

# Σημειώσεις στην Αλγεβρική Θεωρία Αριθμών

Διαλέξεις Αριστείδη Κοντογεώργη

Επιμέλεια : Βουτσαδάκης Δημήτριος - Μπιζάνος Κωνσταντίνος

13 Μαΐου 2024

## Περιεχόμενα

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Μάθημα 01</b>  | <b>3</b>  |
| 1.1      | Κίνητρο και Εισαγωγή . . . . .                            | 3         |
| 1.2      | Ακέραιοι Αλγεβρικοί Αριθμοί . . . . .                     | 6         |
| <b>2</b> | <b>Μάθημα 02</b>  | <b>8</b>  |
| 2.1      | Τετραγωνικά Σώματα Αριθμών . . . . .                      | 8         |
| 2.2      | Η ομάδα των μονάδων . . . . .                             | 11        |
| <b>3</b> | <b>Μάθημα 03</b>  | <b>13</b> |
| 3.1      | Ιδεώδη Σώματος Κλασμάτων και Δακτύλιοι Dedekind . . . . . | 13        |
| 3.2      | Δακτύλιοι και Πρότυπα της Noether . . . . .               | 15        |
| <b>4</b> | <b>Μάθημα 04</b>  | <b>18</b> |
| 4.1      | Δακτύλιοι Dedekind και Πρώτα - Μέγιστα Ιδεώδη . . . . .   | 18        |
| 4.2      | Ακέραια Εξάρτηση . . . . .                                | 19        |
| <b>5</b> | <b>Μάθημα 05</b>  | <b>23</b> |
| 5.1      | Χαρακτηρισμός Δακτυλίων Dedekind . . . . .                | 23        |
| 5.2      | Διαιρετότητα Ιδεωδών . . . . .                            | 25        |
| 5.3      | Το Θεμελιώδες Θεώρημα . . . . .                           | 27        |
| <b>6</b> | <b>Μάθημα 06</b>  | <b>29</b> |
| 6.1      | Η Συνέχεια της Απόδειξης . . . . .                        | 29        |
| 6.2      | Νόρμα, Βάση Ακεραιότητας και Διακρίνουσα . . . . .        | 30        |
| <b>7</b> | <b>Μάθημα 07</b>  | <b>33</b> |
| 7.1      | Norm, ίχνος και εμφυτεύσεις . . . . .                     | 33        |
| 7.2      | Διακρίνουσα $n$ - άδας . . . . .                          | 36        |

|           |  |           |
|-----------|--|-----------|
| <b>8</b>  | <b>Μάθημα 08</b>   | <b>38</b> |
| 8.1       | Ελεύθερες Αβελιανές Ομάδες Πεπερασμένου Βαθμού . . . . .     | 38        |
| 8.2       | Σύνολα Ακεραίων Αλγεβρικών και Ελεύθερες Αβελιανές . . . . . | 41        |
| <b>9</b>  | <b>Μάθημα 09</b>   | <b>42</b> |
| 9.1       | Βάσεις Ακεραιότητας . . . . .                                | 42        |
| 9.2       | Αλγόριθμος Υπολογισμού Βάσης Ακεραιότητας . . . . .          | 45        |
| <b>10</b> | <b>Μάθημα 10</b>   | <b>46</b> |
| 10.1      | Norm Ιδεώδους Αλγεβρικού Σώματος Αριθμών . . . . .           | 46        |
| 10.2      | Ομάδα Κλάσεων Ιδεωδών . . . . .                              | 51        |
| <b>11</b> | <b>Μάθημα 11</b>   | <b>53</b> |
| 11.1      | Ομάδα Κλάσεων Ιδεωδών . . . . .                              | 53        |
| <b>12</b> | <b>Μάθημα 12</b>   | <b>55</b> |
| <b>13</b> | <b>Μάθημα 13</b>   | <b>55</b> |
| 13.1      | Πρώτο Θεώρημα Ανάλυσης . . . . .                             | 55        |
| 13.2      | Νόμος ανάλυσης σε επεκτάσεις Galois . . . . .                | 58        |
| 13.3      | Τάξεις Σωμάτων . . . . .                                     | 59        |
| <b>14</b> | <b>Μάθημα 14</b>   | <b>61</b> |
| 14.1      | Τάξεις και Οδηγοί Τάξεων . . . . .                           | 61        |
| 14.2      | Δεύτερο Θεώρημα Ανάλυσης . . . . .                           | 63        |
| <b>15</b> | <b>Μάθημα 15</b>   | <b>64</b> |
| 15.1      | Αποδείξη του Δεύτερου Θεωρήματος Ανάλυσης . . . . .          | 64        |

# 1 Μάθημα 01

## 1.1 Κίνητρο και Εισαγωγή

**Κίνητρο 1.** Το κίνητρο για την ανάπτυξη της αλγεβρικής θεωρίας αριθμών ήταν η επίλυση διοφαντικών εξισώσεων της μορφής  $f(x_1, \dots, x_n) = 0$ , όπου  $f(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$  και  $(x_1, \dots, x_n) \in \mathbb{Z}^n$ . Ειδικότερα, η εύρεση ακέραιων λύσεων της διοφαντικής εξίσωσης

$$x^n + y^n = z^n \quad (1)$$

**Παράδειγμα 1.** Θεωρούμε τη διοφαντική εξίσωση  $y^3 = x^2 - 16$  (ελλειπτική καμπύλη) και αναζητούμε τις ακέραιες λύσεις της. Έχουμε ότι  $y^3 = x^2 - 16 = (x - 4)(x + 4)$ . Έστω  $d = (x - 4, x + 4)$  και αφού  $d|x - 4$  και  $d|x + 4$  έχουμε ότι  $d|8$ . Διακρίνουμε περιπτώσεις :

- Υποθέτουμε ότι  $x$  είναι περιττός. Τότε, προκύπτει ότι  $d = 1$ .

**Θεώρημα 1** (Θεώρημα Μονοσήμαντης Ανάλυσης). Αν  $a, b, c$  θετικοί ακέραιοι με  $(b, c) = 1$  και  $a^n = bc$  για κάποιο φυσικό αριθμό  $n > 1$ , τότε υπάρχουν ακέραιοι  $a_1, a_2$  πρώτοι μεταξύ τους ώστε  $a = a_1 a_2$  και  $b = a_1^n$  και  $c = a_2^n$ .

Από το Θεώρημα 1, προκύπτει ότι υπάρχουν  $a, b$  στο  $\mathbb{Z}$  ώστε  $x - 4 = a^3$  και  $x + 4 = b^3$  με  $(a, b) = 1$ . Συνεπώς, έχουμε ότι  $b^3 - a^3 = (b - a) \cdot m = 8$ . Εξετάζοντας περιπτώσεις για το  $b - a$  καταλήγουμε ότι η τελευταία σχέση είναι αδύνατη.

- – Αν  $x$  είναι άρτιος, τότε  $2|x - 4, x + 4$ , συνεπώς  $8|y^3$ . Επομένως,  $8|y^3 + 16 = x^2$  άρα προκύπτει ότι  $4|x$  με  $x = 4x_1$ . Επίσης, από τις παραπάνω σχέσεις έχουμε ότι  $y = 4y_1$ , άρα η αρχική εξίσωση γράφεται ως εξής :  $x_1^2 = 4y_1^3 + 1$ , άρα  $x_1$  είναι περιττός.
- Άρα,  $x_1 = 2m + 1$  και προκύπτει ότι  $m^2 + m = m(m + 1) = y_1^2$ . Από το Θεώρημα 1, έχουμε ότι δύο διαδοχικοί αριθμοί είναι κύβοι και αυτό μπορεί να συμβαίνει αν και μόνο αν  $m \in \{-1, 0\}$ . Συνεπώς, έχουμε ότι οι μοναδικές λύσεις της εξίσωσης είναι οι  $(x, y) = (\pm 4, 0)$ .

**Παράδειγμα 2.** Θεωρούμε την διοφαντική εξίσωση  $y^3 = x^2 + 1$  και αναζητούμε ακέραιες λύσεις της. Στο  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$  έχουμε ότι  $y^3 = (x - i)(x + i)$ . Στο  $\mathbb{Z}[i]$  ορίζεται νόρμα

$$N(a + bi) = a^2 + b^2 = (a - bi)(a + bi)$$

και αφήνεται ως άσκηση ναδειχθεί ότι  $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ , όπου  $E(\mathbb{Z}[i])$  η πολλαπλασιαστική ομάδα αντιστρεψίμων του  $\mathbb{Z}[i]$ . Γενικότερα, σε ένα δακτύλιο με μονάδα, το σύνολο  $R \setminus \{0\}$  δεν είναι ομάδα, όμως το σύνολο  $E(R)$  των αντιστρεψίμων στοιχείων του  $R$  αποκτά δομή ομάδας με τον πολλαπλασιασμό του  $R$ .

**Ορισμός 1.** Έστω  $R$  ακέραια περιοχή. Ένα  $a \in R$  με  $a \neq 0$  θα λέγεται **ανάγωγος** αν οποτεδήποτε  $a = bc$ , για κάποια  $b, c \in R$ , τότε  $b \in E(R)$  ή  $c \in E(R)$ .

**Παράδειγμα 3.** Τα  $-7 = (-1) \cdot 7$  και  $7 = (-1) \cdot (-7)$  στο  $\mathbb{Z}$  είναι ανάγωγα.

**Ορισμός 2.** Έστω  $R$  περιοχή. Ένα  $p \in R$  με  $p \neq 0$  και  $p \notin E(R)$  θα λέγεται **πρώτος** αν οποτεδήποτε  $p|ab$ , τότε  $p|a$  ή  $p|b$ .

**Παράδειγμα 4.** Στο  $\mathbb{Z}$  η έννοια του πρώτου και του ανάγωγου στοιχείου ταυτίζονται.

**Παράδειγμα 5.** Στο  $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$  ορίζουμε νόρμα

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$$

αποδεικνύεται ότι  $E(\mathbb{Z}) = \{\pm 1\}$ . Παρατηρούμε ότι το  $2 \in \mathbb{Z}[\sqrt{-5}]$  είναι ανάγωγος (γιατί ;) παρόλα αυτά δεν είναι πρώτος, αφού  $2|6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$  όμως  $2 \nmid (1 \pm \sqrt{-5})$ .

**Ορισμός 3.** Έστω  $R$  περιοχή. Μια απεικόνιση  $\varphi: R \rightarrow \mathbb{Z}$ , η οποία ικανοποιεί τα εξής :

(α)  $\varphi(a) \leq \varphi(ab)$ , για κάθε  $a, b \in R \setminus \{0\}$

(β) για κάθε  $a, b \in R$  με  $b \neq 0$ , υπάρχουν  $\pi, \nu$  ώστε  $a = b \cdot \pi + \nu$  με  $\nu = 0$  ή  $\varphi(\nu) < \varphi(b)$ .

λέγεται **ευκλείδεια συνάρτηση**. Τότε το ζεύγος  $(R, \varphi)$  λέγεται **ευκλείδεια περιοχή**.

**Παράδειγμα 6.** Τα ακόλουθα ζεύγη ορίζουν ευκλείδειες περιοχές.

(α)  $(\mathbb{Z}[i], \varphi)$  με  $\varphi(a + bi) = a^2 + b^2$ .

(β)  $(\mathbb{Z}[\sqrt{-2}], \varphi)$  με  $\varphi(a + b\sqrt{-2}) = a^2 + 2b^2$

(γ) Έστω  $k$  σώμα. Τότε, το ζεύγος  $(k[x], \varphi)$ , όπου

$$\varphi(f(x)) = \begin{cases} \deg f, & \text{αν } f(x) \neq 0 \\ -1, & \text{αν } f(x) = 0 \end{cases}$$

**Παρατήρηση 1.** Σε πλήρη αντιστοιχεία με την περίπτωση των ακεραίων αριθμών, μπορεί να αποδειχθεί ότι σε κάθε ευκλείδεια περιοχή, η έννοια αναγωγού και πρώτου στοιχείου ταυτίζονται.

**Παρατήρηση 2.** Επειδή κάθε ευκλείδεια περιοχή είναι και περιοχή μοναδικής παραγοντοποίησης σε συνδυασμό με την ύπαρξη 'ευκλείδειας διαίρεσης', κληρονομούνται από τους ακέραιους αριθμούς, με φυσιολογικό τρόπο, έννοιες όπως ο μέγιστος κοινός διαιρέτης.

Συνεχίζοντας στο Παράδειγμα 2 ως προσπαθήσουμε να επιλύσουμε την διοφαντική εξίσωση  $y^3 = x^2 + 1 = (x - i)(x + i)$ . Παρατηρούμε ότι ο  $d = \mu.κ.δ.(x - i, x + i)$  πρέπει να ικανοποιεί ότι  $d|2$  (γιατί ;).

**Ορισμός 4.** Έστω  $R$  δακτύλιος και  $a, b \in R$ . Τα  $a, b$  θα λέγονται **ισοδύναμα** (ή **συντροφικά**) αν  $a = ub$ , για κάποιο  $u \in E(R)$ . Στην περίπτωση αυτή συμβολίζουμε με  $a \cong b$ .

- Θα δείξουμε ότι  $d \cong 1$ . Πράγματι, αν  $d \not\cong 1$ , τότε  $d \cong 2$  (με επιχείρημα νορμών) και τότε  $d \cong 2 = (1 + i)^2 i$ . Όμως,  $1 + i$  είναι ανάγωγο στο  $\mathbb{Z}[i]$ , συνεπώς  $1 + i|d$ , άρα  $1 + i|x - i$ . Παιρνώντας σε νόρμες προκύπτει ότι  $2|x^2 + 1 = y^3$ , άρα  $2|y^3$ , συνεπώς  $8|y^3 = x^2 + 1$ . Επομένως,  $x^2 \equiv -1 \pmod{8}$ , όπου καταλήγουμε σε άτοπο (γιατί ;).
- Παρατηρήστε ότι  $E(\mathbb{Z}[i]) = \langle i \rangle$  κυκλική τάξης 4. Από τη μονοσήμαντη ανάλυση έχουμε ότι  $x + i = e\zeta^3$  όπου  $e \in E(R)$ . Αφού η απεικόνιση  $E(\mathbb{Z}[i]) \rightarrow E(\mathbb{Z}[i])$  με  $a \mapsto a^3$  είναι αυτομορφισμός ομάδων, μπορούμε να γράψουμε το  $e$  ως  $e = e_1^3$  και άρα

$$x + i = (e_1\zeta)^3 = h^3 = (a + bi)^3$$

για κάποια  $a, b \in \mathbb{Z}$ . Εξισώνοντας πραγματικά και φανταστικά μέρη συμπεραίνουμε ότι η λύση της αρχικής εξίσωσης είναι  $(x, y) = (0, 1)$ .

**Παράδειγμα 7.** Θεωρούμε την διοφαντική εξίσωση  $2y^3 = x^2 + 5$ . Αν αναχθούμε στο  $\mathbb{Z}[\sqrt{-5}]$  παρατηρούμε ότι  $2y^3 = x^2 + 5 = (x + \sqrt{-5})(x - \sqrt{-5})$ . Αφήνεται ως άσκηση να δειχθεί ότι το 2 είναι ανάγωγο στοιχείο στο  $\mathbb{Z}[\sqrt{-5}]$ .

"Συνεπώς" (;), κοιτώντας την τελευταία εξίσωση προκύπτει ότι  $2|(x + \sqrt{-5})$  ή  $2|(x - \sqrt{-5})$ . Άρα,

$$\frac{x + \sqrt{-5}}{2} = \frac{x}{2} + \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

ή

$$\frac{x - \sqrt{-5}}{2} = \frac{x}{2} - \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

και προφανώς καταλήγουμε σε άτοπο. Παρόλα αυτά παρατηρούμε ότι τα  $(x, y) = (\pm 7, 3)$  αποτελούν λύσεις της εξίσωσης. Ποιο ακριβώς ήταν το λάθος στο συλλογισμό μας ; Το λάθος μας βρίσκεται στο "Συνεπώς" όπου υποθέσαμε λανθασμένα ότι αφού το 2 είναι ανάγωγο, τότε το 2 πρέπει να είναι και πρώτο!

- Επιστρέφοντας στο αρχικό πρόβλημα της Εικασίας του Fermat, είναι σχετικά εύκολο να δούμε ότι για να βρούμε τις λύσεις της εξίσωσης  $x^n + y^n = z^n$  για τυχαίο  $n \geq 1$ , αρκεί να τις βρούμε για κάποιον  $p$  πρώτο.
- Η εξίσωση  $t^p - 1 = 0$  έχει ρίζες τις  $\zeta_p^i$  δηλαδή :

$$t^p - 1 = (t - 1)(t - \zeta_p) \cdots (t - \zeta_p^{p-1})$$

Τότε μπορούμε να γράψουμε

$$z^p = x^p + y^p = \prod_{n=0}^{p-1} (x + \zeta_p^n y)$$

Κάνοντας τη παρανόηση (όπως πριν) ότι στον  $\mathbb{Z}[\zeta_p]$  οι έννοιες του αναγώγου και πρώτου στοιχείου ταυτίζονται, μπορεί κανείς να 'αποδείξει' την εικασία του Fermat (όπως έγινε από τον Kummer το 1837, ο οποίος δέχθηκε ότι όλοι οι  $\mathbb{Z}[\zeta_p]$  είναι περιοχές μονοσήμαντης ανάλυσης). Παρόλα αυτά αυτό δεν ισχύει για παράδειγμα  $p = 37$ .

**Κίνητρο 2.** Ένα ερώτημα που θα μας απασχολήσει στο μάθημα είναι το πότε υπάρχει μονοσήμαντη ανάλυση και τι κάνουμε στην περίπτωση που δεν υπάρχει.

## 1.2 Ακέραιοι Αλγεβρικοί Αριθμοί

**Ορισμός 5.** Ένας  $a \in \mathbb{C}$  θα λέγεται **αλγεβρικός αριθμός** αν είναι ρίζα ενός μονικού πολυωνύμου  $f(x) \in \mathbb{Q}[x]$  με  $f(x) \neq 0$ .

**Ορισμός 6.** Ένας  $a \in \mathbb{C}$  θα λέγεται **ακέραιος αλγεβρικός αριθμός** αν είναι ρίζα ενός μονικού πολυωνύμου  $f(x) \in \mathbb{Z}[x]$  με  $f(x) \neq 0$ .

**Παρατήρηση 3.** Ένας  $a \in \mathbb{Q}$  είναι ακέραιος αλγεβρικός αν και μόνο αν  $a \in \mathbb{Z}$ .

*Απόδειξη.* Η μια κατεύθυνση είναι άμεση. Για τη δεύτερη δείξτε ένα γενικότερο αποτέλεσμα και καταλήξτε στο ζητούμενο. Αν  $a = \frac{m}{n} \in \mathbb{Q}$  με  $(m, n) = 1$  ρίζα του  $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ , τότε  $m|a_0$  και  $n|a_k$ .  $\square$

**Πρόταση 1.** Ο  $a \in \mathbb{C}$  είναι ακέραιος αλγεβρικός αν και μόνο αν η προσθετική ομάδα  $\mathbb{Z}[a] = \{f(a) \mid f(x) \in \mathbb{Z}[x]\}$  είναι πεπερασμένα παραγόμενη.

**Συμβολισμός 1.** Θα συμβολίζουμε με  $\mathcal{A} = \{a \in \overline{\mathbb{Q}} \mid a \text{ ακέραιος αλγεβρικός}\}$ .

Απόδειξη. Υποθέτουμε αρχικά ότι ο  $a$  είναι ακέραιος αλγεβρικός αριθμός. Συνεπώς, υπάρχει  $f(x) \in \mathbb{Z}[x]$  βαθμού  $n$ , μονικό ώστε  $f(a) = 0$ . Έστω  $g(x) \in \mathbb{Z}[x]$ . Τότε, αφού  $f(x)$  μονικό, υπάρχουν  $q(x), r(x) \in \mathbb{Z}[x]$  ώστε  $g(x) = q(x)f(x) + r(x)$  με  $r(x) = 0$  ή  $\deg(r(x)) < n$ . Έτσι έχουμε ότι  $g(a) = r(a)$  και είναι σαφές ότι η  $\mathbb{Z}[a]$  παράγεται από τα  $1, a, a^2, \dots, a^{n-1}$ .

Αντίστροφα, υποθέτουμε ότι  $z_1, \dots, z_n$  παράγουν του  $\mathbb{Z}[a]$ . Τότε, για κάθε  $i = 1, \dots, n$ , υπάρχουν  $\lambda_j^i$  ώστε  $az_i = \sum_{j=1}^n \lambda_j^i z_j$ . Παρατηρήστε ότι η τελευταία σχέση γράφεται ως εξής

$$\left[ aI_n - (\lambda_j^i)_{i,j} \right] \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = 0.$$

Αφού το σύστημα  $\left[ aI_n - (\lambda_j^i)_{i,j} \right] X = 0$  έχει μη μηδενική λύση, τότε

$$f(a) = \det \left[ aI_n - (\lambda_j^i)_{i,j} \right] = 0$$

όπου  $f(x) \in \mathbb{Z}[x]$  μονικό. □

## 2 Μάθημα 02

**Υπενθύμιση 1.** Μια αλγεβρική επέκταση  $F \subseteq K$  θα λέγεται **διαχωρίσιμη** αν για κάθε  $a \in K$ , το ελάχιστο πολυώνυμο  $p(x) = \text{Irr}(a, F)$  είναι διαχωρίσιμο, δηλαδή έχει όλες τις ρίζες του διακεκριμένες στην αλγεβρική θήκη  $\overline{F}$ .

**Υπενθύμιση 2.** Αποδεικνύεται ότι κάθε ανάγωγο πολυώνυμο πάνω από σώμα χαρακτηριστικής 0 είναι διαχωρίσιμο. Συνεπώς, κάθε αλγεβρική επέκταση  $\mathbb{Q} \subseteq K$  είναι διαχωρίσιμη.

**Ορισμός 7.** Μια επέκταση σωμάτων  $F \subseteq K$  θα λέγεται **απλή** αν  $K = F(\vartheta)$  για κάποιο  $\vartheta \in K$ .

**Υπενθύμιση 3** (Θεώρημα Πρωταρχικού Στοιχείου). Αν  $F \subseteq K$  μια πεπερασμένη επέκταση με  $\text{char}F = 0$ , τότε υπάρχει  $\vartheta \in K$  ώστε  $K = F(\vartheta)$ .

Θεωρούμε πεπερασμένη επέκταση  $\mathbb{Q} \subseteq K$ . Από τα παραπάνω έχουμε ότι η επέκταση αυτή είναι διαχωρίσιμη και απλή, δηλαδή  $K = \mathbb{Q}(\vartheta)$ . Συμβολίζουμε με  $\mathcal{O}_K$  του ακέραιους αλγεβρικούς αριθμούς του  $K$ .

**Παρατήρηση 4.** Αν  $a \in \overline{\mathbb{Q}}$ , τότε υπάρχει  $m \in \mathbb{Z}$  ώστε  $ma \in \mathcal{A}$ .

*Απόδειξη.* Έστω  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Q}[x]$  τέτοιο ώστε  $f(a) = 0$ . Τότε, υπάρχει  $m \in \mathbb{Z}$  ώστε  $ma_i \in \mathbb{Z}$ , για κάθε  $i = 0, \dots, n-1$ . Θεωρούμε το πολυώνυμο  $g(x) = x^n + ma_{n-1}x^{n-1} + \dots + m^{n-1}a_1x + m^n a_0 \in \mathbb{Z}$ . Παρατηρήστε ότι  $g(ma) = 0$ .  $\square$

Από την παραπάνω παρατήρηση μπορούμε να υποθέσουμε ότι  $K = \mathbb{Q}(\vartheta)$ , όπου  $\vartheta \in \mathcal{O}_K$  (γιατί ;).

### 2.1 Τετραγωνικά Σώματα Αριθμών

**Ορισμός 8.** Έστω  $\mathbb{Q} \subseteq K$  πεπερασμένη επέκταση. Αν  $[K : \mathbb{Q}] = 2$ , τότε το  $K$  θα λέγεται **τετραγωνικό σώμα αριθμών**.

Όπως πριν αν  $\mathbb{Q} \subseteq K$  με  $[K : \mathbb{Q}] = 2$ , μπορούμε να υποθέσουμε ότι  $K = \mathbb{Q}(\vartheta)$ , όπου  $\vartheta \in \mathcal{O}_K$ .

- Τότε, έχουμε ότι  $\deg \text{Irr}(a, \mathbb{Q}) = 2$ , συνεπώς ισχύει ότι

$$p(x) = \text{Irr}(\vartheta, \mathbb{Q}) = x^2 - ax - b = \left(x - \frac{a}{2}\right)^2 - \frac{a^2}{4} - b$$



- Αν  $\vartheta^* = \vartheta - \frac{a}{2}$  παρατηρήστε ότι  $\vartheta^*$  είναι ρίζα του  $x^2 - b'$ , όπου  $b' = a^2/4 + b$  και μάλιστα

$$\mathbb{Q}(\vartheta) = \mathbb{Q}(\vartheta^*)$$

**Ορισμός 9.** Ένας  $b \in \mathbb{Z}$  καλείται **ελεύθερος τετραγώνου**, αν δεν υπάρχει  $a \in \mathbb{Z}$  ώστε  $a^2|b$ . Στην περίπτωση αυτή συμβολίζουμε  $\square \nmid b$ .

- Αρχικά παρατηρούμε ότι  $b'$  δεν μπορεί να είναι τέλειο τετράγωνο, διότι στην περίπτωση αυτή θα ήταν της μορφής  $b' = r^2$  με  $r \in \mathbb{Q}$ , επομένως αφού  $\vartheta^*$  ρίζα του  $x^2 - b'$ , τότε  $\vartheta \in \mathbb{Q}$  και  $\mathbb{Q}(\vartheta) = \mathbb{Q}$ . Τότε μπορούμε να γράψουμε  $b' = mr^2$ , όπου  $m \in \mathbb{Z}$  ελεύθερο τετραγώνου και  $r \in \mathbb{Q}$ . Παρατηρήστε ότι

$$K = \mathbb{Q}(\vartheta) = \mathbb{Q}(\vartheta^*) = \mathbb{Q}(\sqrt{b'}) = \mathbb{Q}(\sqrt{m})$$

Όλη η προηγούμενη διαδικασία συνοψίζεται στο παρακάτω θεώρημα.

**Θέωρημα 2.** Κάθε τετραγωνικό σώμα αριθμών  $K$  είναι της μορφής  $K = \mathbb{Q}(\sqrt{m})$ , όπου  $m \in \mathbb{Z}$ ,  $m \neq 1$  ελεύθερος τετραγώνου.

Υπάρχουν δύο περιπτώσεις :

- Αν  $m > 0$ , τότε  $K = \mathbb{Q}(\sqrt{m}) \subseteq \mathbb{R}$  και λέγεται **πραγματικό τετραγωνικό σώμα αριθμών**.
- Αν  $m < 0$ , τότε  $K = \mathbb{Q}(\sqrt{m}) \subseteq \mathbb{C}$  και λέγεται **μιγαδικό τετραγωνικό πραγματικό σώμα αριθμών**.

**Ορισμός 10.** Μια επέκταση σωμάτων  $F \subseteq K$  λέγεται **κανονική** αν κάθε  $p(x) \in F[x]$  το οποίο έχει ρίζα στο  $K$ , αναλύεται πλήρως στο  $K$ .

