Αλγεβρικά Σώματα Αριθμών και Αριθμός Κλάσεων Ιδεωδών
Ειδικό Θέμα

Αγγελίδου Μαρία
Επιβλέπουσα Καθηγήτρια: Χαραλάμπους Χαρά

11.11.2019

Περίληψη

Αφορμή της παρούσας εργασίας αποτέλεσε το άρθρο του Καθηγητή Scott T. Chapman, So what is class number 2? Με στόχο την κατανόησή του, έγινε μια εισαγωγή στην Αλγεβρική Θεωρία Αριθμών. Κατευθυντήριος άξονάς μας ήταν το βιβλίο του κυρίου Κ. Λάκκη, Θεωρία Αριθμών, ενώ οι υπόλοιπες αναφορές λειτούργησαν συμπληρωματικά. Η εργασία δομείται από τρεις νοερούς πυλώνες: το Θεώρημα της Μονοσήμαντης Ανάλυσης Ιδεωδών και δύο θεωρήματα που αφορούν τους Αριθμούς Κλάσεων Ιδεωδών 1 και 2, συνοδευόμενα από όλα τα απαραίτητα στοιχεία για την απόδειξή τους. Πιο συγκεκριμένα, αποδεικνύουμε ότι ο δακτύλιος των ακέραιων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών είναι περιοχή μονοσήμαντης ανάλυσης αν και μόνον αν ο αριθμός κλάσεων ιδεωδών είναι ίσος με 1, καθώς επίσης και το Θεώρημα του Carlitz για αριθμό κλάσεων ιδεωδών το πολύ 2.

Περιεχόμενα

1 Αλγεβρικά Σώματα Αριθμών.

1.1 Βασικοί Ορισμοί.

Ορισμός 1.1.1. Ένας μιγαδικός αριθμός που αποτελεί ρίζα πολυωνύμου με μη μηδενικούς ρητούς συντελεστές καλείται αλγεβρικός αριθμός.

Το σύνολο των αλγεβρικών αριθμών είναι υποσύνολο του $\mathbb{C}$ και μάλιστα γνήσιο, διότι αριθμοί όπως ο π δεν είναι αλγεβρικοί. Μάλιστα, αποδεικνύεται ([1], Θεώρημα 1.3, σελίδα 132) ότι το σύνολο των αλγεβρικών αριθμών είναι υπόσωμα του $\mathbb{C}$.

Ορισμός 1.1.2. Ονομάζουμε ανάγωγο πολυώνυμο του αλγεβρικού αριθμού α και συμβολίζουμε με $f_\alpha(x)$ το κανονικό πολυώνυμο ελάχιστου βαθμού του $\mathbb{Q}[x]$ που έχει ρίζα το α.

Ορισμός 1.1.3. Ένας αλγεβρικός αριθμός ονομάζεται ακέραιος αλγεβρικός αριθμός, αν το ανάγωγο πολυώνυμο αυτού έχει ακέραιους συντελεστές.

Παράδειγμα 1.1.4. Ο αριθμός $\frac{1}{2}$ είναι αλγεβρικός, αλλά όχι ακέραιος αλγεβρικός γιατί έχει ανάγωγο πολυώνυμο το $f(x) = x - \frac{1}{2}$.
Το ίδιο ισχύει για όλα τα στοιχεία του $\mathbb{Q} \setminus \mathbb{Z}$.

Παράδειγμα 1.1.5. Ο αριθμός $\sqrt[3]{2}$ είναι ακέραιος αλγεβρικός με ανάγωγο πολυώνυμο $f(x) = x^3 - 2$.

Παράδειγμα 1.1.6. Ο αριθμός $\frac{1+\sqrt{5}}{2}$ είναι ακέραιος αλγεβρικός με ανάγωγο πολυώνυμο $f(x) = x^2 - x - 1$.

Πρόταση 1.1.7. Το ανάγωγο πολυώνυμο $f(x)$ ενός ακέραιου αλγεβρικού αριθμού α έχει μόνο απλές ρίζες.

Απόδειξη. Έστω ότι το $f(x)$ βαθμού n έχει ρίζα β ανώτερης τάξης. Τότε:

$$f(x) = (x - \beta)^k g(x)$$

με $g(x)$κανονικό πολυώνυμο, $k > 1$, $deg(g(x)) = n - k$ και

$$f'(x) = k(x - \beta)^{k-1} g(x) + (x - \beta)^k g'(x).$$

Το $f'(x)$ είναι πολυώνυμο μικρότερου βαθμού από το $f(x)$ και έχει ρίζα το β. Όμως το $f(x)$ είναι ανάγωγο όλων των ριζών του, άρα και της β, έχει δηλαδή τον ελάχιστο βαθμό μεταξύ των πολυωνύμων που μηδενίζονται από το β. Συνεπώς έχουμε άτοπο. □

Ορισμός 1.1.8. Ονομάζουμε πεπερασμένη επέκταση βαθμού n πάνω από το $\mathbb{Q}$, ένα σώμα $\mathrm{K} \supset \mathbb{Q}$ που έχει πεπερασμένη διάσταση n ως διανυσματικός χώρος πάνω από το $\mathbb{Q}$.

Πρόταση 1.1.9. Αν K είναι μια πεπερασμένη επέκταση του $\mathbb{Q}$, η οποία περιέχεται στο $\mathbb{C}$, τότε όλοι οι αριθμοί του K είναι αλγεβρικοί.

Απόδειξη. Έστω n ο βαθμός της επέκτασης $\mathrm{K}/\mathbb{Q}$ και $a \in \mathrm{K}$. Τότε οι αριθμοί $1, a, a^2, \ldots, a^n$ είναι γραμμικά εξαρτημένοι, καθώς το πλήθος τους είναι μεγαλύτερο από το βαθμό n. Άρα υπάρχουν $c_0, c_1, \ldots, c_n \in \mathbb{Q}$ όχι όλοι μηδέν, τέτοιοι ώστε

$$c_0 + c_1 a + \cdots + c_n a^n = 0,$$

δηλαδή ο a είναι ρίζα του μη μηδενικού πολυωνύμου με ρητούς συντελεστές

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

Επομένως ο a είναι αλγεβρικός. □

Ορισμός 1.1.10. Κάθε πεπερασμένη επέκταση K του $\mathbb{Q}$, η οποία περιέχεται στους μιγαδικούς αριθμούς, καλείται σώμα αλγεβρικών αριθμών.

Ορισμός 1.1.11. Το σύνολο R όλων των ακέραιων αλγεβρικών αριθμών του αλγεβρικού σώματος αριθμών K συνιστά τον δακτύλιο ακέραιων αλγεβρικών αριθμών του K.

Έστω θ αλγεβρικός αριθμός. Συμβολίζουμε με $\mathbb{Q}(\theta)$ το ελάχιστο υπόσωμα του $\mathbb{C}$ που περιέχει το θ και το $\mathbb{Q}$. Χρησιμοποιούμε χωρίς απόδειξη τα δύο παρακάτω θεωρήματα:

Θεώρημα 1.1.12. Αν θ είναι ένας αλγεβρικός αριθμός, τότε το σώμα $\mathbb{Q}(\theta)$ είναι ένα αλγεβρικό σώμα αριθμών βαθμού $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, όπου n είναι ο βαθμός του πολυωνύμου $f(x)$. Οι αριθμοί $1, \theta, \theta^2, \ldots, \theta^{n-1}$ αποτελούν βάση της επεκτάσεως $\mathbb{Q}(\theta)/\mathbb{Q}$ και συνεπώς ο τυχαίος αριθμός a του $\mathbb{Q}(\theta)$

έχει μια μονοσήμαντη παράσταση $a = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$, όπου $a_0, a_1, \ldots, a_{n-1}$ είναι ρητοί αριθμοί.

Απόδειξη. Βλέπε [1], Θεώρημα 3.3, σελίδα 142. □

Θεώρημα 1.1.13. Αν K είναι ένα αλγεβρικό σώμα αριθμών, τότε υπάρχει ένας αριθμός ϑ αυτού τέτοιος, ώστε να ισχύει $\mathrm{K} = \mathbb{Q}(\theta)$.

Απόδειξη. Βλέπε [1], Θεώρημα 3.4, σελίδα 142. □

1.2 Συζυγείς αριθμοί. Ίχνος. Νόρμα.

Έστω Κ = $\mathbb{Q}(\theta)$ ένα αλγεβρικό σώμα αριθμών βαθμού $[K : \mathbb{Q}] = n$ και $f_\theta(x)$ το ανάγωγο πολυώνυμο του θ. Συμβολίζουμε με $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ τις ρίζες του $f_\theta(x)$ οπότε ισχύει

$$f_\theta(x) = (x - \theta^{(1)})(x - \theta^{(2)}) \ldots (x - \theta^{(n)}).$$

Από την Πρόταση 1.1.7 οι ρίζες αυτές είναι διάφορες μεταξύ τους.

Επειδή το $f_\theta(x)$ είναι ανάγωγο πολυώνυμο όλων των ριζών του, προκύπτει από το Θεώρημα 1.1.12 ότι τα σώματα $\mathbb{Q}(\theta^{(i)})$, $i = 1, \ldots, n$ έχουν βαθμό n και κάθε αριθμός a του $\mathbb{Q}(\theta^{(i)})$ έχει μία μονοσήμαντη παράσταση της μορφής

$$a = a_0 + a_1\theta^{(i)} + \cdots + a_{n-1}\theta^{(i)(n-1)}$$

όπου $a_0, a_1 \ldots, a_{n-1}$ είναι ρητοί αριθμοί.

Οι πληροφορίες αυτές θα μας χρειαστούν αμέσως παρακάτω, όπου θα ασχοληθούμε με τους $\mathbb{Q}$-ισομορφισμούς του σώματος $\mathbb{Q}(\theta)$ στο σώμα των μιγαδικών αριθμών, δηλαδή με ομομορφισμούς $\mathbb{Q}(\theta) \to L$, όπου L υπόσωμα του $\mathbb{C}$.

Θεώρημα 1.2.1. Υπάρχουν ακριβώς n $\mathbb{Q}$-ισομορφισμοί του σώματος $\mathbb{Q}(\theta)$ στο σώμα των μιγαδικών αριθμών. Οι εικόνες του θ μέσω των ισομορφισμών αυτών είναι οι ρίζες $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ του πολυωνύμου $f(x)$.

Απόδειξη. Θεωρούμε τις συναρτήσεις $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta^{(i)})$ με $\theta \mapsto \theta^{(i)}, i = 1, \ldots, n$
Οι συναρτήσεις αυτές είναι n το πλήθος και ορίζονται ως εξής:

$$\sigma_i(a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}) = a_0 + a_1\theta^{(i)} + \cdots + a_{n-1}\theta^{(i)(n-1)}$$

Εύκολα φαίνεται από το Θεώρημα 1.1.12 ότι οι σ_i είναι ισομορφισμοί, διαφορετικοί μεταξύ τους.
Θα δείξουμε τώρα ότι δεν υπάρχουν άλλοι τέτοιοι ισομορφισμοί. Έστω $\phi : \mathbb{Q}(\theta) \to L$ ένας $\mathbb{Q}$-ισομορφισμός και έστω $\phi(\theta) = \alpha$. Τότε το α είναι ρίζα του ανάγωγου πολυωνύμου του θ. Άρα $\alpha = \theta^{(i)}$, για κάποιο i. □

Σημειώνουμε ότι κάθε τέτοιος ισομορφισμός κρατά αναλλοίωτα τα στοιχεία του $\mathbb{Q}$.

Ορισμός 1.2.2. Αν $\sigma_1, \sigma_2, \ldots, \sigma_n$ είναι οι $\mathbb{Q}$-ισομορφισμοί του σώματος Κ= $\mathbb{Q}(\theta)$ στο σώμα των μιγαδικών αριθμών και a τυχαίος αριθμός του Κ, τότε οι αριθμοί $a^{(i)} = \sigma_i(a)$, $i = 1, \ldots, n$ ονομάζονται συζυγείς αριθμοί του a.

Είναι φανερό ότι οι συζυγείς του θ είναι οι $\theta^{(1)}, \ldots, \theta^{(n)}$ και ότι ο σ_1 είναι ο ταυτοτικός $\mathbb{Q}$-ισομορφισμός.

