμα $e_1 = \theta_1 + \ldots + \theta_n, e_2 = \theta_1\theta_2 + \ldots + \theta_1\theta_3 + \ldots + \theta_{n-1}\theta_n, \ldots, e_n = \theta_1 \cdots \theta_n$. Από τους τύπους του Vieta έχουμε ότι $e_i = \pm p_{n-i}$ όπου $Irr(\theta, \mathbb{Q}) = p_0 + p_1 x + \ldots + p_{n-1}x^{n-1} + x^n$. Οι συντελεστές p_i ανήκουν ήδη στο $\mathbb{Q}$ και άρα $\Delta(1, \theta, \ldots, \theta^{n-1}) \in Q$. Έχουμε ότι $\Delta \neq 0$ εφόσον $\theta_i \neq \theta_s$ αφού δεν έχουμε διπλές ρίζες και άρα δεν συναντάμε το 0 στο γινόμενο.

Θα δείξουμε τώρα τον ισχυρισμό της πρότασης και για τυχαία βάση του K. Έστω $a_1, \ldots, a_n$ τέτοια βάση. Γράφουμε

$$a_k = \sum_j b_{kj}\theta^j, \quad b_{kj} \in Q, k = 1, \ldots, n$$

και έτσι έχουμε

$$\Delta(a_1, \ldots, a_n) = det(\sigma_i(a_k))^2 = det\left(\sum_j b_{kj}\theta^j\right)^2 =$$

$$= det(b_{kj})^2 det(\theta_i^j)^2 = det(b_{kj})^2 \Delta(1, \theta, \ldots, \theta^{n-1})$$

Ισχύει ότι $det(b_{kj}) \neq 0$ γιατί αυτός ο πίνακας είναι πίνακας αλλαγής βάσης διανυσματικού χώρου. Έχουμε ότι $\Delta(1, \theta, \ldots, \theta^{n-1}) \neq 0$ και άρα $\Delta(a_1, \ldots, a_n) \neq 0$. Τέλος, έχουμε ότι

$$det(b_{kj})^2, \Delta(1, \theta, \ldots, \theta^{n-1}) \in Q \implies \Delta(a_1, \ldots, a_n) \in \mathbb{Q}$$

□

Αυτή η απόδειξη μας δίνει κάτι επιπλέον, με το επιχείρημα που χρησιμοποιήθηκε στο τέλος της έχουμε ότι για δύο τυχαίες βάσεις A, A' του K ως $\mathbb{Q}$-διανυσματικού χώρου, αν B είναι ο πίνακας μετάβασης από την A στην A' τότε

$$\Delta(A') = (detB)^2 \Delta(A)$$

Ορισμός (Αλγεβρικοί Ακέραιοι)**.** *Έστω F ένα σώμα αριθμών. Ο δακτύλιος των αλγεβρικών ακεραίων του F είναι η ακέραια θήκη του $\mathbb{Z}$ στο F και θα συμβολίζεται με $\mathcal{O}_F$. (να δω Μαλιάκα)*

Πρόταση 25. *Έστω $a \in K$ όπου το K είναι σώμα αριθμών. Τότε το a είναι αλγεβρικός ακέραιος αν και μόνο αν $Irr(a, \mathbb{Q}) \in \mathbb{Z}[x]$, δηλαδή οι συντελεστές του ελαχίστου πολυωνύμου του a υπεράνω του $\mathbb{Q}$ είναι ακέραιοι.*

Απόδειξη. □

Πόρισμα 10. *Έστω K σώμα αριθμών. Τότε*

$$\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$$

Απόδειξη. □

Πρόταση 26. *Έστω $a_1, \ldots, a_n$ βάση του σώματος αριθμών K ως Q-διανυσματικού χώρου. Αν $a_1, \ldots, a_n \in \mathcal{O}_K$, τότε $\Delta(a_1, \ldots, a_n) \in \mathbb{Z}$.*

Απόδειξη. □

Πρόταση 27. *Έστω K σώμα αριθμών και $a \in K$. Τότε υπάρχει $m \in \mathbb{Z} - \{0\}$ έτσι ώστε $ma \in \mathcal{O}_K$. Ως συνέπεια, $K = \mathbb{Q}(\theta)$ με $\theta \in \mathcal{O}_K$.*

Απόδειξη. □

Θεώρημα 12. *Έστω K ένα σώμα αριθμών βαθμού n. Τότε το $\mathbb{Z}$-πρότυπο $\mathcal{O}_K$ είναι ελεύθερο τάξης n.*

Απόδειξη. □

Πόρισμα 11. *Έστω K ένα σώμα αριθμών. Τότε ο δακτύλιος $\mathcal{O}_K$ των αλγεβρικών ακεραίων του K είναι δακτύλιος της Noether.*

Απόδειξη. □

Πρόταση 28. *Έστω K ένα σώμα αριθμών. Τότε το K είναι το σώμα πηλίκων του $\mathcal{O}_K$.*

