Δήμητρα Χαμηλάκη

ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΑΛΓΕΒΡΙΚΗΣ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ ΣΤΗΝ ΕΠΙΛΥΣΗ ΔΙΟΦΑΝΤΙΚΩΝ ΕΞΙΣΩΣΕΩΝ

Πτυχιακή Εργασία
Παρουσιάσθηκε στις 22-6-2000

Επιβλέπων Καθηγητής Ν.Γ. Τζανάκης

Τμήμα Μαθηματικών

Πανεπιστήμιο Κρήτης - Ηράκλειο

2000

Κεφάλαιο 1

Στοιχεία Αλγεβρικής Θεωρίας Αριθμών

Υποθέτουμε ότι εργαζόμαστε σε ένα αριθμητικό σώμα $\mathbb{K}$, δηλαδή σε πεπερασμένη επέκταση του $\mathbb{Q}$, την οποία θεωρούμε ως υπόσωμα του $\mathbb{C}$

Όταν λέμε **ακέραιος** εννοούμε «*αλγεβρικός ακέραιος*», δηλαδή στοιχείο του $\mathbb{C}$ (συνήθως, στοιχείο του $\mathbb{K}$), το οποίο είναι ρίζα ενός *μονικού* πολυωνύμου με συντελεστές από το $\mathbb{Z}$. Για τους συνήθεις ακεραίους χρησιμοποιούμε τον όρο **ρητός ακέραιος**.

1.1 Θεμελειώδη εργαλεία

Ορισμός 1.1.1 *Έστω το σώμα $\mathbb{K} = \mathbb{Q}(\omega)$, $f(x) \in \mathbb{Z}[x]$ το ελάχιστο πολυώνυμο του ω, βαθμού n και $\omega = \omega_1, \omega_2, \ldots, \omega_n$ οι ρίζες του $f(x)$* [1]*. Κάθε στοιχείο α του $\mathbb{K}$ είναι της μορφής $\alpha = c_0 + c_1\omega + \ldots + c_{n-1}\omega^{n-1}, c_i \in \mathbb{Q}$ $(i = 1, 2, \ldots, n-1)$.* **Συζυγής** *του α λέγεται καθένας από τους*

$$\alpha^{(j)} = c_0 + c_1\omega_j + \ldots + c_{n-1}\omega_j^{n-1}, \;\; 1 \leq j \leq n$$

Παρατηρήσεις. 1)

$$\begin{aligned} \omega^{(j)} &= \omega_j \,,\; j = 1, \ldots n \\ \alpha^{(1)} &= \alpha \,, \forall \alpha \in \mathbb{K} \end{aligned}$$

2) Οι συζυγείς του α δεν είναι κατ¨ ανάγκη διαφορετικοί μεταξύ τους. Για παράδειγμα, στο σώμα $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, οι συζυγείς του $\omega = \sqrt{2}+\sqrt{3}$ είναι

$$\begin{aligned} \omega_1 &= \sqrt{2}+\sqrt{3} \\ \omega_2 &= -\sqrt{2}+\sqrt{3} \\ \omega_3 &= \sqrt{2}-\sqrt{3} \\ \omega_4 &= -\sqrt{2}-\sqrt{3} \end{aligned}$$

[1] Σύμφωνα με το Θεώρημα 1.1.5, αυτές είναι διαφορετικές μεταξύ τους.

δηλαδή, οι ρίζες του $f(x) = x^4 - 10x^2 + 1$. Είναι $\omega^{-1} = \sqrt{3} - \sqrt{2}$, άρα, $\sqrt{3} = (\omega + \omega^{-1})/2$. Παίρνω $\alpha = \sqrt{3}$, οπότε

$$\alpha^{(2)} = \frac{1}{2}\left(\omega_2 + \frac{1}{\omega_2}\right) \ , \ \alpha^{(3)} = \frac{1}{2}\left(\omega_3 + \frac{1}{\omega_3}\right) \ , \ \alpha^{(4)} = \frac{1}{2}\left(\omega_4 + \frac{1}{\omega_4}\right) \ .$$

Όμως

$$\frac{1}{2}\left(\omega_2 + \frac{1}{\omega_2}\right) = \frac{1}{2}(-\sqrt{2} + \sqrt{3}) + \frac{1}{2(-\sqrt{2} + \sqrt{3})} = \sqrt{3}$$

και ανάλογα προκύπτει ότι ο τρίτος με τον τέταρτο συζυγή του $\sqrt{3}$ συμπίπτουν.