**Πόρισμα 1.** Αν  $F \subseteq K$  επέκταση σωμάτων, τότε  $K$  είναι κανονική και πεπερασμένη αν και μόνο αν  $K$  είναι σώμα ριζών κάποιου πολυωνύμου πάνω από το  $F$ .

**Παρατήρηση 5.** Παρατηρήστε ότι η επέκταση  $\mathbb{Q} \subseteq K = \mathbb{Q}(\sqrt{m})$  είναι κανονική (αφού είναι σώμα ριζών του  $x^2 - m$ ) και διαχωρίσιμη, άρα είναι επέκταση Galois. Η αντίστοιχη ομάδα Galois αυτής της επέκτασης είναι η  $\text{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$  με  $\sigma: K \rightarrow K$  και  $\sigma(\sqrt{m}) = -\sqrt{m}$  και  $\sigma(a) = a$ , για κάθε  $a \in \mathbb{Q}$ . Τέλος, παρατηρήστε ότι αν  $p(x) \in F[x]$  και  $a \in K$  ρίζα του  $p(x)$ , τότε και  $\sigma(a)$  ρίζα του  $p(x)$ .

**Ορισμός 11.** Αν  $K = \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ , τότε για κάθε  $c = a + b\sqrt{m} \in K$  ορίζεται

- το **ίχνος** του  $c$  με  $S_K(c) = c + \sigma(c) = 2a$
- και η **νόρμα** του  $c$  με  $N_K(c) = c \cdot \sigma(c) = a^2 - mb^2$ .

Τότε, ισχύει ότι

$$\text{Irr}(c, \mathbb{Q}) = (x - c)(x - \sigma(c)) = x^2 - S_K(c)x + N_K(c) \quad (2)$$

**Κίνητρο 3.** Σκοπός μας είναι να βρούμε ένα "ικανοποιητικό κριτήριο" με σκοπό την εύρεση των ακέραιων αλγεβρικών αριθμών του  $K$ .

**Θέωρημα 3.** Ένας  $\alpha \in \mathbb{Q}(\sqrt{m})$  είναι ακέραιος αλγεβρικός αν και αν μόνο αν  $S_K(\alpha) \in \mathbb{Z}$  και  $N_K(\alpha) \in \mathbb{Z}$ .

*Απόδειξη.* Αν  $\alpha = a + b\sqrt{m}$ , τότε θέτουμε  $c = 2a$  και  $d = 2b$ . Τότε  $S_K(\alpha) \in \mathbb{Z}$  και  $N_K(\alpha) \in \mathbb{Z}$  αν και μόνο αν  $c \in \mathbb{Z}$  και

$$a^2 - mb^2 = \frac{c^2 - md^2}{4} \in \mathbb{Z}$$

Αφού  $m$  είναι ελεύθερο τετραγώνου, οι αρχικές μας απαιτήσεις ισοδυναμούν με το  $c, d \in \mathbb{Z}$  και  $c^2 \equiv md^2 \pmod{4}$ . Αρχικά παρατηρούμε ότι  $x^2 \equiv 0, 1 \pmod{4}$ , για κάθε  $x \in \mathbb{Z}$ . Επίσης έχουμε ότι  $m \equiv 1, 2, 3 \pmod{4}$ , επομένως διακρίνουμε περιπτώσεις :

- Αν  $m \equiv 2, 3 \pmod{4}$ , τότε έχουμε ότι  $c^2 \equiv d^2 \equiv 0 \pmod{4}$ . Τότε, προκύπτει ότι  $c \equiv d \equiv 0 \pmod{2}$ , άρα  $\alpha = \frac{c-d}{2} + d \left( \frac{1+\sqrt{m}}{2} \right)$ .
- Αν  $m \equiv 1 \pmod{4}$ , τότε έχουμε ότι  $c^2 \equiv d^2 \pmod{4}$ . Τότε, προκύπτει ότι  $c \equiv d \pmod{2}$ , άρα  $\alpha = \frac{c-d}{2} + d \left( \frac{1+\sqrt{m}}{2} \right)$ .

Από τις τελευταίες δύο σχέσεις έχουμε ότι  $\alpha$  είναι ακέραιος αλγεβρικός ως άθροισμα τέτοιων. □

*B' Τρόπος.* Η μία κατεύθυνση είναι άμεση από την σχέση 2. Για το αντίστροφο, υποθέτουμε ότι  $\alpha$  είναι ακέραιος αλγεβρικός, άρα υπάρχει  $f(x) \in \mathbb{Z}[x]$  ώστε  $f(\alpha) = 0$ .

- Τότε, υπάρχει  $q(x) \in \mathbb{Q}[x]$  μονικό, θετικού βαθμού ώστε  $f(x) = q(x) \cdot \text{Irr}(a, \mathbb{Q})$ .
- Τότε, βλέπε Θεωρία Galois, μπορεί ναδειχθεί ότι υπάρχουν  $a(x), b(x) \in \mathbb{Z}[x]$  ώστε  $f(x) = a(x)b(x)$  και  $a(x) = c_1q(x)$ ,  $b(x) = c_2\text{Irr}(a, \mathbb{Q})$  με  $c_1, c_2 \in \mathbb{Q}$ .

- Αφού  $f(x), q(x), \text{Irr}(a, \mathbb{Q})$  είναι μονικά, τότε έχουμε ότι  $b(x) = \text{Irr}(a, \mathbb{Q}) \in \mathbb{Z}[x]$  και από την σχέση 2 έχουμε το ζητούμενο.

□

Έτσι συμπεραίνουμε ότι

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{αν } m \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right], & \text{αν } m \equiv 1 \pmod{4} \end{cases}$$

## 2.2 Η ομάδα των μονάδων

Σκοπός είναι να βρούμε τις μονάδες (αντιστρέψιμα στοιχεία) του  $\mathcal{O}_K$ . Για κάθε  $\varepsilon \in \mathcal{O}_K$  έχουμε ότι  $N_K(\varepsilon) \in \mathbb{Z}$  και μάλιστα αποδεικνύεται εύκολα ότι  $\varepsilon \in E[\mathcal{O}_K]$  αν και μόνο αν  $N(\varepsilon) \in \{-1, 1\}$ . Συμβολίζουμε με

$$\omega_m = \begin{cases} \sqrt{m}, & m \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{m}}{2}, & \text{αν } m \equiv 1 \pmod{4} \end{cases}$$

Συνεπώς, αν  $\varepsilon = a + b\omega_n$  με  $a, b \in \mathbb{Z}$  αντιστρέψιμο, τότε έχουμε ότι

$$N_K(\varepsilon) = \begin{cases} a^2 - mb^2, & m \equiv 2, 3 \pmod{4} \\ a^2 + ab + \frac{1-m}{4}b^2, & \text{αν } m \equiv 1 \pmod{4} \end{cases} = \pm 1.$$

Διακρίνουμε περιπτώσεις :

(α) Υποθέτουμε ότι  $m < 0$ .

- Αν  $m \equiv 2, 3 \pmod{4}$ , τότε  $a^2 + |m|b^2 = 1$ .
  - Αν  $|m| > 1$ , τότε έχουμε ότι  $a = \pm 1$  και  $b = 0$ , άρα  $\varepsilon = \pm 1$ .
  - Αν  $m = -1$ , τότε  $a^2 + b^2 = 1$ , συνεπώς έχουμε τέσσερις λύσεις  $a = \pm 1$  και  $b = 0$  και  $a = 0$  και  $b = \pm 1$ . Δηλαδή  $\varepsilon = \pm 1$  ή  $\pm i$
- Αν  $m \equiv 1 \pmod{4}$ , έχουμε ότι

$$a^2 + ab + \frac{1-m}{4}b^2 = \left(a + \frac{b}{2}\right)^2 + \frac{|m|}{4}b^2 = 1.$$

- Αν  $|m| > 4$ , τότε όμοια έχουμε ότι  $b = 0$  και  $a = \pm 1$ .

– Αν  $|m| \leq 4$  και  $m \equiv 1$ , τότε  $m = -3$ . Παρατηρήστε ότι για  $|b| \geq 2$  δεν υπάρχουν λύσεις. Για  $b = 1$ , προκύπτει ότι  $a^2 + a + 1 = 1$ , άρα  $a = 0$  ή  $a = -1$ . Τέλος, αν  $b = 0$ , έχουμε ότι  $a = \pm 1$  και για  $b = -1$  έχουμε  $a = 0$ .

(β) Η περίπτωση  $m > 0$  παραλείπεται. (Βλέπε Αντωνιάδης, Κοντογεώργης (2022) "Αλγεβρική Θεωρία Αριθμών")

### 3 Μάθημα 03

#### 3.1 Ιδεώδη Σώματος Κλασμάτων και Δακτύλιοι Dedekind

Έστω  $R$  ακέραια περιοχή και  $K = \text{Quot}(R)$  το σώμα πηλίκων του  $R$ .

**Ορισμός 12.** Ένα  $A \subseteq K$  λέγεται **ιδεώδες** του  $K$  αν ισχύουν τα ακόλουθα :

- (α)  $a_1 - a_2 \in A$ , για κάθε  $a_1, a_2 \in A$
- (β)  $\lambda a \in A$ , για κάθε  $\lambda \in R$  και  $a \in A$ .
- (γ)  $A \neq \{0_K\}$
- (δ) υπάρχει  $\delta \in K$  ώστε  $\delta A \subseteq R$ .

Αν  $A \subseteq R$  τότε το  $A$  θα λέγεται **ακέραιο** ιδεώδες, αλλιώς θα λέγεται **κλασματικό**.

**Παράδειγμα 8.** Κάθε μη μηδενικό ιδεώδες  $I$  του  $R$ , αφού  $I \subseteq R \subseteq K$ , είναι άμεσο ότι είναι ιδεώδες του  $K$  για  $\delta = 1$ .

**Παράδειγμα 9.** Αν  $R = \mathbb{Z}$  και  $K = \mathbb{Q}$ , τότε  $\frac{1}{3}\mathbb{Z}$  είναι κλασματικό ιδεώδες του  $K$ , για  $\delta = 3$ .

**Ορισμός 13.** Αν  $A, B$  ιδεώδη του  $K$ , τότε ορίζεται το **γινόμενο** τους

$$A \cdot B = \left\{ \sum_{i \in I, I \text{ πεπερασμένο}} a_i b_i \mid a_i \in A, b_i \in B \right\} \quad (3)$$

**Παρατήρηση 6.** Δείξτε ότι  $A \cdot B$  είναι πράγματι ιδεώδες του  $K$ .

**Πρόταση 2** (Ιδιότητες Ιδεωδών). Έστω  $A, B, C$  ιδεώδη του  $K = \text{Quot}(R)$ . Τότε ισχύει ότι :

- (α)  $A \cdot B = B \cdot A$
- (β)  $(A \cdot B) \cdot C = A \cdot (B \cdot C)$
- (γ)  $A \cdot R = R \cdot A = A$

**Παρατήρηση 7.** Το σύνολο των ιδεωδών του  $K$  εφοδιασμένο με πράξη το γινόμενο ιδεωδών είναι μια μεταθετική ημιομάδα με μονάδα (ή αλλιώς μονοϊδές).

**Ορισμός 14.** Αν  $A$  είναι ένα ιδεώδες του  $K$ , ορίζουμε ως **ανάστροφο ιδεώδες** του  $A$

$$A^* = \{x \in K \mid xA \subseteq R\}$$

**Παράδειγμα 10.** Έστω  $R = \mathbb{Z}$ ,  $K = \mathbb{Q}$  και  $A = 3\mathbb{Z}$ . Τότε,  $A^* = \frac{1}{3}\mathbb{Z}$  και  $A \cdot A^* = \mathbb{Z}$ .

**Παρατήρηση 8** (Ιδιότητες Ανάστροφου Ιδεώδους). (α) Αν  $A_1, A_2$  ιδεώδη του  $K$  με  $A_1 \subseteq A_2$ , τότε  $A_2^* \subseteq A_1^*$ .

(β) Αν  $A$  ιδεώδες του  $K$ , τότε  $A^* \cdot A \subseteq R$ . Η ισότητα δεν ισχύει εν γένει!

Απόδειξη. Άσκηση. □

**Παρατήρηση 9.** Έστω  $A$  ιδεώδες του  $K$  και υποθέτουμε ότι  $A$  έχει αντίστροφο, δηλαδή υπάρχει  $B$  ιδεώδες του  $K$  ώστε  $A \cdot B = R$ . Είναι άμεσο ότι  $B \subseteq A^*$ . Επιπρόσθετα, ισχύει ότι

$$A^* = A^* \cdot R = (A^* \cdot A) \cdot B \subseteq B.$$

Έτσι προκύπτει ότι  $B = A^*$ .

Συμβολίζουμε με  $\mathcal{I} = \{A \mid A \text{ ιδεώδες του } K\}$ .

**Λήμμα 1.** Κάθε κύριο ιδεώδες  $aR$  με  $a \in K \setminus \{0\}$  είναι αντιστρέψιμο. Συνεπώς το σύνολο

$$\mathcal{H} = \{aR \mid a \in K \setminus \{0\}\}$$

είναι πολλαπλασιαστική, αβελιανή ομάδα.

Απόδειξη. Έστω  $a \neq 0$  στο  $K$ . Παρατηρήστε ότι  $aR \cdot (a^{-1}R) = R$ . □

**Πρόταση 3.** Το  $\mathcal{J} = \{A \in \mathcal{I} \mid A \text{ είναι αντιστρέψιμο}\}$  είναι πολλαπλασιαστική, αβελιανή ομάδα.

Απόδειξη. Είναι σαφές ότι αν  $A_1, A_2 \in \mathcal{J}$ , τότε και το  $A_1 \cdot A_2 \in \mathcal{J}$  και μάλιστα

$$(A_1 \cdot A_2)^{-1} = A_2^{-1} A_1^{-1} = A_2^* \cdot A_1^*.$$

□

**Ορισμός 15.** Μια περιοχή  $R$  θα λέγεται **δακτύλιος του Dedekind** αν κάθε ιδεώδες του  $K = \text{Quot}(R)$  είναι αντιστρέψιμο.

### 3.2 Δακτύλιοι και Πρότυπα της Noether

**Ορισμός 16.** Έστω  $R$  μεταθετικός δακτύλιος με μονάδα. Ο  $R$  θα λέγεται **δακτύλιος της Noether** αν ισχύει κάποια από τις παρακάτω ισοδύναμες συνθήκες:

- (α) Κάθε αύξουσα ακολουθία ιδεωδών είναι τελικά σταθερή
- (β) Κάθε μη κενό σύνολο ιδεωδών του  $R$  έχει μεγιστικό στοιχείο (ως προς τη σχέση εγκλεισμού).
- (γ) Κάθε ιδεώδες του  $R$  είναι πεπερασμένα παραγόμενο.

*Απόδειξη Ισοδυναμίας.* • (α)  $\rightarrow$  (β) Έστω  $\mathcal{X} \neq \emptyset$  σύνολο ιδεωδών του  $R$  και ιδεώδες  $A_0 \in \mathcal{X}$ . Έστω ότι  $\mathcal{X}$  δεν έχει μεγιστικό στοιχείο.

- Τότε, υπάρχει κάποιο  $A_0 \subsetneq A_1$  στην  $\mathcal{X}$ .
- Το  $A_1$  δεν είναι επίσης μεγιστικό, συνεπώς υπάρχει  $A_1 \subsetneq A_2$  στην  $\mathcal{X}$ .
- Συνεχίζοντας την προηγούμενη διαδικασία, κατασκευάζουμε γνησίως αύξουσα αλυσίδα ιδεωδών

$$A_0 \subsetneq A_1 \subsetneq \cdots \subsetneq A_n \subsetneq A_{n+1} \subsetneq \cdots$$

Από το (α) καταλήγουμε σε άτοπο.

- (β)  $\rightarrow$  (γ) Έστω  $I$  ιδεώδες του  $R$  και  $\mathcal{W}$  το σύνολο των πεπερασμένα παραγόμενων ιδεωδών  $J$  με  $J \subseteq I$ .
  - Αρχικά  $\mathcal{W} \neq \emptyset$ , αφού  $\{0\} \subseteq I$ .
  - Από το (β), υπάρχει  $J \in \mathcal{W}$  μεγιστικό στοιχείο. Θα δείξουμε ότι  $J = I$  και έτσι θα έχουμε το ζητούμενο.
  - Αν  $J \subsetneq I$ , τότε υπάρχει  $x \in I \setminus J$ . Θεωρώντας το ιδεώδες  $J' = J + xR$ , τότε παρατηρούμε ότι  $J \subsetneq J'$ ,  $J'$  πεπερασμένα παραγόμενο και  $J' \subseteq I$ , συνεπώς  $J' \in \mathcal{W}$ . Έτσι καταλήγουμε σε άτοπο.

- (γ)  $\rightarrow$  (α) Θεωρούμε αύξουσα ακολουθία ιδεωδών του  $R$

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

Θα δείξουμε ότι η παραπάνω αλυσίδα είναι τελικά σταθερή.

- Παρατηρούμε ότι  $I = \bigcup_{n=0}^{\infty} I_n$  είναι ένας ιδεώδες του  $R$ , συνεπώς είναι πεπερασμένα παραγόμενο και της μορφής  $I = x_1R + \cdots + x_kR$ .
- Για κάθε  $i = 1, \dots, k$ , υπάρχει  $I_{i_j}$  ώστε  $x_j \in I_{i_j}$ . και αν  $\ell = \max\{i_1, \dots, i_k\}$  έχουμε ότι  $x_1, \dots, x_k \in I_\ell$ .

- Από την παραπάνω σχέση προκύπτει ότι  $I \subseteq I_\ell$ , συνεπώς έχουμε ότι  $I = I_\ell$  και η παραπάνω αλυσίδα είναι τελικά σταθερή.

□

**Παράδειγμα 11.** Το  $\mathbb{Z}$  είναι δακτύλιος της Noether. Αυτό προκύπτει από το γεγονός ότι κάθε ιδεώδες του  $\mathbb{Z}$  είναι κύριο, ειδικότερα πεπερασμένα παραγόμενο.

**Πόρισμα 2.** Κάθε δακτύλιος κύριων ιδεωδών είναι δακτύλιος της Noether.

**Ορισμός 17.** Έστω  $R$  μεταθετικός δακτύλιος με μονάδα και  $M$  ένα  $R$ -πρότυπο. Το  $M$  θα λέγεται **πρότυπο της Noether** αν ισχύει κάποια από τις παρακάτω ισοδύναμες συνθήκες.

- (α) Κάθε αύξουσα ακολουθία υποπροτύπων του  $M$  είναι τελικά σταθερή.
- (β) Κάθε μη κενή οικογένεια υποπροτύπων του  $M$  έχει μέγιστικό στοιχείο (ως προς την σχέση εγκλεισμού).
- (γ) Κάθε υποπρότυπο του  $M$  είναι πεπερασμένα παραγόμενο.

*Απόδειξη.* Η απόδειξη της ισοδυναμίας των παραπάνω γίνεται όμοια με αυτή του προηγούμενου ορισμού, συνεπώς αφήνεται ως άσκηση. □

**Λήμμα 2.** Έστω βραχεία ακριβής ακολουθία

$$0 \rightarrow M_1 \xrightarrow{i} M \xrightarrow{\varphi} M_2 \rightarrow 0$$

Τότε, τα  $M_1, M_2$  είναι πρότυπα της Noether αν και μόνο αν και το  $M$  είναι πρότυπο της Noether.

*Απόδειξη.* Άσκηση. □

**Θέωρημα 4.** (α) Το ευθύ άθροισμα πεπερασμένων το πλήθος προτύπων της Noether είναι πρότυπο της Noether.

- (β) Η ομομορφική εικόνα προτύπου της Noether είναι πρότυπο της Noether.

*Απόδειξη.* Έστω  $A, B$  δύο  $R$ -πρότυπα της Noether.



(α) Για να δείξουμε το ζητούμενο αρκεί να δείξουμε ότι  $A \oplus B$  είναι πρότυπο της Noether. Αυτό όμως προκύπτει άμεσα από το Λήμμα 2, θεωρώντας τη β.α.α.

$$0 \rightarrow A \hookrightarrow A \oplus B \xrightarrow{\pi_B} B.$$

(β) Από το Λήμμα 2, είναι άμεσο ότι ηλικό πρότυπο της Noether είναι πρότυπο της Noether. Χρησιμοποιώντας το Πρώτο Θεώρημα Ισομορφισμών καταλήγουμε στο ζητούμενο.

□

**Παρατήρηση 10.** Από την παραπάνω απόδειξη προκύπτει ότι τα ευθέα άθροίσματα επάγουν βραχείες ακριβείς ακολουθίες, παρόλα αυτά δεν ισχύει εν γένει το αντίστροφο! <sup>1</sup> Πράγματι, θεωρούμε τη β.α.α. αβελιανών ομάδων

$$0 \rightarrow \mathbb{Z}_2 \xrightarrow{\cdot 2} \mathbb{Z}_4 \xrightarrow{\cdot 2} \mathbb{Z}_2 \rightarrow 0.$$

Παρατηρήστε ότι η παραπάνω ακολουθία είναι ακριβής, αλλά είναι προφανές ότι  $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ . Παρόλα αυτά αφήνεται ως άσκηση ναδειχθεί ότι αν

$$0 \rightarrow V_1 \rightarrow V \rightarrow V_2 \rightarrow 0$$

β.α.α. μεταξύ  $k$  - δ.χ. πεπερασμένης διάστασης, τότε προκύπτει ότι  $\dim V = \dim V_1 + \dim V_2$  και συνεπώς  $V \cong V_1 \oplus V_2$  (ως εξωτερικό ευθύ άθροισμα) με επιχείρημα διαστάσεων.

---

<sup>1</sup>Όταν αυτό συμβαίνει η αντίστοιχη β.α.α. λέγεται **διασπώμενη**.

## 4 Μάθημα 04

### 4.1 Δακτύλιοι Dedekind και Πρώτα - Μέγιστα Ιδεώδη

**Ορισμός 18.** Έστω  $R$  μεταθετικός δακτύλιος και  $I$  γνήσιο ιδεώδες του  $R$ .

- (α) Το  $I$  θα λέγεται **πρώτο** αν οποιαδήποτε  $a \cdot b \in I$ , τότε  $a \in I$  ή  $b \in I$ , για  $a, b \in R$ .
- (β) Το  $I$  λέγεται **μέγιστο** αν για οποιοδήποτε  $J$  ιδεώδες του  $R$  για το οποίο ισχύει  $I \subseteq J \subseteq R$ , τότε  $J = I$  ή  $J = R$ .

**Πρόταση 4.** Έστω  $R$  μεταθετικός δακτύλιος.

- Ένα  $\mathfrak{m}$  είναι μέγιστο αν και μόνο αν ο  $R/\mathfrak{m}$  είναι σώμα.
- Ένα  $\mathfrak{p}$  είναι πρώτο αν και μόνο αν ο  $R/\mathfrak{p}$  είναι ακέραια περιοχή.

**Παρατήρηση 11.** Κάθε μέγιστο ιδεώδες είναι πρώτο, όμως το αντίστροφο δεν ισχύει!

Για παράδειγμα, θεωρούμε  $R = \mathbb{Z}[x]$  και  $I = xR$ , δηλαδή το ιδεώδες που περιέχει όλα τα πολυώνυμα που έχουν ρίζα το 0. Από το συνήθη ομομορφισμό εκτίμησης έχουμε ότι  $R/xR \cong \mathbb{Z}$ , το οποίο είναι ακέραια περιοχή, αλλά όχι σώμα, δηλαδή το  $xR$  είναι πρώτο αλλά όχι μέγιστο.

**Παράδειγμα 12.** Έστω  $R = \mathbb{Z}$  και  $I = n\mathbb{Z}$ . Γνωρίζουμε ότι ο  $R/I = \mathbb{Z}_n$  είναι σώμα αν και μόνο αν ο  $n$  είναι πρώτος. Άρα, κάθε μη μηδενικό, πρώτο (και μέγιστο) ιδεώδες του  $\mathbb{Z}$  είναι της μορφής  $I = p\mathbb{Z}$ , όπου  $p$  πρώτος.

**Σημείωση 1.** Γνωρίζουμε ότι κάθε μη μηδενικό, πρώτο ιδεώδες σε Π.Κ.Ι. είναι μέγιστο. Ας εξασθενίσουμε τις υποθέσεις μας σχετικά με την φύση του δακτυλίου  $R$  μπορούμε να πετύχουμε το αντίστοιχο αποτέλεσμα; Αυτό συμβαίνει αν ο δακτύλιος είναι Dedekind.

**Λήμμα 3.** Έστω  $\mathfrak{p}$  πρώτο ιδεώδες ενός δακτυλίου  $R$  και  $A, B$  ιδεώδη του  $R$ . Αν  $A \cdot B \subseteq \mathfrak{p}$ , τότε  $A \subseteq \mathfrak{p}$  ή  $B \subseteq \mathfrak{p}$ .

*Απόδειξη.* Έστω ότι υπάρχει  $b \in B$  με  $b \notin \mathfrak{p}$ . Έστω  $a \in A$ . Τότε, έχουμε ότι  $a \cdot b \in \mathfrak{p}$ . Αφού  $\mathfrak{p}$  είναι πρώτο, τότε  $a \in \mathfrak{p}$  ή  $b \in \mathfrak{p}$ . Από την παραπάνω υπόθεση έχουμε ότι  $a \in \mathfrak{p}$ .  $\square$

**Θέωρημα 5.** Έστω  $R$  δακτύλιος Dedekind. Τότε, ισχύουν τα εξής :

- (α) Ο  $R$  είναι της Noether.

(β) Κάθε μη μηδενικό, πρώτο ιδεώδες του  $R$  είναι μέγιστο.

Απόδειξη. (α) Έστω  $A \neq \{0\}$  ιδεώδες του  $R$ .

- Τότε, υπάρχει ιδεώδες  $A^{-1} = A^*$  του  $K = \text{Quot}(R)$  ώστε  $A \cdot A^{-1} = R$ .
- Επομένως, υπάρχουν  $a_1, \dots, a_m \in A$  και  $b_1, \dots, b_m \in A^*$ , ώστε

$$1 = a_1 b_1 + \dots + a_m b_m.$$

Άρα, για κάθε  $x \in A$  έχουμε ότι  $x = (b_1 x) a_1 + \dots + (b_m x) a_m$ , όπου  $b_i x \in R$ , από το ορισμό του  $A^*$ . Άρα,  $A = a_1 R + \dots + a_m R$ .

(β) Έστω  $\mathfrak{p}$  πρώτο. Αφού  $R$  είναι της Noether, τότε υπάρχει  $\mathfrak{m}$  μέγιστο ώστε  $\mathfrak{p} \subseteq \mathfrak{m}$ . Θα δείξουμε ότι  $\mathfrak{p} = \mathfrak{m}$ .

– Αρχικά, έχουμε ότι

$$\mathfrak{p} \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{m} \cdot \mathfrak{m}^{-1} = R$$

Άρα,  $\mathfrak{p} \cdot \mathfrak{m}^{-1}$  είναι ιδεώδες του  $R$ .

– Έχουμε ότι  $\mathfrak{p} = (\mathfrak{p} \cdot \mathfrak{m}^{-1}) \mathfrak{m}$  και από το Λήμμα 3 προκύπτει ότι  $\mathfrak{p} \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{p}$  ή  $\mathfrak{m} \subseteq \mathfrak{p}$ .