Απόδειξη. Έστω $b \in K$. Το b είναι αλγεβρικό υπεράνω του $\mathbb{Q}$ και άρα υπάρχει πολυώνυμο τέτοιο ώστε

$$q_n b^n + \ldots + q_1 b + q_0 = 0, \quad q_i \in \mathbb{Q}$$

και κάνοντας απαλοιφή των παρονομαστών παίρνουμε

$$a_n b^n + \ldots + a_1 b + a_0 = 0, \quad a_i \in \mathbb{Z}$$

την οποία σχέση την πολλαπλασιάζουμε με a_n^{n-1} και έχουμε ένα μονικό πολυώνυμο με ρίζα το $a_n b$.

$$(a_n b)^n + a_{n-1}(a_n b)^{n-1} + \ldots + a_1 a_n^{n-2}(a_n b) + a_n^{n-1} a_0 = 0$$

συνεπώς το $a_n b \in K$ είναι ακέραιο υπεράνω του $\mathbb{Z}$, άρα $a_n b \in \mathcal{O}_K$. Επίσης $a_n \in \mathbb{Z} \subseteq \mathcal{O}_K$ αφού το $\mathcal{O}_K$ είναι η ακέραια θήκη του $\mathbb{Z}$ στο K. Άρα έχουμε ότι

$$b = \frac{a_n b}{a_n}, \quad a_n b, a_n \in \mathcal{O}_K$$

δηλαδή το K περιέχεται στο σώμα πηλίκων του $\mathcal{O}_K$. Ωστόσο, το σώμα πηλίκων του $\mathcal{O}_K$ είναι το μικρότερο σώμα που το περιέχει. Άρα το σώμα πηλίκων ταυτίζεται με το K. □

Πρόταση 29. *Έστω K ένα σώμα αριθμών, τότε ο δακτύλιος $\mathcal{O}_K$ είναι ακέραια κλειστός στο σώμα πηλίκων του. Ειδικότερα, ο δακτύλιος $\overline{\mathbb{Z}}$ όλων των αλγεβρικών ακεραίων είναι ακέραια κλειστός στο σώμα πηλίκων του.*

Απόδειξη. Δείχνουμε ότι το $\overline{Z}$ είναι ακέραια κλειστό στο σώμα πηλίκων του. Έστω c ένα στοιχείο στο σώμα πηλίκων του $\overline{Z}$ που είναι ακέραιο υπεράνω του $\overline{Z}$. Τότε υπάρχει μονικό πολυώνυμο

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

με $a_i \in \overline{\mathbb{Z}}$ και $f(c) = 0$. Τα a_i ανήκουν και στο σώμα αριθμών $\mathcal{O}_F$ με $F = \mathbb{Q}(a_0, a_1, \ldots, a_{n-1})$ και έχουμε δείξει ότι το $\mathcal{O}_F$ είναι πεπερασμένα παραγόμενο $\mathbb{Z}$-πρότυπο, άρα το $\mathbb{Z}[a_0, \ldots, a_{n-1}]$ είναι πεπερασμένα παραγόμενο $\mathbb{Z}$-πρότυπο. Καθώς $f(c) = 0$, μπορούμε να γράψουμε το c^n ως έναν $\mathbb{Z}[a_0, \ldots, a_{n-1}]$-γραμμικό συνδυασμό των c^i για τα $i < n$. Άρα και ο δακτύλιος $Z[a_0, a_1, \ldots, a_{n-1}, c]$ είναι πεπερασμένα παραγόμενος ως Z-πρότυπο. Εφόσον ο δακτύλιος $\mathbb{Z}$ είναι της Noether ;;;; και το $\mathbb{Z}$-υποπρότυπο $\mathbb{Z}[c]$ είναι πεπερασμένα παραγόμενο. Άρα από πρόταση ;; το c είναι ακέραιο υπεράνω του $\mathbb{Z}$.

ΠΡΟΣΟΧΗ πρέπει να δείξω σώμα πηλίκων αλγεβρικών ακεραίων είναι το $\overline{Q}$;;;;;;;;;;;;;;;
Τώρα για τυχαίο σώμα αριθμών K, έχουμε δείξει ότι το K είναι το σώμα πηλίκων του $\mathcal{O}_K$. Έστω $c \in K$ ακέραιο υπεράνω του $\mathcal{O}_K$. Δηλαδή υπάρχει μονικό πολυώνυμο $f(x) \in \mathcal{O}_K$ με $f(c) = 0$. Επιπλέον $\mathcal{O}_K[x] \subseteq \overline{\mathbb{Z}}[x]$ και άρα αν επαναλάβουμε το παραπάνω επιχείρημα για το $\overline{Z}$ έχουμε ότι $c \in \overline{Z}$. Άρα $c \in K \cap \overline{\mathbb{Z}} = \mathcal{O}_K$. □

Θεώρημα 13. *Έστω K ένα σώμα αριθμών. Τότε το $\mathcal{O}_K$ είναι περιοχή του Dedekind.*

Απόδειξη. Έχουμε ήδη αποδείξει ότι το $\mathcal{O}_K$ είναι δακτύλιος της Noether και ότι είναι ακέραια κλειστό στο σώμα πηλίκων του. Μένει να δείξουμε ότι κάθε πρώτο ιδεώδες είναι και μεγιστικό.