Θεώρημα 1.1.2 *Το σύνολο $\mathcal{O}$ όλων των αλγεβρικών ακεραίων του $\mathbb{C}$ αποτελεί υποδακτύλιο του $\mathbb{C}$. Ειδικώτερα, το σύνολο $\mathcal{O}_{\mathbb{K}}$ όλων των αλγεβρικών ακεραίων του $\mathbb{K}$ αποτελεί υποδακτύλιο του $\mathbb{K}$.*

Απόδειξη. Ο δεύτερος ισχυρισμός είναι άμεση συνέπεια του πρώτου. Όσον αφορά στον πρώτο, αρκεί να αποδείξουμε ότι $\alpha, \beta \in \mathcal{O} \Rightarrow \alpha + \beta, \alpha\beta \in \mathcal{O}$.

Έστω $\alpha, \beta \in \mathcal{O}$. Τα α, β είναι ρίζες κάποιων *μονικών* πολυωνύμων $h(x), g(x) \in \mathbb{Z}[x]$, αντιστοίχως. Έστω $\alpha_1 = \alpha, \ \ \alpha_2, \ldots, \alpha_n$ οι ρίζες του $h(x)$ και $\beta_1 = \beta, \ \ \beta_2, \ldots, \beta_m$ οι ρίζες του $g(x)$, οπότε

$$h(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n), \ g(x) = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_m) \ .$$

Το $\alpha + \beta$ ανήκει στο $\mathcal{O}$ διότι είναι ρίζα του

$$s(x) = \prod_{i,j}(x - (\alpha_i + \beta_j)) \ ,$$

το οποίο είναι μονικό πολυώνυμο βαθμού mn με συντελεστές ρητούς ακεραίους. Πράγματι, για $i = j = 1$ ένας παράγοντας του πολυωνύμου είναι ο $(x - (\alpha_1 + \beta_1))$ οπότε το πολυώνυμο έχει ρίζα το $\alpha + \beta$. Προφανώς είναι μονικό πολυώνυμο και οι συντελεστές του ανήκουν στο

$$\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m] = (\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_n])\,[\beta_1, \beta_2, \ldots, \beta_m] \ .$$

Το $s(x)$ μένει αμετάβλητο από κάθε αντιμετάθεση $\beta_i \leftrightarrow \beta_j$, άρα, κάθε συντελεστής του είναι συμμετρική παράσταση των $\beta_1, \ldots, \beta_m$. Συνεπώς, σύμφωνα με το *Θεμελιώδες Θεώρημα των Συμμετρικών Πολυωνύμων*, οι συντελεστές του $s(x)$ ανήκουν στο $(\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_n])\,[\sigma_1, \sigma_2, \ldots, \sigma_m]$, όπου $\sigma_1, \sigma_2, \ldots, \sigma_m$ οι στοιχειώδεις συμμετρικές παραστάσεις των $\beta_1, \beta_2, \ldots, \beta_m$, οι οποίες, με τη σειρά τους, είναι, κατά προσέγγιση προσήμου, οι συντελεστές του $g(x)$, άρα είναι ρητοί ακέραιοι. Εφαρμόζοντας ξανά το Θεμελιώδες Θεώρημα των Συμμετρικών Πολυωνύμων, συμπεραίνουμε ότι οι συντελεστές του $s(x)$ ανήκουν στο $\mathbb{Z}[\tau_1, \tau_2, \ldots, \tau_n]$, όπου $\tau_1, \tau_2, \ldots, \tau_n$ οι στοιχειώδεις συμμετρικές παραστάσεις των $\alpha_1, \alpha_2, \ldots, \alpha_n$, οι οποίες είναι ρητοί ακέραιοι, αφού συμπίπτουν, κατά προσέγγιση προσήμου, με τους συντελεστές του $h(x)$.