Παράδειγμα 1.2.3. Θα υπολογίσουμε τους $\mathbb{Q}$-ισομορφισμούς του K$=\mathbb{Q}(\sqrt[3]{2})$.
Όπως έχουμε ήδη δει το ανάγωγο πολυώνυμο του $\sqrt[3]{2}$ είναι το

$$\begin{aligned} f(x) &= x^3 - 2 \\ &= (x - \sqrt[3]{2})(x - w\sqrt[3]{2})(x - w^2\sqrt[3]{2}), \text{ όπου } w = \tfrac{1+i\sqrt{3}}{2}. \end{aligned}$$

Εφόσον ο βαθμός του $f(x)$ είναι 3, τότε σύμφωνα με το Θεώρημα 1.1.12. η $(1, \sqrt[3]{2}, \sqrt[3]{2}^2)$ αποτελεί βάση της επεκτάσεως $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ και κάθε στοιχείο του $\mathbb{Q}(\sqrt[3]{2})$ γράφεται μονοσήμαντα ως εξής : $a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2$, με $a_i \in \mathbb{Q}$. Άρα έχουμε:
$\sigma_1(a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2) = a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$
$\sigma_2(a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2) = a_0 + a_1 w\sqrt[3]{2} + a_2 w^2(\sqrt[3]{2})^2 \in \mathbb{Q}(\omega\sqrt[3]{2})$
$\sigma_3(a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2) = a_0 + a_1 w^2\sqrt[3]{2} + a_2 w(\sqrt[3]{2})^2 \in \mathbb{Q}(\omega^2\sqrt[3]{2})$

Πρόταση 1.2.4. Οι συζυγείς αριθμοί $\sigma_i(a)$ ενός στοιχείου α του αλγεβρικού σώματος αριθμών K, διάστασης $[K : \mathbb{Q}] = n$, αποτελούν ρίζες του αναγώγου πολυωνύμου του.

Απόδειξη. Έστω $f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_i \in \mathbb{Q}$ το ανάγωγο πολυώνυμο του a. Ισχύει ότι:

$$\begin{aligned} f_\alpha(a^{(i)}) = f_\alpha(\sigma_i(a)) &= (\sigma_i(a))^n + a_{n-1}(\sigma_i(a))^{n-1} + \cdots + a_0 \\ &= (\sigma_i(a^n)) + a_{n-1}(\sigma_i(a^{n-1})) + \cdots + a_0 \\ &= \sigma_i(a^n) + \sigma_i(a_{n-1}a^{n-1}) + \cdots + \sigma_i(a_0) \\ &= \sigma_i(a^n + a_{n-1}a^{n-1} + \cdots + a_0) \\ &= \sigma_i(f_\alpha(a)) \\ &= \sigma_i(0) = 0. \end{aligned}$$

Στις παραπάνω ισότητες αξιοποιούμε το γεγονός ότι οι σ_i είναι ισομορφισμοί που αφήνουν αναλλοίωτους τους ρητούς αριθμούς. □

Πόρισμα 1.2.5. Αν ο αριθμός α του ακέραιου αλγεβρικού σώματος K είναι ακέραιος αλγεβρικός, τότε οι συζυγείς αριθμοί αυτού είναι επίσης ακέραιοι αλγεβρικοί.

Ορισμός 1.2.6. Αν a τυχαίος αριθμός του K= $\mathbb{Q}(\theta)$, τότε οι αριθμοί

$$S_K(a) = a^{(1)} + a^{(2)} + \cdots + a^{(n)}$$

$$N_K(a) = a^{(1)}a^{(2)} \ldots a^{(n)}$$

καλούνται ίχνος και νόρμα του a αντίστοιχα.

Πρόταση 1.2.7. Αν ο αριθμός a του ακέραιου αλγεβρικού σώματος K είναι ακέραιος αλγεβρικός, τότε οι αριθμοί $S_K(a)$ και $N_K(a)$ ανήκουν στο $\mathbb{Z}$.

Απόδειξη. Προκύπτει από το [1], Θεώρημα 4.4, σελίδα 150. □

Πρόταση 1.2.8. Ο ακέραιος αλγεβρικός αριθμός $a \in$ K ανήκει στο $\mathbb{Z}$, αν και μόνο αν οι συζυγείς του αριθμοί ταυτίζονται.

Απόδειξη. Αν ο a είναι ακέραιος τότε $\sigma_i(a) = a, \forall i = 1, \ldots, n$, διότι οι σ_i αφήνουν τους ρητούς αμετάβλητους.

Αν οι συζυγείς του α ταυτίζονται, τότε το ανάγωγο πολυώνυμο $f_\alpha(x)$, που έχει μόνο απλές ρίζες, θα έχει μοναδική ρίζα. Δηλαδή, $f_\alpha(x) = x - a$. Επιπλέον αφού a ακέραιος αλγεβρικός αριθμός, οι συντελεστές του $f_\alpha(x)$ είναι ακέραιοι αριθμοί. Άρα $a \in \mathbb{Z}$. □

1.3 Βάση ακεραιότητας. Διακρίνουσα.

Ορισμός 1.3.1. Έστω n αριθμοί $a_1, a_2, \ldots, a_n$ του αλγεβρικού σώματος αριθμών Κ. Καλούμε διακρίνουσα των αριθμών $a_1, a_2, \ldots, a_n$ και συμβολίζουμε $d(a_1, a_2, \ldots, a_n)$ τον αριθμό:

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

Ορισμός 1.3.2. Ονομάζουμε διακρίνουσα ενός αριθμού a του αλγεβρικού σώματος αριθμών Κ και συμβολίζουμε με $d(a)$ τη διακρίνουσα των αριθμών $1, a, a^2, , \ldots, a^{n-1}$. Δηλαδή:

$$d(a) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ a^{(1)} & a^{(2)} & \ldots & a^{(n)} \\ (a^{(1)})^2 & (a^{(2)})^2 & \ldots & (a^{(n)})^2 \\ \ldots & \ldots & \ldots & \ldots \\ (a^{(1)})^{n-1} & (a^{(2)})^{n-1} & \ldots & (a^{(n)})^{n-1} \end{vmatrix}^2$$

Παράδειγμα 1.3.3. Ας υπολογίσουμε τη διακρίνουσα του $\sqrt[3]{2}$ του αλγεβρικού σώματος αριθμών $\mathbb{Q}(\sqrt[3]{2})$. Οι συζυγείς αριθμοί του $\sqrt[3]{2}$ είναι οι $a^{(1)} = \sqrt[3]{2}$, $a^{(2)} = \omega\sqrt[3]{2}$, $a^{(3)} = \omega^2\sqrt[3]{2}$. Άρα λοιπόν:

$$\begin{aligned} d(\sqrt[3]{2}) &= \begin{vmatrix} 1 & 1 & 1 \\ \sqrt[3]{2} & w\sqrt[3]{2} & w^2\sqrt[3]{2} \\ \sqrt[3]{2}^2 & w^2\sqrt[3]{2}^2 & w\sqrt[3]{2}^2 \end{vmatrix}^2 \\ &= (\sqrt[3]{2})^6 \begin{vmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{vmatrix}^2 \\ &= 2^2(\omega^2 - \omega - \omega + \omega^2 + \omega^2 - \omega)^2 \\ &= 2^2 3^2(\omega^2 - \omega)^2 = -3 \cdot 2^2 \cdot 3^2 \end{aligned}$$

Θεώρημα 1.3.4. Ισχύει ότι:

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

Απόδειξη.

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

$$=\begin{vmatrix} a_1^{(1)} & a_1^{(2)} & \ldots & a_1^{(n)} \\ a_2^{(1)} & a_2^{(2)} & \ldots & a_2^{(n)} \\ \ldots & \ldots & \ldots & \ldots \\ a_n^{(1)} & a_n^{(2)} & \ldots & a_n^{(n)} \end{vmatrix}\begin{vmatrix} a_1^{(1)} & a_1^{(2)} & \ldots & a_1^{(n)} \\ a_2^{(1)} & a_2^{(2)} & \ldots & a_2^{(n)} \\ \ldots & \ldots & \ldots & \ldots \\ a_n^{(1)} & a_n^{(2)} & \ldots & a_n^{(n)} \end{vmatrix}$$

$$=\begin{vmatrix} a_1^{(1)} & a_1^{(2)} & \ldots & a_1^{(n)} \\ a_2^{(1)} & a_2^{(2)} & \ldots & a_2^{(n)} \\ \ldots & \ldots & \ldots & \ldots \\ a_n^{(1)} & a_n^{(2)} & \ldots & a_n^{(n)} \end{vmatrix}\begin{vmatrix} a_1^{(1)} & a_2^{(1)} & \ldots & a_n^{(1)} \\ a_1^{(2)} & a_2^{(2)} & \ldots & a_n^{(2)} \\ \ldots & \ldots & \ldots & \ldots \\ a_1^{(n)} & a_2^{(n)} & \ldots & a_n^{(n)} \end{vmatrix}$$

$$=\begin{vmatrix} \sum_{i=1}^n a_1^{(i)}a_1^{(i)} & \sum_{i=1}^n a_1^{(i)}a_2^{(i)} & \ldots & \sum_{i=1}^n a_1^{(i)}a_n^{(i)} \\ \sum_{i=1}^n a_2^{(i)}a_1^{(i)} & \sum_{i=1}^n a_2^{(i)}a_2^{(i)} & \ldots & \sum_{i=1}^n a_2^{(i)}a_n^{(i)} \\ \ldots & \ldots & \ldots & \ldots \\ \sum_{i=1}^n a_n^{(i)}a_1^{(i)} & \sum_{i=1}^n a_n^{(i)}a_2^{(i)} & \ldots & \sum_{i=1}^n a_n^{(i)}a_n^{(i)} \end{vmatrix}$$

Επίσης έχουμε για όλα τα $i,j=1,\ldots,n$:

$$\sum_{t=1}^n a_i^{(t)}a_j^{(t)}=\sum_{t=1}^n \sigma_t(a_i)\sigma_t(a_j)=\sum_{t=1}^n \sigma_t(a_ia_j)=\sum_{t=1}^n (a_ia_j)^{(t)}=S_K(a_ia_j)$$

Άρα τελικά:

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

Πόρισμα 1.3.5. Η διακρίνουσα n ακέραιων αλγεβρικών αριθμών $a_1,\ldots,a_n$ του αλγεβρικού σώματος αριθμών Κ είναι ακέραιος αριθμός.

Απόδειξη. Όπως είδαμε στην Πρόταση 1.2.7. για ακέραιο αλγεβρικό αριθμό $a \in \mathrm{K}$ ισχύει $S_K(a) \in \mathbb{Z}$. Άρα σύμφωνα με το αμέσως προηγούμενο θεώρημα η $d(a_1, a_2, \ldots, a_n)$ είναι ακέραιος αριθμός. □

Θεώρημα 1.3.6. Έστω $w_1, w_2, \ldots, w_n$ μια βάση της επεκτάσεως $\mathrm{K}/\mathbb{Q}$ και $a_i = \sum_{j=1}^{n} a_{ij} w_j, a_{ij} \in \mathbb{Q}, i = 1, \ldots, n$. Τότε:

$$d(a_1, a_2, \ldots, a_n) = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}^2 d(w_1, w_2, \ldots, w_n)$$

Απόδειξη. Οι συζυγείς αριθμοί των δεδομένων a_i είναι:

$$\begin{aligned} a_i^{(t)} = \sigma_t(a_i) = \sigma_t\left(\sum_{j=1}^{n} a_{ij} w_j\right) = \sum_{j=1}^{n} \sigma_t(a_{ij} w_j) \\ = \sum_{j=1}^{n} \sigma_t(a_{ij}) \sigma_t(w_j) = \sum_{j=1}^{n} a_{ij} \sigma_t(w_j) = \sum_{j=1}^{n} a_{ij} w_j^{(t)} \end{aligned}$$

Επομένως απο τον ορισμό της διακρίνουσας προκύπτει ότι:

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

$$= \begin{vmatrix} \sum_{j=1}^{n} a_{1j} w_j^{(1)} & \sum_{j=1}^{n} a_{1j} w_j^{(2)} & \ldots & \sum_{j=1}^{n} a_{1j} w_j^{(n)} \\ \sum_{j=1}^{n} a_{2j} w_j^{(1)} & \sum_{j=1}^{n} a_{2j} w_j^{(2)} & \ldots & \sum_{j=1}^{n} a_{2j} w_j^{(n)} \\ \ldots & \ldots & \ldots & \ldots \\ \sum_{j=1}^{n} a_{nj} w_j^{(1)} & \sum_{j=1}^{n} a_{nj} w_j^{(2)} & \ldots & \sum_{j=1}^{n} a_{nj} w_j^{(n)} \end{vmatrix}^2$$

$$= \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}^2 \begin{vmatrix} w_1^{(1)} & w_1^{(2)} & \ldots & w_1^{(n)} \\ w_2^{(1)} & w_2^{(2)} & \ldots & w_2^{(n)} \\ \ldots & \ldots & \ldots & \ldots \\ w_n^{(1)} & w_n^{(2)} & \ldots & w_n^{(n)} \end{vmatrix}^2$$

$$= \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}^2 d(w_1, w_2, \dots, w_n)$$