– Αν υποθέσουμε ότι  $\mathfrak{p} \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{p}$ , τότε παρατηρούμε ότι

$$\mathfrak{m}^{-1} = \mathfrak{p}^{-1} \cdot \mathfrak{p} \cdot \mathfrak{m}^{-1} \subseteq R.$$

Άρα, έχουμε ότι  $R \subseteq \mathfrak{m}$  και καταλήγουμε σε άτοπο. Συνεπώς,  $\mathfrak{m} \subseteq \mathfrak{p}$  και έχουμε το ζητούμενο. □

## 4.2 Ακέραια Εξάρτηση

**Ορισμός 19.** Έστω  $R$  μεταθετικός και  $S \subseteq R$  υποδακτύλιος. Ένα  $a \in R$  θα λέγεται  $S$ -ακέραιος αν υπάρχει  $f(x) \in S[x]$  μονικό ώστε  $f(a) = 0$ .

**Θέωρημα 6.** Έστω  $R \subset L$  υποδακτύλιος ενός σώματος  $L$ . Τα παρακάτω είναι ισοδύναμα:

(α) Το  $a$  είναι  $R$ -ακέραιος.

1. Ο δακτύλιος  $R[a]$  είναι πεπερασμένα παραγόμενο  $R$ -πρότυπο.
2. Υπάρχει ένα πεπερασμένα παραγόμενο, μη-μηδενικό  $R$ -πρότυπο  $M \subset L$  ώστε  $aM \subset M$ .

Απόδειξη. • (α) → (β) Αφού  $a$  είναι ένας  $R$ -ακέραιος, τότε υπάρχει μονικό  $f(x) \in R[x]$ , βαθμού  $n$ , ώστε  $f(a) = 0$ . Αφού ο μεγιστοβάθμιος του  $f(x)$  είναι αντιστρέψιμο στοιχείο του  $R$ , τότε για κάθε  $g(x) \in R[x]$ , υπάρχουν  $q(x), r(x) \in R[x]$  ώστε  $g(x) = q(x)f(x) + r(x)$  με  $\deg r(x) < n$  ή  $r(x) = 0$ . Αφού  $g(a) = r(a)$ , τότε προκύπτει ότι

$$R[a] = \langle 1, a, \dots, a^{n-1} \rangle.$$

- (β) → (α) Άμεσο για  $M = R[a]$ .
- Υποθέτουμε ότι υπάρχει  $M = z_1R + \dots + z_rR$ , με  $z_i \in L$ , ώστε  $aM \subseteq M$ .
  - Τότε, υπάρχει πίνακας  $A = (a_{ij}) \in \mathbb{M}_n(R)$  (βλέπε Πρόταση 1) ώστε

$$A \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} = a \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} \Rightarrow (aI_n - A) \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} = 0.$$

Πολλαπλασιάζοντας την τελευταία σχέση με  $\text{adj}(aI_n - A)$ , τότε προκύπτει ότι

$$\det(aI_n - A) = a^n + \lambda_{n-1}a^{n-1} + \dots + \lambda_1a + \lambda_0 = 0.$$

□

**Πόρισμα 3.** Αν  $a_1, \dots, a_m$  ακέραια πάνω από το  $R$ , τότε το  $R[a_1, \dots, a_m]$  είναι ένα πεπερασμένα παραγόμενο  $R$ -πρότυπο.

**Παρατήρηση 12.** Έστω  $L$  σώμα και  $R \subseteq L$ . Το σύνολο

$$R' = \{a \in L \mid a \text{ είναι } R\text{-ακέραιος}\} \quad (4)$$

είναι υποδακτύλιος του  $L$ .

Απόδειξη. Έστω  $a, b \in R'$ . Από το Θεώρημα 6, προκύπτει ότι υπάρχουν  $M, N$  δύο πεπερασμένα παραγόμενα  $R$ -πρότυπα, τέτοια ώστε  $aM \subseteq M$  και  $bN \subseteq N$ . Δείξτε ότι  $(a - b)MN \subseteq MN$  και  $abMN \subseteq MN$ . □

**Ορισμός 20.** Έστω  $L$  σώμα και  $R \subseteq L$ . Ο δακτύλιος  $R'$  λέγεται **αλγεβρική θήκη** του  $R$  στο  $L$ . Στην περίπτωση που  $L = \text{Quot}(R)$  και  $R' = R$ , τότε λέμε ότι  $R$  είναι **ακέραια κλειστός**.

**Θέωρημα 7.** Έστω  $R$  ακέραια περιοχή και  $R \subseteq K \subseteq L$ , όπου  $K, L$  σώματα. Αν  $S$  είναι η ακέραια θήκη του  $R$  στο  $K$ , τότε η ακέραια θήκη του  $S$  και  $R$  στο  $L$  συμπίπτουν.

Απόδειξη. Έστω  $a \in L$  ώστε να είναι  $S$  - ακέραιο. Τότε, υπάρχουν  $a_0, \dots, a_{n-1} \in S$  ώστε

$$a^n + a_{n-1}a^{n-1} + \dots + a_1a + a_0 = 0$$

Το  $R$  - πρότυπο  $R_1 = R[a_0, \dots, a_{n-1}]$  είναι πεπερασμένα παραγόμενο. Αφού το  $R_1[a]$  είναι πεπερασμένα παραγόμενο  $R_1$  - πρότυπο, τότε  $R_1[a]$  είναι πεπερασμένα παραγόμενο  $R$  - πρότυπο. Συνεπώς,  $a$  είναι ακέραιο πάνω από το  $R$ . Το αντίστροφο έπεται άμεσα.  $\square$

**Θέωρημα 8.** Έστω  $R$  ακέραια περιοχή και  $R \subseteq L$  με  $L$  σώμα. Τότε,  $R'$  είναι ακέραια κλειστή.

**Πρόταση 5.** Κάθε δακτύλιος Dedekind είναι ακέραια κλειστός.

Απόδειξη. Έστω  $a \in R'$ . Συνεπώς, ο δακτύλιος  $R[a]$  είναι ένα π.π.  $R$  - πρότυπο, δηλαδή της μορφής  $R[a] = z_1R + \dots + z_nR$ .

- Τότε, υπάρχει  $\delta \in R$  ώστε  $\delta z_i \in R$ , άρα  $\delta \cdot R[a] \subseteq R$ . Άρα,  $R[a]$  είναι ιδεώδες του  $K$ .
- Αφού  $R[a]$  είναι δακτύλιος, τότε  $R[a]^2 = R[a] \cdot R[a] = R[a]$ , άρα έχουμε ότι

$$R[a] = R[a]^{-1} \cdot R[a]^2 = R[a]^{-1} \cdot R[a] = R$$

άρα έχουμε το ζητούμενο.  $\square$

Συνδυάζοντας τα θεωρήματα 5 και 8 έχουμε το ακόλουθο θεώρημα.

**Θέωρημα 9.** Έστω  $R$  δακτύλιος Dedekind. Τότε, ισχύουν τα εξής :

- Ο  $R$  είναι της Noether.
- Κάθε μη μηδενικό, πρώτο ιδεώδες του  $R$  είναι μέγιστο.
- Ο  $R$  είναι ακέραια κλειστός.

**Κίνητρο 4.** Είδαμε ότι αν  $R$  είναι Dedekind, τότε ικανοποιεί της ιδιότητες (α),(β),(γ). Σκοπός μας είναι να δείξουμε ότι οι ιδιότητες (α),(β),(γ) χαρακτηρίζουν τους δακτύλιους Dedekind.

**Λήμμα 4.** Έστω  $R$  δακτύλιος της Noether και  $0 \neq I$  ιδεώδες του  $R$  με  $I \neq R$ . Τότε, υπάρχουν πρώτα ιδεώδη  $\mathfrak{p}_1, \dots, \mathfrak{p}_k$  ώστε

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq I \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k.$$

*Απόδειξη.* Έστω

$\mathcal{X} = \{I \mid I \text{ μη μηδενικό, γνήσιο ιδεώδες του } R \text{ που δεν ικανοποιεί τη ζητούμενη συνθήκη}\}.$

- Έστω, προς άτοπο, ότι  $\mathcal{X} \neq \emptyset$ . Αφού  $R$  είναι της Noether, τότε η  $\mathcal{X}$  έχει μεγιστικό στοιχείο  $J$ .
- Αφού  $J \in \mathcal{X}$ , τότε  $J$  δεν είναι πρώτο. Συνεπώς, υπάρχουν  $a, b \notin J$  με  $ab \in J$ .
- Τότε, αν  $J_a = J + aR$  και  $J_b = J + bR$ , τότε  $J \subsetneq J_a$  και  $J \subsetneq J_b$ , άρα  $J_a, J_b \notin \mathcal{X}$ , συνεπώς ισχύει η ζητούμενη ιδιότητα.
- Από το γεγονός ότι  $J = J_a \cdot J_b$  καταλήξτε σε άτοπο.

□

## 5 Μάθημα 05

### 5.1 Χαρακτηρισμός Δακτυλίων Dedekind

**Λήμμα 5.** Έστω  $R$  περιοχή που ικανοποιεί τα  $(\alpha), (\beta), (\gamma)$  του Θεωρήματος 9. Τότε, κάθε μη μηδενικό, πρώτο ιδεώδες  $\mathfrak{p}$  είναι αντιστρέψιμο.

*Απόδειξη.* • Από το Λήμμα 4, για κάθε  $a \in \mathfrak{p} \setminus \{0\}$ , για το ιδεώδες  $aR$  ισχύει ότι υπάρχουν πρώτα  $\mathfrak{p}_1, \dots, \mathfrak{p}_k$  ώστε

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq aR \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k.$$

- Διαλέγουμε  $a \in \mathfrak{p} \setminus \{0\}$  για το οποίο υπάρχουν πρώτα  $\mathfrak{p}_1, \dots, \mathfrak{p}_{r_0}$  ώστε  $\mathfrak{p}_1 \cdots \mathfrak{p}_{r_0} \subseteq aR$  και  $r_0 \in \mathbb{N}$  να είναι το ελάχιστο δυνατό.
- Από το Λήμμα 3, χωρίς βλάβη της γενικότητας, υποθέτουμε ότι  $\mathfrak{p}_1 \subseteq \mathfrak{p}$  και από την ιδιότητα  $(\beta)$  προκύπτει ότι  $\mathfrak{p} = \mathfrak{p}_1$ .
- Από την επιλογή του  $a$  προκύπτει ότι  $\mathfrak{p}_2 \cdots \mathfrak{p}_{r_0} \not\subseteq aR$ , συνεπώς υπάρχει  $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_{r_0} \setminus aR$ . Άρα, έχουμε ότι  $b/a \notin R$ .
- Όμως, ισχύει ότι  $b\mathfrak{p} \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_{r_0} \subseteq aR$ , άρα έχουμε ότι  $(b/a)\mathfrak{p} \subseteq R$ . Από την τελευταία σχέση προκύπτει ότι  $b/a \in \mathfrak{p}^*$ . Αφού  $R \subseteq \mathfrak{p}^*$  και  $b/a \notin R$  συμπεραίνουμε ότι  $R \subsetneq \mathfrak{p}^*$ .
- Έχουμε ότι  $\mathfrak{p} = \mathfrak{p}R \subseteq \mathfrak{p} \cdot \mathfrak{p}^* \subseteq R$ , όπου  $\mathfrak{p} \cdot \mathfrak{p}^*$  είναι ιδεώδες του  $R$ .
- Από την ιδιότητα  $(\beta)$ , το  $\mathfrak{p}$  είναι μέγιστο, συνεπώς έχουμε ότι  $\mathfrak{p} \cdot \mathfrak{p}^* = \mathfrak{p}$  ή  $\mathfrak{p} \cdot \mathfrak{p}^* = R$ . Επομένως, για να δείξουμε το ζητούμενο, αρκεί να αποκλείσουμε την περίπτωση  $\mathfrak{p} \cdot \mathfrak{p}^* = \mathfrak{p}$ .
- Υποθέτουμε ότι  $\mathfrak{p} \cdot \mathfrak{p}^* = \mathfrak{p}$ . Από την τελευταία σχέση είναι άμεσο ότι  $\mathfrak{p} = (\mathfrak{p}^*)^n \mathfrak{p}$ , για κάθε  $n \in \mathbb{N}$ . Άρα, για κάθε  $x \in \mathfrak{p} \setminus \{0\}$  και  $y \in \mathfrak{p}^* \setminus R$  ισχύει ότι  $xy^n \in \mathfrak{p} \subseteq R$ .
- Από την τελευταία σχέση προκύπτει ότι για κάθε τέτοια επιλογή  $x, y$  έχουμε ότι  $xR[y] \subseteq R$ . Αφού  $R$  είναι της Noether και  $xR[y]$  ιδεώδες του προκύπτει ότι  $xR[y]$  είναι πεπερασμένα παραγόμενο  $R$  - πρότυπο. Μάλιστα από την τελευταία σχέση έχουμε ότι  $R[y]$  είναι ένα πεπερασμένα παραγόμενο  $R$  - πρότυπο.
- Από το Θεώρημα 6 προκύπτει ότι  $y$  είναι ακέραιο πάνω από τον  $R$  και αφού  $R$  είναι ακέραια κλειστός έχουμε ότι  $y \in R$ . Έτσι καταλήγουμε σε άτοπο. □

**Λήμμα 6.** Έστω  $R$  περιοχή που ικανοποιεί τα  $(\alpha), (\beta), (\gamma)$  του Θεωρήματος 9. Τότε, κάθε μη μηδενικό και γνήσιο ιδεώδες  $I$  του  $R$  γράφεται ως γινόμενο πρώτων ιδεωδών.

Απόδειξη. Θεωρούμε το σύνολο

$$\mathcal{A} = \{A \mid A \text{ μη μηδενικό, γνήσιο ιδεώδες του } R \text{ που δεν γράφεται σαν γινόμενο πρώτων}\}.$$

Θα υποθέσουμε ότι  $\mathcal{A} \neq \emptyset$  και θα καταλήξουμε σε άτοπο.

- Αν  $\mathcal{A} \neq \emptyset$  επιλέγουμε ότι  $A \in \mathcal{A}$  για το οποίο υπάρχουν  $\mathfrak{p}_1, \dots, \mathfrak{p}_{r_0}$  ώστε  $\mathfrak{p}_1 \cdots \mathfrak{p}_{r_0} \subseteq A$  και  $r_0 \in \mathbb{N}$  να είναι το ελάχιστο δυνατό.
- Αφού  $R$  είναι της Noether, γνωρίζουμε ότι υπάρχει  $\mathfrak{p}$  πρώτο ώστε  $A \subseteq \mathfrak{p}$ . Από το Λήμμα 3 και την ιδιότητα (β), χωρίς βλάβη της γενικότητας,  $\mathfrak{p} = \mathfrak{p}_1$ .
- Άρα, από το Λήμμα 5, έχουμε ότι

$$\mathfrak{p}_2 \cdots \mathfrak{p}_{r_0} \subseteq \mathfrak{p}^{-1} \cdot A \subseteq R$$

Το  $\mathfrak{p}^{-1} \cdot A$  είναι ιδεώδες του  $R$  και από την επιλογή του  $A$  έχουμε ότι  $\mathfrak{p}^{-1} \cdot A \notin \mathcal{A}$ . Άρα, το  $\mathfrak{p}^{-1} \cdot A$  γράφεται ως γινόμενο πρώτων, και κατά συνέπεια και το  $A$  γράφεται ως γινόμενο πρώτων και καταλήγουμε σε άτοπο.

□

**Πρόταση 6.** Έστω  $R$  περιοχή που ικανοποιεί τα (α),(β),(γ) του Θεωρήματος 9. Τότε, ο  $R$  είναι δακτύλιος Dedekind.

Απόδειξη. Έστω  $A$  μη μηδενικό ιδεώδες του  $K = \text{Quot}(R)$ . Τότε, υπάρχει  $\delta \in K \setminus \{0\}$  ώστε  $\delta A \subseteq R$ . Από το Λήμμα 6, υπάρχουν μη μηδενικά πρώτα ιδεώδες  $\mathfrak{p}_1, \dots, \mathfrak{p}_k$  ώστε  $\delta A = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ , δηλαδή  $A = (\delta^{-1}R) \mathfrak{p}_1 \cdots \mathfrak{p}_k$ . Από το Λήμμα 5 έχουμε ότι  $A$  είναι αντιστρέψιμο. □

**Πόρισμα 4.** Μια ακέραια περιοχή είναι δακτύλιος του Dedekind αν και μόνο αν ικανοποιεί τις συνθήκες (α),(β),(γ) του Θεωρήματος 9.

**Θέωρημα 10.** Αν  $R$  δακτύλιος του Dedekind, τότε κάθε μη-τετριμμένο ιδεώδες του γράφεται μονοσήμαντα ως γινόμενο πρώτων ιδεωδών, χωρίς να λαμβάνεται υπόψη η σειρά των πρώτων παραγόντων.



*Απόδειξη.* Από το Λήμμα 5 μένει να δείξουμε το μονοσήμαντο της γραφής. Έστω  $A \neq 0$  ιδεώδες του  $R$  και πρώτα ιδεώδες  $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$  τέτοια ώστε

$$A = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Από το Λήμμα 3 σε συνδυασμό με το γεγονός ότι κάθε μη μηδενικό πρώτο είναι μέγιστο ιδεώδες, χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι  $\mathfrak{p}_1 = \mathfrak{q}_1$ . Συνεχίζοντας την προηγούμενη διαδικασία συμπεραίνουμε ότι  $r = s$  και  $\mathfrak{p}_i = \mathfrak{q}_i$  (ενδεχομένως να χρειαστεί να αναδιατάξουμε τα  $\mathfrak{q}_i$ ).  $\square$

**Πόρισμα 5.** Η ομάδα των ιδεωδών του  $K = \text{Quot}(R)$ , όπου  $R$  δακτύλιος Dedekind, είναι ελεύθερη αβελιανή που παράγεται από τα πρώτα ιδεώδη του  $R$ .

*Απόδειξη.* • Έστω  $A$  ιδεώδες του  $K$ . Τότε, υπάρχει  $\delta = b/a \in K$  μη μηδενικό ώστε  $\delta A \subseteq R$ . Το  $\delta A$  είναι μη μηδενικό ιδεώδες του  $R$  και μάλιστα  $A = (\delta^{-1}R) \cdot \delta A$ . Από το Λήμμα 5 αρκεί να δείξουμε ότι  $\delta^{-1}R$  είναι γινόμενο δυνάμεων (όχι κατ' ανάγκη θετικών) πρώτων ιδεωδών.

- Έχουμε ότι  $\delta^{-1}R = (a/b)R$ , δηλαδή ισχύει ότι  $aR$  είναι γινόμενο πρώτων ιδεωδών και  $bR$  είναι γινόμενο πρώτων ιδεωδών. Αφού  $\delta^{-1}R = aR \cdot (b^{-1})R$  έχουμε το ζητούμενο.
- Από την μοναδικότητα της γραφής και από το γεγονός ότι  $\mathfrak{p}^n \neq R$ , για κάθε  $\mathfrak{p}$  πρώτο και  $n \in \mathbb{N}$  έπεται το ζητούμενο αποτέλεσμα.  $\square$

## 5.2 Διαιρετότητα Ιδεωδών

Από τώρα και στο εξής θα θεωρούμε ότι όλοι οι δακτύλιοι είναι δακτύλιοι Dedekind.

**Ορισμός 21.** Έστω  $R$  δακτύλιος και  $A, B$  ιδεώδη του  $K$ . Θα λέμε ότι το  $B$  **διαιρεί** το  $A$ , αν υπάρχει  $C \subseteq R$  ιδεώδες τέτοιο ώστε  $A = BC$ .

**Ορισμός 22.** Έστω  $R$  δακτύλιος και  $A, B$  ιδεώδη του  $K$ . Αν ένα ιδεώδες  $C$  διαιρεί τα  $A, B$  και για κάθε άλλο  $C'$  με  $C'|A$  και  $C'|B$  ισχύει ότι  $C'|C$ , τότε το  $C$  λέγεται **μέγιστος κοινός διαιρέτης** των  $A, B$  και συμβολίζεται με  $(A, B)$ .

**Παρατήρηση 13** (Υπαρξη και Μοναδικότητα Μέγιστου Κοινού Διαιρέτη). Από το Πόρισμα 5 προκύπτει ότι κάθε ιδεώδες  $A$  του  $K$  γράφεται στην μορφή

$$A = \prod_{\mathfrak{p} \text{ πρώτο}} \mathfrak{p}^{a(\mathfrak{p})}$$

όπου  $a(\mathfrak{p}) \geq 0$ . Άρα, αν  $A = \prod_{\mathfrak{p} \text{ πρώτο}} \mathfrak{p}^{a(\mathfrak{p})}$  και  $B = \prod_{\mathfrak{p} \text{ πρώτο}} \mathfrak{p}^{b(\mathfrak{p})}$ , τότε προκύπτει ότι

$$(A, B) = \prod_{\mathfrak{p} \text{ πρώτο}} \mathfrak{p}^{\min\{a(\mathfrak{p}), b(\mathfrak{p})\}} \quad (5)$$

και προφανώς είναι μονοσήμαντα ορισμένος.

**Ορισμός 23.** Με όμοιο τρόπο αν  $R$  δακτύλιος και  $A, B$  ιδεώδη του  $K$ , τότε το **ελάχιστο κοινό πολλαπλάσιο** των  $A, B$  ορίζεται να είναι

$$[A, B] = \prod_{\mathfrak{p} \text{ πρώτο}} \mathfrak{p}^{\max\{a(\mathfrak{p}), b(\mathfrak{p})\}} \quad (6)$$

**Πρόταση 7.** Έστω  $R$  δακτύλιος. Ισχύουν τα ακόλουθα.

- (α) Αν  $A, B$  ιδεώδη του  $K$ , τότε  $A \subseteq B$  αν και μόνο αν υπάρχει ιδεώδες  $C \subseteq R$  με  $A = B \cdot C$ .
- (β) Αν  $A$  ιδεώδες του  $K$ , τότε υπάρχει  $a \in K$  τέτοιο ώστε  $(aR) \cdot A^{-1} \subseteq R$ .
- (γ) Αν  $A, B$  σχετικά πρώτα ιδεώδη το  $R$  (δηλαδή  $(A, B) = R$ ), τότε  $A \cdot B = A \cap B$ .
- (δ) Αν  $A, B$  ιδεώδη το  $R$  (δηλαδή  $(A, B) = R$ ), τότε  $(A, B) = \langle A, B \rangle = A + B$ .

*Απόδειξη.* (α) Η μια κατεύθυνση είναι προφανής. Για την αντιστροφή, παρατηρήστε ότι αν  $C = AB^{-1} \subseteq R$ , τότε  $A = CB$ .

(β) Έστω  $a \neq 0$  στο  $A$ . Τότε,  $aR \subseteq A$  και από το (α) υπάρχει  $C \subseteq R$  ιδεώδες ώστε  $aR = CA$ . Συνεπώς, έχουμε ότι  $(aR) \cdot A^{-1} = C \subseteq R$ .

(γ) Αρκεί να δείξουμε ότι  $A \cap B \subseteq A \cdot B$ . Έχουμε ότι  $A \cap B \subseteq A$  και  $A \cap B \subseteq B$ . Από το (α), προκύπτει ότι  $A|A \cap B$  και  $B|A \cap B$  και αφού  $A, B$  είναι σχετικά πρώτα έπεται ότι  $A \cdot B = [A, B]|A \cap B$ . Από το (α) έχουμε το ζητούμενο.

(δ) Αφού  $A, B \subseteq A+B$ , τότε προκύπτει ότι  $A+B|A$  και  $A+B|B$ . Συνεπώς,  $(A, B) \subseteq A+B$ . Αντίστροφα, από το (α), έχουμε ότι  $A \subseteq (A, B)$  και  $B \subseteq (A, B)$ . Επομένως, ισχύει ότι  $A + B \subseteq (A, B)$ .

□

### 5.3 Το Θεμελιώδες Θεώρημα

**Ορισμός 24 (F.N.).** Ένας δακτύλιος  $R$  θα λέμε ότι ικανοποιεί την **συνθήκη πεπερασμένης νόρμας** αν για κάθε μη μηδενικό ιδεώδες  $A \subseteq R$  ισχύει ότι  $R/A$  είναι πεπερασμένος.

**Παράδειγμα 13.** Το  $\mathbb{Z}$  ικανοποιεί την συνθήκη πεπερασμένης νόρμας, αφού κάθε ιδεώδες του είναι της μορφής  $I = n\mathbb{Z}$  και  $R/I = \mathbb{Z}_n$  πεπερασμένος.

**Παράδειγμα 14.** Ο δακτύλιος  $\mathbb{C}[x]$  δεν ικανοποιεί την συνθήκη πεπερασμένης νόρμας αφού για  $I = \langle x \rangle$ , τότε έχουμε ότι  $\mathbb{C}[x]/I \cong \mathbb{C}$ .

**Θεώρημα 11.** Έστω  $R$  δακτύλιος Dedekind,  $K = \text{Quot}(R)$ . Έστω  $L/K$  πεπερασμένη και διαχωρίσιμη επέκταση σωμάτων και  $S$  η ακέραια θήκη του  $R$  στο  $L$ . Ισχύουν τα ακόλουθα.

- (α) Το  $S$  είναι δακτύλιος Dedekind.
- (β) Αν ο  $R$  ικανοποιεί την F.N. τότε και ο  $S$  ικανοποιεί την F.N..

Για να αποδείξουμε το προηγούμενο Θεμελιώδες Θεώρημα, για το πρώτο σκέλος του, θα δείξουμε ότι ο  $S$  ικανοποιεί τα (α),(β),(γ) του Θεωρήματος 9. Για να πραγματοποιηθεί αυτό θα διασπάσουμε την απόδειξη σε δύο σκέλη.

**Πρόταση 8.** Ο  $S$  ικανοποιεί τα (α),(γ) του Θεωρήματος 9, δηλαδή είναι της Noether και ακέραια κλειστός.

**Απόδειξη.** • Από το **Θεώρημα Πρωτάρχικου Στοιχείου**, αφού  $L/K$  είναι πεπερασμένη και διαχωρίσιμη, τότε υπάρχει  $\vartheta \in L$  ώστε  $L = K(\vartheta)$ . Μάλιστα, αφού  $K = \text{Quot}(R)$ , μπορούμε να υποθέσουμε ότι  $\vartheta \in S$ .

- Σκοπός μας είναι να δείξουμε ότι υπάρχει  $c \in K$  ώστε  $S \subseteq cR[\vartheta]$ . Στην περίπτωση αυτή μπορούμε να δείξουμε ότι  $S$  είναι της Noether και ακέραια κλειστός.

– Πράγματι, θεωρούμε τον επιμορφισμό  $R$  - προτύπων

$$\varphi: \underbrace{R \oplus \cdots \oplus R}_{n \text{ φορές}} \rightarrow cR[\vartheta], \quad (r_0, \dots, r_{n-1}) \mapsto r_{n-1}\vartheta^{n-1} + \cdots + r_1\vartheta + r_0.$$

– Τότε,  $cR[\vartheta]$  είναι  $R$  - πρότυπο της Noether, συνεπώς  $S \subseteq cR[\vartheta]$  είναι  $R$  - πρότυπο της Noether. Από αυτό το γεγονός δείξτε ότι κάθε ιδεώδες του  $S$  είναι π.π.

– Τέλος, από το Θεώρημα 7 έχουμε ότι  $S$  είναι ακέραια κλειστός.