Αρκεί τώρα να δείξουμε ότι το $\alpha\beta$ ανήκει στο $\mathcal{O}$. να αποδείξουμε εύκολα κάποιες ιδιότητες.

Θεώρημα 1.1.3 *Έστω $\sigma : \mathbb{K} \to \mathbb{K}'$ ισομορφισμός σωμάτων, $p(x) \in \mathbb{K}[x]$ ανάγωγο πάνω από το $\mathbb{K}$ και $p'(x) \in \mathbb{K}'[x]$ το αντίστοιχο πολυώνυμο του $p(x)$ (δηλαδή αν $p(x) = a_0 + a_1x + \ldots + a_nx^n$ τότε $p'(x) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^n$). Αν u ρίζα του $p(x)$ σε κάποια επέκταση του $\mathbb{K}$ και v ρίζα του $p'(x)$ σε κάποια επέκταση του $\mathbb{K}'$ τότε ο ισομορφισμός σ επεκτείνεται σε ισομορφισμό $\tilde{\sigma} : \mathbb{K}(u) \to \mathbb{K}'(v)$ με $\tilde{\sigma}(u) = v$.*

Πρόταση 1.1.4 *Έστω $f(x), p(x) \in \mathbb{K}[x]$ και $p(x)$ ανάγωγο. Αν τα πολυώνυμα έχουν κάποια κοινή ρίζα σε κάποια επέκταση του $\mathbb{K}$, τότε το $p(x)$ διαιρεί το $f(x)$.*

Απόδειξη. Έστω ότι το $p(x)$ δεν διαιρεί το $f(x)$. Τότε, αυτά τα πολυώνυμα είναι πρώτα μεταξύ τους, διότι το $p(x)$ είναι ανάγωγο. Έπεται ότι υπάρχουν $f_1(x)$,$p_1(x)$ $\in \mathbb{K}[x]$ τέτοια ώστε $p(x)p_1(x) + f(x)f_1(x) = 1$. Αν ρ η κοινή ρίζα των $p(x), f(x)$ σε κάποια επέκταση του $\mathbb{K}$, η αντικατάσταση $x \leftarrow \rho$ μας δίνει $0 = 1$, άτοπο. □

Πρόταση 1.1.5 *Έστω $p(x) \in \mathbb{K}[x]$ ανάγωγο. Τότε όλες οι ρίζες του $p(x)$ είναι πολλαπλότητας 1.*

Απόδειξη. Συμβολίζουμε με $p'(x)$ την *τυπική παράγωγο* του $p(x)$. Έτσι αν $p(x) = c_0 + c_1x + \ldots + c_nx^n$, $c_n \neq 0$ τότε, εξ ορισμού, $p'(x) = c_1 + c_2x + \ldots + c_nx^{n-1}$. Έστω ότι το $p(x)$ έχει μια ρίζα ρ_0 πολλαπλότητας > 1 σε κάποια επέκταση $\mathbb{L}$ του $\mathbb{K}$. Τότε το ρ_0 είναι ρίζα και του $p'(x)$. Δηλαδή τα $p(x)$ και $p'(x)$ έχουν κοινή ρίζα στο $\mathbb{L}$ και $p(x)$ ανάγωγο. Άρα, από την Πρόταση 1.1.4, $p(x)|p'(x)$ (1). Όπως φαίνεται στον ορισμό του $p'(x)$, $\deg p(x) > \deg p'(x)$ (2). Λόγω των (1),(2) καταλήγουμε σε άτοπο.

□

Με τους συμβολισμούς του Ορισμού 1.1.1 και βάσει της Πρότασης 1.1.5 και του Θεωρήματος 1.1.3, συμπεραίνουμε ότι, για κάθε $i = 1, \ldots, n$, υπάρχει ισομορφισμός $\sigma_i : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega_i)$ με $\sigma_i(q) = q \; \forall q \in \mathbb{Q}$ και $\sigma_i(\omega) = \omega_i$. Συνεπώς,

$$\text{Για κάθε } \alpha \in \mathbb{K},\ \mathbf{N}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)\ . \tag{1.1}$$

Το να βλέπουμε τους συζυγείς ενός αλγεβρικού αριθμού ως εικόνες μέσω των ισομορφισμών σ_i, είναι, συχνά, πολύ βοηθητικό. Για παράδειγμα, έχουμε την