□

Πρόταση 1.3.7. Οι αριθμοί $a_1, \dots, a_n$ του αλγεβρικού σώματος αριθμών Κ είναι γραμμικά ανεξάρτητοι, αν και μόνον αν ισχύει

$$d(a_1, \dots, a_n) \neq 0$$

Απόδειξη. Εφαρμόζουμε τους $\mathbb{Q}$-ισομορφισμούς $\sigma_1, \dots, \sigma_n$ του αλγεβρικού σώματος Κ στη σχέση

$$b_1 a_1 + \dots + b_n a_n = 0, \qquad b_i \in \mathbb{Q}$$

οπότε προκύπτει

$$b_1 \sigma_i(a_1) + \dots + b_n \sigma_i(a_n) = 0 \qquad i = 1, \dots, n$$

δηλαδή

$$b_1 a_1^{(i)} + \dots + b_n a_n^{(i)} = 0 \qquad i = 1, \dots, n$$

Το σύστημα αυτό είναι γραμμικό ως προς $b_1, \dots, b_n$ και έχει μόνο τη μηδενική λύση αν και μόνον αν η ορίζουσα των συντελεστών αυτού

$$\begin{vmatrix} a_1^{(1)} & a_2^{(1)} & \dots & a_n^{(1)} \\ a_1^{(2)} & a_2^{(2)} & \dots & a_n^{(2)} \\ \dots & \dots & \dots & \dots \\ a_1^{(n)} & a_2^{(n)} & \dots & a_n^{(n)} \end{vmatrix}$$

είναι διάφορη του μηδενός, ή ισοδύναμα αν ισχύει

$$d(a_1, \dots, a_n) \neq 0$$

□

Ορισμός 1.3.8. Οι ακέραιοι αλγεβρικοί αριθμοί $w_1, w_2, \dots, w_n$ του αλγεβρικού σώματος αριθμών Κ θα καλούνται βάση ακεραιότητας του Κ, αν είναι γραμμικά ανεξάρτητοι και κάθε ακέραιος αλγεβρικός αριθμός a του Κ έχει μια παράσταση της μορφής $a = a_1 w_1 + a_2 w_2 + \dots + a_n w_n, a_i \in \mathbb{Z}$.

Επειδή οι n το πλήθος αριθμοί $w_1, w_2, \ldots, w_n$ είναι γραμμικά ανεξάρτητοι, αποτελούν βάση της επέκτασης Κ/$\mathbb{Q}$. Συνεπώς η παραπάνω παράσταση του ακέραιου αλγεβρικού αριθμού a είναι μονοσήμαντη.

Γρήγορα διαπιστώνουμε ότι μια βάση ακεραιότητας του Κ είναι ουσιαστικά μια βάση του δακτυλίου R των ακέραιων αλγεβρικών αριθμών αυτού.

Παρατηρούμε επίσης ότι ενώ κάθε βάση ακεραιότητας του σώματος Κ είναι και βάση της επέκτασης Κ/$\mathbb{Q}$, το αντίστροφο δεν ισχύει.

Θεώρημα 1.3.9. Κάθε αλγεβρικό σώμα αριθμών Κ έχει μία τουλάχιστον βάση ακεραιότητας.

Απόδειξη. Θεωρούμε το σύνολο Ω των συστημάτων n γραμμικά ανεξάρτητων ακέραιων αλγεβρικών αριθμών του Κ. Το Ω δεν είναι το κενό σύνολο, καθώς αν Κ=$\mathbb{Q}(\theta)$ και θ ακέραιος αλγεβρικός αριθμός, τότε οι $1, \theta, \theta^2, \ldots, \theta^{n-1}$ ανήκουν στο Ω. Οι απόλυτες τιμές των διακρινουσών των αριθμών αυτών είναι σύμφωνα με το Πόρισμα 1.3.5. φυσικοί αριθμοί, διάφοροι του μηδενός λόγω γραμμικής ανεξαρτησίας. Συνεπάγεται λοιπόν, από την αρχή της καλής διάταξης, ότι υπάρχει ένα στοιχείο $(w_1, w_2, \ldots, w_n)$ με ελάχιστη απόλυτη τιμή διακρίνουσας.

Έστω a τυχαίος ακέραιος αλγεβρικός αριθμός του Κ. Τότε

$$a = a_1 w_1 + a_2 w_2 + \cdots + a_n w_n, \qquad a_i \in \mathbb{Q}$$

διότι οι $w_1, w_2, \ldots, w_n$ αποτελούν βάση της επέκτασης Κ/$\mathbb{Q}$.

Θα δείξουμε ότι αν ένα τουλάχιστον από τα a_i δεν είναι ακέραιος, τότε ο α δεν είναι ακέραιος αλγεβρικός αριθμός. Δίχως βλάβη της γενικότητας υποθέτουμε ότι ο a_1 δεν είναι ακέραιος. Τότε $a_1 \in \mathbb{Q} - \mathbb{Z}$.

Θέτουμε πρώτα $a_1' = a_1 - [a_1]$, οπότε $0 < a_1' < 1$, και στη συνέχεια

$$\beta = a - [a_1]w_1 = a_1' w_1 + a_2 w_2 + \cdots + a_n w_n.$$

Για τη διακρίνουσα των αριθμών $\beta, w_1, w_2, \ldots, w_n$ ισχύει σύμφωνα με το Θεώρημα 1.3.6.

$$d(\beta, w_2, \ldots, w_n) = \begin{vmatrix} a_1' & a_2 & \ldots & a_n \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{vmatrix}^2 d(w_1, w_2, \ldots, w_n)$$

$$= (a_1')^2 d(w_1, w_2, \ldots, w_n) \neq 0$$

Δηλαδή

$$\mid d(\beta, w_2, \ldots, w_n) \mid < \mid d(w_1, w_2, \ldots, w_n) \mid$$

και οι $\beta, w_1, w_2, \ldots, w_n$ είναι γραμμικά ανεξάρτητοι.
Εφόσον η $\mid d(w_1, w_2, \ldots, w_n) \mid$ είναι ελάχιστη, προκύπτει ότι ο β δεν είναι ακέραιος αλγεβρικός αριθμός, άρα ούτε και ο $a = \beta + [a_1]w_1$. Για να έχουμε λοιπόν ακέραιο αλγεβρικό αριθμό πρέπει όλοι οι συντελεστές $a_i \in \mathbb{Z}$, άρα οι $w_1, w_2, \ldots, w_n$ αποτελούν βάση ακεραιότητας του Κ. □

Θεώρημα 1.3.10. Αν η διακρίνουσα των ακέραιων αλγεβρικών αριθμών $\rho_1, \rho_2, \ldots, \rho_n$ του αλγεβρικού σώματος αριθμών Κ βαθμού n είναι ελεύθερη τετραγώνων, τότε οι αριθμοί αυτοί αποτελούν βάση ακεραιότητας του Κ.

Απόδειξη. Έστω $w_1, w_2, \ldots, w_n$ μια βάση ακεραιότητας του Κ. Τότε

$$\rho_i = a_{i1}w_1 + a_{i2}w_2 + \cdots + a_{in}w_n, a_i \in \mathbb{Z}, i = 1, 2, \ldots, n$$

οπότε ισχύει από το Θεώρημα 1.3.6. ότι:

$$d(\rho_1, \rho_2, \ldots, \rho_n) = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}^2 d(w_1, w_2, \ldots, w_n)$$

Επειδή η διακρίνουσα $d(\rho_1, \rho_2, \ldots, \rho_n)$ είναι ελεύθερη τετραγώνων πρέπει να ισχύει:

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = \pm 1$$

Δηλαδή $d(\rho_1, \rho_2, \ldots, \rho_n)$ είναι ελάχιστη και ισχύει

$$d(\rho_1, \rho_2, \ldots, \rho_n) = d(w_1, w_2, \ldots, w_n) \neq 0$$

οπότε οι $\rho_1, \rho_2, \ldots, \rho_n$ είναι γραμμικά ανεξάρτητοι. Τότε λοιπόν σύμφωνα με την πορεία της απόδειξης του προηγούμενου θεωρήματος, οι αριθμοί $\rho_1, \rho_2, \ldots, \rho_n$ αποτελούν βάση ακεραιότητας του Κ. □

Το παραπάνω θεώρημα φαίνεται χρήσιμο για τον εντοπισμό βάσεων ακεραιότητας. Καθώς όμως δεν εμφανίζονται συχνά διακρίνουσες ελεύθερες τετραγώνων, χρησιμοποιούμε το παρακάτω αποτέλεσμα:

Θεώρημα 1.3.11. Έστω $w_1, w_2, \ldots, w_n$ βάση της επέκτασης Κ/$\mathbb{Q}$, αποτελούμενη από ακέραιους αλγεβρικούς αριθμούς, και έστω p πρώτος, τέτοιος ώστε $p^2 \mid d(w_1, w_2, \ldots, w_n)$. Τότε υπάρχει ένας ακέραιος αλγεβρικός αριθμός (όχι πάντα μηδενικός) της μορφής $\frac{1}{p}(\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_n w_n)$ όπου $\lambda_i \in \mathbb{Z}$ και $0 \leq \lambda_i \leq p-1$.

Απόδειξη. Βλέπε [7], Πρόταση 2.21, σελίδα 52. □

Θα προχωρήσουμε τώρα σε ένα παράδειγμα εύρεσης βάσης ακεραιότητας. Τα βήματα του αλγορίθμου που θα ακολουθήσουμε θα απαριθμούνται.

Παράδειγμα 1.3.12. Να βρεθεί βάση ακεραιότητας του Κ= $\mathbb{Q}(\sqrt[3]{2})$.

(1) Όπως έχουμε ήδη παρατηρήσει κάθε βάση ακεραιότητας του Κ είναι και βάση της επέκτασης Κ/$\mathbb{Q}$. Άρα ξεκινάμε βρίσκοντας μία βάση της Κ/$\mathbb{Q}$.

Στο Παράδειγμα 1.2.3. είδαμε ότι η $(1, \sqrt[3]{2}, \sqrt[3]{2}^2)$ είναι μία τέτοια βάση.

(2) Υπολογίζουμε τη διακρίνουσα της βάσης $(1, \sqrt[3]{2}, \sqrt[3]{2}^2)$.
Αν ικανοποιείται το Θεώρημα 1.3.10. τότε έχουμε τελειώσει.

Και πάλι σε συνδυασμό με το Παράδειγμα 1.2.3. προκύπτει ότι:

$$d(1, \sqrt[3]{2}, \sqrt[3]{2}^2) = \begin{vmatrix} \sigma_1(1) & \sigma_2(1) & \sigma_3(1) \\ \sigma_1(\sqrt[3]{2}) & \sigma_2(\sqrt[3]{2}) & \sigma_3(\sqrt[3]{2}) \\ \sigma_1(\sqrt[3]{2}^2) & \sigma_2(\sqrt[3]{2}^2) & \sigma_3(\sqrt[3]{2}^2) \end{vmatrix}^2$$

$$= \begin{vmatrix} 1 & 1 & 1 \\ \sqrt[3]{2} & w\sqrt[3]{2} & w^2\sqrt[3]{2} \\ \sqrt[3]{2}^2 & w^2\sqrt[3]{2}^2 & w\sqrt[3]{2}^2 \end{vmatrix}^2$$

$$= -3 \cdot 4 \cdot 9$$

(3) Εφόσον η διακρίνουσα δεν είναι ελεύθερη τετραγώνων εντοπίζουμε τους πρώτους αριθμούς, το τετράγωνο των οποίων τη διαιρεί.

Στην περίπτωση μας έχουμε $p = 2$ και $p = 3$.

(4) Εφαρμόζουμε το Θεώρημα 1.3.11. για έναν από τους πρώτους αριθμούς του προηγούμενου βήματος. Στη συνέχεια υπολογίζουμε το ίχνος του νέου μας αριθμού και αξιοποιούμε το γεγονός ότι αυτό πρέπει να είναι ακέραιος αριθμός.

Επιλέγουμε $p = 2$. Τότε από το Θεώρημα 1.3.11. υπάρχει ακέραιος αλγεβρικός αριθμός της μορφής: $a = \frac{1}{2}(\lambda_1 + \lambda_2\sqrt[3]{2} + \lambda_3\sqrt[3]{2}^2), 0 \leq \lambda_i \leq 1$. $S_K(a) = \sigma_1(a) + \sigma_2(a) + \sigma_3(a) = \cdots = \frac{3\lambda_1}{2}$. Άρα πρέπει $\lambda_1 \in 2\mathbb{Z}$. Όμως $\lambda_1 \leq 1$ άρα $\lambda_1 = 0$.

