Αλγεβρικη Θεωρια Αριθμων

Φθινοπωρινὸ ἑξάμηνο 2006

Καθηγητὴς Ν. Γ. Τζανάκης

ϝ′ Φυλλάδιο Ἀσκήσεων

1. Ἔστω $K = \mathbb{Q}(\theta)$ καὶ τὸ ἐλάχιστο πολυώνυμο τοῦ θ πάνω ἀπὸ τὸ $\mathbb{Q}$ ἔχει μία τουλάχιστον πραγματικὴ ρίζα. Ἀποδεῖξτε ὅτι οἱ μόνες μιγαδικὲς ρίζες τῆς μονάδος (ὁποιασδήποτε τάξεως), ποὺ ἀνήκουν στὸ K εἶναι οἱ ± 1.

2. Στὸ $K = \mathbb{Q}(\theta)$, ὅπου $\theta = \sqrt{79}$, ἔχομε ἀποδείξει ὅτι ἰσχύουν οἱ ἑξῆς ἀναλύσεις σὲ πρῶτα ἰδεώδη:

$$(3) = \mathfrak{p}_3\mathfrak{p}_3', \quad \mathfrak{p}_3 = (3, 1+\theta), \; \mathfrak{p}_3' = (3, -1+\theta)$$

$$(5) = \mathfrak{p}_5\mathfrak{p}_5', \quad \mathfrak{p}_5 = (5, 2+\theta), \; \mathfrak{p}_5' = (5, -2+\theta)$$

$$(7) = \mathfrak{p}_7\mathfrak{p}_7', \quad \mathfrak{p}_7 = (7, 3+\theta), \; \mathfrak{p}_7' = (7, -3+\theta)$$

$$(13) = \mathfrak{p}_{13}\mathfrak{p}_{13}', \quad \mathfrak{p}_{13} = (13, 1+\theta), \; \mathfrak{p}_{13}' = (13, -1+\theta)$$

καὶ $(2) = \mathfrak{p}_2^2$, $\mathfrak{p}_2 = (9+\theta)$. Εἴδαμε, ἐπίσης, ὅτι ἡ ὁμάδα κλάσεων τοῦ K παράγεται ἀπὸ τὴν κλάση τοῦ $\mathfrak{p}_5$ καὶ ἔχει τάξη 3.

Γιὰ καθένα ἀπὸ τὰ παραπάνω ἰδεώδη $\mathfrak{p}$ ὑπολογῖστε $\alpha \in K$ καὶ $j \in \{0,1,2\}$, τέτοια ὥστε $\mathfrak{p} = \alpha\,\mathfrak{p}_5^j$.
Ὑπόδειξη: Μὲ τὴ βοήθεια τῶν ἀσκήσεων 1 καὶ 2 του Φυλλαδίου Ε′ ἀποδεῖξτε ὅτι $\mathfrak{p}_5 = 5\mathbb{Z} + (2+\theta)\mathbb{Z}$, $\mathfrak{p}_5^2 = 25\mathbb{Z} + (2+\theta)\mathbb{Z}$, $\mathfrak{p}_5^3 = (21 - 2\theta)$.
Βρεῖτε τὴν ἀνάλυση σὲ πρῶτα ἰδεώδη τῶν $(1+\theta)$, $(-1+\theta)$, $(2+\theta)$, $(-2+\theta)$, $(3+\theta)$, $(-3+\theta)$. Μὲ τὴ βοήθεια αὐτῶν τῶν ἀναλύσεων καὶ τῆς $\mathfrak{p}_5^3 = (21-2\theta)$ μπορεῖτε τώρα νὰ ὑπολογίσετε εὔκολα τὰ j καὶ α (τὸ α δὲν εἶναι, ἐν γένει, ἀκέραιο στοιχεῖο.)

