Αλγεβρικη Θεωρια Αριθμων

Φθινοπωρινὸ ἑξάμηνο 2006

Καθηγητὴς Ν. Γ. Τζανάκης

Ε΄ Φυλλάδιο Ἀσκήσεων

1. Ἔστω ὅτι ἔχομε ἐκφράσει τὰ ἰδεώδη I, J τοῦ A ὡς $\mathbb{Z}$-δ.π. ὡς ἑξῆς: $I = \mathbb{Z}\cdot\alpha_1 + \cdots + \mathbb{Z}\cdot\alpha_m$ καὶ $J = \mathbb{Z}\cdot\beta_1 + \cdots + \mathbb{Z}\cdot\beta_n$, μὲ τὰ α_i καὶ β_j στὸ A. Τότε, ἀποδεῖξτε ὅτι τὸ γινόμενο ἰδεωδῶν $I\cdot J$ ταυτίζεται μὲ τὴ $\mathbb{Z}$-δ.π., τῆς ὁποίας γεννήτορες εἶναι ὅλα τὰ $\alpha_i\beta_j$, ($i = 1,\ldots,m$ καὶ $j = 1,\ldots,n$).

2. Στὴν ἄσκηση αὐτή, $D \neq 0, 1$ εἶναι ἀκέραιος ἐλεύθερος τετραγώνου καὶ ἐργαζόμαστε στὸ τετραγωνικὸ σῶμα $K = \mathbb{Q}(\sqrt{D})$. Στὴν περίπτωση ποὺ $D \equiv 2, 3 \pmod 4$, μιὰ ἀκέραια βάση τοῦ K εἶναι ἡ $\{1, \sqrt{D}\}$, ἐνῶ, ἂν $D \equiv 1 \pmod 4$, μιὰ ἀκέραια βάση εἶναι ἡ $\{1, (1+\sqrt{D})/2\}$.

   (α΄) Ἔστω $D \equiv 2, 3 \pmod 4$ καὶ τὸ ἰδεῶδες $I = (a, b+\sqrt{D})$ τοῦ A, ὅπου $a, b \in \mathbb{Z}$ καὶ $a|(b^2 - D)$ (στὸ $\mathbb{Z}$). Ἀποδεῖξτε ὅτι, τότε, τὸ I ταυτίζεται μὲ τὴ $\mathbb{Z}$-δ.π. $\mathbb{Z}\cdot a + \mathbb{Z}\cdot(b+\sqrt{D})$.

   (β΄) Ἔστω $D \equiv 1 \pmod 4$ καὶ τὸ ἰδεῶδες $I = (a, (b+\sqrt{D})/2)$ τοῦ A, ὅπου $a, b \in \mathbb{Z}$, ὁ b εἶναι περιττὸς καὶ $4a|(b^2 - D)$ (στὸ $\mathbb{Z}$). Ἀποδεῖξτε ὅτι, τότε, τὸ I ταυτίζεται μὲ τὴ $\mathbb{Z}$-δ.π. $\mathbb{Z}\cdot a + \mathbb{Z}\cdot(b+\sqrt{D})/2$.

3. Θέτομε $\theta = \sqrt{79}$ καὶ ἐργαζόμαστε στὸ ἀριθμητικὸ σῶμα $K = \mathbb{Q}(\theta)$. Ἔστω τὸ ἰδεῶδες $\mathfrak{p} = (5, 2+\theta)$. Μὲ τὴ βοήθεια τῆς προηγούμενης ἄσκησης ἀποδεῖξτε ὅτι $\mathfrak{p}^2 = (25, 2+\theta)$ καὶ $\mathfrak{p}^3 = (21 - 2\theta)$ (κύριο ἰδεῶδες!).

4. Ἔστω $D \neq 0, 1$ εἶναι ἀκέραιος ἐλεύθερος τετραγώνου καὶ

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

   Στὸ ἀριθμητικὸ σῶμα $K = \mathbb{Q}(\sqrt{D})$ τὰ $1, \omega$ ἀποτελοῦν ἀκέραια βάση. Ἔστω A ὁ δακτύλιος τῶν ἀκεραίων τοῦ K. Μὲ N συμβολίζομε τὴ στάθμη $\mathrm{N}_{K/\mathbb{Q}}$.

   Ἀποδεῖξτε πρῶτα ὅτι ἕνα μὴ μηδενικὸ ἰδεῶδες τοῦ A περιέχει στοιχεῖα $x + y\omega$ μὲ $x, y \in \mathbb{Z}$ καὶ $y \neq 0$. Μετά, ἀποδεῖξτε ὅτι γιὰ κάθε μὴ μηδενικὸ ἰδεῶδες I τοῦ A ἰσχύουν τὰ ἑξῆς:

   (α΄) Γιὰ κάθε $x + y\omega \in I$, $\mathrm{N}(x + y\omega) \in I$ καί, συνεπῶς, τὸ I περιέχει μὴ μηδενικοὺς ρητοὺς ἀκεραίους.

   (β΄) Ἔστω a ὁ ἐλάχιστος θετικὸς ρητὸς ἀκέραιος, ποὺ ἀνήκει στὸ I. Τότε, κάθε ρητὸς ἀκέραιος τοῦ I εἶναι πολλαπλάσιο (στὸ $\mathbb{Z}$) τοῦ a.

      Στὰ παρακάτω ἐρωτήματα, τὸ a διατηρεῖ τὴ σημασία, ποὺ ἔχει καὶ σὲ τοῦτο τὸ ἐρώτημα.

(γ') Ἔστω c ὁ ἐλάχιστος θετικὸς $y \in \mathbb{Z}$, γιὰ τὸν ὁποῖον ὑπάρχει $x \in \mathbb{Z}$ τέτοιο ὥστε $x + y\omega \in I$. Ἀποδεῖξτε ὅτι, γιὰ κάθε $x + y\omega \in I$ ($x, y \in \mathbb{Z}$), ἰσχύει $c|y$ (στὸ $\mathbb{Z}$).

> Στὰ παρακάτω ἐρωτήματα, τὸ c διατηρεῖ τὴ σημασία, ποὺ ἔχει καὶ σὲ τοῦτο τὸ ἐρώτημα.

(δ') Ἀποδεῖξτε ὅτι $c|a$ (στὸ $\mathbb{Z}$).

(ε') Ἔστω ὅτι $x + y\omega \in \mathbb{Z}$ ($x, y \in \mathbb{Z}$). Ἀποδεῖξτε ὅτι $c|x$ (στὸ $\mathbb{Z}$).

(ϛ') Ἀποδεῖξτε ὅτι $I \subseteq (c) = cA$.

(ζ) Ἔστω $b \in \mathbb{Z}$, τέτοιο ὥστε $b + c\omega \in I$. Ἀποδεῖξτε ὅτι $I = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$.