Έστω $\mathfrak{p}$ ένα μη τετριμμένο πρώτο ιδεώδες του $\mathcal{O}_K$. Από τον ομομορφισμό δακτυλίων $\mathbb{Z} \overset{i}{\hookrightarrow} \mathcal{O}_K$ έχουμε ότι το $\mathfrak{p} \cap \mathbb{Z}$ είναι πρώτο ιδεώδες του $\mathbb{Z}$ ως η συστολή ενός πρώτου ιδεωδούς $i^{-1}(\mathfrak{p})$. Επιπλέον, δεν είναι το πρώτο ιδεώδες (0) του $\mathbb{Z}$ καθώς αν $x \in \mathfrak{p}$ τότε το x ως ακέραιο στοιχείο υπεράνω του $\mathbb{Z}$ είναι ρίζα κάποιου μονικού πολυωνύμου ελαχίστου βαθμού, δηλαδή

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}$$

και ο ελάχιστος βαθμός του πολυωνύμου μας εξασφαλίζει ότι $a_0 \neq 0$. Συνεπώς το a_0 ανήκει και στο $\mathfrak{p}$ αφού $x \in \mathfrak{p}$ και αυτό γράφεται ως

$$a_0 = -(x^n + \ldots + a_1 x)$$

Άρα $a_0 \in \mathfrak{p} \cap \mathbb{Z} \neq (0)$. Έτσι, έχουμε ότι το $\mathfrak{p} \cap \mathbb{Z}$ είναι ίσο με το ιδεώδες (p) για κάποιον πρώτο p.

!!!!νδο αυτο το ελαχίστου βαθμού είναι το $Irr(x, \mathbb{Q})$ με λήμμα Gauss!!!!

Έχουμε την σύνθεση ομομορφισμών

$$\mathbb{Z} \overset{i}{\hookrightarrow} \mathcal{O}_K \overset{\pi}{\to} \mathcal{O}_K/\mathfrak{p}$$

η οποία έχει πυρήνα $ker(\pi \circ i) = \mathfrak{p} \cap \mathbb{Z} = (p)$. Έτσι έχουμε έναν μονομορφισμό δακτυλίων

$$\mathbb{Z}/(p) \simeq Im(\pi \circ i) \hookrightarrow \mathcal{O}_K/\mathfrak{p}$$

Έστω τώρα ένα μη μηδενικό $\overline{a} \in \mathcal{O}_K/\mathfrak{p}$. Μπορούμε να θεωρήσουμε το ελάχιστο πολυώνυμο $m(x) = Irr(\overline{a}, \mathbb{Z}/(p))$ που θα έχει μη μηδενικό σταθερό όρο m_0. Έχουμε ότι $m(\overline{a}) = 0$ και αν πολλαπλασιάσουμε αυτή τη σχέση με $-m_0^{-1} \in \mathbb{Z}/(p)$ έχουμε ότι

$$1 = (\overline{a}) \left((\overline{a})^{n-1} + m_{n-1}(\overline{a})^{n-2} + \ldots + m_1 \right) (-m_0^{-1})$$

και άρα το $\overline{a}$ είναι αντιστρέψιμο στοχείο, δηλαδή το $\mathcal{O}_K/\mathfrak{p}$ είναι σώμα. Ισοδύναμα, το $\mathfrak{p}$ είναι μεγιστικό. □

Θεώρημα 14. *Κάθε ιδεώδες του $\mathcal{O}_F$ έχει μοναδική παραγοντοποίηση σε πρώτα ιδεώδη.*

Απόδειξη. υπάρχουν ενδιάμεσες προτάσεις που χρειάζονται □

Ορισμός. *Έστω R μια περιοχή και K το σώμα πηλίκων της. Ένα R-υποπρότυπο M του K λέγεται κλασματικό ιδεώδες του R αν υπάρχει $x \in R, x \neq 0$ τέτοιο ώστε $xM \subseteq R$.*

Ουσιαστικά τα ιδεώδη με την συνήθη έννοια είναι κλασματικά ιδεώδη με $x = 1$. Οποιοδήποτε στοιχείο u στο σώμα πηλίκων K παράγει ένα κλασματικό ιδεώδες (u) το οποίο το λέμε κύριο κλασματικό ιδεώδες επεκτείνωντας τα συνήθη κύρια ιδεώδη.

Για μια περιοχή R, κάθε πεπερασμένα παραγόμενο R-υποπρότυπο M του σώματος πηλίκων K του R είναι ένα κλασματικό ιδεώδες (Macdonald 96) μιλάω και για αντιστρέψιμο κλασματικό ιδεώδες

Τώρα για ένα σώμα αριθμών F, το F είναι το σώμα πηλίκων του $\mathcal{O}_F$ και έτσι τα κλασματικά ιδεώδη του F είναι τα μη μηδενικά πεπερασμένα παραγόμενα $\mathcal{O}_F$-υποπρότυπα του F. Αυτά ορίζουν μια ομάδα $\mathcal{I}_F$ με πράξη το γινόμενο κλασματικών ιδεωδών, όπως έχει οριστεί για τα συνήθη ιδεώδη δηλ ... και για ένα $\mathfrak{a}$ κλασματικό ιδεώδες του F έχουμε ότι

$$\mathfrak{a}^{-1} = \{x \in F : \quad x\mathfrak{a} \subseteq \mathcal{O}_F\}.$$

(απόδειξη/πρόταση) Τα κύρια κλασματικά ιδεώδη του F αποτελούν μια κανονική υποομάδα του $\mathcal{I}_F$ που συμβολίζεται με $\mathcal{P}_F$. Η ομάδα πηλίκο $\mathcal{I}_F/\mathcal{P}_F$ λέγεται ideal class group??? του F.

