Η Θεωρια Αριθμων στην Εκπαιδευση

Καθηγητὴς Ν.Γ. Τζανάκης

Θέματα ποὺ συζητήθηκαν στὶς 8-10-2014

Ἀκέραιοι καὶ μονάδες τετραγωνικοῦ σώματος.

• Ἕνα *τετραγωνικὸ σῶμα* εἶναι τῆς μορφῆς

$$K = \mathbb{Q}(\sqrt{m}) = \{x + y\sqrt{m} : x, y \in \mathbb{Q}\}, \quad m \in \mathbb{Z} \setminus \{0, 1\}, \text{ ἐλεύθερος τετραγώνου.}$$

Εὔκολα βλέπομε ὅτι κάθε ἀριθμὸς τοῦ $\mathbb{Q}(\sqrt{m})$ γράφεται ὡς ἑξῆς:

$$\xi = \frac{a + b\sqrt{m}}{c}, \quad a, b, c \in \mathbb{Z},\ c \geq 1,\ \gcd(a, b, c) = 1. \tag{1}$$

• *Ἀκέραιοι τοῦ* K εἶναι τὸ σύνολο τῶν *ἀλγεβρικῶν ἀκεραίων*, ποὺ ἀνήκουν στὸ K. Αὐτὸ τὸ σύνολο συμβολίζομε μὲ $\mathcal{O}_K$ ἢ $\mathbb{Z}_K$.

Ἀποδείξαμε ὅτι, ἂν ὁ ξ στὴν (1) εἶναι ἀλγεβρικὸς ἀκέραιος, τότε $c \in \{1, 2\}$. Ἀποδείξαμε, ἐπίσης, τὸ ἑξῆς θεώρημα:

Θεώρημα 1. *Ἂν ὁ $m \in \mathbb{Z} \setminus \{0, 1\}$ εἶναι ἐλεύθερος τετραγώνου καὶ $K = \mathbb{Q}(\sqrt{m})$, τότε*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m} & \text{ἂν } m \equiv 2, 3 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\omega & \text{ἂν } m \equiv 1 \pmod 4, \text{ ὅπου } \omega = \frac{1+\sqrt{m}}{2}. \end{cases}$$

• Ὅσον ἀφορᾷ στὴν ὁμάδα $\mathcal{O}_K^*$ τῶν μονάδων τοῦ $\mathcal{O}_K$ (δηλαδή, τῶν ἀντιστρεψίμων στοιχείων τοῦ $\mathcal{O}_K$), ἀποδείξαμε τὸ ἑξῆς θεώρημα:

Θεώρημα 2. *Ἔστω $m \in \mathbb{Z} \setminus \{0, 1\}$ εἶναι ἐλεύθερος τετραγώνου καὶ $K = \mathbb{Q}(\sqrt{m})$. Στὴν περίπτωση $m \equiv 1 \pmod 4$ θέτομε $\omega = \frac{1+\sqrt{m}}{2}$. Τότε,*

$$\mathcal{O}_K^* = \begin{cases} \{\pm 1, \pm i\} & \text{ἂν } m = -1 \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{ἂν } m = -3 \\ \{\pm 1\} & \text{ἂν } m < -3 \\ \{x + y\sqrt{m} : x, y \in \mathbb{Z} \text{ καὶ } x^2 - my^2 = \pm 1\} & \text{ἂν } m > 1 \text{ καὶ } m \equiv 2, 3 \pmod 4 \\ \{x + y\omega : x, y \in \mathbb{Z} \text{ καὶ } x^2 + xy + \frac{1-m}{4}y^2 = \pm 1\} & \text{ἂν } m > 1 \text{ καὶ } m \equiv 1 \pmod 4 \end{cases}.$$

• Σχετικὰ μὲ τὶς δύο περιπτώσεις τοῦ Θεωρήματος 2, στὶς ὁποῖες $m > 1$, ἀναφερθήκαμε[1] στὴ λεγόμενη *ἐξίσωση Pell*, προκειμένου νὰ περιγράψομε ἀκριβέστερα τὴν ὁμάδα O_K^*.

Θεώρημα 3. *Ἔστω ἀκέραιος $D > 1$, ποὺ δὲν εἶναι τέλειο τετράγωνο. Θεωροῦμε τὶς ἐξισώσεις*

$$x^2 - Dy^2 = 1 \tag{2}$$
$$x^2 - Dy^2 = -1. \tag{3}$$

Μιὰ λύση (x, y) τῆς (2) ἢ τῆς (3) θὰ τὴ λέμε θετική, ἂν $x > 0$ καὶ $y > 0$. Ἂν (x, y), (x', y') εἶναι, καὶ οἱ δύο, θετικὲς λύσεις τῆς (2) ἢ τῆς (3), θὰ λέμε ὅτι ἡ (x, y) εἶναι μικρότερη ἀπὸ τὴ (x', y'), ἂν $x < x'$ (ὁπότε καὶ $y < y'$). Ἰσχύουν τὰ ἑξῆς:

Ἡ ἐξίσωση (2) ἔχει πάντα θετικὴ λύση.

Ἡ ἐξίσωση (3), γιὰ ἄλλες τιμὲς τοῦ D ἔχει θετικὴ λύση, ἐνῶ γιὰ ἄλλες δὲν ἔχει.