Πρόταση 1.1.6 *Οι συζυγείς αλγεβρικού ακεραίου είναι, επίσης, αλγεβρικοί ακέραιοι.*

Απόδειξη. Έστω $\alpha \in \mathbb{Q}(\omega)$ αλγεβρικός ακέραιος. Το α είναι ρίζα ενός μονικού πολυωνύμου, $f(x)$, με συντελεστές από το $\mathbb{Z}$. Θεωρούμε τον ισομορφισμό σ_i, όπως προηγουμένως. Τότε $f(\sigma_i(\alpha)) = \sigma_i(f(\alpha)) = \sigma_i(0) = 0$. Άρα και ο συζυγής του α είναι ρίζα του ίδιου πολυωνύμου με συντελεστές από το $\mathbb{Z}$, δηλαδή είναι αλγεβρικός ακέραιος.

□

Συνεχίζουμε με τους συμβολισμούς του Ορισμού 1.1.1.

Πρόταση 1.1.7 *Η στάθμη $\mathbf{N}(\alpha)$ είναι ρητός αριθμός, μη μηδενικός, αν $\alpha \neq 0$. Αν, επιπλέον, ο α είναι αλγεβρικός ακέραιος, τότε η $\mathbf{N}(\alpha)$ είναι ρητός ακέραιος.*

Απόδειξη. Έστω $\alpha \in \mathbb{K} = \mathbb{Q}(\omega)$. Για $\alpha \neq 0$, είναι φανερό, από τον ορισμό της στάθμης, ότι $\mathbf{N}(\alpha) \neq 0$. Υπάρχουν μονοσήμαντα ορισμένοι $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Q}$ τέτοιοι ώστε $\alpha = c_0 + c_1\omega + \ldots + c_{n-1}\omega^{n-1}$, άρα

$$\mathbf{N}(\alpha) = \prod_{j=1}^{n}(c_0 + c_1\omega_j + \ldots + c_{n-1}\omega_j^{n-1}) \in \mathbb{Q}[\omega_1, \ldots, \omega_n] \, .$$

και είναι συμμετρική των $\omega_1, \omega_2, \ldots, \omega_n$. Έτσι, από το Θεμελιώδες Θεώρημα των Συμμετρικών Πολυωνύμων, $\mathbf{N}(\alpha) \in \mathbb{Q}[s_1, s_2, \ldots, s_n]$, όπου $s_1, s_2, \ldots, s_n$ είναι οι στοιχειώδεις συμμετρικές παραστάσεις των $\omega_1, \ldots, \omega_n$. Όμως από τους τύπους του Viète, οι $s_1, \ldots, s_n$, συμπίπτουν, κατά προσέγγιση προσήμου, με τους συντελεστές του $f(x)$, άρα ανήκουν στο $\mathbb{Q}$, οπότε και $\mathbf{N}(\alpha) \in \mathbb{Q}$.

Ο δεύτερος ισχυρισμός απαιτεί περισσότερη δουλειά και αποδεικνύεται στην Παράγραφο 1.1.1.

Πρόταση 1.1.8 *Για τη στάθμη ισχύουν οι ακόλουθες ιδιότητες:*

- $\mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta)$ *και* $\mathbf{N}\left(\frac{\alpha}{\beta}\right) = \frac{\mathbf{N}(\alpha)}{\mathbf{N}(\beta)}$.
- *Αν $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ και $\alpha|\beta$, τότε $\mathbf{N}(\alpha)|\mathbf{N}(\beta)$.*
- *Κάθε ακέραιος είναι διαιρέτης της στάθμης του.*
- *Αν $[\mathbb{K} : \mathbb{Q}] = n$ και $a \in \mathbb{Q}$, τότε $\mathbf{N}(a) = a^n$.*