3. Ἔστω $\theta = \sqrt[3]{6}$ καὶ $\epsilon = 1 - 6\theta + 3\theta^2$. Ὑπολογῖστε τὸ ἐλάχιστο πολυώνυμο τοῦ ϵ πάνω ἀπὸ τὸ $\mathbb{Q}$ καὶ παρατηρῆστε ὅτι τὸ ϵ εἶναι μονάδα. Ἀποδεῖξτε ὅτι ἡ ἐξίσωση $x^\nu = \epsilon$, $\nu \in \{3,7\}$ εἶναι ἀδύνατη σὲ ἀκεραίους x τοῦ K.
Ὑπόδειξη. Ὅταν $\nu = 3$ ἐργασθῆτε $\pmod{\mathfrak{p}}$ μὲ $\mathfrak{p}$ πρῶτο διαιρέτη τοῦ 7. Ὅταν $\nu = 7$ ἐργασθῆτε ἀνάλογα, μὲ $\mathfrak{p}$ πρῶτο διαιρέτη τοῦ 29.

4. Σ' αὐτὴ τὴν ἄσκηση ἀποδεικνύεται ὅτι ὁ ἀριθμὸς κλάσεων ἰδεωδῶν τοῦ σώματος $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{6}$, εἶναι 1.

(α′) Δεῖξτε ὅτι ἀρκεῖ ν' ἀποδείξει κανεὶς πὼς κάθε πρῶτο (ἀκέραιο) ἰδεῶδες στάθμης ≤ 19 εἶναι κύριο.

(β′) Παρατηρῆστε πρῶτα ὅτι $\mathrm{N}(2-\theta) = 2$ καὶ ἀποδεῖξτε μετὰ ὅτι ἡ ἀνάλυση τοῦ (2) σὲ πρῶτα ἰδεώδη εἶναι $(2) = \mathfrak{p}_2^3$, ὅπου $\mathfrak{p}_2 = (2-\theta)$.

(γ') Ἀποδεῖξτε ὅτι ἕνα μόνο πρῶτο ἰδεῶδες $\mathfrak{p}_3$ ὑπάρχει, ποὺ διαιρεῖ τὸ (3). Ἀποδεῖξτε ὅτι τὸ $\mathfrak{p}_3$ εἶναι κύριο.
Ὑπόδειξη. $\mathrm{N}(\theta) = \cdots$.

(δ') Ἀποδεῖξτε ὅτι $(5) = \mathfrak{p}_5\mathfrak{p}_5'$, ὅπου $\mathrm{N}(\mathfrak{p}_5) = 5$ καὶ $\mathrm{N}(\mathfrak{p}_5') = 25$, καὶ ἀποδεῖξτε ὅτι αὐτὰ τὰ πρῶτα ἰδεώδη εἶναι κύρια.
Ὑπόδειξη. $\mathrm{N}(-1+\theta) = \cdots$.

(ε') Ἀποδεῖξτε ὅτι ἡ ἀνάλυση τοῦ (7) σὲ πρῶτα ἰδεώδη εἶναι

$$(7) = \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7'' \,, \quad \mathfrak{p}_7 = (7, 1+\theta)\,,\ \mathfrak{p}_7' = (7, 2+\theta)\,,\ \mathfrak{p}_7'' = (7, -3+\theta)\,.$$

Ἀποδεῖξτε ὅτι καὶ οἱ τρεῖς πρῶτοι διαιρέτες τοῦ (7) εἶναι κύρια ἰδεώδη.
Ὑπόδειξη. Ὑπολογῖστε τὶς στάθμες $\mathrm{N}(1+\theta), \mathrm{N}(2+\theta), \mathrm{N}(-3+\theta)$.

(ϝ') Ἀποδεῖξτε ὅτι τὸ (11) ἔχει ἕνα μόνο πρῶτο διαιρέτη $\mathfrak{p}_{11}$ βαθμοῦ 1 καὶ αὐτὸς διαιρεῖ τὸ $3+\theta$. Ἐξ αὐτοῦ συμπεράνετε ὅτι τὸ $\mathfrak{p}_{11}$ εἶναι κύριο. Ἀνάλογα καὶ γιὰ τὸ (17).

(ζ') Ἀποδεῖξτε ὅτι τὰ ἰδεώδη (13) καὶ (19) εἶναι πρῶτα.