- Αν  $x \in L$  θα συμβολίζουμε με  $x^{(i)}$  το  $i$ -**συζυγές** του  $x$ . Αν  $\bar{K}$  η αλγεβρική θήκη του  $K$  και  $\sigma \in \text{Gal}(\bar{K}/K)$ , όπου  $\text{Gal}(\bar{K}/K)$  η **ομάδα Galois**

$$\text{Gal}(\bar{K}/K) = \{ \sigma \in \text{Aut}(\bar{K}) \mid \sigma(x) = x, \text{ για κάθε } x \in K \}$$

τότε έχουμε ότι  $\sigma(x) = x^{(i)}$ , για κάποιο  $i$ .

- Από την παραπάνω παρατήρηση προκύπτει ότι αν  $\alpha \in S$  με  $\alpha = \sum_{k=0}^{n-1} a_k \vartheta^k$ , τότε προκύπτει ότι  $\alpha^{(i)} = \sum_{k=0}^{n-1} a_k (\vartheta^{(i)})^k$ .

- Τότε, προκύπτει  $n \times n$  γραμμικό σύστημα (με αγνώστους  $a_k$ ) της μορφής :

$$\begin{aligned} \alpha &= \alpha^{(0)} = a_0 + a_1 \vartheta^{(1)} + \dots + a_{n-1} (\vartheta^{(1)})^{n-1} \\ &\vdots \\ \alpha^{(n-1)} &= a_0 + a_1 \vartheta^{(n-1)} + \dots + a_{n-1} (\vartheta^{(n-1)})^{n-1} \end{aligned}$$

Η ορίζουσα το γραμμικού συστήματος είναι μια ορίζουσα Vandermode :

$$D = \det \begin{pmatrix} 1 & \vartheta^{(0)} & (\vartheta^{(0)})^2 & \dots & (\vartheta^{(0)})^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \vartheta^{(n-1)} & (\vartheta^{(n-1)})^2 & \dots & (\vartheta^{(n-1)})^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (\vartheta^{(i)} - \vartheta^{(j)}) \neq 0$$

όπου  $D \neq 0$ , γιατί  $L/K$  είναι διαχωρίσιμη. Από την μέθοδο Cramer έχουμε ότι

$$a_k = \frac{A_k}{D}, \quad A_k, D \in S, \text{ για κάθε } k = 0, 1, \dots, n-1.$$

- Αφού  $L = K(\vartheta)$ , τότε θεωρούμε την  $N = K[\vartheta^{(0)}, \dots, \vartheta^{(n-1)}]$  την **κανονική θήκη** του  $L$  πάνω από το  $K$ . Συνεπώς, η ομάδα  $\text{Gal}(N/K)$  αποτελείται από τις μεταθέσεις του  $[n] = \{0, \dots, n-1\}$ , άρα προκύπτει ότι  $\sigma(D) = \pm D$ , για κάθε  $\sigma \in \text{Gal}(N/K)$ .

- Αφού η ποσότητα  $D^2$  μένει αναλλοίωτη από την δράση της  $\text{Gal}(N/K)$ , τότε  $D^2 \in \text{Fix}[\text{Gal}(N/K)] = K$ . Αφού,  $R$  είναι ακέραια κλειστός, τότε  $D^2 \in S \cap K = R$ .

- Συνεπώς, γράφοντας

$$K \ni a_k = \frac{A_k D}{D^2}$$

και από το γεγονός ότι  $D^2 \in R$  έχουμε ότι  $K \ni a_k \cdot D^2 = A_k \cdot D \in S \cap K = R$ .

- Συνεπώς, για το δοθέν  $\alpha \in S$  προκύπτει ότι

$$\alpha = \sum_{k=0}^{n-1} a_k \vartheta^k = \sum_{k=0}^{n-1} \frac{A_k \cdot D}{D^2} \cdot \vartheta^k = \frac{1}{D^2} \cdot \sum_{k=0}^{n-1} A_k \cdot D \cdot \vartheta^k \in cR[\vartheta]$$

όπου  $c = 1/D^2$ . Έτσι προκύπτει το ζητούμενο αποτέλεσμα. □

## 6 Μάθημα 06

### 6.1 Η Συνέχεια της Απόδειξης

**Λήμμα 7.** Με βάση τις υποθέσεις του Θεωρήματος 11 ισχύουν τα εξής.

- (α) Αν  $\mathfrak{p}$  πρώτο ιδεώδες του  $S$ , τότε  $\mathfrak{p}' = \mathfrak{p} \cap R$  είναι πρώτο ιδεώδες του  $R$ .
- (β) Έστω  $\mathfrak{p}_1, \mathfrak{p}_2$  πρώτα ιδεώδη του  $S$  με  $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ . Αν  $\mathfrak{p}'_1 = \mathfrak{p}'_2$ , τότε  $\mathfrak{p}_1 = \mathfrak{p}_2$ .

*Απόδειξη.* (α) Αν  $\varphi$  είναι η σύνθεση  $R \hookrightarrow S \xrightarrow{\pi} S/\mathfrak{p}$ , τότε έχουμε ότι  $\ker \varphi = \mathfrak{p}'$ . Τώρα, αφού  $R/\mathfrak{p}' \cong \text{Im} \varphi$  και  $S/\mathfrak{p}$  είναι περιοχή, τότε  $R/\mathfrak{p}'$  είναι περιοχή.

- (β) • Θεωρούμε, προς άτοπο, ότι  $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ . Τότε, υπάρχει  $x \in \mathfrak{p}_2 \setminus \mathfrak{p}_1$ . Αφού  $x \in S$ , τότε υπάρχουν  $a_0, \dots, a_{n-1} \in R$  ώστε

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

- Αν ίσχυε ότι  $a_0, \dots, a_{n-1} \in \mathfrak{p}'_1$ , τότε  $x^n \in \mathfrak{p}_1$ , συνεπώς  $x \in \mathfrak{p}_1$ . Επομένως, διαλέγουμε το μέγιστο  $j$  ώστε  $a_j \notin \mathfrak{p}'_1$ .
- Τότε, έχουμε ότι

$$x^j (x^{n-j} + a_{n-1}x^{n-j-1} + \dots + a_{j+1}x + a_j) = -a_{j-1}x^{j-1} - \dots - a_0 \in \mathfrak{p}_1$$

Αφού  $x \notin \mathfrak{p}_1$ , τότε έχουμε ότι  $x^{n-j} + a_{n-1}x^{n-j-1} + \dots + a_{j+1}x + a_j \in \mathfrak{p}_1$ . Αφού,  $x \in \mathfrak{p}_2$ , τότε έχουμε ότι  $a_j \in \mathfrak{p}'_2 = \mathfrak{p}'_1$  και καταλήγουμε σε άτοπο. □

*Απόδειξη του Θεωρήματος 11.* (α) Έχουμε ήδη δείξει ότι ο  $S$  ικανοποιεί τις συνθήκες (α) και (γ). Θα δείξουμε ότι κάθε μη μηδενικό πρώτο ιδεώδες του  $S$  είναι μέγιστο.

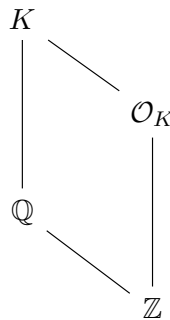
- Έστω  $\mathfrak{p}_1$  μη μηδενικό, πρώτο ιδεώδες του  $S$ . Αφού  $S$  της Noether, τότε υπάρχει μέγιστο  $\mathfrak{p}_2$  τέτοιο ώστε  $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ . Θα δείξουμε ότι  $\mathfrak{p}_1 = \mathfrak{p}_2$ .
  - Τώρα, έχουμε ότι  $\mathfrak{p}'_1 \subseteq \mathfrak{p}'_2$ . Από το Λήμμα 7 και από το γεγονός ότι  $R$  είναι Dedekind έχουμε το ζητούμενο.
- (β) Υποθέτουμε ότι  $R$  ικανοποιεί την συνθήκη F.N..

i. Έστω  $\mathfrak{p}$  μη μηδενικό, πρώτο ιδεώδες (άρα και μέγιστο) του  $S$ . Θα δείξουμε ότι  $S/\mathfrak{p}$  είναι πεπερασμένος. Αφού  $S \subseteq cR[\vartheta]$ , τότε η επέκταση σωμάτων  $R/\mathfrak{p}' \subseteq S/\mathfrak{p}$  είναι πεπερασμένη και αφού  $R/\mathfrak{p}'$  είναι πεπερασμένος έχουμε το ζητούμενο.

- ii. Αν  $A$  μη μηδενικό ιδεώδες του  $S$ , τότε αφού  $S$  είναι Dedekind από το 10 και από Κινέζικο Θεώρημα Υπολοίπων προκύπτει το ζητούμενο. (Εξετάστε την περίπτωση  $S/\mathfrak{p}^i$ )

□

**Πόρισμα 6.** Έστω η επέκταση  $\mathbb{Z} \subseteq \mathbb{Q}$ . Ο  $\mathbb{Z}$  είναι δακτύλιος του Dedekind. Έστω  $\mathcal{O}_K$  ο δακτύλιος των ακέραιων αριθμών του  $K$ . Ο  $\mathcal{O}_K$  δεν είναι απαραίτητα δακτύλιος μοναδικής παραγοντοποίησης, όμως με βάση το παραπάνω θεώρημα είναι δακτύλιος Dedekind, συνεπώς κάθε ιδεώδες του γράφεται μονοσήμαντα ως γινόμενο πρώτων ιδεωδών.



Επίσης, αφού ο  $\mathbb{Z}$  ικανοποιεί την F.N., τότε και  $\mathcal{O}_K$  ικανοποιεί την F.N..

**Παράδειγμα 15.** Ο δακτύλιος  $\mathbb{C}[x]$  είναι Dedekind, αλλά δεν ικανοποιεί την F.N., αφού  $\mathbb{C}[x]/(x-1) \cong \mathbb{C}$ .

## 6.2 Νόρμα, Βάση Ακεραιότητας και Διακρίνουσα

Έστω  $K \subseteq L$  σώματα πεπερασμένη, όπου  $L = K(\vartheta)$  πρωταρχικό στοιχείο της επέκτασης.

- Αφού  $\vartheta$  πρωταρχικό, τότε υπάρχει  $\text{Irr}(\vartheta, K) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ . Μέσω του ομομορφισμού εκτίμησης  $\varphi_\vartheta: K[x] \rightarrow K[\vartheta]$  με  $f(x) \mapsto f(\vartheta)$  μπορούμε να δείξουμε ότι  $K[x]/\langle \text{Irr}(\vartheta, K) \rangle \cong K[\vartheta]$ , από όπου προκύπτει ότι  $K(\vartheta) = K[\vartheta]$ .
- Τότε,  $B = \{1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}\}$  είναι βάση της επέκτασης με βαθμό επέκτασης

$$[L : K] = n = \dim_K L = \deg \text{Irr}(\vartheta, K).$$

- Έστω  $a \in L$ . Θεωρούμε την απεικόνιση  $L_a: L \rightarrow L$  με  $L_a(x) = ax$ . Τότε, για κάθε  $i = 0, \dots, n-1$  υπάρχουν  $a_{j,i} \in K$  με  $j = 0, \dots, n-1$  τέτοια ώστε

$$a\vartheta^i = \sum_{j=0}^{n-1} a_{j,i}\vartheta^j$$

Έστω  $A(a) = (a_{j,i}) \in \mathbb{M}_n(K)$  ο πίνακας της  $L_a$  ως προς την βάση  $B$ . Έτσι ορίζεται απεικόνιση  $A: L \rightarrow \mathbb{M}_n(K)$  με τις ακόλουθες ιδιότητες :

- (α)  $A(a + b) = A(a) + A(b)$  , για κάθε  $a, b \in L$
- (β)  $A(\lambda a) = \lambda A(a)$  , για κάθε  $a \in L$ , και  $\lambda \in K$
- (γ)  $A(ab) = A(a) \cdot A(b)$  , για κάθε  $a, b \in L$ .
- (δ)  $A(1_L) = I_n$ .

Από τις παραπάνω ιδιότητες συμπεραίνουμε ότι η  $A$  είναι ομομορφισμός  $K$  - αλγεβρών.

**Ορισμός 25.** Ορίζουμε ως **ίχνος** του  $a \in L$  ως προς την επέκταση  $L/K$  το  $\text{Tr}_{L/K}(a) = \text{Tr}(A(a))$ . Ορίζουμε ως **νόρμα** του  $a \in L$  ως προς την επέκταση  $L/K$  το  $N_{L/K}(a) = \det(A(a))$ . Το **χαρακτηριστικό πολυώνυμο** του  $a$  ως προς την επέκταση  $L/K$  είναι το  $\chi_{a,L/K}(x) = \det(xI_n - A(a))$

**Πρόταση 9.** Έστω  $a \in L$  και  $\chi_{a,L/K}(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$ . Τότε ισχύουν τα ακόλουθα.

- (α)  $N_{L/K}(a) = (-1)^n c_0$  και  $\text{Tr}_{L/K}(a) = -c_{n-1}$
- (β) Το  $a$  είναι ρίζα του  $\chi_{a,L/K}(x)$ .
- (γ) Το  $\chi_{a,L/K}(x)$  (και συνεπώς και η  $\text{norm}$  καθώς και το  $\text{ίχνος}$ ) είναι ανεξάρτητα της επιλογής της βάσης.
- (δ)  $\text{Tr}_{L/K}(\lambda a + \mu b) = \lambda \cdot \text{Tr}_{L/K}(a) + \mu \cdot \text{Tr}_{L/K}(b)$ , για κάθε  $\lambda, \mu \in K$
- (ε)  $N_{L/K}(ab) = N_{L/K}(a) \cdot N_{L/K}(b)$  και  $N_{L/K}(a) = 0$  αν και μόνο αν  $a = 0$ . Συνεπώς, η απεικόνιση  $N_{L/K}: L \setminus \{0\} \rightarrow K \setminus \{0\}$  είναι μονομορφισμός ομάδων.

*Απόδειξη.* (α) Άμεσο, αφού

$$c_0 = \chi_{a,L/K}(0) = \det[-A(a)] = (-1)^n \det[A(a)] = N_{L/K}(a)$$

και

$$\chi_{a,L/K}(x) = x^n - \left( \sum_{i=0}^{n-1} a_{ii} \right) x^{n-1} + h(x), \quad \deg h(x) \leq n-2$$

- (β) Αν θεωρήσουμε την βάση  $B = \{1, \theta, \theta^2, \dots, \theta^{n-1}\}$  ειδικωμένη ως στήλη, τότε

$$aB = Ba = B \cdot A(a) \Rightarrow B \cdot (a \cdot I_n - A(a)) = 0$$

Αφού το παραπάνω ομογενές σύστημα έχει μη τετριμμένη λύση έχουμε το ζητούμενο.

- (γ) Γνωστό από γραμμική άλγεβρα.
- (δ) Η γραμμικότητα του ίχνους προκύπτει από τη γραμμικότητα του  $A$ .
- (ε) Η πολλαπλασιαστικότητα της νόρμας προκύπτει από την πολλαπλασιαστικότητα του  $A$  και της ορίζουσας.

□

**Παρατήρηση 14.** • Έστω  $a \in L$  και  $p(x) = \text{Irr}(a, K)$  το ελάχιστο πολυώνυμο του  $a$  πάνω από  $K$ . Ορίζουμε τον ομομορφισμό εκτίμησης

$$\varphi_a: K[x] \rightarrow K[a], \quad f(x) \mapsto f(a)$$

ο οποίος είναι επιμορφισμός δακτυλίων. Παρατηρήστε ότι  $\ker \varphi_a = \langle p(x) \rangle$ . Αφού  $\chi_{a,L/K}(x)$  έχει ρίζα το  $a$  από την Πρόταση 9 έχουμε ότι  $p(x) | \chi_{a,L/K}(x)$ .

- Αν  $a$  είναι πρωταρχικό στοιχείο, τότε  $\deg p(x) = n$ , συνεπώς με επιχείρημα βαθμών και αφού  $p(x), \chi_{a,L/K}(x)$  είναι μονικά, τότε  $p(x) = \chi_{a,L/K}(x)$ .
- Αφού  $\text{Tr}_{1_L, L/K} = \text{Tr}(I_n) = n \neq 0$ , τότε συμπεραίνουμε ότι  $\text{Tr}(L) \neq 0$ .

**Πρόταση 10.** Έστω  $K \subseteq L$  με  $L = K(a)$  πεπερασμένη επέκταση και  $p(x) = \text{Irr}(a, K)$ . Ισχύουν τα ακόλουθα.

- (α)  $\chi_{a,L/K}(x) = p(x)^{[L:K(a)]}$
- (β)  $N_{L/K}(a) = (N_{K(a)/K})^{[L:K(a)]}$
- (γ)  $\text{Tr}_{L/K}(a) = [L : K(a)] \cdot \text{Tr}_{K(a)/K}(a)$

*Απόδειξη.* Έστω  $[L : K] = n$ ,  $[L : K(a)] = m$  και  $[K(a) : K] = \ell$  οι βαθμοί των επεκτάσεων. Από τον κανόνα των πύργων ισχύει ότι  $n = m \cdot \ell$ .

- Αν  $\{\gamma_1, \dots, \gamma_m\}$  μια βάση του  $L/K(a)$  και  $\underline{B} = \{\beta_1, \dots, \beta_\ell\}$  μια βάση του  $K(a)/K$ , τότε έχουμε ότι

$$B = \{\gamma_i \beta_j \mid i = 1, \dots, m \ j = 1, \dots, \ell\} = \{\gamma_1 \underline{B}, \dots, \gamma_m \underline{B}\}$$

Η τελευταία σχέση προκύπτει θεωρώντας το  $\underline{B}$  σαν στήλη.

- Θέλουμε να υπολογίσουμε τον  $A_{L/K}(a)$  ως προς την βάση  $B$ , συνεπώς,

$$aB = \{\gamma_1 \underline{B}a, \dots, \gamma_m \underline{B}a\} = \{\gamma_1 A_{K(a)/K}(a), \dots, \gamma_m A_{K(a)/K}(a)\}.$$



- Συνεπώς, ο πίνακας  $A_{L/K}(a)$  γράφεται στην μορφή

$$A_{L/K}(a) = \begin{pmatrix} A_{K(a)/K}(a) & \mathbb{O} & \mathbb{O} \\ & \ddots & \\ & \mathbb{O} & \mathbb{O} & A_{K(a)/K}(a) \end{pmatrix}$$

δηλαδή ένας πίνακας σε block - μορφή. Από την τελευταία σχέση προκύπτει άμεσα το ζητούμενο. □

**Παράδειγμα 16.** Έστω  $f(x) = x^3 - x^2 - 2x - 8 \in \mathbb{Q}[x]$  και  $\vartheta$  μια ρίζα του.

- Είναι άμεσο ότι  $f(x)$  είναι ανάγωγο στο  $\mathbb{Q}[x]$ , αφού είναι βαθμού 3 και δεν έχει ρίζες στο  $\mathbb{Q}$ .
- Συνεπώς,  $\text{Irr}(\vartheta, \mathbb{Q}) = f(x)$  και μάλιστα  $B = \{1, \vartheta, \vartheta^2\}$  είναι μια βάση του  $L = \mathbb{Q}(\vartheta)/\mathbb{Q}$ .
- Θεωρούμε το  $a = \frac{\vartheta^2 - 2}{2}$ . Θα υπολογίσουμε  $\chi_{a, K/\mathbb{Q}}(x)$ ,  $N_{L/\mathbb{Q}}(a)$  και  $\text{Tr}_{L/\mathbb{Q}}(a)$ . Έχουμε ότι

$$\begin{aligned} a \cdot \vartheta &= \vartheta + 4 \\ a \cdot \vartheta^2 &= \vartheta^2 + 4\vartheta \end{aligned}$$

όπου για να εξάγουμε τις τελευταίες σχέσεις εφαρμόστε ευκλείδεια διαίρεση και υπολογίστε στο  $\vartheta$ . Άρα, προκύπτει ότι

$$A_{L/\mathbb{Q}}(a) = \begin{pmatrix} 0 & 4 & 0 \\ -1/2 & 1 & 4 \\ 1/2 & 0 & 1 \end{pmatrix}.$$

Έτσι υπολογίζοντας έχουμε ότι  $\chi_a(x) = x^3 - 2x^2 + 3x + 10$ ,  $N(a) = 10$  και  $\text{Tr}(a) = 2$ .

## 7 Μάθημα 07

### 7.1 Norm, ίχνος και εμφυτεύσεις

**Παρατήρηση 15.** Έστω  $K \subseteq L \subseteq M$  επεκτάσεις αλγεβρικών σωμάτων.

- Αφού τα παραπάνω σώματα έχουν χαρακτηριστική 0, τότε οι παραπάνω επεκτάσεις είναι διαχωρίσιμες και μάλιστα απλές με  $L = K(\vartheta)$  και  $M = L(\eta) = K(\vartheta, \eta)$ .
- Αν  $[L : K] = n$  και  $[M : L] = m$  συμβολίζουμε με  $\vartheta = \vartheta_1, \dots, \vartheta_n$  και  $\eta = \eta_1, \dots, \eta_m$  τα συζυγή στοιχεία των  $\vartheta$  και  $\eta$  αντίστοιχα.

- Αν  $N = K(\vartheta_1, \dots, \vartheta_n, \eta_1, \dots, \eta_m)$ , τότε αν  $\sigma: L \rightarrow N$  ένας  $K$  - μονομορφισμός, τότε είναι εύκολο να δειχθεί ότι  $\sigma(\vartheta) \in \{\vartheta_1, \dots, \vartheta_n\}$ . Αφού  $\sigma$  καθορίζεται πλήρως από την τιμή του  $\vartheta$  είναι άμεσο ότι υπάρχουν ακριβώς  $n$  το πλήθος  $K$  - εμφυτεύσεις του  $L$  τις οποίες συμβολίζουμε με  $\sigma_i$  και για τις οποίες ισχύει  $\sigma_i(\vartheta) = \vartheta_i$ .
- Με ακριβώς αντίστοιχα επιχειρήματα κάθε  $\sigma_i: L \rightarrow N$  μπορεί να επεκταθεί σε ένα  $K$  - μονομορφισμό  $\sigma_{i,j}: M \rightarrow N$ , όπου  $\sigma_{i,j} = \vartheta_i$  και  $\sigma_{i,j}(\eta) = \eta_j$ .
- Αφού  $[M : K] = mn$  το πλήθος των  $K$  - μονομορφισμών  $M \rightarrow N$  είναι ίσο με  $mn$  και συνεπώς από τις παραπάνω παρατηρήσεις είναι ακριβώς οι  $\sigma_{i,j}$ .

**Πρόταση 11.** Έστω  $K \subseteq L$  επέκταση αλγεβρικών σωμάτων αριθμών με  $[L : K] = n$ . Αν  $a \in L$ , τότε ισχύει ότι

$$N_{L/K}(a) = \prod_{i=1}^n \sigma_i(a) \quad \text{και} \quad \text{Tr}_{L/K}(a) = \sum_{i=1}^n \sigma_i(a) \quad (7)$$

όπου  $\sigma_i: L \rightarrow N$  η  $i$  - εμφύτευση του  $L$  στην κανονική θήκη  $N$ .

*Απόδειξη.* Έστω  $a \in L$ . Διακρίνουμε περιπτώσεις.

- (α) Υποθέτουμε ότι  $a$  είναι πρωταρχικό στοιχείο, δηλαδή  $L = K(a)$ . Στην περίπτωση αυτή  $\deg p(x) = n$ , όπου  $p(x) = \text{Irr}(a, K)$ . Τότε, ισχύει ότι

$$x^n - \text{Tr}_{L/K}(a)x^{n-1} + \dots + (-1)^n N_{L/K}(a) = \chi_{L/K,a}(x) = p(x) = \prod_{i=1}^n (x - \sigma_i(a)).$$

Από την παραπάνω σχέση έχουμε το ζητούμενο.

- (β) Αν  $a \in L$  όχι κατ' ανάγκη πρωταρχικό θεωρούμε τις επεκτάσεις  $K \subseteq K(a) \subseteq L$ .

- Από την Πρόταση 10, αν  $[L : K(a)] = m$  και  $[K(a) : K] = n$ , τότε προκύπτει ότι

$$N_{L/K}(a) = (N_{K(a)/K}(a))^m = \prod_{i=1}^n \sigma_i(a)^m$$

όπου η δεύτερη ισότητα προκύπτει από το (α) σκέλος της απόδειξης με  $\sigma_i: K(a) \rightarrow N$ , όπου  $N$  κάποια κανονική θήκη που περιέχει το  $L$ .

- Από την Παρατήρηση 15, υπάρχουν ακριβώς  $m$  επεκτάσεις  $\sigma_{i,j}$  των  $\sigma_i$ . Οι  $\sigma_{i,j}$  είναι ακριβώς οι  $K$  - μονομορφισμοί  $L \rightarrow N$  και μάλιστα  $\sigma_{i,j}(a) = \sigma_i(a)$ , για κάθε  $j = 1, \dots, m$ . Από την τελευταία σχέση προκύπτει το ζητούμενο. Ομοίως, προκύπτει το ζητούμενο για το  $\text{Tr}_{L/K}(a)$ .

□

**Παρατήρηση 16.** Έστω  $K \subseteq L$  επέκταση αλγεβρικών σωμάτων αριθμών με  $[L : K] = n$  και  $L = K(a)$ . Γνωρίζουμε ότι για κάθε  $a \in L$ , τότε  $N_{L/K}(a), \text{Tr}_{L/K}(a) \in K$ .

- Έστω  $R, S$  οι ακέραιες θήκες των  $K, L$  πάνω από το  $\mathbb{Z}$ . Θα δείξουμε ότι αν  $a \in S$ , τότε  $N_{L/K}(a), \text{Tr}_{L/K}(a) \in R$ .
- Θεωρούμε τις  $K$  - εμφυτεύσεις  $\sigma_i : L \rightarrow N$ . Τότε, από την Πρόταση 11, έχουμε ότι  $N_{L/K}(a) = \prod_{i=1}^n \sigma_i(a)$  και  $\text{Tr}_{L/K}(a) = \sum_{i=1}^n \sigma_i(a)$ .
- Αφού  $a$  είναι ακέραιος αλγεβρικός, τότε υπάρχει  $f(x) \in \mathbb{Z}[x]$  με  $f(a) = 0$ . Είναι εύκολο να δείξει κανείς ότι  $\sigma_i(a)$  είναι επίσης ρίζες του  $f(x)$ . Συνεπώς,  $\sigma_i(a)$  είναι  $R$  - ακέραιοι αλγεβρικοί αριθμοί του  $N$ .
- Συνεπώς,  $N_{L/K}(a)$  και  $\text{Tr}_{L/K}(a)$  είναι  $R$  - ακέραιοι αλγεβρικοί στο  $N$  ως άθροισμα και γινόμενο τέτοιων αντίστοιχα. Αφού  $N_{L/K}(a), \text{Tr}_{L/K}(a) \in K$  και χρησιμοποιώντας το Θεώρημα 7 για την επέκταση  $R \subseteq K \subseteq N$  έχουμε ότι  $N_{L/K}(a), \text{Tr}_{L/K}(a) \in R$ .