(5) Υπολογίζουμε τη νόρμα του νέου αριθμού από το Θεώρημα 1.3.11. αντικαθιστώντας τα ευρήματά μας από το προηγούμενο βήμα και λαμβάνοντας υπόψη ότι η νόρμα είναι ακέραιος αριθμός.

Αντικαθιστώντας $\lambda_1 = 0$ έχουμε $a' = \frac{1}{2}(\lambda_2\sqrt[3]{2} + \lambda_3\sqrt[3]{2}^2)$.
Οπότε $N_K(a') = \sigma_1(a')\sigma_2(a')\sigma_3(a') = \cdots = \frac{\lambda_2^3 + 2\lambda_3^3}{4}$. Άρα πρέπει $\lambda_2^3 + 2\lambda_3^3 \in 4\mathbb{Z}$. Ελέγχουμε όλες τις περιπτώσεις:
Αν $\lambda_2 = 0$ και $\lambda_3 = 1$ τότε $\lambda_2^3 + 2\lambda_3^3 = 2 \notin 4\mathbb{Z}$.
Αν $\lambda_2 = 1$ και $\lambda_3 = 0$ τότε $\lambda_2^3 + 2\lambda_3^3 = 2 \notin 4\mathbb{Z}$.
Αν $\lambda_2 = 1$ και $\lambda_3 = 1$ τότε $\lambda_2^3 + 2\lambda_3^3 = 3 \notin 4\mathbb{Z}$.
Επομένως πρέπει $\lambda_1 = \lambda_2 = \lambda_3 = 0$, δηλαδή δεν υπάρχουν νέοι ακέραιοι αλγεβρικοί αριθμοί της μορφής του Θεωρήματος 1.3.11. για $p = 2$.

(6) Επαναλαμβάνουμε τα βήματα (4) και (5) για τους υπόλοιπους πρώτους αριθμούς του βήματος (3).

Ακολουθούμε τα ίδια βήματα για $p = 3$ και βλέπουμε ότι και πάλι δεν προκύπτουν νέοι αλγεβρικοί αριθμοί.

Συμπεραίνουμε λοιπόν ότι η $(1, \sqrt[3]{2}, \sqrt[3]{2}^2)$ αποτελεί βάση ακεραιότητας του K.

1.4 Ιδεώδη. Βάση Ιδεώδους. Νόρμα ακέραιου ιδεώδους.

Ορισμός 1.4.1. Ένα υποσύνολο A του αλγεβρικού σώματος αριθμών Κ, θα καλείται ιδεώδες του Κ, αν πληρούνται οι παρακάτω προϋποθέσεις:

- $(A, +)$ ομάδα.
- $a \in A, \rho \in R \Rightarrow a\rho \in A$, όπου R ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του Κ.
- $A \neq \{0\}$.
- Υπάρχει $0 \neq \delta \in$ Κ τέτοιο ώστε $\delta A \subset R$.

Αν το ιδεώδες A περιέχεται στο δακτύλιο R των ακέραιων αλγεβρικών αριθμών του Κ, τότε θα καλείται ακέραιο ιδεώδες του Κ. Διαφορετικά, το A ονομάζεται κλασματικό ιδεώδες του Κ.

Αν $0 \neq a \in K$, τότε το σύνολο $(a) = aR = \{a\rho : \rho \in R\}$ είναι ιδεώδες του Κ, το οποίο καλούμε κύριο ιδεώδες του Κ που παράγεται από τον a. Αν a είναι ακέραιος αλγεβρικός αριθμός, τότε το ιδεώδες (a) είναι προφανώς ακέραιο. Διαφορετικά το (a) είναι κλασματικό.

Πρόταση 1.4.2. Αν Α, Β τυχαία ακέραια ιδεώδη του αλγεβρικού σώματος αριθμών Κ, τότε $AB \subset A \cap B$.

Απόδειξη. Ορίζεται ότι $AB = \left\{ \sum^{n} ab : a \in A, b \in B \right\}$. Από τον ορισμό του ιδεώδους κάθε όρος του αθροίσματος $\sum^{n} ab$ ανήκει στο A, άρα και ολόκληρο το άθροισμα ανήκει στο A. Όμοια και για το B. Επομένως $AB \subset A \cap B$. □

Η παραπάνω πρόταση ισχύει γενικότερα για γινόμενα $P_1 \dots P_n$ πρώτων ιδεωδών.

Πρόταση 1.4.3. Κάθε ιδεώδες A του αλγεβρικού σώματος αριθμών Κ περιέχει και φυσικούς αριθμούς διάφορους του μηδενός.

Απόδειξη. Για το ιδεώδες Α, υπάρχει εξ ορισμού $\delta \in$ Κ, τέτοιο ώστε $\delta A \in R$. Έστω $a \in A$. Τότε $\delta a \in R$. Άρα από την Πρόταση 1.2.7. $N_K(\delta a) \in \mathbb{Z}$.

Ισχύει ότι $N_K(\delta a) = (\delta a)^{(1)}(\delta a)^{(2)} \dots (\delta a)^{(n)}$, όπου $(\delta a)^{(i)}$ οι συζυγείς του δa. Καθώς ο δa είναι ακέραιος αλγεβρικός αριθμός, οι συζυγείς του θα είναι επίσης ακέραιοι αλγεβρικοί αριθμοί, σύμφωνα με το Πόρισμα 1.2.6. Άρα $N_K(\delta a) = \delta a\beta$, όπου $\delta a = (\delta a)^{(1)}$ και $\beta = (\delta a)^{(2)} \dots (\delta a)^{(n)} \in R$. Τέλος,

$$N_K(\delta a) = \delta a\beta = (\delta\beta)a \Rightarrow N_K(\delta a) \in \mathbb{Z} \cap A$$

. □

Ορισμός 1.4.4. Οι αριθμοί $a_1, \dots, a_n$ του ιδεώδους A του αλγεβρικού σώματος αριθμών K βαθμού $[K : \mathbb{Q}] = n$, ονομάζονται βάση του ιδεώδους A, αν είναι γραμμικά ανεξάρτητοι και κάθε αριθμός του A έχει μια μονοσήμαντη παράσταση της μορφής $a = \beta_1 a_1 + \dots + \beta_n a_n$, $\beta_i \in \mathbb{Z}$.

Θεώρημα 1.4.5. Κάθε ιδεώδες A του αλγεβρικού σώματος αριθμών Κ έχει μια τουλάχιστον βάση.

Απόδειξη. Έστω ότι το A είναι ακέραιο ιδεώδες. Έστω επίσης $w_1, \dots, w_n$ μια βάση ακεραιότητας του Κ και $0 \neq a \in A$. Τότε τα $aw_1, \dots, aw_n$ είναι γραμμικά ανεξάρτητα.
Επιλέγουμε $a_1, \dots, a_n \in A$ γραμμικά ανεξάρτητα, με την ελάχιστη $|d(a_1, \dots, a_n)|$. Προφανώς, κάθε στοιχείο της μορφής

$$b_1 a_1 + \dots + b_n a_n, b_i \in \mathbb{Z}$$

ανήκει στο A. Θα δείξουμε ότι τα $a_1, \dots, a_n$ είναι βάση του A. δηλαδή το A αποτελείται μόνο από στοιχεία της παραπάνω μορφής.
Υποθέτουμε ότι ένας τουλάχιστον από τους $b_1, \dots, b_n$ δεν είναι ακέραιος και θα δείξουμε ότι τότε $a \notin A$. Έστω ότι $b_1 \notin \mathbb{Z}$. Τότε θεωρούμε

$$b_1' = b_1 - [b_1] \text{ και } b = a - [b_1]a_1 = b_1' a_1 + \dots + b_n a_n.$$

Τότε από το Θεώρημα 1.3.6. έχουμε

$$|d(b, a_2, \dots, a_n)| = \begin{vmatrix} b_1' & b_2 & \dots & b_n \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{vmatrix}^2 |d(a_1, \dots, a_n)|$$

$$= (b_1')^2 |d(a_1, \dots, a_n)|$$

$$< |d(a_1, \dots, a_n)|$$

Η $|d(b, a_1, \ldots, a_n)| \neq 0$ άρα οι αριθμοί $b, a_2, \ldots, a_n$ είναι γραμμικά ανεξάρτητοι. Καθώς όμως $|d(b, a_2, \ldots, a_n)| < |d(a_1, \ldots, a_n)|$, η οποία είναι η ελάχιστη διακρίνουσα για n γραμμικά ανεξάρτητα στοιχεία του A, προκύπτει ότι $b \notin A$. Επομένως, $a = b + [b_1]a_1$ δεν ανήκει στο A.
Έστω τώρα ότι το A δεν είναι ακέραιο ιδεώδες. Τότε υπάρχει εξ ορισμού $\delta \in K$ τέτοιο ώστε $\delta A \subset R$. Αν $\delta a_1, \delta a_2, \ldots, \delta a_n$ είναι μια βάση του δA, τότε $a_1, \ldots, a_n$ είναι μια βάση του A. □

Σημειώνουμε ότι τα ιδεώδη του δακτυλίου ακέραιων αλγεβρικών αριθμών $R \setminus \{0\}$, δεν είναι παρά τα ακέραια ιδεώδη του K.

Ορισμός 1.4.6. Ονομάζουμε δακτύλιο της Noether έναν δακτύλιο R, ο οποίος ικανοποιεί μία από τις ακόλουθες ισοδύναμες συνθήκες:

- Κάθε αύξουσα ακολουθία ιδεωδών του R γίνεται σταθερή.
- Κάθε μη κενό σύνολο ιδεωδών του R έχει μέγιστο στοιχείο.
- Κάθε ιδεώδες του R είναι πεπερασμένα παραγόμενο.

Για την απόδειξη της ισοδυναμίας των παραπάνω συνθηκών βλέπε [2] Θεώρημα 3.1.1, σελίδα 33.

Πόρισμα 1.4.7. Ο δακτύλιος R των ακέραιων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών K είναι δακτύλιος της Noether.

Απόδειξη. Κάθε ιδεώδες του R έχει μια βάση, συνεπώς είναι πεπερασμένα παραγόμενο. □

Έστω M ένα ακέραιο ιδεώδες του αλγεβρικού σώματος αριθμών K. Το M ορίζει στον R σχέση ισοδυναμίας ως εξής:

$$a \equiv \beta \mod M \Leftrightarrow a - \beta \in M$$

Πράγματι, ικανοποιούνται οι εξής ιδιότητες:

- ανακλαστική ιδιότητα
  $a \equiv a \mod M \Leftrightarrow a - a \in M \Leftrightarrow 0 \in M$

- συμμετρική ιδιότητα
  $a \equiv \beta \mod M \Leftrightarrow a - \beta \in M \Leftrightarrow -(a-\beta) \in M \Leftrightarrow \beta - a \in M \Leftrightarrow \beta \equiv a \mod M$.

- μεταβατική ιδιότητα
  $a \equiv \beta \mod M \Leftrightarrow a - \beta \in M$
  $\beta \equiv \gamma \mod M \Leftrightarrow \beta - \gamma \in M$
  Προσθέτουμε και παίρνουμε $a - \gamma \in M \Leftrightarrow a \equiv \gamma \mod M$.

Η σχέση αυτή χωρίζει το R σε κλάσεις ισοδυναμίας, το σύνολο των οποίων συμβολίζουμε με $R/M = \{a + M : a \in R\}$. Σημειώνουμε ότι ο R/M είναι ο δακτύλιος πηλίκο.

Ορισμός 1.4.8. Αν M είναι ένα ακέραιο ιδεώδες του αλγεβρικού σώματος αριθμών Κ, τότε το πλήθος των στοιχείων του R/M το ονομάζουμε νόρμα του M και το συμβολίζουμε $N_K(M)$.

Πρόταση 1.4.9. Αν M είναι ακέραιο ιδεώδες του αλγεβρικού σώματος αριθμών Κ και R ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του Κ, τότε ο δακτύλιος R/M έχει πεπερασμένου πλήθους στοιχεία.