Ἔστω

$$(x_1, y_1) = \begin{cases} \text{ἡ ἐλάχιστη θετικὴ λύση } (x, y) \text{ τῆς (2) ἂν ἡ (3) δὲν ἔχει λύση.} \\ \text{ἡ ἐλάχιστη θετικὴ λύση } (x, y) \text{ τῆς (3) ἂν ἡ (3) ἔχει λύση.} \end{cases}$$

Ἂν ἡ (3) δὲν ἔχει λύση, τότε ὅλες οἱ λύσεις (x, y) τῆς (2) λαμβάνονται ἀπὸ τὴ σχέση

$$x + y\sqrt{D} = \pm(x_1 + y_1\sqrt{D})^n, \quad n \in \mathbb{Z}.$$

Ἂν ἡ (3) ἔχει λύση, τότε ὅλες οἱ λύσεις (x, y) τῆς (2) λαμβάνονται ἀπὸ τὴ σχέση

$$x + y\sqrt{D} = \pm(x_1 + y_1\sqrt{D})^{2n}, \quad n \in \mathbb{Z}.$$

καὶ ὅλες οἱ λύσεις (x, y) τῆς (3) λαμβάνονται ἀπὸ τὴ σχέση

$$x + y\sqrt{D} = \pm(x_1 + y_1\sqrt{D})^{2n+1}, \quad n \in \mathbb{Z}.$$

Ἀνάλογο θεώρημα ἰσχύει καὶ γιὰ τὶς ἐξισώσεις $x^2 - Dy^2 = \pm 4$.

Βάσει αὐτῶν τῶν θεωρημάτων μποροῦμε νὰ περιγράψομε τὴν ὁμάδα O_K^* ὅταν $m > 1$.

Θεώρημα 4. *Ἔστω $m > 1$, ἐλεύθερος τετραγώνου καὶ $K = \mathbb{Q}(\sqrt{m})$.*

1. Περίπτωση $m \equiv 2, 3 \pmod 4$. Θεωροῦμε τὶς ἐξισώσεις

$$x^2 - my^2 = 1 \tag{4}$$
$$x^2 - my^2 = -1 \tag{5}$$

[1] Χωρὶς ἀποδείξεις.

καὶ θέτομε

$$(x_1, y_1) = \begin{cases} \text{ἐλάχιστη θετικὴ λύση } (x, y) \text{ τῆς (4) ἂν ἡ (5) δὲν ἔχει λύση.} \\ \text{ἐλάχιστη θετικὴ λύση } (x, y) \text{ τῆς (5) ἂν ἡ (5) ἔχει λύση.} \end{cases}$$

Τότε, $\mathcal{O}_K^* = \{\pm(x_1 + y_1\sqrt{m})^n : n \in \mathbb{Z}\}$.

2. *<u>Περίπτωση $m \equiv 1 \pmod 4$</u>. Θεωροῦμε τὶς ἐξισώσεις*

$$x^2 + xy + \left(\tfrac{1-m}{4}\right)y^2 = 1 \quad (6)$$

$$x^2 + xy + \left(\tfrac{1-m}{4}\right)y^2 = -1, \quad (7)$$

(παρατηροῦμε ὅτι αὐτὲς γράφονται ἰσοδύναμα ὡς $(2x + y)^2 - my^2 = \pm 4$*) καὶ θέτομε*[2]

$$(x_1, y_1) = \begin{cases} \text{ἐλάχιστη θετικὴ λύση } (x, y) \text{ τῆς (6) ἂν ἡ (5) δὲν ἔχει λύση.} \\ \text{ἐλάχιστη θετικὴ λύση } (x, y) \text{ τῆς (7) ἂν ἡ (7) ἔχει λύση.} \end{cases}$$

Τότε, $\mathcal{O}_K^* = \{\pm(x_1 + y_1\omega)^n : n \in \mathbb{Z}\}$.

Ἄσκηση. 1. *Ἔστω* $p \in \{31, 43, 71, 107, 131, 383, 499, 659\}$ *(ὅλοι αὐτοὶ οἱ ἀριθμοὶ εἶναι πρῶτοι) καὶ* $K = \mathbb{Q}(\sqrt{p})$.

- *Ἀποδεῖξτε ὅτι ἡ ἐξίσωση* $x^2 - py^2 = -1$ *δὲν ἔχει ἀκέραιες λύσεις.*
- *Περιγρᾶψτε τὴν ὁμάδα* $\mathcal{O}_K^*$.

2. *Ἔστω* $q \in \{73, 89, 109, 113, 137, 157, 181, 277\}$ *(ὅλοι αὐτοὶ οἱ ἀριθμοὶ εἶναι πρῶτοι) καὶ* $K = \mathbb{Q}(\sqrt{q})$.

- *Θεωρῆστε δεδομένο ὅτι ἡ ἐξίσωση* $x^2 - qy^2 = -4$ *ἔχει ἀκέραιες λύσεις.*
- *Περιγρᾶψτε τὴν ὁμάδα* $\mathcal{O}_K^*$.

Ὑπόδειξη. Θὰ χρειαστεῖ νὰ γράψετε ἕνα ὑποτυπῶδες προγραμματάκι στὸν ὑπολογιστή. ☺

[2] Στὴν περίπτωση $m \equiv 1 \pmod 4$, ὁ ὅρος "θετικὴ λύση" (x, y) σημαίνει λύση μὲ $x \geq 0$ καὶ $y > 0$.