**Πρόταση 12.** Έστω  $K \subseteq L \subseteq M$  επεκτάσεις αλγεβρικών σωμάτων αριθμών. Τότε, για κάθε  $a \in M$  ισχύει ότι

$$N_{L/K}(N_{M/L}(a)) = N_{M/K}(a) \quad \text{και} \quad \text{Tr}_{L/K}(\text{Tr}_{M/L}(a)) = \text{Tr}_{M/K}(a).$$

*Απόδειξη.* Από την Παρατήρηση 15 έχουμε ότι  $N_{M/L}(a) = \prod_{i=1}^n \sigma_i(a)$ . Τώρα, αν  $\tau_j : L \rightarrow N$  οι  $K$  - μονομορφισμοί του  $L$  στην  $N$  έχουμε ότι

$$N_{L/K}(N_{M/L}(a)) = \prod_{j=1}^m \tau_j \left( \prod_{i=1}^n \sigma_i(a) \right)$$

- Παρότι  $\tau_j$  είναι πολλαπλασιαστικές δεν μπορούμε να γράψουμε απήφιστα την σχέση

$$\tau_j \left( \prod_{i=1}^n \sigma_i(a) \right) = \prod_{i=1}^n \tau_j \circ \sigma_i(a)$$

αφού  $\sigma_i(a)$  βρίσκονται στο  $N$  και όχι κατ' ανάγκη στο  $L$ .

- Παρόλα αυτά κάθε  $\tau_j$  μπορεί να επεκταθεί σε ένα  $K$  - αυτομορφισμό της  $N$  τον οποίο θα συμβολίζουμε πάλι με  $\tau_j$ . Με τις παραπάνω παρατηρήσεις, η παραπάνω σχέση μπορεί να γραφτεί ως εξής :

$$N_{L/K}(N_{M/L}(a)) = \prod_{i,j=1}^{n,m} \tau_j \circ \sigma_i(a)$$

όπου

$$M \xrightarrow{\sigma_i} N \xrightarrow{\tau_j} N$$

είναι μια  $K$  - εμφύτευση του  $M$  στο  $N$ . Είναι εύκολο ναδειχθεί ότι οι  $\tau_j \circ \sigma_i$  είναι διακεκριμένες, συνεπώς είναι ακριβώς οι  $K$  - εμφύτευσεις του  $M$  στο  $N$ . Από την Πρόταση 11 έχουμε το ζητούμενο. Ομοίως, δείχνουμε το ζητούμενο στην περίπτωση του  $\text{Tr}$ .

□

## 7.2 Διακρίνουσα $n$ - άδας

**Ορισμός 26.** Έστω  $K \subseteq L$  πεπερασμένη και διαχωρίσιμη επέκταση με  $[L : K] = n$  και  $\sigma_i : L \rightarrow N$  οι  $K$  - μονομορφισμοί του  $L$  στην κανονική θήκη  $N$ . Αν  $(a_1, \dots, a_n) \in L^n$  η ορίζουσα του  $(a_1, \dots, a_n) \in L^n$  είναι η ποσότητα

$$D_{L/K}(a_1, \dots, a_n) = \det [\sigma_i(a_j)]^2 = \left[ \det \begin{pmatrix} \sigma_1(a_1) & \cdots & \sigma_n(a_1) \\ \vdots & & \vdots \\ \sigma_1(a_n) & \cdots & \sigma_n(a_n) \end{pmatrix} \right]^2.$$

**Παρατήρηση 17.** Αν ισχύουν οι παραπάνω υποθέσεις, τότε  $D_{L/K}(a_1, \dots, a_n) \in K$ .

Απόδειξη. Αν  $A = [\sigma_i(a_j)]_{i,j}$  παρατηρήστε ότι

$$D_{L/K}(a_1, \dots, a_n) = (\det A)^2 = \det (A \cdot A^t) = \det [\text{Tr}_{L/K}(a_i a_j)] \in K$$

□

**Πόρισμα 7.** Αν ισχύουν οι παραπάνω υποθέσεις και  $R, S$  είναι το σύνολο των ακεραίων αλγεβρικών των  $K, L$  πάνω από το  $\mathbb{Z}$ , τότε για κάθε  $(a_1, \dots, a_n) \in S^n$  ισχύει ότι  $D_{L/K}(a_1, \dots, a_n) \in R$ .

Απόδειξη. Άμεσο από τις Παρατηρήσεις 16 και 17.

□

**Παρατήρηση 18.** Έστω  $K \subseteq L$  πεπερασμένη και διαχωρίσιμη επέκταση με  $[L : K] = n$  και  $\sigma_i: L \rightarrow N$  οι  $K$ -μονομορφισμοί του  $L$  στην κανονική θήκη  $N$ . Αν  $L = K(\vartheta)$  και  $f(x) = \text{Irr}(\vartheta, K)$ , τότε έχουμε ότι  $f(x) = \prod_{i=1}^n (x - \vartheta_i)$ , όπου  $\vartheta_i = \sigma_i(\vartheta)$ . Τότε, η  $D_{L/K}(1, \vartheta, \dots, \vartheta^{n-1}) = \det \left( \vartheta_i^j \right)^2$  είναι μια ορίζουσα Vandermonde και έχουμε ότι

$$D_{L/K}(\vartheta) := D_{L/K}(1, \vartheta, \dots, \vartheta^{n-1}) = \prod_{1 \leq i < j \leq n} (\vartheta_i - \vartheta_j) \neq 0.$$

Η ποσότητα  $D_{L/K}(\vartheta)$  λέγεται **ορίζουσα** του  $\vartheta$  πάνω από το  $K$ .

**Θέωρημα 12.** Με τους παραπάνω συμβολισμούς ισχύει ότι

$$D(\vartheta) = (-1)^{n(n-1)/2} N_{L/K}(f'(\vartheta)).$$

*Απόδειξη.* Από την παραπάνω παρατήρηση έχουμε ότι

$$\begin{aligned} D(\vartheta) &= \prod_{1 \leq i < j \leq n} (\vartheta_i - \vartheta_j) = (-1)^{n(n-1)/2} \prod_{i=1}^n \prod_{j \neq i} (\vartheta_i - \vartheta_j) \\ &= (-1)^{n(n-1)/2} \prod_{i=1}^n \prod_{j \neq i} (x - \vartheta_j) \Big|_{x=\vartheta_i} = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(\vartheta_i) \\ &= (-1)^{n(n-1)/2} N_{L/K}(f'(\vartheta)) \end{aligned}$$

□

**Παράδειγμα 17.** Θεωρούμε την επέκταση  $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$  με  $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$  και

$$f(x) = \text{Irr}(\zeta_p, \mathbb{Q}) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}.$$

Αφού  $(x - 1)f(x) = x^p - 1$ , παραγωγίζοντας, έχουμε ότι  $f'(\zeta_p) = \frac{p\zeta_p^{p-1}}{\zeta_p - 1}$ . Έχουμε ότι

$$N(p) = p^{p-1}, \quad N(\zeta_p^{p-1}) = 1 \quad \text{και} \quad N(\zeta_p - 1) = p.$$

Από το παραπάνω θεώρημα και την πολλαπλασιαστικότητα της νόρμας προκύπτει ότι

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = (-1)^{(p-1)(p-2)/2} \cdot p^{p-2}.$$

## 8 Μάθημα 08

### 8.1 Ελεύθερες Αβελιανές Ομάδες Πεπερασμένου Βαθμού

**Κίνητρο 5.** Έστω  $K$  αλγεβρικό σώμα αριθμών και  $\mathcal{R}_K$  οι ακέραιοι αλγεβρικοί του  $K$  πάνω από το  $\mathbb{Z}$ . Σκοπός μας είναι να δείξουμε ότι  $\mathcal{R}_K$  είναι ελεύθερη αβελιανή ομάδα με  $\text{rank}(\mathcal{R}_K) = n$ , όπου  $n = [K : \mathbb{Q}]$

**Ορισμός 27.** Μια ομάδα  $M$  καλείται **ελεύθερη αβελιανή** αν ισχύουν τα εξής :

(α)  $M = m_1\mathbb{Z} + m_2\mathbb{Z} + \dots + m_n\mathbb{Z}$

(β) Για κάθε  $x_1, \dots, x_n \in \mathbb{Z}$  τέτοια ώστε

$$m_1x_1 + \dots + m_nx_n = 0$$

τότε  $x_1 = \dots = x_n = 0$ .

Το  $n$  καλείται **rank** της  $M$ , τα το σύνολο  $\{m_1, \dots, m_n\}$  καλείται **βάση** της  $M$ .

**Παρατήρηση 19.** Έστω  $M$  ελεύθερη αβελιανή ομάδα πεπερασμένου rank. Τότε, κάθε δύο βάσεις της  $M$  είναι ισοπληθικές.

*Απόδειξη.* Αν η  $M$  έχει μια βάση με  $n$  το πλήθος στοιχείων, τότε  $M \cong \mathbb{Z}^n$ . Επίσης αν  $M$  είχε μια βάση με πλήθος στοιχείων  $m$ , τότε θα έπρεπε  $\mathbb{Z}^m \cong \mathbb{Z}^n$ . Όμως για τυχόν  $p$  πρώτο ισχύει ότι

$$\mathbb{Z}^n \xrightarrow{\cong} \mathbb{Z}^m \xrightarrow{\pi^m} \mathbb{Z}_p^m$$

όπου από την τελευταία σχέση προκύπτει ότι  $\mathbb{Z}_p^n \cong \mathbb{Z}_p^m$ , δηλαδή  $n = m$ . □

**Ορισμός 28.** Ένας πίνακας  $A = (a_{ij}) \in \mathbb{Z}^{n \times n}$  λέγεται **unimodular** αν  $\det A \in \{-1, 1\}$ .

**Θέωρημα 13.** Έστω  $\{m_1, \dots, m_n\}, \{m'_1, \dots, m'_n\}$  βάσεις μιας ελεύθερης αβελιανής ομάδας πεπερασμένου βαθμού (rank), τότε υπάρχει πίνακας  $A$  με

$$\begin{pmatrix} m'_1 \\ \vdots \\ m'_n \end{pmatrix} = A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

αν και μόνο αν  $A$  είναι unimodular.

Απόδειξη. " Αντωνιάδης, Ι., Κοντογεώργης, Α. (2021). Αλγεβρική Θεωρία Αριθμών "  $\square$

**Παράδειγμα 18.** Στο  $\mathbb{Z}^2$  μία βάση είναι  $\{(0, 1), (1, 0)\}$  και ένας unimodular πίνακας που επάγει νέες βάσεις είναι ο πίνακας  $A = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ .

**Πρόταση 13.** Έστω  $(M, +)$  μία ελεύθερη αβελιανή ομάδα πεπερασμένου βαθμού  $n$  και  $T \leq M$ .

- (α) Η  $T$  είναι ελεύθερη αβελιανή ομάδα πεπερασμένου βαθμού και  $\text{rank}T \leq \text{rank}M$ .
- (β) Υπάρχει μία βάση  $\{w_1, \dots, w_n\}$  της  $M$  και  $e_1, \dots, e_d \in \mathbb{Z} \setminus \{0\}$  με  $d \leq n$  τέτοια ώστε η  $\{e_1w_1, \dots, e_dw_d\}$  να είναι βάση της  $T$  και  $e_1 \mid e_2 \mid \dots \mid e_d$ .

Απόδειξη. (α) Θα δείξουμε το ζητούμενο με επαγωγή στο  $\text{rank}M = n$ .

- Αν  $n = 1$ , τότε  $M = \mathbb{Z}m_1 \cong \mathbb{Z}$  κυκλική και οι υποομάδες της είναι της μορφής  $T = \mathbb{Z}t$ .
- Υποθέτουμε ότι το ζητούμενο ισχύει για όλες τις ελεύθερες αβελιανές ομάδες με  $\text{rank} = n-1$ . Τότε για την  $M = \bigoplus_{i=1}^n \mathbb{Z}m_i$  ορίζουμε την υποομάδα  $M_{n-1} = \bigoplus_{i=1}^{n-1} \mathbb{Z}m_i$  και την  $T_{n-1} = T \cap M_{n-1}$ . Από την αρχική υπόθεση ισχύει ότι  $T_{n-1} \leq M_{n-1}$  και είναι ελεύθερη αβελιανή και μάλιστα  $\text{rank}(T_{n-1}) \leq n-1$ .
- Θα δείξουμε ότι υπάρχει  $t_n \in T$  τέτοιο ώστε  $T = T_{n-1} \oplus t_n\mathbb{Z}$ .
- Από το μονοσήμαντο της γραφής  $m = \sum_{i=1}^n x_i m_i$  μπορούμε να ορίσουμε ομομορφισμό αβελιανών ομάδων  $\pi_j: M \rightarrow \mathbb{Z}$  με  $\pi_j(m) = x_j$ . Τότε, παρατηρούμε ότι το σύνολο

$$\pi_n(T) = \{x \in \mathbb{Z} \mid \exists t \in T : \pi_n(t) = x\}$$

είναι ιδεώδες του  $\mathbb{Z}$ . Συνεπώς, υπάρχει  $e_0 \in \mathbb{Z}$  ώστε  $\pi_n(T) = e_0\mathbb{Z}$ . Συνεπώς, υπάρχει  $t_0 \in T$  ώστε  $\pi_n(t_0) = e_0$

- Αν  $\pi_n(T) = 0$ , τότε έχουμε ότι  $T = T_{n-1} \leq M_{n-1}$  και έχουμε το ζητούμενο.
- Υποθέτουμε ότι  $\pi_n(T) \neq 0$ , συνεπώς  $e_0 \neq 0$  και  $t_0 \neq 0$ . Θα δείξουμε ότι  $T = T_{n-1} \oplus \mathbb{Z}t_0$ . Έστω  $xt_0 \in T_{n-1}$ , τότε έχουμε ότι  $\pi_n(xt_0) = xe_0 = 0$ , δηλαδή  $x = 0$ .
- Αν  $t \in T$ , τότε έχουμε ότι

$$\pi_n(t) = x_0e_0 = \pi_n(x_0t_0) \Rightarrow t - x_0t_0 \in \ker \pi_n = M_{n-1}$$

και έχουμε το ζητούμενο.

- (β) Για κάθε  $\varphi \in \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$  είναι σαφές ότι  $\varphi(T)$  είναι ιδεώδες του  $\mathbb{Z}$ . Θεωρούμε την οικογένεια

$$\mathcal{J} = \{\varphi(T) \mid \varphi \in \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z})\} \neq \emptyset$$

- Αφού  $\mathbb{Z}$  είναι της Noether, υπάρχει μεγιστικό στοιχείο  $\varphi_0: M \rightarrow \mathbb{Z}$  ομομορφισμός αβελιανών ομάδων.
- Τότε, ομοίως με παραπάνω, υπάρχουν  $e_0 \in \mathbb{Z}$  ώστε  $\varphi_0(T) = e_0\mathbb{Z}$  και  $t_0 \in T$  ώστε  $\varphi_0(t_0) = e_0$ . Θα δείξουμε ότι υπάρχει  $w_0 \in M$  ώστε  $t_0 = e_0w_0$
- Αν  $\{m_1, \dots, m_n\}$  μια βάση του  $M$ , τότε έχουμε ότι

$$t = \pi_1(t)m_1 + \dots + \pi_n(t)m_n.$$

Για να δείξουμε το ζητούμενο αρκεί να δείξουμε ότι  $e_0 | \pi_i(t)$ , για κάθε  $i = 1, \dots, n$ .

- Αν δείξουμε ότι

$$e_0\mathbb{Z} = e_0\mathbb{Z} + \pi_t\mathbb{Z} = (ke_0 + \ell\pi_i(t))$$

για κάθε  $k, \ell \in \mathbb{Z}$ , τότε θα έχουμε το ζητούμενο.

- Θεωρούμε τον ομομορφισμό ομάδων

$$\varphi_{k,\ell}: M \rightarrow \mathbb{Z}, \quad \varphi_{k,\ell}(m) = k\varphi_0(m) + \ell\pi_i(m)$$

Τότε, παρατηρούμε ότι  $\varphi_{k,\ell}(T) \in \mathcal{J}$  και από την μεγιστικότητα του  $\varphi_0(T)$  καταλήξτε σε ισότητα.

- Αφήνεται ως άσκηση ναδειχθεί ότι  $M = \mathbb{Z}\omega_0 \oplus \ker \varphi_0$  και  $T = \mathbb{Z}t_0 + (\ker \varphi_0 \cap T)$ . Τότε, από την επαγωγική υπόθεση, υπάρχει  $\omega_1, \dots, \omega_{n-1}$  βάση του  $\ker \varphi_0$  και  $e_1 | \dots | e_d$  ώστε  $e_1\omega_1, \dots, e_{d-1}\omega_{d-1}$  βάση του  $T \cap \ker \varphi_0$
- Θεωρώντας κατάλληλη  $\varphi: M \rightarrow \mathbb{Z}$ , δείξτε ότι  $e_0 | e_1$ . Τότε έχουμε το ζητούμενο. □

**Παρατήρηση 20.** Αντίστοιχο αποτέλεσμα ισχύει και για  $R$  ελεύθερα πρότυπα στην περίπτωση που  $R$  είναι περιοχή κύριων ιδεωδών.

**Πρόταση 14.** Έστω  $M = \mathbb{Z}m_1 \oplus \dots \oplus \mathbb{Z}m_n$  και  $T = \mathbb{Z}t_1 \oplus \dots \oplus \mathbb{Z}t_n$  ελεύθερες αβελιανές και  $T \leq M$  με  $\text{rank}M = \text{rank}T = n$ . Τότε, αν υπάρχει μονοσήμαντα ορισμένος  $A \in \mathbb{M}_n(\mathbb{Z})$  τέτοιος ώστε

$$\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

τότε ισχύει ότι  $[M : T] = |\det A|$ .



Απόδειξη. Γνωρίζουμε ότι υπάρχουν βάση  $w_1, \dots, w_n$  της  $M$  και  $e_1 | \dots | e_n$  τέτοια ώστε  $T = \mathbb{Z}e_1w_1 \oplus \dots \oplus \mathbb{Z}e_nw_n$ . Από το Θεώρημα 13 προκύπτει ότι υπάρχουν  $B, C$  unimodular ώστε

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = B \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \quad \text{και} \quad \begin{pmatrix} e_1w_1 \\ \vdots \\ e_nw_n \end{pmatrix} = C \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}.$$

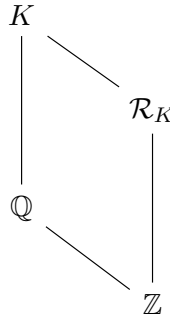
Επίσης, ισχύει ότι

$$\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = C^{-1} \cdot \text{diag}(e_1, \dots, e_n) \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = C^{-1} \cdot \text{diag}(e_1, \dots, e_n) \cdot B \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

Από το μονοσήμαντο του  $A$  έχουμε ότι  $A = C^{-1} \cdot \text{diag}(e_1, \dots, e_n) \cdot B$  και έτσι προκύπτει ότι  $|\det A| = |e_1| \cdot \dots \cdot |e_n|$ . Τέλος, είναι άμεσο ότι  $M/T = \bigoplus \mathbb{Z}_{|e_i|}$ , συνεπώς έχουμε το ζητούμενο.  $\square$

## 8.2 Σύνολα Ακεραίων Αλγεβρικών και Ελεύθερες Αβελιανές

**Πρόταση 15.** Έστω  $K$  αλγεβρικό σώμα αριθμών με  $[K : \mathbb{Q}] = n$ . Ο δακτύλιος  $\mathcal{R}_K$  των ακεραίων αλγεβρικών του  $K$  πάνω από το  $\mathbb{Z}$  είναι ελεύθερη αβελιανή ομάδα με  $\text{rank} \mathcal{R}_K = n$ .



Απόδειξη. Υποθέτουμε ότι  $K = \mathbb{Q}(\vartheta)$ . Από την απόδειξη της Πρότασης 8 έχουμε ότι

$$\mathbb{Z}(\vartheta) \subseteq \mathcal{R}_K \subseteq \frac{1}{D_K(\vartheta)} \mathbb{Z}(\vartheta)$$

Τα  $\mathbb{Z}$  - πρότυπα

$$\mathbb{Z}(\vartheta) = \bigoplus_{i=0}^{n-1} \mathbb{Z}\vartheta^i \quad \text{και} \quad \frac{1}{D_K(\vartheta)} \mathbb{Z}(\vartheta) = \bigoplus_{i=0}^{n-1} \mathbb{Z} \left( \vartheta^i / \frac{1}{D_K(\vartheta)} \right)$$

είναι ελεύθερες αβελιανές ομάδες βαθμού  $n$ , συνεπώς από την Πρόταση 13 έχουμε το ζητούμενο.  $\square$

**Πρόταση 16.** Θεωρούμε  $\{w_1, \dots, w_n\}$  βάση της  $K/\mathbb{Q}$  και  $a_i = \sum_{j=1}^n a_{ij}w_j$ . Αν  $A = (a_{ij})$ , τότε ισχύει ότι

$$D_K(a_1, \dots, a_n) = (\det A)^2 \cdot D_K(w_1, \dots, w_n)$$

Απόδειξη. Αφού  $D_K(a_1, \dots, a_n) = \det(\text{Tr}_K(a_i a_j))$  έχουμε

$$\text{Tr}_{K/\mathbb{Q}}(a_k a_\ell) = \text{Tr}_{K/\mathbb{Q}} \left[ \left( \sum_{i=1}^n a_{ki} w_i \right) \cdot \left( \sum_{j=1}^n a_{\ell j} w_j \right) \right] = \sum_{i=1}^n \sum_{j=1}^n a_{ki} a_{\ell j} \text{Tr}_{K/\mathbb{Q}}(w_i w_j)$$

. Από την παραπάνω σχέση καταλήγουμε στην ισότητα πινάκων

$$(\text{Tr}_{K/\mathbb{Q}}(a_k \cdot a_\ell))_{1 \leq k, \ell \leq n} = (a_{ki}) \cdot \text{Tr}_{K/\mathbb{Q}}(w_i w_j) \cdot (a_{\ell j})^t$$

Από την παραπάνω σχέση έχουμε το ζητούμενο. □

## 9 Μάθημα 09

### 9.1 Βάσεις Ακεραιότητας

**Ορισμός 29.** Έστω  $K$  αλγεβρικό σώμα αριθμών με  $[K : \mathbb{Q}] = n$ . Τα  $\mathbb{Q}$ -γραμμικά ανεξάρτητα στοιχεία  $\omega_1, \dots, \omega_n \in \mathcal{R}_K$  λέγονται **βάση ακεραιότητας** αν είναι βάση της ελευθέρως αβελιανής ομάδας  $\mathcal{R}_K$ , δηλαδή

$$\mathcal{R}_K = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_n.$$

**Παρατήρηση 21.** Προφανώς, κάθε βάση ακεραιότητας του  $K$  είναι και βάση της επέκτασης  $K/\mathbb{Q}$ .

**Παρατήρηση 22.** Έστω  $\{\omega_1, \dots, \omega_n\}$  και  $\{\omega'_1, \dots, \omega'_n\}$  δύο βάσεις ακεραιότητας του  $K$ . Τότε, από το Θεώρημα 13 υπάρχει  $A$  unimodular ώστε

$$\begin{pmatrix} \omega'_1 \\ \vdots \\ \omega'_n \end{pmatrix} = A \cdot \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Από την Πρόταση 16 έχουμε ότι

$$D_K(\omega'_1, \dots, \omega'_n) = \det(A)^2 \cdot D_K(\omega_1, \dots, \omega_n) = D_K(\omega_1, \dots, \omega_n).$$

**Ορισμός 30.** Έστω  $\{\omega_1, \dots, \omega_n\}$  βάση ακεραιότητας του  $K$ . Η **ορίζουσα** του  $K$  ορίζεται να είναι η

$$D_K = D_K(\omega_1, \dots, \omega_n).$$

Από το Πρόσμμα 7 είναι σαφές ότι  $D_K \in \mathbb{Z}$ .

**Κίνητρο 6.** Έστω  $a_1, \dots, a_n \in \mathcal{R}_K$  γραμμικά ανεξάρτητα πάνω από το  $\mathbb{Q}$ . Μπορούμε να βρούμε ένα κριτήριο ώστε να εξετάζουμε αν τα  $a_1, \dots, a_n \in \mathcal{R}_K$  είναι βάση ακεραιότητας; Στην περίπτωση που δεν είναι μπορούμε να κατασκευάσουμε ένα αλγόριθμο ώστε να " παραχθεί " μια βάση ακεραιότητας από το αρχικό σύνολο  $\{a_1, \dots, a_n\}$  ;

**Πρόταση 17.** Έστω  $a_1, \dots, a_n \in \mathcal{R}_K$  γραμμικά ανεξάρτητα πάνω από το  $\mathbb{Q}$  και  $\{\omega_1, \dots, \omega_n\}$  βάση ακεραιότητας του  $K$ . Τότε ισχύει ότι

$$D_K(a_1, \dots, a_n) = m^2 D_K(\omega_1, \dots, \omega_n), \quad \text{με } m = \left[ \mathcal{R}_K : \bigoplus_{i=1}^n \mathbb{Z}a_i \right].$$

**Πρόταση 18.** Άμεσο από την Πρόταση 14

**Πρόσμμα 8.** Έστω  $a_1, \dots, a_n \in \mathcal{R}_K$  γραμμικά ανεξάρτητα πάνω από το  $\mathbb{Q}$ . Αν  $D_K(a_1, \dots, a_n)$  είναι ελεύθερη τετραγώνου, τότε  $a_1, \dots, a_n$  είναι βάση ακεραιότητας του  $K$ .

**Παράδειγμα 19.** Το αντίστροφο του προηγούμενου πορίσματος δεν ισχύει γενικά! Έστω  $K = \mathbb{Q}(i)$  με  $[K : \mathbb{Q}] = 2$  και  $\mathcal{R}_K = \mathbb{Z}[i]$ . Τότε, είναι άμεσο ότι  $\{1, i\}$  είναι μια βάση ακεραιότητας του  $K$ . Παρόλα αυτά

$$D_K(1, i) = \left[ \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \right]^2 = -4$$

συνεπώς  $D_K$  δεν είναι ελεύθερη τετραγώνου.

**Θέωρημα 14.** Ισχύει ότι  $D_K \equiv 0, 1 \pmod{4}$ .

Απόδειξη. Έστω  $\omega_1, \dots, \omega_n$  βάση ακεραιότητας του  $K$ . Αν με  $\omega_i^{(j)}$  συμβολίζουμε τα συζυγή των  $\omega_i$ , τότε έχουμε ότι  $D_K^{1/2} = \det [\omega_i^{(j)}]$ . Από εναλλακτικό ορισμό της ορίζουσας έχουμε ότι

$$\det [\omega_i^{(j)}] = \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^n \omega_i^{\sigma(i)} = \underbrace{\sum_{\sigma \in A_n} \prod_{i=1}^n \omega_i^{\sigma(i)}}_A - \underbrace{\sum_{\sigma \in S_n \setminus A_n} \prod_{i=1}^n \omega_i^{\sigma(i)}}_B$$

Συνεπώς, έχουμε ότι  $D_K = (A - B)^2 = (A + B)^2 - 4AB$ . Αν δείξουμε ότι  $A + B, AB \in \mathbb{Q}$ , δεδομένου ότι  $A + B, AB$  είναι ακέραιοι αλγεβρικοί πάνω από το  $\mathbb{Z}$  σε μια κανονική θήκη  $N$ , τότε θα έχουμε ότι  $A + B, AB \in \mathbb{Z}$ . Δεδομένου αυτού θα έχουμε ότι

$$D_K \equiv (A + B)^2 \equiv 0, 1 \pmod{4}.$$

Παρατηρήστε ότι  $A + B, AB$  παραμένουν αναλλοίωτα στις δράσεις των  $\sigma \in \text{Gal}(N, \mathbb{Q})$  και αφού  $N/\mathbb{Q}$  είναι επέκταση Galois, τότε έχουμε ότι

$$A + B, AB \in \text{Fix}[\text{Gal}(N, \mathbb{Q})] = \mathbb{Q}.$$

□

**Παράδειγμα 20.** Θεωρούμε το ανάγωγο πολυώνυμο  $f(x) = x^3 - x - 2 \in \mathbb{Z}[x]$  και  $\vartheta$  μια ρίζα του σε επέκταση. Τότε  $[K : \mathbb{Q}] = 3$ , όπου  $K = \mathbb{Q}(\vartheta)$ .