Απόδειξη. Επιλέγουμε τον ελάχιστο φυσικό αριθμό m του M, που υπάρχει λόγω της Πρότασης 1.4.3. και θεωρούμε $w_1, \ldots, w_n$ μια βάση ακεραιότητας του Κ. Τότε κάθε $a \in R$ έχει μια μονοσήμαντη ανάλυση της μορφής

$$a = a_1 w_1 + \cdots + a_n w_n$$

όπου $a_i \in \mathbb{Z}$.
Θεωρούμε τους φυσικούς αριθμούς $a_1', \ldots, a_n'$ τέτοιους ώστε

$$0 \leq a_i' < m \text{ και } a_i \equiv a_i' \mod m \Rightarrow a_i - a_i' = m\beta_i$$

όπου $\beta_i \in \mathbb{Z}$. Δηλαδή οι a_i' είναι τα υπόλοιπα της διαίρεσης των a_i με το m.
Ο ακέραιος αλγεβρικός αριθμός

$$a' = a_1' w_1 + \cdots + a_n' w_n$$

ανήκει στην κλάση ισοδυναμίας $a + M$, καθώς

$$\begin{aligned} a_i - a_i' &= (a_1 - a_1')w_1 + \cdots + (a_n - a_n')w_n \\ &= m\beta_1 w_1 + \cdots + m\beta_n w_n \\ &= m(\beta_1 w_1 + \cdots + \beta_n w_n) \\ &= m\beta \in M \end{aligned}$$

όπου $\beta \in R$.
Συνεπώς για την τυχαία κλάση ισοδυναμίας $a+M$ βρήκαμε αντιπρόσωπο

$$a' = a'_1 w_1 + \cdots + a'_n w_n$$

με $0 \leq a'_i < m$. Για τον a' υπάρχουν m^n δυνατότητες. Άρα το πλήθος των στοιχείων του R/M είναι το πολύ m^n. □

Πρόταση 1.4.10. Για κάθε ακέραιο ιδεώδες M του αλγεβρικού σώματος Κ ισχύει $N_K(M) \in M$.

Απόδειξη. Έχουμε ορίσει ότι $N_K(M) = |R/M|$, δηλαδή ο $N_K(M)$ είναι η τάξη της ομάδας πηλίκου R/M. Άρα για κάθε $a + M \in R/M$, ισχύει

$$N_K(M)(a + M) = 0 + M \Rightarrow aN_K(m) \in M,$$

για κάθε $a \in R$. Αν $a = 1$, τότε προκύπτει το ζητούμενο. □

1.5 Μονοσήμαντη Ανάλυση Ιδεωδών σε Γινόμενο Πρώτων Ιδεωδών.

Σε αυτό το σημείο θα ορίσουμε τις έννοιες πρώτων και μέγιστων ιδεωδών για τα ακέραια ιδεώδη.

Ορισμός 1.5.1. Ένα ακέραιο ιδεώδες P του αλγεβρικού σώματος αριθμών Κ ονομάζεται πρώτο, αν είναι διάφορο του R και ισχύει

$$P|(a)(\beta), \quad a \in R, \beta \in R \Rightarrow P|(a) \text{ ή } P|(\beta)$$

ή ισοδύναμα

$$a\beta \in P, \quad a \in R, \beta \in R \Rightarrow a \in P \text{ ή } \beta \in P$$

Ορισμός 1.5.2. Ένα ακέραιο ιδεώδες Μ του αλγεβρικού σώματος αριθμών Κ θα καλείται μέγιστο, αν είναι διάφορο του R και για κάθε ακέραιο ιδεώδες Α του Κ για το οποίο ισχύει Μ⊂Α προκύπτει Α=Μ ή Α= R.

Πρόταση 1.5.3. Κάθε πρώτο ιδεώδες P του αλγεβρικού σώματος αριθμών Κ είναι μέγιστο.

Απόδειξη. Γνωρίζουμε ότι P πρώτο $\Leftrightarrow$ R/P ακέραια περιοχή. Από την Πρόταση 1.4.9. ο R/P έχει πεπαρασμένου πλήθους στοιχεία, είναι δηλαδή πεπερασμένη ακέραια περιοχή, συνεπώς σώμα.
Γνωρίζουμε επίσης ότι P μέγιστο $\Leftrightarrow$ R/P σώμα. Άρα τελικά το P είναι μέγιστο. Ακόμα, ισχύει ότι P μέγιστο $\Rightarrow$ P πρώτο. Συμπεραίνουμε λοιπόν, πως για τα ιδεώδη του Κ ισχύει ότι P πρώτο $\Leftrightarrow$ P μέγιστο.

□

Πρόταση 1.5.4. Κάθε ακέραιο ιδεώδες $A \neq R$ έχει έναν τουλάχιστον πρώτο διαιρέτη.

Απόδειξη. Αν το A είναι πρώτο, τότε ο ζητούμενος πρώτος διαιρέτης είναι το ίδιο το A.
Έστω ότι το A δεν είναι πρώτο. Τότε δεν είναι ούτε μέγιστο, δηλαδή υπάρχει A_1, με $A \subsetneq A_1 \subsetneq R$. Αν το A_1 είναι πρώτο τότε συνιστά το ζητούμενο διαιρέτη. Αλλιώς, αν δεν είναι πρώτο, δεν είναι ούτε μέγιστο και υπάρχει A_2 τέτοιο ώστε $A_1 \subsetneq A_2 \subsetneq R$.
Συνεχίζοντας δημιουργούμε μια αύξουσα ακολουθία ιδεωδών του R

$$A \subsetneq A_1 \subsetneq A_2 \subsetneq \dots$$

Καθώς ο R είναι δακτύλιος Noether θα υπάρχει δείκτης s τέτοιος ώστε

$$A_s = A_{s+1} = A_{s+2} = \dots$$

Το A_s θα είναι τότε μέγιστο, άρα πρώτο και θα διαιρεί το A. □

Πρόταση 1.5.5. Αν A είναι ένα ακέραιο ιδεώδες του αλγεβρικού σώματος αριθμών Κ διάφορο του R, τότε υπάρχουν πρώτα ιδεώδη $P_1, \dots, P_r$ του Κ τέτοια ώστε να ισχύει $P_1 \dots P_r \subset A$.

Απόδειξη. Έστω Ω το σύνολο των ακέραιων ιδεωδών του Κ, για τα οποία δεν ισχύει η πρόταση. Καθώς ο R είναι δακτύλιος της Noether, αν το Ω δεν είναι το κενό σύνολο, τότε θα έχει μέγιστο στοιχείο, έστω A.
Το ιδεώδες A δεν είναι πρώτο, γιατί τότε θα ίσχυε η πρόταση για $r = 1$ και $P_1 = A$.
Επομένως υπάρχουν $\beta \notin A$ και $\gamma \notin A$ τέτοια ώστε $\beta\gamma \in A$. Θεωρούμε τα ιδεώδη

$$B = A + \beta R \text{ και } \Gamma = A + \gamma R$$

Προφανώς $B\Gamma \subset A$, $B \supsetneq A$ και $\Gamma \supsetneq A$. Ακόμα $B \neq R$ και $\Gamma \neq R$ διότι σε αντίθετη περίπτωση

$$\Gamma = R\Gamma = B\Gamma \subset A$$

ενώ $\Gamma \supsetneq A$, άτοπο. Άρα $B, \Gamma \notin \Omega$ οπότε ισχύει η πρόταση και υπάρχουν $P_1, \dots, P_r, Q_1, \dots, Q_s$ τέτοια ώστε

$$P_1 \dots P_r \subset B \text{ και } Q_1 \dots Q_s \subset \Gamma$$

Τότε όμως

$$P_1 \dots P_r Q_1 \dots Q_s \subset B\Gamma \subset A,$$

άτοπο. Άρα Ω=∅. □

Γράφουμε $P|A$ αν ο P είναι πρώτος διαιρέτης του Α. Σημειώνουμε ότι αν $P|A$ τότε $A \subset P$.

Πρόταση 1.5.6. Έστω P πρώτο και Α, Β ακέραια ιδεώδη του αλγεβρικού σώματος αριθμών Κ. Τότε

$$P|AB \Rightarrow P|A \text{ ή } P|B$$

Απόδειξη. Από τη σχέση $P|AB$ προκύπτει ότι $AB \subset P$. Έστω $A \not\subset P$ και $B \not\subset P$. Τότε υπάρχει $a \in A - P$ και $\beta \in B - P$. Τότε όμως προκύπτει από τον ορισμό του πρώτου ιδεώδους ότι $a\beta \notin P$, το οποίο είναι άτοπο, διότι $a\beta \in AB \subset P$. Τελικά λοιπόν, $A \subset P$ ή $B \subset P$, δηλαδή $P|A$ ή $P|B$. □

Πρόταση 1.5.7. Για κάθε ακέραιο ιδεώδες A του Κ, το σύνολο

$$A^{-1} = \{x \in K : xA \subset R\}$$

αποτελεί ιδεώδες του Κ. Αν $A \neq R$, τότε $A^{-1} \supsetneqq R$.

Απόδειξη. Θα δείξουμε πρώτα ότι το A^{-1} είναι ιδεώδες.

- $x_1 \in A^{-1}, x_2 \in A^{-1} \Rightarrow x_1 - x_2 \in A^{-1}$, αφού $(x_1 - x_2)a = x_1a - x_2a \in A, \forall a \in A$
- $\rho \in R, x \in A^{-1} \Rightarrow \rho x \in A^{-1}$, αφού $xA \subset R$ και $(\rho x)a = \rho(xa), \forall a \in A$.
- $\forall \delta \in A \subset K$ ισχύει εξ ορισμού $\delta A^{-1} \subset R$

Άρα το A^{-1} είναι ιδεώδες του Κ.
Για το ακέραιο ιδεώδες A υπάρχει από την Πρόταση 1.5.4. ένας πρώτος διαιρέτης P. Δηλαδή $P|A \Rightarrow A \subset P$. Ισχύει ότι $P^{-1} \subset A^{-1}$ καθώς

$$x \in P^{-1} \Rightarrow xP \subset R \Rightarrow xA \subset xP \subset R \Rightarrow xA \subset R \Rightarrow x \in A^{-1}$$

Παρατηρούμε ότι εξ ορισμού ισχύει $A^{-1} \supset R$. Για να δείξουμε ότι $A^{-1} \neq R$ αρκεί να δείξουμε ότι $P^{-1} \neq R$. Θα βρούμε λοιπόν, ένα στοιχείο του P^{-1} που δεν ανήκει στον R.
Έστω $a \in P, a \neq 0$. Με εφαρμογή της Πρότασης 1.5.5. για το ακέραιο ιδεώδες $(a) = aR$, έχουμε $P_1 \dots P_r \subset (a)$, όπου r επιλέγουμε το ελάχιστο πλήθος ιδεωδών που ικανοποιούν αυτήν την σχέση.

$$a \in P \Rightarrow (a) \subset P \Rightarrow P_1 \dots P_r \subset P \Rightarrow P|P_1 \dots P_r$$

Καθώς P πρώτο, θα διαιρεί ένα από τα $P_1, \dots, P_r$. Δίχως βλάβη της γενικότητας υποθέτουμε ότι $P|P_1 \Rightarrow P_1 \subset P$. Αφού τα P_1, P είναι πρώτα θα είναι και μέγιστα. Άρα $P_1 = P$.
Λόγω της επιλογής του r, που είναι ελάχιστο, έχουμε ότι $P_2 \dots P_r \not\subset (a)$. Άρα υπάρχει $\beta \in P_2 \dots P_r$ με $\beta \notin (a)$. Όμως

$$\beta P \subset P_1P_2 \dots P_r \subset (a) = aR \Rightarrow \beta a^{-1}P \subset R \Rightarrow \beta a^{-1} \in P^{-1}$$

Ενώ $\beta \notin (a) = aR \Rightarrow \beta a^{-1} \notin R$. Άρα $P^{-1} \neq R$. □

Θεώρημα 1.5.8. Κάθε ακέραιο ιδεώδες $A \neq R$ του αλγεβρικού σώματος αριθμών Κ αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών του Κ.

Απόδειξη. Έστω Ω το σύνολο των ακέραιων ιδεωδών του Κ, τα οποία είναι διάφορα του R και για τα οποία δεν ισχύει η πρόταση. Επειδή ο R είναι δακτύλιος Noether, αν το Ω δεν είναι κενό, έχει μέγιστο στοιχείο, έστω A. Από την Πρόταση 1.5.4. υπάρχει πρώτος διαιρέτης P του Α. Οπότε έχουμε

$$P|A \Rightarrow A \subset P \Rightarrow P^{-1} \subset A^{-1}$$

Ακόμα από την Πρόταση 1.5.7. έχουμε $P^{-1} \supsetneq R$. Άρα τελικά

$$R \subsetneq P^{-1} \subset A^{-1} \Rightarrow A \subsetneq AP^{-1} \subset R$$

Άρα το AP^{-1} δεν ανήκει στο Ω και υπάρχουν πρώτα ιδεώδη τέτοια ώστε $AP^{-1} = P_2 \dots P_r$. Αν ονομάσουμε $P = P_1$, τότε $A = P_1 \dots P_r$, το οποίο είναι άτοπο. Άρα Ω=$\varnothing$.
Θα δείξουμε τώρα ότι η ανάλυση είναι μονοσήμαντη. Υποθέτουμε αντίθετα ότι υπάρχουν πρώτα ιδεώδη $P_1, \dots, P_r, Q_1, \dots, Q_s$ τέτοια ώστε

$$A = P_1 \dots P_r = Q_1 \dots Q_s$$

Έστω ότι $P_1 \neq Q_j$, για κάθε $j = 1, \dots, s$. Τότε μπορούμε να διαλέξουμε στοιχεία $q_j \in Q_j$ τέτοια ώστε $q_j \notin P_1$. Οπότε

$$\prod_{j=1}^{s} q_j \in \prod_{j=1}^{s} Q_j = A \subset P_1$$

διότι $P_1|A$. Αυτό όμως είναι άτοπο γιατί το P_1 είναι πρώτο άρα

$$a\beta \in P_1 \Rightarrow a \in P_1 \text{ ή } \beta \in P_1$$

Επομένως θα ισχύει ότι το P_1 είναι ίσο με κάποιο από τα Q_j, δηλαδή

$$P_2 \dots P_r = Q_2 \dots Q_s$$

Συνεχίζοντας με τον ίδιο τρόπο προκύπτει το ζητούμενο. □

2 Αριθμός Κλάσεων Ιδεωδών.