5. Σ' αὐτὴ τὴν ἄσκηση ἀποδεικνύεται ὅτι ἡ ἐξίσωση $x^3 + 6y^3 = 10z^3$ δὲν ἔχει ἀκέραιες λύσεις (x, y, z) μὲ $xyz \neq 0$. Σύμφωνα μὲ ὅ,τι ἔχομε 'δεῖ στὸ μάθημα, εἴτε στὶς ἀσκήσεις, στὸ σῶμα $K = \mathbb{Q}(\theta)$, ὅπου $\theta = \sqrt[3]{6}$, μία ἀκέραια βάση εἶναι ἡ $\{1, \theta, \theta^2\}$, θεμελιώδης μονάδα εἶναι ἡ $\epsilon = 1 - 6\theta + 3\theta^2$ καὶ ὁ ἀριθμὸς κλάσεων ἰδεωδῶν εἶναι 1. Θὰ χρειασθῆτε κάποια ἀπὸ τὰ ἀποτελέσματα τῆς ἀσκήσεως 4. Ἀκολουθῆστε τὰ παρακάτω βήματα:

(α') Ἀποδεῖξτε ὅτι δὲν βλάπτεται ἡ γενικότητα ἂν ὑποθέσομε ὅτι οἱ x, y, z εἶναι ἀνὰ δύο πρῶτοι μεταξύ τους. Κατόπιν, συμπεράνατε ὅτι $(x, 3) = 1$, $(y, 10) = 1$ καὶ $(z, 6) = 1$.

(β') Παραγοντοποιῆστε τὴν ἐξίσωση ὡς

$$(x + y\theta)(x^2 - xy\theta + y^2\theta^2) = (x + y\theta)[(x + y\theta)^2 - 3xy\theta] = 10z^3\,. \tag{1}$$

Ἀποδεῖξτε πρῶτα ὅτι τὰ μόνα πρῶτα ἰδεώδη, ποὺ δὲν ἀποκλείεται νὰ διαιροῦν συγχρόνως τὰ $(x + y\theta)$ καὶ $(x^2 - xy\theta + y^2\theta^2)$ εἶναι τὰ $\mathfrak{p}_2, \mathfrak{p}_3$. Ἀποκλεῖστε κατόπιν τὸ $\mathfrak{p}_3$. Ἀντιθέτως, ἀποδεῖξτε ὅτι $\mathfrak{p}_2|(x + y\theta)$, $\mathfrak{p}_2^2|(x^2 - xy\theta + y^2\theta^2)$, ὁπότε ἡ (1) συνεπάγεται τὴν ἐξίσωση ἰδεωδῶν

$$\frac{(x + y\theta)}{\mathfrak{p}_2} \cdot \frac{(x^2 - xy\theta + y^2\theta^2)}{\mathfrak{p}_2^2} = \mathfrak{p}_5\mathfrak{p}_5'(z)^3\,, \tag{2}$$

ὅπου οἱ δύο παράγοντες στὸ ἀριστερὸ μέλος εἶναι ἰδεώδη πρῶτα μεταξύ τους.

(γ') Ὑπολογῖστε $\pi_5, \pi_5' \in \mathbb{Z}[\theta]$, τέτοια ὥστε $\mathfrak{p}_5 = (\pi_5)$ καὶ $\mathfrak{p}_5' = (\pi_5')$.

(δ') Συμπεράνατε ἀπὸ τὴν (2) ὅτι

$$(x + y\theta) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{a}^3 \quad \text{εἴτε} \quad (x + y\theta) = \mathfrak{p}_2\mathfrak{p}_5'\mathfrak{a}^3\,,$$

ὅπου $\mathfrak{a} = (u + v\theta + w\theta^2)$ εἶναι ἀκέραιο κύριο ἰδεῶδες. Ἀπὸ τὶς ἰσότητες ἰδεωδῶν περᾶστε σὲ ἰσότητες στὸ $\mathbb{Z}[\theta]$.

(ε′) Παρατηρῆστε ὅτι $\epsilon \equiv 1 \pmod 3$ καὶ $(u + v\theta + w\theta^2)^3 \equiv u \pmod 3$ καί, κατόπιν, διαπιστῶστε ὅτι οἱ σχέσεις, στὶς ὁποῖες καταλήξατε στὸ βῆμα (δ′), σᾶς ὁδηγοῦν στὴν $x \equiv 0 \pmod 3$, ἄρα σὲ ἀντίφαση.