- Γνωρίζουμε ότι  $\{1, \vartheta, \vartheta^2\}$  είναι βάση της επέκτασης  $K/\mathbb{Q}$ . Είναι όμως βάση ακεραιότητας ;
- Από το Θεώρημα 12 έχουμε ότι  $D(\vartheta) = -N_K(f'(\vartheta))$ . Έχουμε ότι  $f'(\vartheta) = 3\vartheta^2 - 1$ , συνεπώς ισχύει ότι

$$D(\vartheta) = -(3\vartheta_1^2 - 1) \cdot (3\vartheta_2^2 - 1) \cdot (3\vartheta_3^2 - 1)$$

όπου  $\vartheta = \vartheta_1, \vartheta_2, \vartheta_3$  είναι τα συζυγή του  $\vartheta$ .

- Από τον ορισμό του  $f(x)$  και τους τύπους Vieta έχουμε ότι

$$\begin{aligned} \vartheta_1 + \vartheta_2 + \vartheta_3 &= 0 \\ \vartheta_1\vartheta_2 + \vartheta_1\vartheta_3 + \vartheta_2\vartheta_3 &= 1 \\ \vartheta_1\vartheta_2\vartheta_3 &= 2 \end{aligned}$$

- Από το  $D(\vartheta)$  και από τις παραπάνω σχέσεις, υπολογίζοντας, προκύπτει ότι  $D(\vartheta) = -104 = -26 \cdot 2^2$
- Από την Πρόταση 17 ισχύει ότι  $D(\vartheta) = -2^2 \cdot 26 = m^2 D_K$ . Συνεπώς, έχουμε ότι  $m = 1$  ή  $m = 2$ . Αν  $m = 2$ , τότε  $D_K = -26 \equiv 2 \pmod{4}$  και από το παραπάνω θεώρημα καταλήγουμε σε άτοπο. Άρα,  $\{1, \vartheta, \vartheta^2\}$  είναι βάση ακεραιότητας του  $K$ .

**Παράδειγμα 21** (Τετραγωνικά Σώματα Αριθμών). Έστω  $K$  ένα τετραγωνικό σώμα αριθμών. Από τα αποτελέσματα της Διάλεξης 2 έχουμε ότι  $K = \mathbb{Q}[\sqrt{d}]$ , όπου  $d$  είναι ένας ακέραιος ελεύθερος τετραγώνου και

$$\mathcal{R}_K = \begin{cases} \mathbb{Z}[d], & \text{αν } d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{αν } d \equiv 1 \pmod{4} \end{cases}$$

i. Αν  $d \not\equiv 1 \pmod{4}$ , τότε  $\{1, \sqrt{d}\}$  είναι μια βάση ακεραιότητας του  $K$ , συνεπώς έχουμε ότι

$$D_K = \left[ \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} \right]^2 = 4d$$

ii. Αν  $d \equiv 1 \pmod{4}$ , τότε  $\left\{1, \left(1 + \sqrt{d}\right)/2\right\}$  και η αντίστοιχη ορίζουσα ισούται με  $D_K = d$ .

## 9.2 Αλγόριθμος Υπολογισμού Βάσης Ακεραιότητας

**Κίνητρο 7.** Έστω  $K$  αλγεβρικό σώμα αριθμών με  $[K : \mathbb{Q}] = n$ . Σκοπός μας είναι δοσμένους ενός  $\mathbb{Q}$ -γραμμικά ανεξάρτητου υποσυνόλου του  $\mathcal{R}_K$  να βρούμε μια βάση ακεραιότητας του  $K$ .

**Παρατήρηση 23.** Έστω  $K$  αλγεβρικό σώμα αριθμών με  $[K : \mathbb{Q}] = n$  και  $a_1, \dots, a_n \in \mathcal{R}_K$  γραμμικά ανεξάρτητα πάνω από το  $\mathbb{Q}$ . Αν  $m = [\mathcal{R}_K : H] \neq 1$ , τότε υπάρχει  $p|m$  πρώτος, συνεπώς  $p || \mathcal{R}_K/H$ . Από το Θεώρημα του Cauchy, υπάρχει  $\vartheta \in \mathcal{R}_K/H$  τάξης  $p$ , δηλαδή  $p\vartheta \in H$ . Αφού  $\vartheta \notin H$ , μπορούμε να επιλέξουμε  $0 \leq m_1, \dots, m_n < p$  τέτοια ώστε

$$\vartheta = \frac{m_1\omega_1 + \dots + m_n\omega_n}{p} \quad (8)$$

**Παρατήρηση 24.** Έστω  $K$  αλγεβρικό σώμα αριθμών με  $[K : \mathbb{Q}] = n$  και  $a_1, \dots, a_n \in \mathcal{R}_K$  γραμμικά ανεξάρτητα πάνω από το  $\mathbb{Q}$ . Αν  $\omega_1, \dots, \omega_n$  μια βάση ακεραιότητας του  $K$ , τότε έχουμε ότι

$$D_K(a_1, \dots, a_n) = m^2 D_K(\omega_1, \dots, \omega_n), \quad m = [\mathcal{R}_K : H]$$

όπου  $H = \bigoplus \mathbb{Z}_i a_i$ .

### Αλγόριθμος Εύρεσης Βάσης Ακεραιότητας

Έστω  $K$  αλγεβρικό σώμα αριθμών με  $[K : \mathbb{Q}] = n$  και  $B = \{a_1, \dots, a_n\} \subseteq \mathcal{R}_K$ .

- (α) Υπολογίζουμε την ορίζουσα  $D_K(a_1, \dots, a_n)$  την οποία αναλύοντας σε πρώτους γράφεται στην μορφή

$$D_K(a_1, \dots, a_n) = p_1^2 \cdots p_k^2 \cdot d$$

όπου  $d$  είναι ελεύθερο τετραγώνου. Αν  $k = 0$ , τότε το παραπάνω σύνολο είναι βάση ακεραιότητας.

- (β) Για κάθε  $p_1, \dots, p_k$  εξετάζουμε αν υπάρχει  $\vartheta$  της μορφής 8. Αν δεν υπάρχει, από την Παρατήρηση 23, το  $B$  είναι βάση ακεραιότητας.

- (γ) Αν υπάρχει τέτοιο  $p_j$ , χωρίς βλάβη της γενικότητας θεωρούμε το  $p_1$ , ώστε να υπάρχει  $\vartheta$  της μορφής 8, τότε "πετώντας κατάλληλο"  $a_\ell$ , χωρίς βλάβη της γενικότητας το  $a_n$ , και αντικαθιστώντας το  $\vartheta$  (ή ενδεχομένως με ακέραιο πολλαπλασιό του), προκύπτει μια καινούρια βάση της επέκτασης  $B' = \{a_1, \dots, a_{n-1}, \vartheta\}$  για την οποία ισχύει

$$D_K(B') = \frac{1}{p_1^2} D_K(B) = p_2^2 \cdots p_k^2 \cdot d$$

- (δ) Ακολουθούμε την ίδια διαδικασία μέχρι να καταλήξουμε τελικά σε μια βάση ακεραιότητας του  $K$ .

## 10 Μάθημα 10

### 10.1 Norm Ιδεώδους Αλγεβρικού Σώματος Αριθμών

**Παρατήρηση 25.** Έστω  $K$  ένα αλγεβρικό σώμα αριθμών και  $\mathcal{R}_K$  ο δακτύλιος των ακεραίων αλγεβρικών του  $K$  πάνω από το  $\mathbb{Z}$ . Από το Πόρισμα 6, έχουμε ότι  $\mathcal{R}_K$  είναι δακτύλιος του Dedekind και μάλιστα ικανοποιεί την συνθήκη  $FN$ . Συνεπώς, για κάθε ιδεώδες  $A \subseteq \mathcal{R}_K$ , ισχύει ότι  $|\mathcal{R}_K/A| < \infty$ .

**Ορισμός 31.** Αν  $A$  ακέραιο ιδεώδες του  $\mathcal{R}_K$  ορίζουμε ως **norm** του  $A$  το φυσικό αριθμό

$$N_K(A) = |\mathcal{R}_K/A|$$

**Κίνητρο 8.** Αφού ο  $\mathcal{R}_K$  είναι δακτύλιος Dedekind, τότε κάθε ακέραιο (ή κλασματικό) ιδεώδες  $A$  γράφεται ως

$$A = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} \mathfrak{p}^{a(\mathfrak{p})}$$

με  $a(\mathfrak{p}) \in \mathbb{N}$  (ή  $a(\mathfrak{p}) \in \mathbb{Z}$ ), όπου με  $\text{Spec}(\mathcal{R}_K)$  συμβολίζουμε το σύνολο των πρώτων ιδεωδών του  $\mathcal{R}_K$ . Θα δείξουμε ότι ο υπολογισμός της  $\text{norm}$  γίνεται απλούστερος, δείχνοντας ότι

$$N_K(A) = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} N_K(\mathfrak{p})^{a(\mathfrak{p})}$$

Για να δειχθεί όμως το παραπάνω πρέπει να αποδείξουμε μια σειρά από προτάσεις.

**Παρατήρηση 26.** Έστω  $\mathfrak{p}, \mathfrak{q} \in \text{Spec}(\mathcal{R}_K)$  διαφορετικά πρώτα ιδεώδη. Θα δείξουμε ότι  $\mathfrak{p}, \mathfrak{q}$  είναι comaximal, δηλαδή  $\mathfrak{p} + \mathfrak{q} = \mathcal{R}_K$ .

*Απόδειξη.* Για να δείξουμε το ζητούμενο αποτέλεσμα, αρκεί να δείξουμε ότι  $\mathfrak{p} \cdot \mathfrak{q} = \mathfrak{p} \cap \mathfrak{q}$ .

(α) Αφού  $\mathfrak{p} \cdot \mathfrak{q} \subseteq \mathfrak{p} \cap \mathfrak{q}$ , υπάρχει  $A$  ακέραιο ιδεώδες ώστε

$$\mathfrak{p} \cdot \mathfrak{q} = (\mathfrak{p} \cap \mathfrak{q}) \cdot A$$

1. Από τη μοναδικότητα της ανάλυσης σε πρώτα ιδεώδη, έχουμε ότι  $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p}$  ή  $\mathfrak{q}$  ή  $\mathfrak{p} \cdot \mathfrak{q}$ .
2. Αφού  $\mathfrak{p} \neq \mathfrak{q}$  και αφού κάθε μη μηδενικό πρώτο ιδεώδες είναι μέγιστο, τότε οι πρώτες δύο περιπτώσεις απορρίπτονται και προκύπτει ότι  $\mathfrak{p} \cdot \mathfrak{q} = \mathfrak{p} \cap \mathfrak{q}$ .

□

**Πόρισμα 9.** Για κάθε  $n, m \in \mathbb{N}$  και  $\mathfrak{p}, \mathfrak{q} \in \text{Spec}(\mathcal{R}_K)$  διακεκριμένα, ισχύει

$$\mathfrak{p}^n + \mathfrak{q}^m = \mathcal{R}_K.$$

*Απόδειξη.* Χρησιμοποιήστε την παραπάνω παρατήρηση και την Άσκηση 2.40 του [Fulton, 2008].

□

**Θέωρημα 15** (Κινέζικο Θεώρημα Υπολοίπων). Έστω  $A_1, \dots, A_k$  comaximal ανά δύο πρώτα ιδεώδη του  $\mathcal{R}_K$ . Τότε, η απεικόνιση

$$\varphi: \mathcal{R}_K / \bigcap_{i=1}^k A_i \rightarrow \prod_{i=1}^k \mathcal{R}_K / A_i, \quad \varphi \left( x + \bigcap_{i=1}^k A_i \right) = (x + A_1, \dots, x + A_k)$$

είναι ισομορφισμός δακτυλίων.

*Απόδειξη.* Η απόδειξη παρατίθεται στο [Scott, 2015] και στο [Antoniadis, 2021]

□

**Πρόταση 19.** Έστω  $A$  ένα ιδεώδες του  $\mathcal{R}_K$ , το οποίο αναλύεται σε γινόμενο πρώτων ιδεωδών ως εξής

$$A = \prod_{i=1}^{\ell} \mathfrak{p}_i^{a_i(A)}$$

Τότε, ισχύει ότι

$$\mathcal{R}_K/A \cong \prod_{i=1}^{\ell} \mathcal{R}_K/\mathfrak{p}_i^{a_i(A)}.$$

*Απόδειξη.* Το ζητούμενο έπεται άμεσα από το Πρόσχημα 9 και το Θεώρημα 15.  $\square$

**Λήμμα 8.** Έστω  $\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)$ . Τότε, οι προσθετικές ομάδες  $\mathcal{R}_K/\mathfrak{p}$  και  $\mathfrak{p}^n/\mathfrak{p}^{n+1}$  είναι ισόμορφες.

*Απόδειξη.* • Από την μοναδικότητα της ανάλυσης σε πρώτα ιδεώδη, τότε  $\mathfrak{p}^{n+1} \subsetneq \mathfrak{p}^n$ , συνεπώς υπάρχει  $a \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$ .

- Θεωρούμε την απεικόνιση  $\varphi: \mathcal{R}_K \rightarrow \mathfrak{p}^n$  με  $\varphi(x) = ax$ , η οποία προφανώς είναι ομομορφισμός ομάδων. Αν  $\psi$  είναι η παρακάτω σύνθεση

$$\underbrace{\mathcal{R}_K \xrightarrow{\varphi} \mathfrak{p}^n \xrightarrow{\pi} \mathfrak{p}^n/\mathfrak{p}^{n+1}}_{\psi}$$

Τότε, παρατηρούμε ότι  $\mathfrak{p} \subseteq \ker \psi$ , με  $\ker \psi = \{x \in \mathcal{R}_K \mid ax \in \mathfrak{p}^{n+1}\}$ . Παρότι  $\psi$  είναι ομομορφισμός ομάδων, ισχύει ότι  $\ker \psi$  είναι ιδεώδες του  $\mathcal{R}_K$  και αφού  $\mathfrak{p}$  είναι μέγιστο και  $\ker \psi \subsetneq \mathcal{R}_K$ , τότε  $\ker \psi = \mathfrak{p}$ .

- Συνεπώς, ορίζεται μονομορφισμός ομάδων

$$\tilde{\psi}: \mathcal{R}_K/\mathfrak{p} \rightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1}, \quad \tilde{\psi}(x + \mathfrak{p}) = ax + \mathfrak{p}^{n+1}.$$

- Η  $\tilde{\psi}$  είναι ισομορφισμός. Για να δείξουμε ότι  $\tilde{\psi}$  είναι επί, αρκεί να δείξουμε ότι

$$a \cdot \mathcal{R}_K + \mathfrak{p}^{n+1} = \mathfrak{p}^n.$$

Αρχικά αφού  $a \in \mathfrak{p}^n$ , τότε είναι σαφές ότι  $a \cdot \mathcal{R}_K + \mathfrak{p}^{n+1} \subseteq \mathfrak{p}^n$ , συνεπώς υπάρχει αθέραιο ιδεώδες  $A$  ώστε

$$a \cdot \mathcal{R}_K + \mathfrak{p}^{n+1} = A \cdot \mathfrak{p}^n.$$



Ομοίως μπορούμε να δείξουμε ότι υπάρχει ιδεώδες  $B$  τέτοιο ώστε

$$\mathfrak{p}^{n+1} = B \cdot (a \cdot \mathcal{R}_K + \mathfrak{p}^{n+1}) = AB \cdot \mathfrak{p}^n.$$

Από τη μοναδικότητα ανάλυσης σε πρώτα ιδεώδη, διακρίνοντας περιπτώσεις για τα  $A, B$ , προκύπτει ότι  $A = \mathcal{R}_K$  και έχουμε το ζητούμενο.  $\square$

**Θέωρημα 16** (Πολλαπλασιαστικότητα της Norm). Έστω  $A, B$  ακέραια ιδεώδη του  $K$ . Τότε, ισχύει ότι

$$N_K(A \cdot B) = N_K(A) \cdot N_K(B).$$

Απόδειξη. • Αρχικά θα δείξουμε ότι για κάθε  $\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)$  ισχύει ότι

$$N_K(\mathfrak{p}^n) = [N_K(\mathfrak{p})]^n, \quad \text{για κάθε } n \in \mathbb{N}.$$

Η απόδειξη της παραπάνω σχέσης είναι άμεση με χρήση επαγωγής και του 2ου θεωρήματος ισομορφισμών ομάδων

$$\mathcal{R}_K/\mathfrak{p}^n \cong \frac{\mathcal{R}_K/\mathfrak{p}^{n+1}}{\mathfrak{p}^n/\mathfrak{p}^{n+1}}$$

όπου από το προηγούμενο λήμμα προκύπτει ότι

$$|\mathcal{R}_K/\mathfrak{p}^{n+1}| = |\mathcal{R}_K/\mathfrak{p}^n| \cdot |\mathcal{R}_K/\mathfrak{p}|.$$

- Θεωρούμε  $A$  ακέραιο ιδεώδες του  $K$ , το οποίο γράφεται ως γινόμενο πρώτων ιδεωδών στη μορφή

$$A = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} \mathfrak{p}^{a(\mathfrak{p})}$$

Από το Κινέζικο Θεώρημα Υπολοίπων και το πρώτο σκέλος της απόδειξης είναι άμεσο ότι

$$N_K(A) = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} N_K(\mathfrak{p})^{a(\mathfrak{p})}$$

- Έστω  $A, B$  ακέραια ιδεώδη του  $K$  τα οποία επιδέχονται ανάλυση σε γινόμενο πρώτων ιδεωδών ως εξής:

$$A = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} \mathfrak{p}^{a(\mathfrak{p})} \quad \text{και} \quad B = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} \mathfrak{p}^{b(\mathfrak{p})}$$

Συνεπώς, έχουμε ότι

$$N_K(A \cdot B) = N_K \left( \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} \mathfrak{p}^{a(\mathfrak{p})+b(\mathfrak{p})} \right) = N_K(A) \cdot N_K(B).$$

□

**Παρατήρηση 27.** Με βάση το παραπάνω θεώρημα, δείξαμε ότι για κάθε ακέραιο ιδεώδες  $A = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} \mathfrak{p}^{a(\mathfrak{p})}$ , ισχύει ότι

$$N_K(A) = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} N_K(\mathfrak{p})^{a(\mathfrak{p})}$$

Συνεπώς, με αυτό το τρόπο μπορούμε να γενικεύσουμε τον ορισμό της norm ιδεώδους και σε κλασματικά ιδεώδη ως εξής : Αν  $A = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} \mathfrak{p}^{a(\mathfrak{p})}$ , με  $a(\mathfrak{p}) \in \mathbb{Z}$ , τότε ορίζουμε norm του  $A$  να είναι η ποσότητα

$$N_K(A) := \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)} N_K(\mathfrak{p})^{a(\mathfrak{p})}$$

**Πρόταση 20.** Η norm πρώτου ιδεώδους του  $K$  είναι ίση με δύναμη κάποιου πρώτου αριθμού.

*Απόδειξη.* Έστω  $\mathfrak{p} \in \text{Spec}(\mathcal{R}_K)$  μη μηδενικό. Τότε,  $\mathfrak{p}$  είναι μέγιστο, άρα το πηλίκο  $\mathcal{R}_K/\mathfrak{p}$  είναι ένα πεπερασμένο σώμα, του οποίου το πλήθος ισούται με κάποια δύναμη πρώτου αριθμού. □

**Πρόταση 21.** Έστω  $a \in \mathcal{R}_K \setminus \{0\}$ . Τότε, ισχύει ότι

$$N_K(a\mathcal{R}_K) = |N_{K/\mathbb{Q}}(a)|$$

*Απόδειξη.* Έστω  $\{\omega_1, \dots, \omega_n\}$  μια βάση ακεραιότητας του  $K$ . Αφού  $\mathcal{R}_K/a\mathcal{R}_K$  είναι πεπερασμένο, τότε  $a\mathcal{R}_K$  είναι ελεύθερη αβελιανή τάξης  $n$  και μάλιστα

$$a\mathcal{R}_K = \bigoplus \mathbb{Z}a\omega_i.$$

Έχουμε ότι

$$a \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A(a) \cdot \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Από την Πρόταση 14 και του ορισμό της νόρμας έχουμε ότι

$$N_K(a\mathcal{R}_K) = [\mathcal{R}_K : a\mathcal{R}_K] = |\det(A(a))| = |N_{K/\mathbb{Q}}(a)|$$

□

**Παρατήρηση 28.** Αφήνεται ως άσκηση να δειχθεί ότι, για κάθε  $A$  ιδεώδες του  $\mathcal{R}_K$ , τότε ισχύει ότι  $N_{K/\mathbb{Q}}(A) \in A$ .

**Παράδειγμα 22.** Έστω  $K = \mathbb{Q}(\sqrt{6})$ , όπου  $m \equiv 2 \pmod{4}$ . Επομένως, από το Παράδειγμα 21, έχουμε ότι  $\mathcal{R}_K = \mathbb{Z}[\sqrt{6}] = \mathbb{Z} + \mathbb{Z}\sqrt{6}$ . Θα υπολογίσουμε την ποσότητα  $N_K(A)$ , όπου  $A$  είναι το κλασματικό ιδεώδες  $A = \mathbb{Z} + \mathbb{Z}(\sqrt{6}/2)$ .

- Παρατηρήστε ότι  $A = (1/2)I$ , όπου  $I = 2\mathbb{Z} + \mathbb{Z}\sqrt{6}$ , συνεπώς έχουμε ότι  $N_K(A) = [N_K(2\mathcal{R}_K)]^{-1} \cdot N_K(I) = N_K(I)/4$ .
- Τώρα, παρατηρούμε ότι  $\{2, \sqrt{6}\}$  είναι μια βάση του  $I$  και μάλιστα

$$\begin{pmatrix} 2 \\ \sqrt{6} \end{pmatrix} = \underbrace{\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}}_A \begin{pmatrix} 1 \\ \sqrt{6} \end{pmatrix}$$

συνεπώς, έχουμε ότι  $N_K(I) = |\mathcal{R}_K/I| = |\det(A)| = 2$ . Από την τελευταία σχέση προκύπτει ότι  $N_K(A) = 1/2$ .

**Παράδειγμα 23.** Έστω  $K = \mathbb{Q}(\sqrt{-5})$  με  $-5 \equiv 3 \pmod{4}$ . Επομένως, από το Παράδειγμα 21, έχουμε ότι

$$\mathcal{R}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}.$$

Θα υπολογίσουμε την ποσότητα  $N_K(A)$ , όπου  $A = 2\mathbb{Z} + \mathbb{Z}(1 + \sqrt{-5})$ . Παρατηρήστε ότι

$$\begin{pmatrix} 2 \\ 1 + \sqrt{-5} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{-5} \end{pmatrix}$$

Ομοίως με το παραπάνω παράδειγμα είναι άμεσο ότι  $N_K(A) = 2$ .

## 10.2 Ομάδα Κλάσεων Ιδεωδών

Έστω  $K$  αλγεβρικό σώμα αριθμών με  $[K : \mathbb{Q}] = n$ ,  $\mathcal{I}_K$  η ομάδα κλασματικών ιδεωδών του  $K$  (χωρίς το 0) και  $\mathcal{H}_K = \{a\mathcal{R}_K \mid a \in K \setminus \{0\}\}$ .

**Ορισμός 32.** Θα ονομάζουμε ομάδα κλάσεων ιδεωδών την ομάδα πηλίκο

$$\mathcal{C}_K = \mathcal{I}_K / \mathcal{H}_K.$$

Με  $h_k$  συμβολίζουμε την τάξη της ομάδας  $\mathcal{C}_K$

**Παρατήρηση 29.** Γνωρίζουμε, ότι κάθε περιοχή κύριων ιδεωδών είναι περιοχή μοναδικής παραγοντοποίησης. Παρόλα αυτά το αντίστροφο δεν ισχύει γενικά. Για παράδειγμα, ο δακτύλιος  $\mathbb{Z}[x, y]$  είναι Π.Μ.Π., αλλά δεν είναι Π.Κ.Ι. Παρόλα αυτά το αντίστροφο ισχύει κάτω από ειδικές προϋποθέσεις!

**Πρόταση 22.** Ο αριθμός κλάσεων της ομάδας κλάσεων ιδεωδών ισούται με 1 αν και μόνο αν  $\mathcal{R}_K$  είναι περιοχή μοναδικής παραγοντοποίησης.

*Απόδειξη.* • Το ευθύ είναι άμεσο, καθώς αν  $h_K = 1$ , τότε  $\mathcal{R}_K$  είναι Π.Κ.Ι.

- Αντίστροφα, υποθέτουμε ότι  $\mathcal{R}_K$  είναι περιοχή μοναδικής παραγοντοποίησης. Αρχεί να δείξουμε ότι κάθε πρώτο ιδεώδες του  $\mathcal{R}_K$  είναι κύριο. Έστω  $\mathfrak{p} \in \text{Spec}(R)$  και  $a \in \mathfrak{p} \setminus \{0\}$ . Τότε, υπάρχουν ανάγωγα στοιχεία  $p_1, \dots, p_k \in \mathcal{R}_K$  ανάγωγα και  $a_1, \dots, a_k \in \mathbb{Z}$  τέτοια ώστε

$$a = p_1^{a_1} \cdots p_k^{a_k}$$

- Γνωρίζουμε ότι σε Π.Μ.Π. κύρια ιδεώδη που παράγονται από ανάγωγα στοιχεία είναι πρώτα. Άρα, κάθε ιδεώδες  $\mathfrak{p}_i = \langle p_i \rangle$  είναι πρώτο.
- Έχουμε ότι

$$\langle a \rangle = \prod_{i=1}^k \mathfrak{p}_i^{a_i} \subseteq \mathfrak{p}$$

- Αφού  $\mathfrak{p} | \langle a \rangle$ , από την μοναδικότητα ανάλυσης σε πρώτα ιδεώδη, προκύπτει ότι υπάρχει  $j$  ώστε  $\mathfrak{p} = \mathfrak{p}_j$  και έχουμε το ζητούμενο. □

**Κίνητρο 9.** Θα δείξουμε ότι  $h_K$  είναι πεπερασμένη. Για να αποδειχθεί αυτό όμως πρέπει να αποδείξουμε μια σειρά από βοηθητικά λήμματα. Παρόλα αυτά, αν για την ώρα υποθέσουμε ότι ο παραπάνω ισχυρισμός είναι σωστός, μπορούμε να δείξουμε τα ακόλουθα αποτελέσματα.

**Πρόταση 23.** Έστω  $A$  ακέραιο ιδεώδες του  $K$ , για το οποίο υπάρχει  $m$  φυσικός αριθμός ώστε  $A^m$  να είναι κύριο με  $(m, h_K) = 1$ . Τότε, το  $A$  είναι κύριο.