2.1 Αρχικοί Ορισμοί.

Έστω G το σύνολο όλων των ιδεωδών του Κ. Έστω $A, B \in G$. Ορίζουμε σχέση ισοδυναμίας ως εξής: $A \sim B$ αν και μόνον αν $B = \delta A$, όπου $0 \neq \delta \in K$.
Ελέγχουμε ότι είναι πράγματι σχέση ισοδυναμίας:

- ανακλαστική ιδιότητα
  $A \sim A$ γιατί $A = 1 \cdot A$.

- συμμετρική ιδιότητα
  $A \sim B \Leftrightarrow B = \delta A \Leftrightarrow A = \delta^{-1} B \Leftrightarrow B \sim A$

- μεταβατική ιδιότητα
  $A \sim B \Leftrightarrow B = \delta_1 A$
  $B \sim \Gamma \Leftrightarrow \Gamma = \delta_2 B = \delta_2 \delta_1 A \Leftrightarrow A \sim \Gamma$

Επομένως έχουμε πράγματι σχέση ισοδυναμίας. Συμβολίζουμε την κλάση ισοδυναμίας του αντιπροσώπου A με $[A]$ και το σύνολο όλων των κλάσεων ισοδυναμίας της $\sim$ με C.
Ορίζουμε την πράξη $+ : C \times C \to C$ ως εξής $[A] + [B] = [AB]$, για $A, B \in G$. Ελέγχουμε ότι η πράξη αυτή είναι καλά ορισμένη. Πράγματι,

$$[A_1] = [A_2] \Leftrightarrow A_1 \sim A_2 \Leftrightarrow A_2 = \delta_1 A_1$$
$$[B_1] = [B_2] \Leftrightarrow B_1 \sim B_2 \Leftrightarrow B_2 = \delta_2 B_1$$

Πολλαπλασιάζουμε κατά μέλη και παίρνουμε ότι

$$A_2 B_2 = \delta_1 \delta_2 A_1 B_1 \Leftrightarrow A_1 B_1 \sim A_2 B_2 \Leftrightarrow [A_1 B_1] = [A_2 B_2]$$

Επομένως η πράξη που ορίσαμε είναι καλά ορισμένη.

Η $(C, +)$ αποτελεί ομάδα. Πράγματι, ικανοποιούνται τα εξής:

- προσεταιριστική ιδιότητα
  $([A]+[B])+[\Gamma] = [AB]+[\Gamma] = [AB\Gamma] = [A]+[B\Gamma] = [A]+([B]+[\Gamma])$

- ουδέτερο στοιχείο
  $[A] + [(1)] = [A(1)] = [A] = [(1)A] = [(1)] + [A]$
  Άρα το $[(1)] = [R]$ είναι το ουδέτερο στοιχείο της $+$.

- αντίθετο στοιχείο
  $[A] + [A^{-1}] = [AA^{-1}] = [R] = [A^{-1}A] = [A^{-1}] + [A]$
  Άρα το $[A^{-1}]$ είναι το αντίθετο στοιχείο του $[A]$.

Ορισμός 2.1.1. Η $(C, +)$ καλείται ομάδα κλάσεων ιδεωδών του Κ.

Ορισμός 2.1.2. Ο πληθικός αριθμός της $(C, +)$ ονομάζεται αριθμός κλάσεων ιδεωδών της Κ και συμβολίζεται με $|C|$.

Πρόταση 2.1.3. Για κάθε φυσικό αριθμό $s > 0$ υπάρχουν πεπερασμένου πλήθους ακέραια ιδεώδη ενός αλγεβρικού σώματος αριθμών Κ που έχουν νόρμα το s.

Απόδειξη. Έστω A ένα ακέραιο ιδεώδες με $N_K(A) = s$. Τότε από την Πρόταση 1.4.10, $N_K(A) \in A$, δηλαδή $s \in A \Rightarrow (s) \subset A \Rightarrow A|(s)$. Το πλήθος των ακέραιων ιδεωδών που διαιρούν το (s) είναι πεπερασμένο όπως προκύπτει από τη μονοσήμαντη ανάλυση ιδεωδών σε γινόμενο πρώτων ιδεωδών. Άρα υπάρχουν πεπερασμένου πλήθους ακέραια ιδεώδη A του Κ με $N_K(A) = s$. □

Πρόταση 2.1.4. Για κάθε αλγεβρικό σώμα αριθμών Κ, υπάρχει ένας θετικός αριθμός m, τέτοιος ώστε για κάθε ακέραιο ιδεώδες A του Κ να υπάρχει ένα στοιχείο $a \neq 0$ του A για το οποίο να ισχύει $|N_K(a)| \leq N_K(A)m$.

Απόδειξη. Έστω $w_1, \ldots, w_n$ μια βάση ακεραιότητας του Κ και s ένας φυσικός αριθμός επιλεγμένος έτσι ώστε $s^n \leq N_K(A) < (s+1)^n$.
Θεωρούμε το σύνολο Ω= $\{x_1w_1 + \cdots + x_nw_n : 0 \leq x_i \leq s\}$. Ο αριθμός των στοιχείων του Ω είναι $(s+1)^n$, δηλαδή μεγαλύτερος της $N_K(A)$. Άρα υπάρχουν δύο στοιχεία στο Ω που ανήκουν στην ίδια κλάση ισοδυναμίας $moduloA$, έστω $\beta, \gamma \in$Ω.
Τότε $\beta \equiv \gamma \mod A \Leftrightarrow \beta - \gamma \in A$, δηλαδή $\beta - \gamma = a \in A$. Έστω $a = a_1w_1 + \cdots + a_nw_n$, $a_i \in \mathbb{Z}$. Ισχύει $|a_i| \leq s$ και

$$\begin{aligned} |N_K(a)| &= \left| \prod_{i=1}^{n} \sum_{j=1}^{n} a_j w_j^{(i)} \right| = \prod_{i=1}^{n} \left| \sum_{j=1}^{n} a_j w_j^{(i)} \right| \leq \prod_{i=1}^{n} s \sum_{j=1}^{n} |w_j^{(i)}| \\ &= s^n \prod_{i=1}^{n} \sum_{j=1}^{n} |w_j^{(i)}| \leq N_K(A)m \end{aligned}$$

όπου $m = \prod_{i=1}^{n} \sum_{j=1}^{n} |w_j^{(i)}|$. □

Στη συνέχεια θα χρησιμοποιήσουμε το παρακάτω αποτέλεσμα:

Θεώρημα 2.1.5. Όλες οι βάσεις ενός ακέραιου ιδεώδους αλγεβρικού σώματος αριθμών έχουν ίσες διακρίνουσες.

Απόδειξη. Βλέπε [1], Θεώρημα 11.4, σελίδα 200. □

Πρόταση 2.1.6. Αν $w_1, \ldots, w_n$ είναι μια βάση ακεραιότητας του αλγεβρικού σώματος αριθμών K, τότε κάθε ακέραιο ιδεώδες A του K έχει μια κάτω τριγωνική βάση της μορφής:

$$\begin{aligned} a_1 &= a_{11}w_1 \\ a_2 &= a_{21}w_1 + a_{22}w_2 \\ \vdots &\quad \vdots \quad\quad \vdots \\ a_n &= a_{n1}w_1 + a_{n2} + \cdots + a_{nn} \end{aligned}$$

όπου a_{ij} θετικοί ακέραιοι.

Απόδειξη. Για κάθε $i = 1, \ldots, n$ θεωρούμε τους αριθμούς του A της μορφής

$$x_1w_1 + \cdots + x_nw_n$$

όπου x_i ακέραιοι διάφοροι του μηδενός. Από τους αριθμούς αυτούς επιλέγουμε τους

$$a_i = a_{i1}w_1 + \cdots + a_{ii}w_i$$

όπου ο a_{ii} είναι ο ελάχιστος κατά απόλυτη τιμή συντελεστής του w_i. Θα δείξουμε ότι οι $a_1, \ldots, a_n$ είναι βάση του A.
Βλέπουμε αρχικά ότι οι αριθμοί αυτοί είναι γραμμικά ανεξάρτητοι καθώς:

$$\begin{aligned} d(a_1, \ldots, a_n) &= \begin{vmatrix} a_{11} & 0 & 0 & \ldots & 0 \\ a_{21} & a_{22} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \ldots & a_{nn} \end{vmatrix}^2 d(w_1, \ldots, w_n) \\ &= (\prod_{i=1}^{n} a_{ii})^2 d(w_1, \ldots, w_n) \neq 0 \end{aligned}$$

Έστω

$$a = b_1w_1 + \cdots + b_nw_n$$

ένα στοιχείο του A. Έστω επίσης

$$b_1 = a_{nn}q_n + r_n \text{ με } 0 \leq r_n < a_{nn}$$

Ο αριθμός

$$a - q_n a_n = a - q_n(a_{n1}w_1 + \cdots + a_{nn}w_n) = b'_1 w_1 + \cdots + b'_{n-1}w_{n-1} + r_n w_n$$

ανήκει στο Α ως διαφορά στοιχείων του Α και είναι της μορφής των στοιχείων που θεωρήσαμε. Καθώς έχουμε ότι $|r_n| < a_{nn}$ και λόγω της επιλογής του a_{nn} θα πρέπει να ισχύει $r_n = 0$. Άρα

$$a - q_n a_n = b'_1 w_1 + \cdots + b'_{n-1}w_{n-1}$$

Συνεχίζοντας να αφαιρούμε στοιχεία

$$a - q_n a_n - q_{n-1}a_{n-1} = b''_1 w_1 + \cdots + b''_{n-2}w_{n-2} + r_{n-1}w_{n-1}$$

προκύπτει $r_{n-1} = 0$.
Τελικά

$$a - q_n a_n - \cdots - q_1 a_1 = 0 \Rightarrow a = q_1 a_1 + \cdots + q_n a_n$$

Δηλαδή τα στοιχεία του Α παράγονται από τα $a_1, \ldots, a_n$. Επομένως τα $a_1, \ldots, a_n$ είναι βάση του ιδεώδους Α. □

Πρόταση 2.1.7. Αν $w_1, \ldots, w_n$ είναι μια βάση ακεραιότητας του αλγεβρικού σώματος αριθμών Κ και $a_1, \ldots, a_n$ κάτω τριγωνική βάση του ιδεώδους Α, τότε:

$$d(a_1, \ldots, a_n) = N_K(A)^2 d(w_1, \ldots, w_n)$$

Απόδειξη. Όπως δείξαμε στην προηγούμενη απόδειξη

$$d(a_1, \ldots, a_n) = (\prod_{i=1}^{n} a_{ii})^2 d(w_1, \ldots, w_n)$$

Επομένως αρκεί να δείξουμε ότι $N_K(A) = \prod_{i=1}^{n} a_{ii}$. Θεωρούμε το σύνολο των αριθμών της μορφής $\sum_{i=1}^{n} r_i w_i$, όπου $r_i \in \mathbb{Z}$ και $0 \leq r_i < a_{ii}$. Το πλήθος των αριθμών αυτών είναι $\prod_{i=1}^{n} a_{ii}$. Αρκεί να δείξουμε ότι οι αριθμοί αυτοί αποτελούν ένα πλήρες σύστημα αντιπροσώπων των κλάσεων moduloA.
Έστω $\sum_{i=1}^{n} r_i w_i, \sum_{i=1}^{n} r'_i w_i$ δύο τέτοιοι αριθμοί.