Απόδειξη. Πράγματι χρησιμοποιώντας τη σχέση (1.1) έχουμε

$$\begin{aligned}
\mathbf{N}(\alpha\beta) &= \sigma_1(\alpha\beta)\sigma_2(\alpha\beta)\ldots\sigma_n(\alpha\beta) \\
&= \sigma_1(\alpha)\sigma_1(\beta)\sigma_2(\alpha)\sigma_2(\beta)\ldots\sigma_n(\alpha)\sigma_n(\beta) \\
&= \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha)\sigma_1(\beta)\sigma_2(\beta)\ldots\sigma_n(\beta) \\
&= \mathbf{N}(\alpha)\mathbf{N}(\beta) \, .
\end{aligned}$$

$$\mathbf{N}\left(\frac{\alpha}{\beta}\right) = \sigma_1\left(\frac{\alpha}{\beta}\right)\sigma_2\left(\frac{\alpha}{\beta}\right)\ldots\sigma_n\left(\frac{\alpha}{\beta}\right) = \frac{\sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha)}{\sigma_1(\beta)\sigma_2(\beta)\ldots\sigma_n(\beta)} = \frac{\mathbf{N}(\alpha)}{\mathbf{N}(\beta)}$$

Η τρίτη ιδιότητα είναι άμεση συνέπεια της πρώτης.

Για την τέταρτη ιδιότητα, χρησιμοποιούμε τους συμβολισμούς του Ορισμού 1.1.1. Αν ο α είναι ακέραιος, τότε είναι ρίζα ενός μονικού πολυωνύμου με συντελεστές από το $\mathbb{Z}$. Όμως, κάθε συζυγής του α είναι ρίζα του ίδιου πολυωνύμου, άρα είναι αλγεβρικός ακέραιος. Αν, λοιπόν, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ είναι οι συζυγείς

του του α, τότε, $\alpha_2 \cdots \alpha_n = \mathbf{N}(\alpha)/\alpha_1$, οπότε το αριστερό μέλος, βάσει του Θεωρήματος 1.1.2, είναι αλγεβρικός ακέραιος. Το δεξιό μέλος, από την Πρόταση 1.1.7, ανήκει στο $\mathbb{K}$. Άρα, η $\mathbf{N}(\alpha)$ είναι γινόμενο του α επί έναν αλγεβρικό ακέραιο του $\mathbb{K}$, δηλαδή, διαιρείται από τον α.

Η πέμπτη ιδιότητα είναι άμεση συνέπεια της σχέσης (1.1). □

Ορισμός 1.1.9 *Έστω ϵ ακέραιος του σώματος $\mathbb{K}$. Το ϵ λέγεται* **μονάδα** *αν υπάρχει ακέραιος ϵ' τέτοιος ώστε $\epsilon\epsilon' = 1$.*

Προφανώς, το ϵ' του παραπάνω ορισμού είναι, επίσης, μονάδα. Συμβολίζουμε το σύνολο των μονάδων του $\mathbb{K}$ με $E(\mathbb{K})$ και είναι προφανές ότι αποτελεί υποομάδα της πολλαπλασιαστικής ομάδας $\mathbb{K}^*$.

Πρόταση 1.1.10 *Ένας ακέραιος $\epsilon \in \mathbb{K}$ είναι μονάδα αν και μόνο αν $\mathbf{N}(\epsilon) = \pm 1$. Όλοι οι διαιρέτες μιας μονάδας είναι μονάδες.*

Απόδειξη. Έστω ϵ μονάδα του $\mathbb{K}$. Τότε $\epsilon\epsilon' = 1$, άρα (Πρόταση 1.1.8), $1 = \mathbf{N}(1) = \mathbf{N}(\epsilon\epsilon') = \mathbf{N}(\epsilon)\mathbf{N}(\epsilon') = 1$. Όμως, από την Πρόταση 1.1.7, $\mathbf{N}(\epsilon)$ είναι ρητός ακέραιος, άρα $\mathbf{N}(\epsilon) = \pm 1$.

Αντιστρόφως, έστω $\epsilon \in \mathbb{K}$ με $\mathbf{N}(\epsilon) = \pm 1$. Αν $\epsilon_1 = \epsilon, \epsilon_2, \ldots, \epsilon_n$ είναι οι συζυγείς του ϵ, τότε ο αριθμός $\epsilon_2 \cdots \epsilon_n$ είναι ακέραιος του $\mathbb{K}$ (πρβλ. απόδειξη του τέταρτου ισχυρισμού της Πρότασης 1.1.8 με το ϵ στη θέση του α). Αν τον συμβολίσουμε με ϵ', τότε $\epsilon\epsilon' = \mathbf{N}(\epsilon) = \pm 1$, άρα το ϵ είναι μονάδα του $\mathbb{K}$.