Αναφορά σε αποτέλεσμα: Αυτή η ομάδα είναι πεπερασμένη για κάθε αριμητικό σώμα F και η τάξη της λέγεται ο αριθμός της κλάσης του F.

Έστω μια πεπερασμένη επέκταση K/F αλγεβρικών αριθμητικών σωμάτων. Θεωρούμε το ιδεώδες $\mathfrak{p}\mathcal{O}_K$ όπου το $\mathfrak{p}$ είναι μη τετριμμένο πρώτο ιδεώδες του $\mathcal{O}_F$. Εφόσον έχουμε μοναδική παραγοντοποίηση ιδεωδών στο $\mathcal{O}_K$ τότε έχουμε

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$$

όπου τα $\mathfrak{P}_i$ είναι διακεκριμένα πρώτα ιδεώδη του $\mathcal{O}_K$ και $n = n(\mathfrak{p})$ μαζί με e_i θετικοί ακέραιοι. Ονομάζουμε το e_i δείκτη διακλάδωσης (ramification index) του $\mathfrak{P}_i/\mathfrak{p}$. Αν η αρχική επέκταση K/F είναι Galois τότε η ομάδα Galois μεταθέτει τα $\mathfrak{P}_i$ μεταβατικά, (;δρα μεταβατικα;) έτσι ώστε $e_1 = \ldots = e_n = e$.

Καθώς τα πρώτα ιδεώδη είναι μεγιστικά σε μια περιοχή του Dedekind, οι δακτύλιοι πηλίκο $\mathcal{O}_K/\mathfrak{P}_j$ και $\mathcal{O}_F/\mathfrak{p}$ είναι σώματα που τα ονομάζουμε σώματα υπολοίπων. Είναι πεπερασμένα σώματα χαρακτηριστικής p με $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Μπορούμε να δούμε το σώμα $\mathcal{O}_F/\mathfrak{p}$ ως υπόσωμα του $\mathcal{O}_K/\mathfrak{P}_i$. Έτσι ο βαθμός επέκτασης των σωμάτων υπολοίπων θα συμβολίζεται:

$$f(\mathfrak{P}_i/\mathfrak{p}) = [\mathcal{O}_K/\mathfrak{P}_j : \mathcal{O}_F/\mathfrak{p}]$$

(απόδειξη/πρόταση) Αν η επέκταση K/F είναι Galois τότε $f(\mathfrak{P}_1/\mathfrak{p}) = f(\mathfrak{P}_2/\mathfrak{p}) = \ldots = f(\mathfrak{P}_n/\mathfrak{p}) = f$

Γενικότερα έχουμε

$$\sum_{i=1}^{n} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) = [K : F]$$

και όταν η επέκταση των σωμάτων αριθμών είναι Galois τότε $[K : F] = efn$

Αν K/F είναι μια επέκταση αριθμητικών σωμάτων, θα λέμε ότι το πρώτο ιδεώδες $\mathfrak{p}$ είναι αδιακλάδωτο στην επέκταση K/F αν $e(\mathfrak{P}_i/\mathfrak{p}) = 1$ για κάθε i. Θα λέμε επίσης ότι το $\mathfrak{p}$ είναι τελείως διακλαδωμένο στην επέκταση K/F αν υπάρχει μοναδικό πρώτο ιδεώδες $\mathfrak{P}$ πάνω από το $\mathfrak{p}$ και $e(\mathfrak{P}/\mathfrak{p}) = [K : F]$. Επιπλέον, το $\mathfrak{p}$ θα λέμε ότι είναι αδρανή στην επέκταση K/F αν το $\mathfrak{p}\mathcal{O}_K$ είναι πρώτο ιδεώδες του $\mathcal{O}_K$ και επιπλέον το $\mathfrak{p}$ διασπάται πλήρως στην επέκταση αν $n = [K : F]$.

Για δοσμένη επέκταση K/F αριθμητικών σωμάτων και πρώτο ιδεώδες $\mathfrak{p}$ του $\mathcal{O}_F$, ένας τρόπος για να βρούμε παραγοντοποίηση βασίζεται στο ακόλουθο θεώρημα:

Θεώρημα 15 (Dedekind-Kummer)**.** *Έστω K/F μια επέκταση αριθμητικών σωμάτων και υποθέτουμε ότι $\mathcal{O}_K = \mathcal{O}_F[a]$. Έστω $f(x) = Irr(a, F)$ το ελάχιστο πολυώνυμο του a υπεράνω του F και έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες του $\mathcal{O}_F$. Θέτουμε $\mathbb{F}_\mathfrak{p} = \mathcal{O}_F/\mathfrak{p}$ και συμβολίζουμε την εικόνα του $f(x)$ στο $\mathbb{F}_\mathfrak{p}$ με $\overline{f(x)}$, δηλαδή παίρνουμε νέο πολυώνυμο από το $f(x)$ με τους συντελεστές του $mod\mathfrak{p}$. Υποθέτουμε ότι στο $\mathbb{F}_\mathfrak{p}[x]$ έχουμε παραγοντοποίηση του $\overline{f(x)}$:*

$$\overline{f(x)} = \overline{p_1(x)}^{e_1} \cdots \overline{p_n(x)}^{e_n}$$

όπου τα $\overline{p_i}$ είναι διακεκριμένα ανάγωγα πολυώνυμα του $\mathbb{F}_\mathfrak{p}[x]$. Για κάθε i, έστω $p_i(x)$ ένα μονικό πολυώνυμο του $\mathcal{O}_F$ που αντιστοιχεί στο $\overline{p_i(x)}$ αν πάρουμε τους συντελεστές του $mod\mathfrak{p}$. Έστω $\mathfrak{P}_i$ το ιδεώδες του $\mathcal{O}_K$ που παράγεται από τα $\mathfrak{p}$ και $p_i(a)$. Τότε

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$$

με τα $\mathfrak{P}_i$ να είναι διακεκριμένα πρώτα ιδεώδη του $\mathcal{O}_K$.

Απόδειξη. □

!!Διακρίνουσα γενικά για στοιχεία και βάση αριθμητικών σωμάτων από Μαλιάκα και notes (και Trace αν χρειάζεται)

Όπως ορίσαμε την διακρίνουσα για μια βάση ενός αριθμητικού σώματος υπεράνω του $\mathbb{Q}$ θα επεκτείνουμε την έννοια και για πεπερασμένες επεκτάσεις αριθμητικών σωμάτων. Αν έχουμε δηλαδή μια πεπερασμένη επέκταση K/F αριθμητικών σωμάτων με $\{v_1, \ldots, v_n\}$ μια βάση του K ως F-διανυσματικού χώρου, τότε ορίζουμε την διακρίνουσα της συγκεκριμένης βάσης να είναι ο μιαγαδικός αριθμός

$$\Delta(v_1, v_2, \ldots, v_n) = det[\sigma_i(v_j)]^2$$

όπου αντί για μονομορφισμούς από το $K \to \mathbb{C}$ που κρατάνε σταθερό το $\mathbb{Q}$ έχουμε $\sigma_1, \ldots, \sigma_n : K \hookrightarrow F^{\text{alg}}$ μονομορφισμούς που κρατάνε σταθερό το F

Η σχέση για τις διακρίνουσες από διαφορετικές βάσεις του K υπεράνω του F δίνεται με βάση τον πίνακα αλλαγής βάσης μεταξύ τους. Αν A είναι ο $n \times n$ πίνακας αλλαγής βάσης, δηλαδή $(w_1, \ldots, w_n)^T = A(v_1, \ldots, v_n)^T$, τότε

$$\Delta(w_1, \ldots, w_n) = (detA)^2 \Delta(v_1, \ldots, v_n)$$

(απόδειξη/ πρόταση/ ορισμός vandermode)Στην περίπτωση που $K = F(a)$ με $[K : F] = n$, ο πίνακας $[\sigma_i(a^{j-1})]$ (;) είναι πίνακας Vandermode, δηλαδή

$$\Delta(1, a, \ldots, a^{n-1}) = \prod_{1 \leq i < j \leq n} (\sigma_i(a) - \sigma_j(a))^2$$

Πιο συγκεκριμένα, αν $\mathcal{O}_K = \mathcal{O}_F[a]$ και $f(x)$ είναι το έλαχιστο πολυώνυμο του a υπεράνω του F τότε

$$N_{K/F}(f'(a)) = (-1)^{\frac{n(n-1)}{2}} \Delta(1, a, \ldots, a^{n-1})$$

Με την σχέση του πίνακα αλλαγής βάσης έχουμε ότι οι διακρίνουσες δεν είναι απαραίτητα ίσες για διαφορετικές βάσεις. Άρα αν θέλουμε να ορίσουμε την διακρίνουσα μιας επέκτασης αριθμητικών σωμάτων K/F τότε πρέπει να το κάνουμε για όλες τις δυνατές βάσεις του K ως F-διανυσματικού χώρου. Θα ορίσουμε ένα πρότυπο που τις περιέχει.

Έστω M ένα μη τετριμμένο $\mathcal{O}_F$-πρότυπο που περιέχει μια F-βάση του K. Ορίζουμε ως $d(M)$ το $\mathcal{O}_F$-πρότυπο που παράγεται από όλα τα στοιχεία $\Delta(v_1, \ldots, v_n)$ για κάθε $\{v_1, \ldots, v_n\}$ F-βάση του K που περιέχεται στο M.

(Πρόταση/απόδειξη) Αν το M είναι κλασματικό ιδεώδες του K τότε το $d(M)$ είναι κλασματικό ιδεώδες του F. (Πρόταση/απόδειξη) Αν το M είναι ελεύθερο $\mathcal{O}_F$ πρότυπο, δηλαδή

$$M = \bigoplus_{i=1}^{n} w_i \mathcal{O}_F = \bigoplus_{i=1}^{n} (w_i)$$

τότε

$$d(M) = \Delta(w_1, \ldots, w_n)\mathcal{O}_F = (\Delta(w_1, \ldots, w_n))$$

(σχετική) διακρίνουσα της επέκτασης K/F είναι $d_{K/F} = d(\mathcal{O}_K)$ όπου θεωρούμε το $\mathcal{O}_K$ ως πεπερασμένα παραγόμενο $\mathcal{O}_F$-πρότυπο. Έπεται (;) ότι το $d_{K/F}$ είναι ακέραιο ιδεώδες του $\mathcal{O}_F$.