$$\sum_{i=1}^{n} r_i w_i \equiv \sum_{i=1}^{n} r'_i w_i \mod A \Leftrightarrow \sum_{i=1}^{n} (r_i - r'_i) w_i \equiv 0 \mod A \Leftrightarrow$$

$$\sum_{i=1}^{n-1}(r_i-r_i')w_i+(r_n-r_n')w_n \equiv 0 \mod A \Leftrightarrow \pm\sum_{i=1}^{n-1}(r_i-r_i')w_i+|r_n-r_n'|w_n \equiv 0 \mod A$$

Καθώς $0 \leq r_i < a_{ii}$ έχουμε ότι $|r_n - r_n'| < a_{nn}$. Όμως ο a_{nn} είναι ο ελάχιστος κατά απόλυτη τιμή μη μηδενικός συντελεστής του w_n. Άρα πρέπει

$$|r_n - r_n'| = 0 \Rightarrow r_n = r_n'$$

Συνεχίζοντας με τον ίδιο τρόπο προκύπτει $r_i = r_i'$ για κάθε $i = 1, \ldots, n$. Άρα τελικά

$$\sum_{i=1}^{n} r_i w_i \equiv \sum_{i=1}^{n} r_i' w_i \mod A \Leftrightarrow \sum_{i=1}^{n} r_i w_i = \sum_{i=1}^{n} r_i' w_i$$

Δηλαδή οι δύο αριθμοί ανήκουν στην ίδια κλάση moduloA αν και μόνον αν ταυτίζονται.
Θα δείξουμε τώρα ότι κάθε αριθμός του R είναι ισοδύναμος moduloA με έναν $\sum_{i=1}^{n} r_i w_i$. Έστω

$$a = x_1 w_1 + \cdots + x_n w_n$$

όπου $x_i \in \mathbb{Z}$. Έστω επίσης

$$x_n = a_{nn} q_n + r_n, \text{ με } 0 \leq r_i < a_{ii}$$

Τότε

$$a - q_n a_n = x_1' w_1 + \cdots + x_{n-1}' w_{n-1} + r_n w_n$$

και συνεχίζοντας να αφαιρούμε $q_i a_i$ κατά τον ίδιο τρόπο προκύπτει

$$a - q_n a_n - \cdots - q_1 a_1 = r_1 w_1 + \cdots + r_n w_n$$

Δηλαδή

$$a - \sum_{i=1}^{n} r_i w_i = \sum_{i=1}^{n} q_i a_i \in A \Rightarrow a \equiv \sum_{i=1}^{n} r_i w_i \mod A$$

Επομένως έχουμε ένα πλήρες σύστημα αντιπροσώπων κλάσεων moduloA και $N_K(A) = \prod_{i=1}^{n} a_{ii}$. □

Πόρισμα 2.1.8. Αν $w_1, \ldots, w_n$ είναι μια βάση ακεραιότητας του K και $a_1, \ldots, a_n$ μια βάση του ακέραιου ιδεώδους A, τότε

$$d(a_1, \ldots, a_n) = N_K(A)^2 d(w_1, \ldots, w_n)$$

Απόδειξη. Το πόρισμα προκύπτει από την Πρόταση 2.1.6. δεδομένου ότι όλες οι βάσεις ενός ιδεώδους έχουν ίσες διακρίνουσες. □

Πρόταση 2.1.9. Έστω $a \in$ K. Τότε ισχύει $N_K(aR) = |N_K(a)|$.

Απόδειξη. Αν $a = a^{(1)}, a^{(2)}, \ldots, a^{(n)}$ είναι οι συζυγείς αριθμοί του a, τότε ισχύει $N_K(a) = \prod_{i=1}^{n} a^{(i)}$. Έστω $w_1, \ldots, w_n$ μια βάση ακεραιότητας του K. Τότε οι αριθμοί $aw_1, \ldots, aw_n$ αποτελούν βάση του aR. Άρα από το Πόρισμα 2.1.8.

$$d(aw_1, \ldots, aw_n) = N_K(aR)^2 d(w_1, \ldots, w_n)$$

Όμως

$$\begin{aligned} d(aw_1, \ldots, aw_n) &= \begin{vmatrix} a^{(1)}w_1^{(1)} & \ldots & a^{(1)}w_n^{(1)} \\ \vdots & \ddots & \vdots \\ a^{(n)}w_1^{(n)} & \ldots & a^{(n)}w_n^{(n)} \end{vmatrix}^2 \\ &= \left(\prod_{i=1}^{n} a^{(i)}\right)^2 \begin{vmatrix} w_1^{(1)} & \ldots & w_n^{(1)} \\ \vdots & \ddots & \vdots \\ w_1^{(n)} & \ldots & w_n^{(n)} \end{vmatrix}^2 \\ &= (N_K(a))^2 d(w_1, \ldots, w_n) \end{aligned}$$

Συγκρίνοντας τις δύο σχέσεις προκύπτει

$$N_K(aR)^2 = N_K(a)^2 \Rightarrow N_K(aR) = |N_K(a)|$$

□

Θεώρημα 2.1.10. Ο αριθμός κλάσεων ιδεωδών ενός αλγεβρικού σώματος αριθμών K είναι πεπερασμένος.

Απόδειξη. Θεωρούμε τον αριθμό m της Πρότασης 2.1.4. Σύμφωνα με την Πρόταση 2.1.3. υπάρχουν πεπερασμένου πλήθους ιδεώδη $A_1, \ldots, A_r$ τέτοια ώστε $N_K(A_i) \leq m$. Θα αποδείξουμε ότι κάθε ιδεώδες του K είναι ισοδύναμο με ένα από τα A_i οπότε ο αριθμός κλάσεων ιδεωδών θα είναι μικρότερος ή ίσος του r.
Έστω A κλασματικό ιδεώδες του K. Υπάρχει $\delta \in K$ τέτοιο ώστε $\delta A = B \subset R$. Συνεπώς $A \sim B$ και αρκεί να δείξω ότι κάθε ακέραιο ιδεώδες του K

είναι ισοδύναμο με ένα A_i.
Έστω A ακέραιο ιδεώδες του Κ. Για το $A^{-1} \supsetneq R$ υπάρχει $\delta \in K$ τέτοιο ώστε $\delta A^{-1} = B \subset R$. Σύμφωνα με την Πρόταση 2.1.4. υπάρχει αριθμός $0 \neq \beta \in \delta A^{-1}$ τέτοιος ώστε να ισχύει

$$N_K(\beta R) = |N_K(\beta)| \leq N_K(\delta A^{-1})m$$

Το ιδεώδες $\beta\delta^{-1}A$ είναι ακέραιο γιατί $\beta\delta^{-1} \in A^{-1}$. Συνεπώς

$$\begin{aligned} N_K(\beta\delta^{-1}A)N_K(\delta R) &= N_K(\beta A) = N_K(A)N_K(\beta R) \\ &\leq N_K(A)N_K(\delta A^{-1})m = N_K(\delta R)m \end{aligned}$$

Δηλαδή $N_K(\beta\delta^{-1}A) \leq m$, άρα υπάρχει A_i τέτοιο ώστε να ισχύει

$$\beta\delta^{-1}A = A_i \Rightarrow A \sim A_i.$$

□

2.2 Αριθμός Κλάσεων Ιδεωδών 1.

Θα δείξουμε τώρα τι σημαίνει για ένα αλγεβρικό σώμα αριθμών Κ να έχει αριθμό κλάσεων ιδεωδών ίσο με 1.
Ένα στοιχείο $\pi \in R$ θα καλείται πρώτο ή ανάγωγο, αν είναι μη μηδενικό, μη αντιστρέψιμο και δεν αναλύεται σε γινόμενο $\pi = \alpha\beta$, όπου $\alpha,\beta \in R$ μη αντιστρέψιμα.

Πρόταση 2.2.1. Αν ο δακτύλιος R των ακέραιων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών Κ είναι περιοχή κυρίων ιδεωδών ή δακτύλιος με μονοσήμαντη ανάλυση, τότε για κάθε πρώτο αριθμό π του R το ιδεώδες $(\pi) = \pi R$ είναι πρώτο.

Απόδειξη. Έστω ότι ο R είναι περιοχή κυρίων ιδεωδών και έστω $\pi \in R$ πρώτος αριθμός του R. Υποθέτουμε ότι το ιδεώδες (π) δεν είναι πρώτο. Τότε έστω

$$(\pi) = P_1 \dots P_s$$

μια ανάλυση του (π) σε γινόμενο πρώτων ιδεωδών. Καθώς R περιοχή κυρίων ιδεωδών, ισχύει $P_i = (\pi_i)$, οπότε

$$(\pi) = (\pi_1) \dots (\pi_s) \Rightarrow \pi = \rho\pi_1 \dots \pi_s$$

με $\rho \in R$ μη αντιστρέψιμο. Αυτό είναι άτοπο γιατί υποθέσαμε ότι π πρώτος. Άρα το ιδεώδες (π) είναι πρώτο.
Έστω τώρα ότι ο R είναι δακτύλιος μονοσήμαντης ανάλυσης. Θεωρούμε π έναν πρώτο αριθμό και (π) το κύριο ιδεώδες που παράγεται από αυτόν. Έστω $a\beta \in (\pi)$. Τότε

$$a\beta = \rho\pi$$

Συνεπώς λόγω μονοσήμαντης ανάλυσης θα πρέπει

$$\pi | a \text{ ή } \pi | \beta$$

Άρα $a \in (\pi)$ ή $\beta \in (\pi)$. Επομένως το (π) είναι πρώτο ιδεώδες. □

Θεώρημα 2.2.2. Ο δακτύλιος R των ακέραιων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών Κ είναι δακτύλιος με μονοσήμαντη ανάλυση, αν και μόνο αν ο R είναι περιοχή κυρίων ιδεωδών ή ισοδύναμα, αν και μόνον αν ο αριθμός των κλάσεων ιδεωδών είναι ίσος με 1.

Απόδειξη. Θα δείξουμε πρώτα ότι ο R είναι δακτύλιος με μονοσήμαντη ανάλυση αν και μόνον αν είναι περιοχή κυρίων ιδεωδών.
Έστω λοιπόν ότι ο R είναι δακτύλιος με μονοσήμαντη ανάλυση. Ισχύει

ότι $R = (1)$ και (1) κύριο ιδεώδες. Λόγω της μονοσήμαντης ανάλυσης ιδεωδών σε γινόμενο πρώτων ιδεωδών, αρκεί να δείξουμε ότι κάθε πρώτο ιδεώδες P είναι κύριο. Τότε κάθε ιδεώδες του R θα γράφεται ως γινόμενο κυρίων ιδεωδών, θα είναι επομένως κύριο. Έστω

$$N_K(P) = \pi_1 \dots \pi_s$$

η ανάλυση της $N_K(P)$ σε γινόμενο πρώτων αριθμών. Σύμφωνα με την Πρόταση 1.4.10.

$$N_K(P) \in P \Rightarrow \pi_1 \dots \pi_s \in P \Rightarrow \pi_i \in P$$

για κάποιο $i = 1, \dots, s$, εξ ορισμού των πρώτων ιδεωδών.

$$\pi_i \in P \Rightarrow (\pi_i) \subset P$$

Έχουμε ότι τόσο το (π_i), λόγω της προηγούμενης πρότασης, όσο και το P είναι πρώτα ιδεώδη. Επομένως, σύμφωνα με την Πρόταση 1.5.3. είναι και μέγιστα. Άρα $P = (\pi_i)$, δηλαδή το P είναι κύριο ιδεώδες.
Έστω τώρα ότι ο R είναι δακτύλιος κυρίων ιδεωδών. Θεωρούμε

$$a = \pi_1 \dots \pi_r = \pi'_1 \dots \pi'_s$$

δύο αναλύσεις του $a \in R$ σε γινόμενο πρώτων αριθμών. Τότε

$$(a) = (\pi_1) \dots (\pi_r) = (\pi'_1) \dots (\pi'_s)$$

Σύμφωνα με την προηγούμενη πρόταση τα (π_i) είναι πρώτα ιδεώδη. Επομένως προκύπτει από τη μονοσήμαντη ανάλυση ιδεωδών ότι $r = s$ και τα $\pi_1 \dots \pi_r$ έιναι συντροφικά με τα $\pi'_1 \dots \pi'_r$. Δηλαδή ο R είναι δακτύλιος μονοσήμαντης ανάλυσης.
Θα δείξουμε τώρα ότι ο R είναι περιοχή κυρίων ιδεωδών αν και μόνον αν έχει αριθμό κλάσεων ιδεωδών 1.
Έστω ότι ο R είναι περιοχή κυρίων ιδεωδών. Τότε ο R έχει μόνο μία κλάση ιδεωδών, αυτή των κύριων. Άρα $|C| = 1$.
Έστω $|C| = 1$. Τότε καθώς $(C, +)$ ομάδα, θα πρέπει να περιέχει το ουδέτερο στοιχείο της, που είναι το $[(1)]$. Συνεπώς όλα τα ιδεώδη είναι ισοδύναμα με το (1), είναι δηλαδή κύρια. □

2.3 Αριθμός Κλάσεων Ιδεωδών 2.