Όσον αφορά στον δεύτερο ισχυρισμό, αν ϵ είναι μονάδα και ν διαιρέτης του ϵ, έχω $\epsilon = \nu\kappa$ για κάποιο ακέραιο κ, άρα, $\mathbf{N}(\epsilon) = \mathbf{N}(\nu\kappa) = \mathbf{N}(\nu)\mathbf{N}(\kappa)$, απ' όπου, λόγω και του πρώτου ισχυρισμού, που αποδείξαμε, $\pm 1 = \mathbf{N}(\nu)\mathbf{N}(\kappa)$. Οι δύο παράγοντες του δεξιού μέλους είναι ρητοί ακέραιοι (Πρόταση 1.1.7), άρα $\mathbf{N}(\nu) = \pm 1$, οπότε, βάσει του πρώτου ισχυρισμού, που αποδείξαμε, το ν είναι μονάδα του $\mathbb{K}$. □

Ορισμός 1.1.11 *Έστω $\beta \in \mathbb{K}$ ακέραιος.* **Συνεταιρικός** *του β λέγεται κάθε ακέραιος β' της μορφής $\beta' = \epsilon\beta$ όπου ϵ μονάδα του $\mathbb{K}$.*

Προφανείς διαιρέτες κάθε ακεραίου β του $\mathbb{K}$ είναι οι μονάδες του $\mathbb{K}$ και οι συνεταιρικοί του β – οι λεγόμενοι **τετριμμένοι διαιρέτες** του.

Πράγματι, έστω ϵ μονάδα. Τότε υπάρχει μονάδα ϵ', έτσι ώστε $\epsilon\epsilon' = 1$. Άρα $\beta = \beta \cdot 1 = \beta \cdot \epsilon \cdot \epsilon'$, δηλαδή $\epsilon|\beta$. Επίσης, αν ο β' είναι συνεταιρικός του β, τότε β/β' είναι μονάδα· ειδικώτερα $\beta'|\beta$.

Ορισμός 1.1.12 *Αν α, β ακέραιοι,* **μέγιστος κοινός διαιρέτης** *των α, β λέγεται κάθε ακέραιος δ με τις ιδιότητες*

(α') *ο δ διαιρεί τα α, β*

(β') *για κάθε δ' που διαιρεί τα α, β ο δ' διαιρεί το δ.*

Πρόταση 1.1.13 *Έστω α, β ακέραιοι στο $\mathbb{K}$. Οι μέγιστοι κοινοί διαιρέτες των α, β διαφέρουν κατά μονάδες του $\mathbb{K}$· είναι, δηλαδή, συνεταιρικοί μεταξύ τους.*

Απόδειξη. Αν δ_1, δ_2 είναι μέγιστοι κοινοί διαιρέτες των α, β, τότε, εξ ορισμού, $\delta_1|\delta_2$ και $\delta_2|\delta_1$. Επομένως υπάρχουν ακέραιοι κ, λ, τέτοιοι ώστε $\delta_2 = \kappa\delta_1, \delta_1 = \lambda\delta_2$. Έπεται $\delta_1 = \lambda\kappa\delta_1$ άρα $\lambda\kappa = 1$ και, συνεπώς, κ, λ είναι μονάδες.

□

Αν οι μόνοι κοινοί διαιρέτες δύο ακεραίων είναι μονάδες, οι ακέραιοι λέγονται **πρώτοι μεταξύ τους**.

Ορισμός 1.1.14 *Έστω ξ μη μηδενικός ακέραιος. Οι ακέραιοι α, β λέγονται* **ισοδύναμοι** $\bmod \xi$ *αν η διαφορά $\alpha - \beta$ διαιρείται δια ξ. Γράφουμε τότε $\alpha \equiv \beta \pmod{\xi}$ και λέμε ότι τα α, β ανήκουν στην ίδια κλάση ισοδυναμίας* $\bmod \xi$.

