Αλγεβρικη Θεωρια Αριθμων

Φθινοπωρινὸ ἑξάμηνο 2006

Καθηγητὴς Ν. Γ. Τζανάκης

Δ′ Φυλλάδιο Ἀσκήσεων

Στὸ φυλλάδιο αὐτό:

- Τὸ K εἶναι ἀριθμητικὸ σῶμα μὲ δακτύλιο ἀκεραίων A.
- *Ἰδεῶδες τοῦ K* σημαίνει *κλασματικὸ* (ἐν γένει) ἰδεῶδες.
- *Ἰδεῶδες τοῦ A* σημαίνει ἰδεῶδες τοῦ A, ὑπὸ τὴ συνήθη ἔννοια. Ὅταν πρέπει νὰ τονισθεῖ ὅτι πρόκειται γιὰ ἰδεῶδες τοῦ A, ὑπὸ τὴ συνήθη ἔννοια, τότε χρησιμοποιεῖται ὁ ὅρος *ἀκέραιο ἰδεῶδες*.
- Ἂν $x, y \in A$, (x) καὶ (x, y) σημαίνουν, ἀντιστοίχως, τὰ ἰδεῶδη xA καὶ $xA + yA$ τοῦ A.
- $\mathbb{P}$ εἶναι τὸ σύνολο τῶν μὴ μηδενικῶν πρώτων ἰδεωδῶν τοῦ A.
- Τὸ σύμβολο $\mathrm{N}(\cdot)$ σημαίνει $\mathrm{N}_{K/Q}(\cdot)$.

1. Ἀποδεῖξτε ὅτι $A \subsetneqq K$.

2. Ἂν $\kappa \in K$, ἀποδεῖξτε ὅτι τὸ σύνολο κA εἶναι ἰδεῶδες τοῦ K. Τέτοια ἰδεώδη θὰ τὰ λέμε *κύρια ἰδεώδη τοῦ K*.

3. Στὰ ἰδεώδη τοῦ K ἡ πρόσθεση καὶ ὁ πολλαπλασιασμὸς ὁρίζονται κατ᾽ ἀναλογίαν τῶν ἀντιστοίχων πράξεων μεταξὺ ἀκεραίων ἰδεωδῶν. Ἀποδεῖξτε ὅτι οἱ πράξεις αὐτὲς εἶναι καλὰ ὁρισμένες, δηλαδή, τὸ ἄθροισμα καὶ τὸ γινόμενο ἰδεωδῶν τοῦ K εἶναι, ἐπίσης, ἰδεώδη τοῦ K.

4. Ἔστω $d \in \mathbb{Z} \setminus \{-1, 0, 1\}$ καὶ $dA = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ ἡ ἀνάλυση τοῦ dA σὲ πρῶτα ἰδεώδη τοῦ A. Τότε, τὸ ἰδεῶδες $d^{-1}A$ τοῦ K ἀναλύεται ὡς $d^{-1}A = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}$.

5. Ἀποδεῖξτε ὅτι τὸ σύνολο τῶν μὴ μηδενικῶν ἰδεωδῶν τοῦ K, ἐφοδιασμένο μὲ τὴν πράξη τοῦ πολλαπλασιασμοῦ ἰδεωδῶν, εἶναι ἀβελιανὴ ὁμάδα, τὴν ὁποία ἂς συμβολίσομε $\mathcal{I}$. Τὸ σύνολο τῶν μὴ μηδενικῶν κυρίων ἰδεωδῶν τοῦ K (πρβλ. ἄσκηση 2) ἂς συμβολίσομε $\mathcal{I}_0$. Ἀποδεῖξτε ὅτι τὸ $\mathcal{I}_0$ εἶναι ὑποομάδα τῆς $\mathcal{I}$.

   Ἀποδεῖξτε ὅτι ὑπάρχει ἕνας ἐπιμορφισμὸς ὁμάδων $K^* \twoheadrightarrow \mathcal{I}_0$, τοῦ ὁποίου ὁ πυρήνας εἶναι ἡ ὁμάδα τῶν μονάδων (= ἀντιστρεψίμων στοιχείων) τοῦ A, ἡ ὁποία συμβολίζεται U_K.