(απόλυτη) διακρίνουσα του K θα είναι $d_K = d_{K/\mathbb{Q}}$

Το $\mathcal{O}_K$ είναι ελεύθερο $\mathbb{Z}$-πρότυπο τάξης $n = [K : \mathbb{Q}]$, οπότε το $d_K = d_{K/\mathbb{Q}}$ είναι (κύριο) ιδεώδες του $\mathbb{Z}$ που παράγεται από το $\Delta(v_1, \ldots, v_n)$ όπου $\{v_1, \ldots, v_n\}$ είναι οποιαδήποτε $\mathbb{Z}$-βάση του $\mathcal{O}_K$.

οι διακρίνουσες όπως θα δούμε μεταφέρουν πληροφορία για το ποιοι πρώτοι (εννοεί πρώτα ιδεώδη;;; εν τέλει συμπίπτουν με ιδεώδη που παράγονται από πρώτους;;) διακλαδώνονται σε μια επέκταση Πρόταση: Έστω ένα μη τετριμμένο πρώτο ιδεώδες $\mathfrak{p}$ του $\mathcal{O}_F$. Έχουμε ότι το $\mathfrak{p}$ είναι διακλαδωμένο στην επέκταση K/F αν και μόνο αν $\mathfrak{p} | d_{K/F}$.

Εφόσον έχουμε ορίσει την νόρμα για στοιχεία (;) θα ορίσουμε την νόρμα ενός κλασματικού ιδεωδούς. Έστω K/F μια πεπερασμένη επέκταση αριθμητικών σωμάτων. Έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες του $\mathcal{O}_F$ και $\mathfrak{P}$ ένα πρώτο ιδεώδες του $\mathcal{O}_K$ που διαιρεί το $\mathfrak{p}\mathcal{O}_K$. Ορίζουμε την νόρμα του $\mathfrak{P}$ να είναι

$$N_{K/F}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$$

και επεκτείνουμε την έννοια σε τυχαία κλασματικά ιδεώδη του K ως εξής:

$$N_{K/F}(\mathfrak{P}_1^{a_1}\mathfrak{P}_2^{a_2}\cdots\mathfrak{P}_t^{a_t}) = N_{K/F}(\mathfrak{P}_1)^{a_1} N_{K/F}(\mathfrak{P}_2)^{a_2} \cdots N_{K/F}(\mathfrak{P}_t)^{a_t}$$

Έτσι η νόρμα ενός κλασματικού ιδεωδούς του K είναι ένα κλασματικό ιδεώδες του F.

(πρόταση) Αν τώρα η επέκταση K/F είναι Galois τότε

$$N_{K/F}(\mathfrak{U})\mathcal{O}_K = \prod_{\sigma \in Gal(K/F)} \sigma(\mathfrak{U})$$

και έστω $a \in K$, τότε $N_{K/F}(a\mathcal{O}_K) = N_{K/F}(a)\mathcal{O}_F$ όπου $N_{K/F}(a)$ είναι η συνήθης νόρμα του στοιχείου a.

Επιπλέον, αν $F \subseteq E \subseteq K$ είναι σώματα αριθμών, τότε (Πρόταση) $N_{K/F} = N_{E/F} \circ N_{K/E}$

Όταν $F = \mathbb{Q}$ τότε $N_{K/\mathbb{Q}}(\mathfrak{U}) = a\mathbb{Z}$ για κάποιο $a \in \mathbb{Q}$.

Έστω μια Galois επέκταση K/F σωμάτων αριθμών με ομάδα Galois G, έστω ένα μη τετριμμένο πρώτο ιδεώδες $\mathfrak{p}$ του $\mathcal{O}_F$ και ένα πρώτο ιδεώδες $\mathfrak{P}$ του $\mathcal{O}_K$ με $\mathfrak{P}|\mathfrak{p}\mathcal{O}_K$. Ορίζουμε την ομάδα διάσπασης:

$$Z(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

Η $Z(\mathfrak{P}/\mathfrak{p})$ δρα στο πεπερασμένο σώμα $\mathbb{F} = \mathcal{O}_K/\mathfrak{P}$ και σταθεροποιεί κατά σημείο το $\mathcal{O}_F/\mathfrak{p}$, άρα υπάρχχει ένας φυσικός ομομορφισμός ομάδων:

$$Z(\mathfrak{P}/\mathfrak{p}) \longrightarrow Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$$

Θεώρημα 16. *Έστω K/F μια επέκταση Galois σωμάτων αριθμών με Galois ομάδα G. Έστω $\mathfrak{p}$ ένα μη τετριμμένο ιδεώδες του $\mathcal{O}_F$. τότε*