Σε αυτό το τελευταίο κομμάτι της εργασίας θα εξετάσουμε τι συμβαίνει όταν ο αριθμός κλάσεων ιδεωδών ενός δακτυλίου ακέραιων αλγεβρικών αριθμών είναι 2. Πιο συγκεκριμένα θα παρουσιάσουμε το κεντρικό θεώρημα της εργασίας του Καθηγητή Scott T. Chapman, So what is Class Number 2? Αυτό είναι το Θεώρημα του Carlitz.

Πρόταση 2.3.1. Έστω R δακτύλιος αλγεβρικών αριθμών του Κ με $\mid C \mid = 2$. Αν το $\alpha \in R$ είναι ανάγωγο, τότε ισχύει ένα από τα παρακάτω:

- $(\alpha) = P$, P πρώτο, κύριο.
- $(\alpha) = P^2$, P πρώτο, μη κύριο.
- $(\alpha) = PQ$, P, Q πρώτα, μη κύρια, διαφορετικά μεταξύ τους.

Απόδειξη. Έχουμε ότι $\mid C \mid = 2$. Άρα $C = \{[R], [A]\}$, όπου Α μη κύριο ιδεώδες του Κ.
Έστω ανάγωγο $\alpha \in R$. Το ιδεώδες $(\alpha) \subset R$ είναι κύριο οπότε $[(\alpha)] = [R]$. Θεωρούμε $(\alpha) = P_1 \dots P_n$ τη μονοσήμαντη ανάλυση του (α) σε γινόμενο πρώτων ιδεωδών. Για καθένα από τα πρώτα P_i ισχύει ότι αν P_i είναι κύριο, τότε $P_i \in [R]$. Διαφορετικά $P_i \in [A]$.
Έστω ότι υπάρχει κύριο P_i στην ανάλυση του (α). Δίχως βλάβη της γενικότητας υποθέτουμε ότι αυτό είναι το P_1. Τότε $[P_1] = [R]$ και υπάρχει μη αντιστρέψιμο $x \in R$ τέτοιο ώστε $P_1 = (x)$. Θα δείξουμε ότι $n = 1$. Έστω $n > 1$. Τότε,

$$[R] = [(\alpha)] = [P_1 \dots P_n] = [P_1] + [P_2 \dots P_n] = [R] + [P_2 \dots P_n].$$

Προκύπτει, δηλαδή,

$$[P_2 \dots P_n] = [R].$$

Επειδή $P_2 \dots P_n \neq R$, υπάρχει μη αντιστρέψιμο $y \in R$ τέτοιο ώστε

$$(y) = P_2 \dots P_n.$$

Τότε όμως

$$(\alpha) = (x)(y) \Rightarrow \alpha = \rho xy,$$

όπου $\rho \in R$ αντιστρέψιμο. Αυτό όμως είναι άτοπο γιατί υποθέσαμε ότι α ανάγωγο. Άρα $n = 1$ και $(\alpha) = P_1$, με P_1 πρώτο, κύριο ιδεώδες.
Έστω ότι κανένα από τα P_i δεν είναι κύριο. Τότε $\forall i, P_i \in [A]$, δηλαδή $[P_i] = [A]$ και $\mid [P_i] \mid = 2$. Θα δείξουμε ότι $n = 2$ δηλαδή $(\alpha) = P_1 P_2$.
Ισχύει ότι για κάθε i, j,

$$[P_i P_j] = [P_i] + [P_j] = [A] + [A] = [R],$$

διότι $\mid [A] \mid = 2$. Επειδή $P_iP_j \neq R$, υπάρχει μη αντιστρέψιμο $x \in R$, τέτοιο ώστε $(x) = P_iP_j$. Από τη σχέση

$$[R] = [(\alpha)] = [P_1 \dots P_n] = [P_1] + \cdots + [P_n]$$

προκύπτει ότι ο n πρέπει να είναι άρτιος. Έστω ότι $n > 2$. Τότε

$$[R] = [(\alpha)] = [P_1P_2] + [P_3 \dots P_n] \Rightarrow [P_3 \dots P_n] = [R].$$

Καθώς $P_3 \dots P_n \neq R$, υπάρχει μη αντιστρέψιμο $y \in R$ τέτοιο ώστε

$$(y) = P_3 \dots P_n$$

Τότε όμως

$$(\alpha) = (x)(y) \Rightarrow \alpha = \rho xy,$$

το οποίο είναι άτοπο γιατί υποθέσαμε ότι α ανάγωγο. Άρα $n = 2$, δηλαδή $(\alpha) = P_1P_2$, όπου P_1, P_2 πρώτα, μη κύρια ιδεώδη. Για τα P_1, P_2 υπάρχουν δύο δυνατότητες:

- $P_1 = P_2$, οπότε $(\alpha) = P_1^2$
- $P_1 \neq P_2$ οπότε $(\alpha) = P_1P_2$

□

Γενικότερα ισχύει η παρακάτω πρόταση:

Πρόταση 2.3.2. Έστω R δακτύλιος ακέραιων αλγεβρικών αριθμών και x μη μηδενικό, μη αντιστρέψιμο στοιχείο του R. Έστω επίσης ότι

$$(x) = P_1 \dots P_n$$

όπου $n \geq 1$ και τα P_i είναι πρώτα ιδεώδη, όχι απαραίτητα διαφορετικά μεταξύ τους. Το στοιχείο x είναι ανάγωγο στον R αν και μόνον αν:

1. $\sum_{i=1}^{n} [P_i] = [R]$
2. αν $\varnothing \neq S \subsetneq \{1, \dots, n\}$ τότε $\sum_{i \in S} [P_i] \neq [R]$

Απόδειξη. Έστω ότι το x είναι ανάγωγο στον R. Τότε

$$\sum_{i=1}^{n} [P_i] = [P_1] + \cdots + [P_n] = [P_1 \dots P_n] = [(x)] = [R].$$

Έστω ότι υπάρχει $\varnothing \neq S \subsetneq \{1, \ldots, n\}$ τέτοιο ώστε $\sum_{i \in S} [P_i] = [R]$. Τότε για το $S' = \{1, \ldots, n\} - S$ ισχύει

$$\sum_{i=1}^{n} [P_i] = \sum_{i \in S} [P_i] + \sum_{i \in S'} [P_i] \Rightarrow \sum_{i \in S'} [P_i] = [R]$$

Άρα υπάρχουν $y, z \in R$ όχι μονάδες τέτοια ώστε

$$(y) = \prod_{i \in S} P_i \text{ και } (z) = \prod_{i \in S'} P_i$$

Τότε όμως

$$(x) = (y)(z) \Rightarrow x = \rho yz$$

με ρ αντιστρέψιμο στοιχείο του R. Αυτό όμως είναι άτοπο γιατί υποθέσαμε ότι το x είναι ανάγωγο.
Έστω τώρα ότι ισχύουν οι προϋποθέσεις της πρότασης. Υποθέτουμε ότι το x δεν είναι ανάγωγο, δηλαδή $x = yz$. Θα υπάρχουν τότε $S, S' \subsetneq \{1, \ldots, n\}$ τέτοια ώστε

$$(y) = \prod_{i \in S} P_i \text{ και } (z) = \prod_{i \in S'} P_i$$

Τότε όμως

$$\sum_{i \in S} [P_i] = [(y)] = [R]$$

το οποίο είναι άτοπο καθώς υποθέσαμε ότι ισχύει η 2. □

Πρόταση 2.3.3. Έστω R δακτύλιος ακέραιων αλγεβρικών αριθμών με αριθμό κλάσεων ιδεωδών μεγαλύτερο του 2. Τότε υπάρχουν ανάγωγα στοιχεία του $a_1, a_2, \beta_1, \beta_2, \beta_3$ όχι απαραίτητα διαφορετικά μεταξύ τους τέτοια ώστε

$$a_1 a_2 = \beta_1 \beta_2 \beta_3$$

Απόδειξη. Έστω ότι η $(C, +)$ περιέχει ένα στοιχείο $[P]$ με $|[P]| = n > 2$. Τότε επιλέγουμε:

- P_1 πρώτο ιδεώδες της $[P]$
- P_2 πρώτο ιδεώδες της $2[P]$
- P_3 πρώτο ιδεώδες της $(n-2)[P]$
- P_4 πρώτο ιδεώδες της $(n-1)[P]$

Δημιουργούμε στη συνέχεια τα ιδεώδη:

- $(a) = P_1P_4$
- $(\beta) = P_1^2P_3$
- $(\gamma) = P_2P_3$
- $(\delta) = P_2P_4^2$

Τα a, β, γ, δ είναι ανάγωγα σύμφωνα με την Πρόταση 2.3.2. Επιπλέον

$$(P_1^2P_3)(P_4^2P_2) = (P_1P_4)^2(P_2P_3) \Rightarrow (\beta\delta) = (a)^2(\gamma) \Rightarrow \beta\delta = \rho a^2\gamma$$

όπου ρ αντιστρέψιμο στοιχείο του R.
Έστω τώρα ότι όλα τα μη ταυτοτικά στοιχεία του $(C, +)$ έχουν τάξη 2. Τότε έστω $[Q_1], [Q_2] \in C$ με $[Q_1] \neq [Q_2]$. Θεωρούμε ακόμα $[Q_3] = [Q_1] + [Q_2]$. Έστω P_1, P_2, P_3 πρώτα ιδεώδη επιλεγμένα από τις $[Q_1], [Q_2], [Q_3]$ αντίστοιχα. Τότε λόγω της Πρότασης 2.3.2.

$$P_1^2 = (\beta_1), P_2^2 = (\beta_2), P_3^2 = (\beta_3) \text{ και } P_1P_2P_3 = (a)$$

με $\beta_1, \beta_2, \beta_3, a$ ανάγωγα στοιχεία του R. Τότε έχουμε $a^2 = \rho\beta_1\beta_2\beta_3$, όπου ρ αντιστρέψιμο στοιχείο του R.
Αποδεικνύεται λοιπόν το ζητούμενο. □

Θεώρημα 2.3.4. (Carlitz) Έστω R δακτύλιος ακέραιων αλγεβρικών αριθμών. Ο R έχει αριθμό κλάσεων ιδεωδών το πολύ 2, αν και μόνον αν όποτε $a_1, \ldots, a_n$, $\beta_1, \ldots, \beta_m$ είναι ανάγωγα στοιχεία του R με

$$a_1 \ldots a_n = \beta_1 \ldots \beta_m$$

τότε $n = m$.

Απόδειξη. Η αντίστροφη κατεύθυνση φαίνεται εύκολα από την προηγούμενη πρόταση.
Για την άλλη κατεύθυνση θεωρούμε $x = \alpha_1 \ldots \alpha_n = \beta_1 \ldots \beta_m \in R$. Τότε

$$(x) = (\alpha_1) \ldots (\alpha_n) = (\beta_1) \ldots (\beta_m).$$

Από την Πρόταση 2.3.1. προκύπτει ότι n_1 από τα (α_i) και m_1 από τα (β_j) είναι πρώτα και κύρια, ενώ τα υπόλοιπα, έστω n_2 και m_2 αντίστοιχα, είναι γινόμενα δύο πρώτων, μη κύριων, όχι απαραίτητα διαφορετικών ιδεωδών. Έστω η μονοσήμαντη ανάλυση

$$(x) = Q_1 \ldots Q_s P_1 \ldots P_t,$$

όπου τα πρώτα ιδεώδη Q_i είναι κύρια ενώ τα P_i όχι. Τότε θα πρέπει $s = n_1 = m_1$ και $t = 2n_2 = 2m_2$. Συνεπώς ισχύει ότι $n = m = s + t/2$. □

Αναφορές

[1] Κ.Λάκκης, Θεωρία Αριθμών, 1991

[2] Χ. Χαραλάμπους, Μια εισαγωγή στην Αντιμεταθετική Άλγεβρα (ηλεκτρονικές σημειώσεις)

[3] R. Chapman, Algebraic Number Theory, Summary of Notes, 2005

[4] S. Chapman, So what is Class Number 2?, Amer. Math. Monthly 126(2019), 330-339

[5] J.P.Cook, Computing Integral Bases (ηλεκτρονικές σημειώσεις)

[6] F. Oggier, Introduction to Algebraic Number Theory, Lecture Notes NTU 2010

[7] Stewart, Ian & Tall, David, Algebraic Number Theory and Fermats Last Theorem (3rd edition), A.K. Peters Ltd, Natick, MA,2002