Ορισμός 1.1.15 *Ένας ακέραιος που δεν είναι μονάδα και έχει μόνο τους τετριμμένους διαιρέτες, λέγεται* **ανάγωγος**.

Πρόταση 1.1.16 *Κάθε ακέραιος ξ με στάθμη πρώτο, είναι ανάγωγος.*

Απόδειξη. Έστω ξ ακέραιος με $\mathbf{N}(\xi) = p, p \in \mathbb{P}$. Αρκεί να δείξω ότι αν $\xi = \nu\kappa$ τότε ένας από τους ν, κ είναι μονάδα (οπότε ο άλλος είναι συνεταιρικός του ξ). Αν $\xi = \nu\kappa$ τότε έχω : $\mathbf{N}(\xi) = \mathbf{N}(\nu\kappa) \Rightarrow p = \mathbf{N}(\nu)\mathbf{N}(\kappa) \Rightarrow \mathbf{N}(\nu) = \pm 1$ ή $\mathbf{N}(\kappa) = \pm 1$ άρα, από την Πρόταση 1.1.10, ο ν, είτε ο κ, είναι μονάδα. □

Ορισμός 1.1.17 *Έστω π ακέραιος του $\mathbb{K}$, ο οποίος δεν είναι μονάδα. Ο π λέγεται* **πρώτος** *αν αληθεύει η συνεπαγωγή*

$$\pi|\alpha\beta \text{ και } \alpha, \beta \text{ ακέραιοι} \Rightarrow \pi|\alpha \text{ είτε } \pi|\beta.$$

Στο εξής, λέγοντας «*πρώτος*» θα εννοούμε «*πρώτος του* $\mathbb{K}$», ενώ για τους συνήθεις πρώτους θα χρησιμοποιούμε τον όρο «ρητός πρώτος».

Πρόταση 1.1.18 *Κάθε πρώτος του $\mathbb{K}$ είναι και ανάγωγος.*

Απόδειξη. Έστω π πρώτος του $\mathbb{K}$. Αρκεί να δείξω ότι αν $\pi = \alpha\beta$, ένας από τους α, β είναι μονάδα και ο άλλος συνεταιρικός του π. Αφού $\pi = \alpha\beta$, συμπεραίνω, ειδικώτερα, ότι ο π διαιρεί το γινόμενο $\alpha\beta$ και επειδή είναι πρώτος, διαιρεί τουλάχιστον ένα από τους α, β. Ας υποθέσω, χωρίς βλάβη της γενικότητας, ότι διαιρεί τον α. Τότε υπάρχει ακέραιος γ τέτοιος ώστε $\alpha = \pi\gamma$. Όμως, $\pi = \alpha\beta$, άρα $\alpha = \alpha\beta\gamma$ και, συνεπώς, $\beta\gamma = 1$. Η τελευταία σχέση λέει ότι το β είναι μονάδα.

□

Το αντίστροφο της προηγούμενης πρότασης δεν ισχύει, εν γένει. Δηλαδή, υπάρχουν ανάγωγοι, που δεν είναι πρώτοι. Για παράδειγμα, στο σώμα $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$ $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Εύκολα διαπιστώνεται ότι το 3 είναι ανάγωγο και προφανώς διαιρεί το γινόμενο $(1 + \sqrt{-5})(1 - \sqrt{-5})$. Όμως

δεν διαιρεί κανένα από τους $(1+\sqrt{-5}), (1-\sqrt{-5})$. Πράγματι, αν $3|(1\pm\sqrt{-5})$, υπάρχει $\alpha, \alpha = b + c\sqrt{-5},\ b, c \in \mathbb{Z}$ [2] έτσι ώστε $(1\pm\sqrt{-5}) = 3\cdot\alpha$. Έπεται ότι $(1\pm\sqrt{-5}) = 3(b+c\sqrt{-5})$ οπότε $3b = 1, 3c = \pm 1$. Άτοπο γιατί οι b, c είναι ακέραιοι.

□

Παρακάτω, στην Παράγραφο 1.2 θα δούμε ότι υπάρχουν σώματα στα οποία ισχύει το αντίστροφο, οπότε οι έννοιες «*ανάγωγος*» και «*πρώτος*» ταυτίζονται. Χάρη σ' αυτή την ιδιότητα, αυτά τα σώματα μας επιτρέπουν να μεταφέρουμε στους ακεραίους τους τις σημαντικότερες ιδιότητες της Αριθμητικής των συνηθισμένων ακεραίων.