*Απόδειξη.* Υπάρχει  $x, y \in \mathbb{Z}$  ώστε  $1 = xm + yh_K$ . Τότε, ισχύει ότι

$$A\mathcal{H}_K = A^1\mathcal{H}_K = \left[ (A^{h_K}) \right]^y \mathcal{H}_K \cdot [(A^m)]^x \mathcal{H}_K = \mathcal{H}_K.$$

□

## 11 Μάθημα 11

### 11.1 Ομάδα Κλάσεων Ιδεωδών

**Λήμμα 9.** Έστω  $K$  αλγεβρικό σώμα αριθμών και  $\omega_1, \dots, \omega_n$  μια βάση ακεραιότητας του  $K$ . Τότε, υπάρχει σταθερά  $C > 0$  ώστε για κάθε  $(x_1, \dots, x_n) \in \mathbb{Q}^n$  να ισχύει ότι

$$\left| N_{K/\mathbb{Q}} \left( \sum_{i=1}^n x_i \omega_i \right) \right| \leq C \cdot \left( \max_i |x_i| \right)^n$$

*Απόδειξη.* Έστω  $\sigma_1, \dots, \sigma_n$  οι  $\mathbb{Q}$ -εμφυτεύσεις του  $K$  στο  $\mathbb{C}$ . Τότε, ισχύει ότι

$$\begin{aligned} \left| N_{K/\mathbb{Q}} \left( \sum_{i=1}^n x_i \omega_i \right) \right| &= \left| \prod_{j=1}^n \sum_{i=1}^n [x_i \sigma_j(\omega_i)] \right| = \prod_{j=1}^n \left| \sum_{i=1}^n [x_i \sigma_j(\omega_i)] \right| \\ &\leq \left( \prod_{j=1}^n \left| \sum_{i=1}^n [\sigma_j(\omega_i)] \right| \right) \cdot \left( \max_i |x_i| \right)^n \end{aligned}$$

Άρα, για  $C = \prod_{j=1}^n \left| \sum_{i=1}^n [\sigma_j(\omega_i)] \right| > 0$  έχουμε το ζητούμενο.  $\square$

**Παράδειγμα 24.** Έστω  $K = \mathbb{Q}(i)$  και  $\mathbb{Z}[i]$  με  $\{1, i\}$  βάση ακεραιότητας του  $K$ . Αν  $\sigma_1, \sigma_2$  οι  $\mathbb{Q}$ -εμφυτεύσεις του  $K$  στο  $\mathbb{Q}$ , τότε  $\sigma_1(i) = i$  και  $\sigma_2(i) = -i$ . Συνεπώς, για κάθε  $x_1, x_2 \in \mathbb{Q}$ , έχουμε ότι

$$\left| N_{K/\mathbb{Q}}(x_1 + x_2 \cdot i) \right| = x_1^2 + x_2^2 \leq 2 \cdot (\max\{|x_1|, |x_2|\})^2.$$

**Πρόταση 24.** Αν  $C > 0$  η σταθερά του Λήμματος 9 και  $A$  μη μηδενικό ιδεώδες του  $\mathcal{R}_K$ , τότε υπάρχει  $a \in A \setminus \{0\}$  τέτοιο ώστε

$$\left| N_{K/\mathbb{Q}}(a) \right| \leq C \cdot N_K(A).$$

*Απόδειξη.* Θεωρούμε το σύνολο

$$\mathcal{A} = \left\{ \sum_{i=1}^n x_i \omega_i \mid x_i \in \mathbb{Z}, 1 \leq x_i \leq \sqrt[n]{N_K(A)} + 1 \right\}$$

Αφού  $|\mathcal{A}| = \left( \sqrt[n]{N_K(A)} + 1 \right)^n > N_K(A) = |\mathcal{R}_K/A|$ , από την αρχή του περιστέρωνα, υπάρχουν  $\xi_1 \neq \xi_2$  στο  $\mathcal{A}$  ώστε  $\xi_1 - \xi_2 \in A$ . Δείξτε ότι το  $a = \xi_1 - \xi_2$  ικανοποιεί τη ζητούμενη σχέση.  $\square$

**Λήμμα 10.** Έστω  $C > 0$  η σταθερά του Λήμματος 9 και  $c \in \mathcal{C}_K$ . Τότε, υπάρχει  $A \in c$  ακέραιο, τέτοιο ώστε  $|N_K(A)| < C$ .

*Απόδειξη.* • Έστω  $A' \in c^{-1}$ . Τότε, υπάρχει  $a \in K$  τέτοιο ώστε  $aA' \subseteq \mathcal{R}_K$ , συνεπώς  $aA' \equiv A' \pmod{H_K}$ , άρα χ.β.γ. μπορούμε να υποθέσουμε ότι  $A'$  είναι ιδεώδες του  $\mathcal{R}_K$ .

- Από την Πρόταση 24, υπάρχει  $b \in A' \setminus \{0\}$ , τέτοιο ώστε  $|N_{K/\mathbb{Q}}(b)| \leq C \cdot N_K(A')$ .
- Ορίζουμε  $A = (b \cdot \mathcal{R}_K) \cdot (A')^{-1} \in c$ . Είναι άμεσο ότι  $A \subseteq \mathcal{R}_K$ , αφού  $b \in A'$ . Τώρα, από την πολλαπλασιαστικότητα της  $N_K$ , παρατηρούμε ότι

$$|N_K(A)| = \frac{|N_K(b \cdot \mathcal{R}_K)|}{|N_K(A')|} = \frac{|N_{K/\mathbb{Q}}(b)|}{|N_K(A')|} \leq C.$$

□

**Λήμμα 11.** Υπάρχουν πεπερασμένα το πλήθος ακέραια ιδεώδη  $A$  με την ιδιότητα  $N_K(A) \leq C$ .

*Απόδειξη.* Αν δείξουμε ότι για κάθε  $m \in \mathbb{N}$ , τότε υπάρχουν πεπερασμένα το πλήθος ακέραια ιδεώδη  $A$  τ.ω.  $N_K(A) = m$ , τότε προφανώς έχουμε το ζητούμενο.

- Έστω  $A$  ακέραιο ιδεώδες με  $N_K(A) = m$ . Τότε, για κάθε  $a \in \mathcal{R}_K$ , ισχύει ότι  $ma \in A$ , συνεπώς  $m \cdot \mathcal{R}_K \subseteq A$ .
- Θέτουμε  $B = m \cdot \mathcal{R}_K \cdot A^{-1}$  ακέραιο ιδεώδες του  $K$ .
- Τότε, υπάρχουν  $\mathfrak{p}_1, \dots, \mathfrak{p}_s \in \text{Spec}(\mathcal{R}_K)$  τέτοια ώστε

$$\prod_{i=1}^s \mathfrak{p}_i^{m_i} = m \cdot \mathcal{R}_K = A \cdot B$$

Από την μοναδικότητα της ανάλυσης σε πρώτα ιδεώδη, υπάρχουν πεπερασμένες επιλογές για το  $A$ .

□

**Πόρισμα 10.** Αν  $h_K = |\mathcal{C}_K| = |\mathcal{I}_K/\mathcal{H}_K|$ , τότε το  $h_K$  είναι πεπερασμένο.

*Απόδειξη.* Άμεσο από τα Λήμματα 10 και 11.

□

## 12 Μάθημα 12

## 13 Μάθημα 13

### 13.1 Πρώτο Θεώρημα Ανάλυσης

Θεωρούμε αλγεβρικά σώματα αριθμών  $K \subseteq L \subseteq M$  και τα αντίστοιχους δακτυλίους Dedekind των ακεραίων αλγεβρικών  $R \subseteq S \subseteq T$ . Θεωρούμε τα αντίστοιχα πρώτα ιδεώδη  $\mathfrak{p} \in \text{Spec}(R)$ ,  $\mathfrak{q} \in \text{Spec}(S)$  και  $\mathfrak{u} \in \text{Spec}(T)$ . Οι προηγούμενοι συμβολισμοί θα παραμείνουν ως αναλλοίωτοι στη συνέχεια.

**Παρατήρηση 30.** Παρατηρούμε ότι το  $\mathfrak{p}S = \langle ps \mid p \in \mathfrak{p}, s \in S \rangle$  είναι ιδεώδες του  $S$ . Παρότι  $\mathfrak{p}$  είναι πρώτο, το ιδεώδες  $\mathfrak{p}S$  δεν είναι κατ' ανάγκη πρώτο παρόλα αυτά, επειδή  $S$  είναι του Dedekind, γράφεται μοναδικά

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} \quad (9)$$

όπου  $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \text{Spec}(S)$ .

**Κίνητρο 10.** Παρότι υπαρκτικά γνωρίζουμε ότι το  $\mathfrak{p}S$  γραφεται όπως παραπάνω, θα θέλαμε να γνωρίζουμε πλήρως ποια είναι τα ιδεώδη  $\mathfrak{q}_1, \dots, \mathfrak{q}_r$  καθώς και τους αντίστοιχους εκθέτες  $e_1, \dots, e_r$ .

**Πρόταση 25.** Τα ακόλουθα είναι ισοδύναμα.

- (α)  $\mathfrak{q} \mid \mathfrak{p}S$
- (β)  $\mathfrak{p}S \subseteq \mathfrak{q}$
- (γ)  $\mathfrak{p} \subseteq \mathfrak{q}$
- (δ)  $\mathfrak{p} = R \cap \mathfrak{q}$
- (ε)  $\mathfrak{p} = K \cap \mathfrak{q}$

**Ορισμός 33.** Αν ισχύει κάποια από τις παραπάνω σχέσεις, θα λέμε ότι το  $\mathfrak{q}$  βρίσκεται πάνω από το  $\mathfrak{p}$  ή ότι το  $\mathfrak{p}$  βρίσκεται κάτω από το  $\mathfrak{q}$ .

**Πρόταση 26.** Με βάση την ισότητα 9, τα  $\mathfrak{q}_1, \dots, \mathfrak{q}_r$  είναι τα μοναδικά πρώτα ιδεώδη του  $S$  που βρίσκονται πάνω από το  $\mathfrak{p}$  στην επέκταση  $L/K$ .

**Ορισμός 34.** (α) Γνωρίζουμε ότι

$$\mathfrak{p}S = \prod_{\mathfrak{q} \in \text{Spec}(S)} \mathfrak{q}^{\alpha(\mathfrak{q})}$$

Ο εκθέτης  $e(\mathfrak{q}/\mathfrak{p}) = \alpha(\mathfrak{q})$  λέγεται **δείκτης διακλάσωσης** του  $\mathfrak{q}$  υπεράνω του  $\mathfrak{p}$ .

(β) Αν  $e(\mathfrak{q}/\mathfrak{p}) > 1$ , θα λέμε ότι το  $\mathfrak{q}$  **διακλαδίζεται** υπεράνω του  $\mathfrak{p}$ .

(γ) Θα λέμε ότι  $\mathfrak{p}$  **διακλαδίζεται** υπέρ του  $L$  αν υπάρχει  $\mathfrak{q} \in \text{Spec}(S)$ , ώστε  $e(\mathfrak{q}/\mathfrak{p}) > 1$ .

**Παρατήρηση 31.** Έστω ότι  $\mathfrak{q}$  είναι πάνω από το  $\mathfrak{p}$ . Τότε,  $\mathfrak{p} \subseteq \mathfrak{q}$ . Θεωρούμε τον μονομορφισμό σωμάτων

$$i: R/\mathfrak{p} \rightarrow S/\mathfrak{q}, \quad r + \mathfrak{p} \mapsto r + \mathfrak{q}.$$

Επομένως, μπορούμε να θεωρήσουμε το  $R/\mathfrak{p}$  ως υπόσωμα του  $S/\mathfrak{q}$ .

**Ορισμός 35.** Αν  $\mathfrak{q}$  βρίσκεται πάνω από το  $\mathfrak{p}$ , τότε ο ακέραιος

$$f(\mathfrak{q}/\mathfrak{p}) = [S/\mathfrak{q} : R/\mathfrak{p}]$$

λέγεται **βαθμός αδράνειας** του  $\mathfrak{q}$  πάνω από το  $\mathfrak{p}$ .

**Πρόταση 27.** Αν  $\mathfrak{q}$  βρίσκεται πάνω από το  $\mathfrak{p}$ , τότε ισχύει ότι

$$N_{L/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\mathfrak{p})^{f(\mathfrak{q}/\mathfrak{p})}.$$

*Απόδειξη.* Θυμίζει από την θεωρία πεπερασμένων σωμάτων, ότι αν  $\mathbb{F}' \subseteq \mathbb{F}$  πεπερασμένα σώματα με  $|\mathbb{F}'| = p^m$  και  $|\mathbb{F}| = p^n$ , τότε έχουμε ότι  $m|n$  και μάλιστα  $[\mathbb{F} : \mathbb{F}'] = n/m \in \mathbb{Z}$ . Μέσω αυτή της παρατήρησης και του ορισμού της νόρμας, έχουμε το ζητούμενο.  $\square$

*Απόδειξη.* Αν  $\mathfrak{u}$  βρίσκεται πάνω από το  $\mathfrak{q}$  και  $\mathfrak{q}$  βρίσκεται πάνω από το  $\mathfrak{p}$ , τότε

$$e(\mathfrak{u}/\mathfrak{p}) = e(\mathfrak{u}/\mathfrak{q}) \cdot e(\mathfrak{q}/\mathfrak{p}) \quad \text{και} \quad f(\mathfrak{u}/\mathfrak{p}) = f(\mathfrak{u}/\mathfrak{q}) \cdot f(\mathfrak{q}/\mathfrak{p})$$

$\square$

*Απόδειξη.* Η πρώτη ισότητα προκύπτει άμεσα από την μοναδικότητα της ανάλυσης σε πρώτα ιδεώδη. Για την δεύτερη ισότητα, το ζητούμενο προκύπτει άμεσα από την παραπάνω πρόταση και το γεγονός  $N_{K/\mathbb{Q}}(\mathfrak{p}) \geq 2$ , αφού  $\mathfrak{p} \subsetneq R$ .  $\square$



**Θέωρημα 17** (Πρώτο Θεώρημα Ανάλυσης). Έστω  $[L : K] = n$  και  $\mathfrak{p} \in \text{Spec}(R)$ . Αν  $\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ ,  $e_i = e(\mathfrak{q}_i/\mathfrak{p})$  και  $f_i = f(\mathfrak{q}_i/\mathfrak{p})$ , τότε

$$n = e_1 f_1 + \cdots + e_r f_r = \sum_{\mathfrak{q} \supseteq \mathfrak{p}} e(\mathfrak{q}/\mathfrak{p}) \cdot f(\mathfrak{q}_i/\mathfrak{p}).$$

Απόδειξη. Από την ανάλυση του  $\mathfrak{p}S$ , την πολλαπλασιαστικότητα της νόρμας και από την Πρόταση 27 έχουμε ότι

$$N_{L/\mathbb{Q}}(\mathfrak{p}S) = N_{K/\mathbb{Q}}(\mathfrak{p})^{\sum_{i=1}^r e_i f_i}$$

Αφού  $\mathfrak{p} \subsetneq R$ , τότε  $N_{K/\mathbb{Q}}(\mathfrak{p}) \geq 2$ , συνεπώς, αρκεί να δείξουμε ότι  $N_{L/\mathbb{Q}}(\mathfrak{p}S) = N_{K/\mathbb{Q}}(\mathfrak{p})^n$ .

- Αφού  $h_K < \infty$ , τότε υπάρχει  $a \neq 0$  στο  $R$  τέτοιο ώστε  $\mathfrak{p}^{h_K} = aR$ . Συνεπώς, έχουμε ότι  $\mathfrak{p}^{h_K} S = aS$ .
- Αν δείξουμε ότι

$$N_{L/\mathbb{Q}}(\mathfrak{p}S)^{h_K} = N_{L/\mathbb{Q}}(\mathfrak{p}^{h_K} S) = N_{K/\mathbb{Q}}(\mathfrak{p})^{n \cdot h_K}$$

τότε θα έχουμε δείξει το ζητούμενο.

- Έχουμε ότι

$$N_{L/\mathbb{Q}}(\mathfrak{p}^{h_K} S) = N_{L/\mathbb{Q}}(aS) = |N_{L/\mathbb{Q}}(a)|$$

Από τις Προτάσεις 11,12 προκύπτει ότι

$$|N_{L/\mathbb{Q}}(a)| = |N_{K/\mathbb{Q}}(N_{L/K}(a))| = |N_{K/\mathbb{Q}}(a)^n| = N_{K/\mathbb{Q}}(\mathfrak{p})^{n \cdot h_K}.$$

□

**Παράδειγμα 25.** Έστω  $L$  τετραγωνικό σώμα αριθμών ( $K = \mathbb{Q}$ ) και  $[K : \mathbb{Q}] = 2$ . Τότε, έχουμε ότι  $R = \mathbb{Z}$ . Θεωρούμε πρώτο ιδεώδες  $\mathfrak{p} = p\mathbb{Z}$  του  $R$ . Από το Πρώτο Θεώρημα Ανάλυσης έχουμε ότι οι πιθανές αναλύσεις του  $\mathfrak{p}S$  σε πρώτα ιδεώδη είναι

$$\mathfrak{p}S = \begin{cases} \mathfrak{q}, & f(\mathfrak{q}/\mathfrak{p}) = 2, e(\mathfrak{q}/\mathfrak{p}) = 1 \\ \mathfrak{q}_1 \mathfrak{q}_2, & f(\mathfrak{q}_i/\mathfrak{p}) = 1, e(\mathfrak{q}_i/\mathfrak{p}) = 1 \\ \mathfrak{q}^2, & f(\mathfrak{q}/\mathfrak{p}) = 1, e(\mathfrak{q}/\mathfrak{p}) = 2 \end{cases}$$

### 13.2 Νόμος ανάλυσης σε επεκτάσεις Galois

**Πρόταση 28.** Έστω  $\sigma$  ένας  $K$  αυτομορφισμός του  $L$ . Υποθέτουμε ότι  $\mathfrak{q}$  βρίσκεται πάνω από το  $\mathfrak{p}$ . Ισχύουν τα ακόλουθα.

- (α) Το  $\sigma(\mathfrak{q})$  είναι πρώτο ιδεώδες του  $S$ .
- (β)  $\mathfrak{p} \subseteq \sigma(\mathfrak{q})$
- (γ)  $f(\mathfrak{q}/\mathfrak{p}) = f(\sigma(\mathfrak{q})/\mathfrak{p})$
- (δ)  $e(\mathfrak{q}/\mathfrak{p}) = e(\sigma(\mathfrak{q})/\mathfrak{p})$

*Απόδειξη.* Δείχνοντας ότι  $\sigma(S) \subseteq S$  έχουμε ότι  $\sigma(S) = S$  (κάνοντας το ίδιο για την  $\sigma^{-1}$ ). Συνεπώς,  $\sigma|_S: S \rightarrow S$  είναι ένας  $K$  - αυτομορφισμός του  $S$ .

- (α) Από την παραπάνω παρατήρηση είναι σαφές ότι  $\sigma(\mathfrak{q})$  είναι ιδεώδες του  $S$ . Θεωρούμε την απεικόνιση

$$\tilde{\sigma}: \frac{S}{\mathfrak{q}} \rightarrow \frac{S}{\sigma(\mathfrak{q})}, \quad s + \mathfrak{q} \mapsto \sigma(s) + \sigma(\mathfrak{q}).$$

η οποία είναι ισομορφισμός δακτυλίων. Συνεπώς, έχουμε ότι  $\sigma(\mathfrak{q})$  πρώτο.

- (β) Έχουμε ότι

$$\sigma(\mathfrak{q}) \cap K = \sigma(\mathfrak{q} \cap K) = \sigma(\mathfrak{p}) = \mathfrak{p}$$

όπου οι παραπάνω σχέσεις ισχύουν γιατί  $\sigma$  είναι  $K$  - αυτομορφισμός.

- (γ) Από τον παραπάνω ισομορφισμό προκύπτει άμεσα και το ζητούμενο.

- (δ) Αν  $\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ , τότε αφού  $\sigma(\mathfrak{p}S) = \mathfrak{p}S$ , έχουμε ότι

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} = \sigma(\mathfrak{q}_1)^{e_1} \cdots (\mathfrak{q}_r)^{e_r} = \sigma(\mathfrak{p}S)$$

Από την μοναδικότητα της ανάλυσης σε πρώτα ιδεώδη έχουμε το ζητούμενο.

□

**Θέωρημα 18.** Έστω  $L/K$  επέκταση Galois και  $G = \text{Gal}(K/L)$ . Αν

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

τότε η  $G$  δρα μεταβατικά στο  $\{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ . Δηλαδή, για κάθε  $\mathfrak{q}_i, \mathfrak{q}_j$ , υπάρχει  $\sigma \in G$  ώστε  $\mathfrak{q}_j = \sigma(\mathfrak{q}_i)$ .

Απόδειξη. Έστω, προς άτοπο, ότι υπάρχουν  $\mathfrak{q}_i, \mathfrak{q}_j$  τέτοια ώστε  $\mathfrak{q}_j \notin \{\sigma(\mathfrak{q}_i \mid \sigma \in G)\}$ . Από αυτό το γεγονός, προκύπτει ότι τα ιδεώδη  $\mathfrak{q}_j, \sigma(\mathfrak{q}_i)$  (για κάθε  $\sigma \in G$ ) είναι σχετικά πρώτα, άρα από το Κινέζικο Θεώρημα Υπολοίπων, το σύστημα

$$\begin{aligned} x &\equiv 0 \pmod{\mathfrak{q}_j} \\ x &\equiv 1 \pmod{\sigma(\mathfrak{q}_i)}, \quad \text{για κάθε } \sigma \in G \end{aligned}$$

έχει λύση  $s \in S$ . Συνεπώς, αφού  $s \in S$ , έχουμε ότι

$$N_{L/K}(s) = \prod_{\sigma \in G} \sigma(s) \in K \cap S = R.$$

Αφού  $s \equiv 0 \pmod{\mathfrak{q}_j}$ , τότε  $s \in \mathfrak{q}_j$ , συνεπώς από την Παρατήρηση 28  $N_{L/K}(s) \in \mathfrak{q}_j \cap R = \mathfrak{p}$ . Από τις σχέσεις  $s \equiv 1 \pmod{\sigma(\mathfrak{q}_i)}$ , για κάθε  $\sigma \in G$  έχουμε ότι  $\sigma(s) = s \notin \mathfrak{q}_i$ . Επομένως,

$$N_{L/K}(s) = \prod_{\sigma \in G} \sigma(s) \notin \mathfrak{q}_i \cap K = \mathfrak{p}$$

και έτσι καταλήγουμε σε άτοπο. □

**Πόρισμα 11.** Αν  $L/K$  επέκταση Galois, τότε για κάθε  $\mathfrak{p} \in \text{Spec}(R)$  ισχύει ότι

$$\mathfrak{p}S = (\mathfrak{q}_1 \cdots \mathfrak{q}_r)^e$$

όπου  $e = e(\mathfrak{q}_i/\mathfrak{p})$  και  $f = f(\mathfrak{q}_i/\mathfrak{p})$ , για κάθε  $i = 1, \dots, r$ . Επιπλέον,  $n = efr$ .

Απόδειξη. Το ζητούμενο έπεται άμεσα από την Πρόταση 28, το παραπάνω Θεώρημα και τον Πρώτο Νόμο Ανάλυσης. □

### 13.3 Τάξεις Σωμάτων

**Κίνητρο 11.** Το πρώτο θεώρημα ανάλυσης μας δίνει πληροφορίες σχετικά με τους βαθμούς διακλάδωσης και αδράνειας, αλλά δεν δίνει καμία πληροφορία σχετικά με το ποια είναι τα ιδεώδη που εμφανίζονται στην ανάλυση του  $\mathfrak{p}S$ . Αυτό το κενό έρχεται να καλυφθεί το δεύτερο θεώρημα ανάλυσης.

**Ορισμός 36.** Έστω  $L$  αλγεβρικό σώμα αριθμών με  $n = [L : \mathbb{Q}]$  και  $\mathcal{O} \subseteq L$ . Το  $\mathcal{O}$  θα λέγεται **τάξη** του  $L$ , αν ισχύουν τα παρακάτω :

- (α) Το  $\mathcal{O}$  είναι ελεύθερη αβελιανή ομάδα τάξης  $n$ .
- (β) Το  $\mathcal{O}$  είναι υποδακτύλιος του  $L$  με  $1 \in \mathcal{O}$ .

**Παρατήρηση 32.** Έστω  $\mathcal{O}$  τάξη του  $L$ . Ισχύουν τα ακόλουθα.

- (α)  $\mathcal{O} \subseteq S$ , όπου  $S$  ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του  $L$ .
- (β)  $[S : \mathcal{O}] = m < \infty$
- (γ)  $mS \subseteq \mathcal{O}$

*Απόδειξη.* (α) Έστω  $\{\omega_1, \dots, \omega_n\}$  μια βάση του  $\mathcal{O}$  και  $s \in \mathcal{O}$ . Τότε, υπάρχει  $A \in M_n(\mathbb{Z})$  ώστε να ισχύουν τα παρακάτω :

$$s \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A \cdot \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \Leftrightarrow (A - sI_n) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = 0.$$

Αφού το σύστημα  $(A - sI_n)X = 0$  έχει μη μηδενική λύση, τότε  $\det(A - sI_n) = 0$ , συνεπώς  $s \in \mathcal{O}$  είναι ακέραιος αλγεβρικός.

- (β) Αφού  $\mathcal{O} \subseteq S$  και  $\mathcal{O}, S$  είναι ελεύθερες αβελιανές τάξης  $n$ , τότε  $[S : \mathcal{O}] = m < \infty$ .
- (γ) Άμεσο από το (β).

□

**Παρατήρηση 33.** Έστω  $K \subseteq L$  σώματα και  $R, S$  οι αντίστοιχοι δακτύλιοι των ακεραίων αλγεβρικών. Αφού  $L/K$  είναι διαχωρίσιμη, υπάρχει  $\vartheta \in S$  τ.ω.  $L = K(\vartheta)$ . Θα δείξουμε ότι  $S^* = R[\vartheta]$  είναι τάξη του  $L$ .

- Γνωρίζουμε ότι ισχύει η παρακάτω σχέση

$$R[\vartheta] \subseteq S \subseteq D_K(\vartheta)^{-1} \cdot R[\vartheta]$$

Αφού  $S$  είναι ελεύθερη αβελιανή βαθμού  $n$  και ισχύουν οι παρακάτω σχέσεις περιέχονται

$$D_K(\vartheta) \cdot S \subseteq R[\vartheta] \subseteq S$$

όπως και στην Πρόταση 15, προκύπτει ότι  $R[\vartheta]$  είναι ελεύθερη αβελιανή βαθμού  $n$ .

- Γνωρίζουμε ότι  $R[\vartheta]$  είναι υποδακτύλιος τους  $S$  με  $1 \in R[\vartheta]$ .

**Ορισμός 37.** Έστω  $S^*$  μια τάξης του αλγεβρικού σώματος  $L$ , όπου  $S$  είναι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του  $L$ . Ο **οδηγός** τάξης  $S^*$  ορίζεται να είναι το σύνολο

$$\mathcal{F} = \mathcal{F}_{S/S^*} = \{\xi \in S^* \mid \xi \cdot S \subseteq S^*\}$$

## 14 Μάθημα 14

### 14.1 Τάξεις και Οδηγοί Τάξεων

**Παρατήρηση 34.** Έστω  $S^*$  μια τάξης του αλγεβρικού σώματος  $L$ , όπου  $S$  είναι ο δακτύλιος των ακέραιων αλγεβρικών αριθμών του  $L$ . Ισχύουν τα ακόλουθα.

- (α) Το  $\mathcal{F}$  είναι ιδεώδες του  $S$ .
- (β) Αν  $m = [S : S^*]$ , τότε  $mS \subseteq \mathcal{F}$ .