6. Ἔστω ὅτι $\alpha, \beta \in A\backslash\{0\}$ καὶ $(\mathrm{N}(\alpha), \mathrm{N}(\beta)) = d \in \mathbb{Z}$ (ἡ τελευταία σχέση ἀναφέρεται στὸ $\mathbb{Z}$). Ἔστω $\mathfrak{p}$ πρῶτο ἰδεῶδες ὑπεράνω τοῦ ρητοῦ πρώτου p, τὸ ὁποῖο εἶναι κοινὸς διαιρέτης τῶν (α) καὶ (β). Ἀποδεῖξτε ὅτι, στὸ $\mathbb{Z}$, ὁ p εἶναι κοινὸς διαιρέτης τῶν $\mathrm{N}(\alpha)$ καὶ $\mathrm{N}(\beta)$.
   Εἰδικὴ περίπτωση: Ἂν οἱ α, β εἶναι ρητοὶ ἀκέραιοι πρῶτοι μεταξύ τους, τότε καὶ τὰ ἰδεώδη $(\alpha), (\beta)$ εἶναι πρῶτα μεταξύ τους.

7. Ἔστω πρῶτο ἰδεῶδες $\mathfrak{p} = (p, \pi)$, ὅπου p εἶναι ρητὸς πρῶτος καὶ $\pi \in A$. Ἔστω, ἐπίσης, σ ἕνας $\mathbb{Q}$-αὐτομορφισμὸς τοῦ K (δηλαδή, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$). Ἀποδεῖξτε ὅτι τὸ ἰδεῶδες $\mathfrak{p}' = (p, \sigma(\pi))$ εἶναι, ἐπίσης, πρῶτο.
   (Ὑπόδειξη: Οἱ δακτύλιοι $A/\mathfrak{p}$ καὶ $A/\mathfrak{p}'$ εἶναι ἰσόμορφοι.)
   Περαιτέρω, ἀποδεῖξτε ὅτι, ἂν $\alpha \in A$ καὶ $\mathfrak{p}|\alpha$, τότε $\mathfrak{p}'|\sigma(\alpha)$.

8. Ἔστω $\beta_1, \ldots, \beta_n$ ἀκέραια βάση καὶ $\gamma = a_1\beta_1 + \cdots + a_n\beta_n$, ὅπου $a_1, \ldots, a_n \in \mathbb{Z}$. Ἔστω, ἀκόμη, $m \in \mathbb{Z}$ καὶ $\gamma' = a_1'\beta_1 + \cdots + a_n'\beta_n$, ὅπου $a_1', \ldots, a_n' \in \mathbb{Z}$ μὲ $a_i' \equiv a_i \pmod{m}$, $i = 1, \ldots, n$ (ἰσοτιμίες στὸ $\mathbb{Z}$). Ἀποδεῖξτε ὅτι $(m, \gamma) = (m, \gamma')$.

9. Στὸ μάθημα ἀρχίσαμε νὰ μελετοῦμε τὴ διοφαντικὴ ἐξίσωση $x^2 - 79y^2 = 5z^3$. Ἐργασθήκαμε στὸ ἀριθμητικὸ σῶμα $K = \mathbb{Q}(\theta)$, ὅπου $\theta^2 = 79$. Στὸ K, ἡ ἀνάλυση τοῦ (5) σὲ πρῶτα ἰδεώδη εἶναι $(5) = \mathfrak{p}_5\mathfrak{p}_5'$, ὅπου $\mathfrak{p}_5 = (5, 7+\theta)$ καὶ $\mathfrak{p}_5' = (5, 3+\theta)$. Ἀποδεῖξτε ὅτι, ἂν ἕνα ἀπὸ τὰ $\mathfrak{p}_5$ καὶ $\mathfrak{p}_5'$ διαιρεῖ τὸ $(x + y\theta)$, τότε τὸ ἄλλο διαιρεῖ τὸ $(x - y\theta)$.
   (Ὑπόδειξη: Ἐφαρμογὴ τῶν δύο προηγουμένων ἀσκήσεων.)