(1) *Η G δρα μεταβατικά στο σύνολο των πρώτων ιδεωδών $\mathfrak{P}$ του $\mathcal{O}_K$ τα οποία διαιρούν το $\mathfrak{p}\mathcal{O}_K$ και έτσι*

$$[G : Z(\mathfrak{P}/\mathfrak{p})] = \#\{ \text{ πρώτα ιδεώδη } \mathfrak{P} \text{ του } \mathcal{O}_K : \quad \mathfrak{P}|\mathfrak{p}\mathcal{O}_K\} = n = n(\mathfrak{p})$$

όπου n είναι το πλήθος των διακεκριμένων πρώτων $\mathfrak{P}$ που διαιρούν το $\mathfrak{p}\mathcal{O}_K$. Επιπλέον, αν $\mathfrak{P}, \mathfrak{P}'$ είναι πρώτα ιδεώδη του $\mathcal{O}_K$ που διαιρούν το $\mathfrak{p}\mathcal{O}_K$, τότε οι ομάδες $Z(\mathfrak{P}/\mathfrak{p})$ και $Z(\mathfrak{P}/\mathfrak{p})$ είναι G-συγυζείς.

(2) *$N_{K/\mathbb{Q}}(\mathfrak{p}) = |\mathbb{F}_{\mathfrak{p}}|, N_{K/\mathbb{Q}}(\mathfrak{P}) = |\mathbb{F}_{\mathfrak{P}}|$ και η ομάδα $Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ είναι κυκλική, παράγεται από τον αυτομορφισμό του Frobenius $\phi_{\mathfrak{p}} : x \mapsto x^{N_{K/Q}(\mathfrak{p})}$.*

(3) *Ο ομομορφισμός ομάδων $Z(\mathfrak{P}/\mathfrak{p}) \to Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ είναι επιμορφισμός. Ο πυρήνας του θα ονομάζεται υποομάδα αδράνειας και θα συμβολίζεται με $T(\mathfrak{P}/\mathfrak{p})$. Έτσι θα έχουμε ότι $[Z(\mathfrak{P}/\mathfrak{p}) : T(\mathfrak{P}/\mathfrak{p})] = f$ και ότι η ομάδα $T(\mathfrak{P}/\mathfrak{p})$ έχει τάξη e.*

Απόδειξη. □

Έστω ότι η επέκταση σωμάτων αριθμών K/F είναι Galois. Τότε μέσω της αντιστοιχίας Galois οι ομάδες διάσπασης και αδράνειας αντιστοιχούν σε ενδιάμεσα σώματα της επέκτασης τα οποία ονομάζουμε σώμα διάσπασης και σώμα αδράνειας αντίστοιχα. Έστω K_Z και K_T να είναι τα σταθερά σώματα των $Z(\mathfrak{P}/\mathfrak{p})$ και $T(\mathfrak{P}/\mathfrak{p})$ αντίστοιχα. Για μια αβελιανή επέκταση, η παραγοντοποίηση των ιδεωδών που παράγονται από το $\mathfrak{p}$ σε αυτά τα ενδιάμεσα σώματα δίνεται από το ακόλουθο θεώρημα:

Θεώρημα 17 (Layer)**.** *Έστω $\mathfrak{p}$ ένα μη τετριμμένο πρώτο ιδεώδες του $\mathcal{O}_F$, όπου K/F είναι μια αβελιανή επέκταση σωμάτων αριθμών. Τότε το $\mathfrak{p}$ διασπάται πλήρως στην επέκταση K_Z/F. Τα πρώτα ιδεώδη (;)πάνω(;) από το $\mathfrak{p}$ παραμένουν αδρανή στην επέκταση K_Z/K_T και διακλαδώνονται πλήρως στην επέκταση K/K_T.*

Απόδειξη. □

Αν τώρα $e(\mathfrak{P}/\mathfrak{p}) = 1$ τότε από τον φυσικό ομομορφισμό του (3) του θεωρήματος ref; έχουμε τον ισομορφισμό $Z(\mathfrak{P}/\mathfrak{p}) \simeq Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ κυκλικών ομάδων τάξης $f = f(\mathfrak{P}/\mathfrak{p})$. Η ομάδα Galois των σωμάτων υπολοίπων παράγεται από τον αυτομορφισμό του Frobenius $\phi_{\mathfrak{p}}$ και έτσι υπάρχει μοναδικό $\sigma \in Z(\mathfrak{P}/\mathfrak{p})$ που αντιστοιχεί στο $\phi_{\mathfrak{p}}$ κάτω από τον φυσικό ισομορφισμό. Έχουμε $Z(\mathfrak{P}/\mathfrak{p}) =< \sigma >$. Το στοιχείο σ λέγεται το στοιχείο του Frobenius στο $\mathfrak{B}$. Το συμβολίζουμε με

$$\sigma = \left(\frac{\mathfrak{P}}{K/F}\right) = (\mathfrak{P}, K/F)$$

Πρόταση 30. *Έστω K/F μια επέκταση Galois σωμάτων αριθμών, $\mathfrak{p}$ ένα μη τετριμμένο πρώτο ιδεώδες που είναι αδιακλάδωτο στην επέκταση K/F και $\mathfrak{P}$ ένα πρώτο ιδεώδες του $\mathcal{O}_K$ με $\mathfrak{P}|\mathfrak{p}\mathcal{O}_K$. Τότε το στοιχείο του Frobenius στο $\mathfrak{P}$ είναι το μοναδικό στοιχείο $\sigma \in Gal(K/F)$ που ικανοποιεί την σχέση*

$$\sigma(a) = a^{N_{K/Q}(\mathfrak{p})} \quad (mod \mathfrak{P})$$

για κάθε $a \in \mathcal{O}_K$.