**Παράδειγμα 26.** Έστω  $L = \mathbb{Q}(\sqrt{d})$ , όπου  $d$  είναι ελεύθερο τετραγώνου. Έχουμε δείξει ότι  $S = \mathbb{Z} + \mathbb{Z}\omega$ , όπου

$$\omega = \begin{cases} \sqrt{d}, & d \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod{4} \end{cases}$$

Θα χαρακτηρίσουμε πλήρως τις τάξεις του  $K$ . Έστω  $S^*$  τάξη του  $K$ , άρα είναι ελεύθερη αβελιανή τάξης 2 και  $1 \in S^*$ .

- Έστω  $\{\omega_1, \omega_2\}$  μια βάση της  $S^*$ . Τότε, έχουμε ότι

$$\omega_1 = x_1 + y_1\omega \quad \text{και} \quad \omega_2 = x_2 + y_2\omega$$

Έχουμε ότι  $1 \in S^*$ , συνεπώς υπάρχουν  $n_1, n_2 \in \mathbb{Z}$  τ.ω.

$$1 = n_1\omega_1 + n_2\omega_2 \Rightarrow n_1x_1 + n_2x_2 = 1 \quad \text{και} \quad n_1y_1 + n_2y_2 = 0$$

- Θεωρούμε τον πίνακα

$$A = \begin{pmatrix} n_1 & n_2 \\ -x_2 & x_1 \end{pmatrix}$$

Αν  $\omega' = -x_2\omega_1 + x_1\omega_2$ , παρατηρήστε ότι  $\{1, \omega'\}$  είναι μια βάση της  $S^*$ , διότι

$$\begin{pmatrix} 1 \\ \omega' \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

και  $A$  είναι unimodular από την παραπάνω σχέση.

- Επίσης, υπάρχει μονασήμαντα ορισμένος πίνακας  $B$  τ.ω.

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = B \cdot \begin{pmatrix} 1 \\ \omega \end{pmatrix}, \quad B = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$$

Από την Πρόταση 14, προκύπτει ότι  $m = [S : S^*] = \pm \det B$ . Συνδυάζοντας τις προηγούμενες σχέσεις έχουμε ότι

$$\begin{pmatrix} 1 \\ \omega' \end{pmatrix} = AB \begin{pmatrix} 1 \\ \omega \end{pmatrix} \Leftrightarrow \begin{pmatrix} 1 \\ \omega' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & -\det B \end{pmatrix} \begin{pmatrix} 1 \\ \omega \end{pmatrix}$$

Επομένως,  $\omega' = a \pm m\omega$ , από όπου προκύπτει ότι  $S^* = \mathbb{Z} \oplus \mathbb{Z}(m\omega)$ . Προφανώς, και αντίστροφα κάθε  $S^* = \mathbb{Z} \oplus \mathbb{Z}(m\omega)$ , όπου  $m \in \mathbb{N}$  είναι τάξη του  $K$ . Άρα, οι τάξεις του  $K$  είναι 1-1 και επί αντιστοιχία με τους φυσικούς αριθμούς.

**Πρόταση 29.** Έστω  $S^*$  τάξη του  $L$  με οδηγό  $\mathcal{F}$ . Τότε τα σύνολα

$$D_S(\mathcal{F}) = \{A \mid A \text{ ακέραιο ιδεώδες του } S, A + \mathcal{F} = S\}$$

και

$$D_{S^*}(\mathcal{F}) = \{A^* \mid A^* \text{ ακέραιο ιδεώδες του } S^*, A^* + \mathcal{F} = S^*\}$$

είναι πολλαπλασιαστικές ημιομάδες που ισχύει ο νόμος της διαγραφής.

*Απόδειξη.* • Αρχικά θα δείξουμε ότι  $D_S(\mathcal{F})$  είναι πολλαπλασιαστική ημιομάδα. Έστω  $A, B \in D_S(\mathcal{F})$ , δηλαδή  $A + \mathcal{F} = A + \mathcal{F} = S$ . Πολλαπλασιάζοντας τις δύο σχέσεις προκύπτει ότι  $AB + \mathcal{F} = S$ . Ο νόμος διαγραφής ισχύει, αφού ο  $S$  είναι δακτύλιος του Dedekind και άρα κάθε μη μηδενικό ιδεώδες αντιστρέφεται.

- Όπως παραπάνω, προκύπτει άμεσα ότι  $D_{S^*}(\mathcal{F})$  είναι ημιομάδα. Ο νόμος διαγραφής προκύπτει από το αποτέλεσμα του παρακάτω θεωρήματος, όπου θα δείξουμε ότι  $D_S(\mathcal{F})$  και  $D_{S^*}(\mathcal{F})$  είναι ισόμορφες ως ημιομάδες.

□

**Υπενθύμιση 4.** (α) Έστω  $A, B, C$  προσθετικές υποομάδες μιας  $(G, +)$ . Αν  $A \subseteq C$ , τότε  $(A + B) \cap C = A \cap (B \cap C)$ .

(β) Αν  $A, B$  ιδεώδη δακτυλίου  $R$  τ.ω.  $A + B = S$ , τότε  $AB = A \cap B$ .

**Θέωρημα 19.** Έστω  $S^*$  τάξη του  $L$  με οδηγό  $\mathcal{F}$ . Ισχύουν τα ακόλουθα.

(α) Η απεικόνιση  $i: D_{S^*}(\mathcal{F}) \rightarrow D_S(\mathcal{F})$  με  $i(A^*) = SA^*$  είναι ισομορφισμός ημιομάδων με αντίστροφη

$$j: D_S(\mathcal{F}) \rightarrow D_{S^*}(\mathcal{F}), \quad j(A) = A \cap S^*$$

(β) Για κάθε  $A \in D_S(\mathcal{F})$  ισχύει ότι  $S/A \cong S^*/A^*$ , όπου  $A^* = A \cap S^*$ .

Απόδειξη. (α) • Αρχικά πρέπει να δείξουμε ότι η  $i$  είναι καλά ορισμένη. Έστω  $A^* \in D_{S^*}(\mathcal{F})$ , δηλαδή  $A^* + \mathcal{F} = S^*$ . Συνεπώς, έχουμε ότι

$$\begin{aligned} SA^* + S\mathcal{F} &= SS^* \\ SA^* + \mathcal{F} + S & \end{aligned}$$

όπου η δεύτερη ισότητα ισχύει γιατί  $\mathcal{F}$  είναι ιδεώδες του  $S$  και  $1 \in S^*$ .

- Είναι άμεσο ότι η  $i$  είναι ομομορφισμός ημιομάδων.
- Για να δείξουμε ότι  $i$  είναι μονομορφισμός, αρκεί να δείξουμε ότι έχει αριστερή αντίστροφο την  $j$ . Δηλαδή, θα δείξουμε ότι

$$j \circ i(A^*) = A^* \Leftrightarrow (SA^*) \cap S^* = A^*$$

Έχουμε ότι

$$\begin{aligned} (SA^*) \cap S^* &= (SA^*) \cap (A^* + \mathcal{F}) = A^* + SA^* \cap \mathcal{F} = A^* + SA^*\mathcal{F} \\ &= A^* + A^*\mathcal{F} = A^*(S^* + \mathcal{F}) = A^*S^* = A^* \end{aligned}$$

- Θα δείξουμε ότι  $i$  είναι επιμορφισμός, δείχνοντας ότι έχει δεξιά αντίστροφο την  $j$ . Δηλαδή θα δείξουμε ότι

$$i \circ j(A) = A \Leftrightarrow S(S^* \cap A) = A$$

Έχουμε ότι

$$\begin{aligned} S(S^* \cap A) &= (A + \mathcal{F})(S^* \cap A) = A \cdot (S^* \cap A) + \mathcal{F} \cdot (S^* \cap A) \\ &= A \cdot (S^* \cap A) + \mathcal{F} \cap A = A \cdot (S^* \cap A) + \mathcal{F} \cdot A = A \cdot (S^* \cap A + \mathcal{F}) = AS^* = A \end{aligned}$$

(β) Θεωρούμε την  $\varphi: S^*/A^* \rightarrow S/A$  με  $\varphi(s + A^*) = s + A$ . Η  $\varphi$  είναι άμεσα μονομορφισμός και επί προκύπτει από το γεγονός  $A + \mathcal{F} = S$ . □

## 14.2 Δεύτερο Θεώρημα Ανάλυσης

**Παρατήρηση 35.** • Έστω  $K \subseteq L$  αλγεβρικά σώματα αριθμών,  $R, S$  οι αντίστοιχοι δακτύλιοι ακεραίων αλγεβρικών με  $L = K(\vartheta)$ , όπου  $\vartheta \in S$ . Έστω  $\mathcal{F}$  ο οδηγός της τάξης  $R[\vartheta]$  και  $g(x) = \text{Irr}(\vartheta, K) \in R[x]$  (αφού  $\vartheta \in S$ ).

- Θεωρούμε  $\mathfrak{p} \in \text{Spec}(R)$  τ.ω.  $\mathfrak{p}S + \mathcal{F} = S$ . Αφού  $\mathfrak{p}$  είναι μέγιστο, τότε  $R/\mathfrak{p}$  είναι σώμα, επομένως  $(R/\mathfrak{p})[x]$  είναι Π.Κ.Ι., επομένως και Π.Μ.Π.

- Συνεπώς, το αντίστοιχο πολυώνυμο  $\bar{g}(x) \in (R/\mathfrak{p})[x]$  γράφεται στην μορφή

$$\bar{g}(x) = \bar{g}_1(x)^{c_1} \cdots \bar{g}_t(x)^{c_t}.$$

όπου  $g_i(x) \in R[x]$  είναι μονικά και  $\bar{g}_i(x) \in (R/\mathfrak{p})[x]$  είναι ανάγωγα.

- Έστω  $\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ , η ανάλυση του  $\mathfrak{p}S$  σε πρώτα ιδεώδη. Θα δείξουμε ότι με τις παραπάνω υποθέσεις μπορούμε να βρούμε ακριβώς ποια είναι τα  $\mathfrak{q}_i$  καθώς και τους αντίστοιχους βαθμούς διακλάδωσης και αδράνειας.

**Θέωρημα 20** (Δεύτερο Θεώρημα Ανάλυσης). Με τις παραπάνω υποθέσεις ισχύουν τα παρακάτω.

- (α) Το πλήθος των ιδεωδών  $\mathfrak{q}_i$  στην ανάλυση του  $\mathfrak{p}S$  είναι ίσο με  $r = t$ . Επίσης

$$\mathfrak{q}_i = \mathfrak{p}S + g_i(\vartheta) \cdot S \quad i = 1, \dots, t$$

με  $f_i = \deg(g_i(x))$  και  $e_i = c_i$ .

- (β) Τα ιδεώδη  $\mathfrak{q}_k^* = i^{-1}(\mathfrak{q}_k)$  δίνονται από την σχέση

$$\mathfrak{q}_k^* = \mathfrak{q}_k \cap R[\vartheta] = \mathfrak{p}[\vartheta] + g_i(\vartheta) \cdot R[\vartheta]$$

## 15 Μάθημα 15

### 15.1 Αποδείξη του Δεύτερου Θεωρήματος Ανάλυσης

**Σημείωση 2.** Για να αποδείξουμε το παραπάνω θεώρημα χρειάζεται να αναφέρουμε μια σειρά από λήμματα. Με τις παραπάνω υποθέσεις θα συμβολίζουμε με  $\bar{R} = R/\mathfrak{p}$  και για  $f(x) = \sum_i a_i x^i$  θα συμβολίζουμε με  $\bar{f}(x) = \sum_i \bar{a}_i x^i$ .

**Λήμμα 12.** (α) Αν  $m = [S : R[\vartheta]]$  και  $\mathfrak{p} + mR = R$ , τότε  $\mathfrak{p}S + \mathcal{F} = S$ .

(β) Αν  $\mathfrak{p} \nmid D_{K/L}(\vartheta) \cdot R$ , τότε  $\mathfrak{p}S + \mathcal{F} = S$ .

**Απόδειξη.** (α) Έχουμε ότι  $mS \subseteq R[\vartheta]$ . Συνεπώς, από την Παρατήρηση 34, έχουμε ότι

$$S = S(\mathfrak{p} + mR) = \mathfrak{p}S + mS \subseteq \mathfrak{p}S + \mathcal{F}$$

και έτσι έχουμε τη ζητούμενη ισότητα.



(β) Αφού  $\mathfrak{p} \nmid D_{K/L}(\vartheta) \cdot R$ , τότε  $\mathfrak{p} + D_{K/L}(\vartheta) \cdot R = R$ . Επίσης, αφού  $D_{L/K}(\vartheta) \cdot S \subseteq R[\vartheta]$ , τότε  $D_{L/K}(\vartheta) \cdot S \subseteq \mathcal{F}$  και ομοία με το (α) έχουμε το ζητούμενο.  $\square$

**Λήμμα 13.** Ισχύει ότι

$$R[\vartheta]/\mathfrak{p}[\vartheta] \cong \overline{R}[x]/\langle \overline{g}(x) \rangle$$

Απόδειξη. Αφήνεται ως άσκηση ναδειχθεί ότι η απεικόνιση

$$\varphi: R[\vartheta] \rightarrow \overline{R}[x]/\langle \overline{g}(x) \rangle, \quad \varphi(h(\vartheta)) = \overline{h}(x) + \langle \overline{g}(x) \rangle$$

είναι καλά ορισμένος επιμορφισμός δακτυλίων με πυρήνα  $\mathfrak{p}[\vartheta]$ .  $\square$

**Λήμμα 14** (Θεώρημα Αντιστοιχίας Ιδεωδών). Έστω  $R$  μεταθετικός δακτύλιος με μονάδα και  $I$  ιδεώδες του  $R$ . Υπάρχει μια 1-1 και επί αντιστοιχία των (πρώτων, μέγιστων) ιδεωδών του  $R$  που περιέχουν το  $I$  με τα (πρώτα, μέγιστα) ιδεώδη του  $R/I$ .

Απόδειξη. Πραφανώς, αν  $I \subseteq J$  ιδεώδες του  $R$ , τότε  $J/I$  ιδεώδες του  $R$ . Αντίστροφα, μέσω της προβολής  $\pi: R \rightarrow R/I$ , αν  $\overline{J} \subseteq R/I$  ιδεώδες, τότε γνωρίζουμε ότι  $J = \pi^{-1}(\overline{J})$  ιδεώδες που περιέχει το  $I$  και μάλιστα  $J/I = \overline{J}$ . Η περίπτωση των πρώτων και μέγιστων ιδεωδών αφήνεται ως άσκηση.  $\square$

**Παρατήρηση 36.** Έστω  $\tilde{R}$  ένας δακτύλιος κύριων ιδεωδών. Θεωρούμε  $a \in \tilde{R} \setminus \{0\}$ . Τότε το  $a$  γράφεται μοναδικά στην μορφή

$$a = p_1^{c_1} \cdots p_t^{c_t}$$

όπου  $p_1, \dots, p_t \in \tilde{R}$  ανάγωγα.

- Σε κάθε δακτύλιο κύριων ιδεωδών, ένα ιδεώδες είναι πρώτο αν και μόνο αν παράγεται από ανάγωγο στοιχείο. Έτσι έχουμε ότι

$$aR = \mathfrak{p}_1^1 \cdots \mathfrak{p}_t^{c_t}$$

όπου  $\mathfrak{p}_i = \langle p_i \rangle$  τα μοναδικά πρώτα ιδεώδη που βρίσκονται πάνω από το  $aR$ .

- Από το παραπάνω λήμμα, είναι σαφές ότι τα μοναδικά πρώτα ιδεώδη του  $R/aR$  είναι τα  $\mathfrak{p}_i/aR$ , για κάθε  $i = 1, \dots, t$ .

**Απόδειξη** (Δεύτερου Θεωρήματος Ανάλυσης). • Από την παραπάνω παρατήρηση έχουμε ότι τα ιδεώδη  $\langle \bar{g}_i(x) \rangle / \langle \bar{g}(x) \rangle$  είναι τα μοναδικά πρώτα ιδεώδη του  $\bar{R}[x] / \langle \bar{g}(x) \rangle$ .

- Μέσω του επαγόμενου ισομορφισμού  $\rho$  του Λήμματος 13, έχουμε ότι τα μοναδικά πρώτα ιδεώδη του  $R[\vartheta] / \mathfrak{p}[\vartheta]$  είναι τα

$$\rho^{-1}(\langle \bar{g}_i(x) \rangle / \langle \bar{g}(x) \rangle) = \frac{g_i(\vartheta) \cdot R[\vartheta] + \mathfrak{p}[\vartheta]}{\mathfrak{p}[\vartheta]}$$

- Από το Θεώρημα Αντιστοιχίας Ιδεωδών, τότε τα  $g_i(\vartheta) \cdot R[\vartheta] + \mathfrak{p}[\vartheta]$  είναι τα μοναδικά πρώτα ιδεώδη του  $R[\vartheta]$  που περιέχουν το  $\mathfrak{p}[\vartheta]$ , για κάθε  $i = 1, \dots, t$ .
- Αφού  $\mathfrak{p}[\vartheta] = \mathfrak{p}S \cap R[\vartheta]$ , μέσω της απεικόνισης  $i$  που ορίστηκε στο Θεώρημα 19, έχουμε ότι  $r = t$  και ότι τα μοναδικά ιδεώδη που βρίσκονται πάνω από το  $\mathfrak{p}S$  είναι τα

$$\mathfrak{q}_i = \mathfrak{p}S + g_i(\vartheta)(S)$$

Μέσω της παραπάνω σχέσης έχουμε δείξει το πρώτο σκέλος του ερωτήματος (α), καθώς και το ερώτημα (β).

- Θα δείξουμε ότι  $f_i = f(\mathfrak{q}_i / \mathfrak{p}) = \deg(g_i(x))$ . Έχουμε ότι

$$N_{K/\mathbb{Q}}(\mathfrak{p})^{f_i} = |R/\mathfrak{p}|^{f_i} = |S/\mathfrak{q}_i| = |R[\vartheta]/\mathfrak{q}_i^*| = |R[\vartheta]/(g_i(\vartheta) \cdot S + \mathfrak{p}[\vartheta])|$$

όπου η τρίτη ισότητα έπεται από το Θεώρημα 19 (β). Από το Λήμμα 13 έχουμε ότι

$$|R[\vartheta]/(g_i(\vartheta) \cdot S + \mathfrak{p}[\vartheta])| = \left| \frac{R[\vartheta]/\mathfrak{p}[\vartheta]}{(g_i(\vartheta) \cdot S + \mathfrak{p}[\vartheta])/\mathfrak{p}[\vartheta]} \right| = \left| \frac{\bar{R}[x]/\langle \bar{g}(x) \rangle}{\langle \bar{g}_i(x) \rangle / \langle \bar{g}(x) \rangle} \right| = \left| \frac{\bar{R}[x]}{\langle \bar{g}_i(x) \rangle} \right|$$

Αφού τα  $g_i(x)$  επιλέχθηκαν έτσι ώστε  $\deg(g_i(x)) = \deg(\bar{g}_i(x))$ , τότε έχουμε ότι

$$\left| \frac{\bar{R}[x]}{\langle \bar{g}_i(x) \rangle} \right| = |\bar{R}|^{\deg(g_i(x))} = N_{K/\mathbb{Q}}(\mathfrak{p})^{\deg(g_i(x))}$$

Συνδυάζοντας τις παραπάνω σχέσεις έχουμε το ζητούμενο.

- Αρχικά θα δείξουμε ότι  $\prod_{i=1}^t \mathfrak{q}_i^{c_i} \subseteq \mathfrak{p}S$ . Από ιδιότητες διαιρετότητας και την μοναδικότητα της ανάλυσης σε πρώτα ιδεώδη, θα ισχύει ότι  $e_i \leq c_i$ . Έχουμε ότι

$$\prod_{i=1}^t \mathfrak{q}_i^{c_i} = \mathfrak{p}S + \left( \prod_{i=1}^t g_i(\vartheta) \right) S$$

Αν δείξουμε ότι  $(\prod_{i=1}^t g_i(\vartheta)) S \subseteq \mathfrak{p}S$  θα έχουμε δείξει το ζητούμενο. Από την σχέση

$$\bar{g}(x) = \bar{g}_1(x)^{c_1} \cdots \bar{g}_t(x)^{c_t}.$$

έχουμε ότι

$$\left( \prod_{i=1}^t g_i(\vartheta) \right) = \left( \prod_{i=1}^t g_i(\vartheta) \right) - g(\vartheta) \in \mathfrak{p}[\vartheta]$$

Συνεπώς, προκύπτει ότι

$$\left( \prod_{i=1}^t g_i(\vartheta) \right) S \subseteq S \cdot \mathfrak{p}[\vartheta] = \mathfrak{p}S.$$

- Τέλος, παρατηρήστε ότι

$$[L : K] = n = \deg(g(x)) = \sum_{i=1}^t \deg(g_i(x)) \cdot c_i = \sum_{i=1}^t f_i c_i \leq \sum_{i=1}^f f_i e_i = n$$

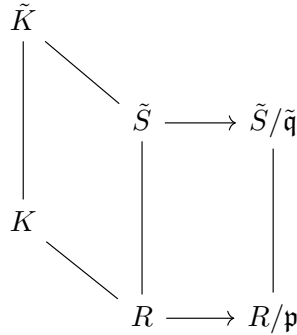
όπου η τελευταία ισότητα προκύπτει από το πρώτο θεώρημα ανάλυσης. Αφού ισχύει ότι  $f_i \geq 0$  και  $c_i \leq e_i$ , τελικώς από την παραπάνω ισότητα έχουμε ότι  $c_i \leq e_i$ , για κάθε  $i = 1, \dots, t$ .

□

**Θέωρημα 21.** Έστω  $L = K(\vartheta)$ ,  $\vartheta \in S$ . Αν  $\mathfrak{p} \in \text{Spec}(R)$  δεν διαιρεί την  $D_{L/K}(\vartheta)$  (δηλαδή  $D_{L/K}(\vartheta) \notin \mathfrak{p}$ ), τότε δεν διακλαδίζεται στο  $L$ .

*Απόδειξη.* Από το Λήμμα 12 και το Θεώρημα 20 αρκεί να δείξουμε ότι το  $\bar{g}(x)$  έχει μόνο απλές ρίζες, όπου  $g(x) = \text{Irr}(\vartheta, K) \in R[x]$ .

- Έστω  $\vartheta = \vartheta_1, \dots, \vartheta_n$  οι ρίζες του  $g(x)$  και  $\tilde{K}$  το σώμα ανάλυσης του  $g(x)$  πάνω από το  $K$ , δηλαδή  $\tilde{K} = K(\vartheta_1, \dots, \vartheta_n)$ . Επίσης, συμβολίζουμε με  $\tilde{S}$  το σύνολο των ακεραίων αλγεβρικών πάνω από το  $\tilde{K}$ .
- Θεωρούμε  $\tilde{\mathfrak{q}} \in \text{Spec}(\tilde{S})$  που βρίσκεται πάνω από το  $\mathfrak{p}$ . Από την Παρατήρηση 31 έχουμε το παρακάτω διάγραμμα



- Αφού  $\vartheta = \vartheta_1, \dots, \overline{\vartheta_n} \in \tilde{S}$  είναι ρίζες του  $g(x)$ , τότε  $\overline{\vartheta_1}, \dots, \vartheta_n$  είναι οι ρίζες του  $\overline{g}(x)$  ( $\overline{g}(x) \in \tilde{S}/\tilde{\mathfrak{q}}[x]$ ).
- Υποθέτουμε, προς άτοπο, ότι οι ρίζες του  $\overline{g}(x)$  δεν είναι απλές. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι  $\overline{\vartheta_1} = \overline{\vartheta_2}$ , δηλαδή  $\vartheta_1 - \vartheta_2 \in \tilde{\mathfrak{q}}$ .
- Συνεπώς, προκύπτει ότι

$$D_{L/K}(\vartheta) = \prod_{1 \leq i < j \leq n} (\vartheta_i - \vartheta_j) \in \tilde{\mathfrak{q}} \cap K = \mathfrak{p}$$

Από την τελευταία σχέση καταλήγουμε σε άτοπο. □

**Πόρισμα 12.** Υπάρχουν το πολύ πεπερασμένα το πλήθος πρώτα ιδεώδη του  $R$  τα οποία διακλαδίζονται στο  $L$ .

*Απόδειξη.* Το ζητούμενο προκύπτει άμεσα από το παραπάνω θεώρημα και το θεώρημα ανάλυσης σε πρώτα ιδεώδη, εφαρμοσμένο στο ιδεώδες  $D_{L/K}(\vartheta) \cdot R$ . □

**Παρατήρηση 37.** Έστω  $K$  αλγεβρικό σώμα αριθμών με  $[K : \mathbb{Q}] = n$  με  $K = \mathbb{Q}(\vartheta)$  με  $\vartheta \in R_K$ .

- Έστω  $D_{K/\mathbb{Q}}(\vartheta) \in \mathbb{Z}$  και  $p \nmid D_{K/\mathbb{Q}}(\vartheta)$  πρώτος. Τότε, έχουμε ότι  $\mathfrak{p} = p\mathbb{Z} \nmid D_{K/\mathbb{Q}}(\vartheta)\mathbb{Z}$ .
- Έχουμε ότι  $\mathbb{Z}/\mathfrak{p} = \mathbb{F}_p$ . Αν  $f(x) = \text{Irr}(\vartheta, \mathbb{Q}) \in \mathbb{Z}[x]$ , τότε θεωρούμε την ανάλυση του  $\overline{f}(x) \in \mathbb{F}_p[x]$

$$\overline{f}(x) = \overline{f_1}(x)^{c_1} \cdots \overline{f_t}(x)^{c_t}.$$

- Συνεπώς, έχουμε ότι

$$\mathfrak{p}R_K = \mathfrak{q}_1^{c_1} \cdots \mathfrak{q}_t^{c_t}$$

όπου

$$\mathfrak{q}_i = f_i(\vartheta)R_K + pR_K = \langle f_i(\vartheta), p \rangle$$

- Τέλος, επιλέγοντας  $f_i(x)$  κατάλληλα ώστε  $\deg f_i(x) = \deg \overline{f_i}(x)$ , έχουμε ότι

$$f_i = f(\mathfrak{q}_i/\mathfrak{p}) = \deg f_i(x) = \deg \overline{f_i}(x)$$

συνεπώς

$$N_{K/\mathbb{Q}}(\mathfrak{q}_i) = |R_K/\mathfrak{q}_i| = |\mathbb{Z}/\mathfrak{p}|^{f_i} = p^{f_i}.$$

**Σημείωση 3.** Συνεπώς, στην ειδική περίπτωση όπου  $K$  είναι ένα αλγεβρικό σώμα αριθμών, για την εύρεση των πρώτων ιδεωδών του  $\mathbb{Z}$  που διακλαδίζονται στο  $K$  προσανατολιζόμαστε στα  $\mathfrak{p} = p\mathbb{Z}$ , όπου  $p \nmid D_{L/K}(\vartheta)$  με  $K = \mathbb{Q}(\vartheta)$ .

## References

- [Antoniadis, 2021] Antoniadis, K. (2021). An introduction to algebraic number theory. *Algebraic Number Theory*.
- [Fulton, 2008] Fulton, W. (2008). Algebraic curves. *An Introduction to Algebraic Geom*, 54.
- [Scott, 2015] Scott, G. (2015). Algebra notes. *Ideals and the Chinese Remainder Theorem*.