Απόδειξη. □

Αν υποθέσουμε επιπλέον ότι η ομάδα Galois της επέκτασης είναι αβελιανή, τότε από το (1) του θεωρήματος ref; παίρνουμε ότι η ομάδα $Z(\mathfrak{P}/\mathfrak{p})$ εξαρτάται μόνο το $\mathfrak{p}$ και έτσι την γράφουμε ως $Z(\mathfrak{p})$. Αν το $\mathfrak{p}$ είναι αδιακλάδωτο στην επέκταση K/F τότε με βάση την πρόταση που ακολουθεί, δείχνουμε ότι το στοιχείο του Frobenius στο $\mathfrak{P}$ εξαρτάται μόνο από το $\mathfrak{p}$. Σε αυτή τη περίπτωση, ονομάζουμε το στοιχείο ως τον αυτομορφισμό του Artin για το $\mathfrak{p}$ και το συμβολίζουμε με

$$\left(\frac{\mathfrak{p}}{K/F}\right) = (\mathfrak{p}, K/F)$$

Επιπλέον, ορίζουμε την απεικόνιση

$$\{ \text{ πρώτα ιδεώδη του } \mathcal{O}_F \text{ που είναι αδιακλάδωτα στην επέκταση } K/F\} \longrightarrow G$$

$$\mathfrak{p} \longmapsto \sigma_{\mathfrak{p}} = \left(\frac{\mathfrak{p}}{K/F}\right)$$

Πρόταση 31. *Έστω K/F μια αβελιανή επέκταση σωμάτων αριθμών, $\mathfrak{p}$ ένα μη τετριμμένο πρώτο ιδεώδες του $\mathcal{O}_F$ που είναι αδιακλάδωτο στην επέκταση K/F και $\mathfrak{P}$ ένα πρώτο ιδεώδες του $\mathcal{O}_K$ με $\mathfrak{P}|\mathfrak{p}\mathcal{O}_K$. Τότε το $\sigma = \left(\frac{\mathfrak{P}}{K/F}\right)$ δεν εξαρτάται από την επιλογή του πρώτου $\mathfrak{P}$ πάνω από το $\mathfrak{p}$.*

Απόδειξη. □

Πρόταση 32. *Έστω K/F μια αβελιανή επέκταση με ομάδα Galois G και ένα ενδιάμεσο σώμα L (άρα και οι επεκτάσεις L/F και K/L είναι αβελιανές). Έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες του $\mathcal{O}_F$ που είναι αδιακλάδωτο στην επέκταση K/F. Τότε τα στοιχεία $\left(\frac{\mathfrak{p}}{L/F}\right)$ και $\left(\frac{\mathfrak{p}}{K/F}\right)$ είναι ορισμένα και ισχύει ότι*

$$\left(\frac{\mathfrak{p}}{L/F}\right) = \left(\frac{\mathfrak{p}}{K/F}\right)\Big|_L$$

Απόδειξη. □

Πρόταση 33. *Αν ζ, ζ' είναι m-οστές ρίζες της μονάδας στο K και $\mathfrak{P}|p\mathbb{Z}$ είναι αδιακλάδωτο με $\zeta = \zeta'(mod \mathfrak{P})$, τότε $\zeta = \zeta'$.*

Απόδειξη. □

τώρα με βάση τον αυτοομορφισμό του Artin θα δείξουμε το ακόλουθο αποτέλεσμα για τους πρώτους που διασπώνται πλήρως σε ενδιάμεσες επεκτάσεις κυκλοτομικών σωμάτων.

Κεντρικό Θεώρημα:

Θεώρημα 18. *Έστω K υπόσωμα του $\mathbb{Q}(\zeta_m)$. Υπενθυμίζουμε ότι η ομάδα $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα του δακτυλίου $\mathbb{Z}/m\mathbb{Z}$. Έστω H η υποομάδα της $(\mathbb{Z}/m\mathbb{Z})^x$ που αντιστοιχεί μέσω του ισομορφισμού στην ομάδα $Gal(\mathbb{Q}(\zeta_m)/K)$. Τότε οι πρώτοι αριθμοί p οι οποίοι δεν διαιρούν το m και διασπώνται πλήρως στην επέκταση $K/\mathbb{Q}$ είναι ακριβώς εκείνοι για τους οποίους ισχύει $p \ mod \ m \in H$.*

Απόδειξη. □

παραδείγματα!!!!!

Θεώρημα 19 (Minkowski)**.** *Έστω T ένα υποσύνολο του V που είναι συμπαγές, κυρτό και συμμετρικό στο* 0 *(origin). Αν*

$$\mu(T) \geq 2^n \mu(D)$$

τότε το T περιέχει ένα σημείο του δικτυωτού lattice εκτός από το origin.

Απόδειξη. □