1.1.1 Στάθμη αλγεβρικού ακεραίου

Σ' αυτή την παράγραφο αποδεικνύουμε τον δεύτερο ισχυρισμό της Πρότασης 1.1.7, ότι η στάθμη ακεραίου είναι ρητός ακέραιος. Αυτό προκύπτει ως άμεση συνέπεια της τελευταίας σχέσης αυτής της παραγράφου, η οποία, καθ' εαυτήν, είναι ενδιαφέρουσα. Χρειαζόμαστε πρώτα ένα απλό γενικό λήμμα, σχετικό με ομάδες.

Λήμμα 1.1.19 *Έστω G πεπερασμένη ομάδα και H, K υποομάδες της, τέτοιες ώστε $G > H > K$ και $[H:K] = \nu$. Τότε, για κάθε σύμπλοκο gH, υπάρχουν ακριβώς ν το πλήθος διαφορετικά σύμπλοκα $g_1K, \ldots, g_\nu K$, τέτοια ώστε $g_iH = gH,\ i = 1, \ldots, \nu$.*

Απόδειξη. Έστω G/K το σύνολο των αριστερών συμπλόκων. Ορίζουμε τη σχέση ισοδυναμίας

$$g_1K \sim g_2K \overset{ορσ}{\Leftrightarrow} g_1H = g_2H\ .$$

Ο ισχυρισμός του λήμματος ισοδυναμεί με το ότι, για κάθε g, η κλάση ισοδυναμίας $[gK]$ περιέχει ακριβώς ν στοιχεία (σύμπλοκα).

Θα δείξουμε πρώτα ότι όλες οι κλάσεις ισοδυναμίας έχουν το ίδιο πλήθος στοιχείων. Αν $[gK], [g'K]$ είναι δύο κλάσεις, θεωρώ $g'' \in G$, τέτοιο ώστε $g''\cdot g = g'$. Εύκολα βλέπουμε ότι η απεικόνιση

$$[gK] \ni g_1K \longmapsto g''\cdot g_1K \in [g'K]$$

είναι αμφιμονοσήμαντη. Λόγω συμμετρίας, υπάρχει, επίσης, αμφιμονοσήμαντη απεικόνιση $[g'K] \longrightarrow [gK]$. Άρα, οι κλάσεις $[gK], [g'K]$ είναι ισοπληθείς. Συνεπώς, κάθε κλάση $[gK]$ περιέχει τόσα σύμπλοκα, όσα και η $[K]$. Για να δουμε πόσα σύμπλοκα περιέχει η $[K]$ εξετάζουμε τη συνθήκη $gK \in [K]$. Αυτή ισοδυναμεί με την $gH = H$, δηλαδή με την $g \in H$. Συνεπώς

$$[K] = \{gK : g \in H\} = \text{σύνολο } H/K \text{ των αριστερών συμπλόκων.}$$

[2] ο α είναι ακέραιος του $\mathbb{Q}(\sqrt{-5})$ λόγω του θεωρήματος 1.4.1

Καθώς είναι γνωστό, το τελευταίο σύνολο έχει πληθάριθμο ίσο με $[H : K]$.

□

Εφαρμογή. Διατηρούμε τους συμβολισμούς του Ορισμού 1.1.1. Έστω $\mathbb{L}$ το σώμα ριζών του $f(x)$ πάνω από το $\mathbb{Q}$. Έστω, επίσης, $\alpha \in \mathbb{K}$ και $g(x) \in \mathbb{Z}[x]$ το ελάχιστο (μονικό) πολυώνυμό του. Ας υποθέσουμε ότι το $g(x)$ είναι βαθμού d και ας συμβολίσουμε τις ρίζες του $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$. Επειδή $\alpha \in \mathbb{K} \subseteq \mathbb{L}$ και η επέκταση $\mathbb{L}/\mathbb{Q}$ είναι Galois, όλες οι ρίζες του $g(x)$ ανήκουν στο $\mathbb{L}$.

Εξ ορισμού της στάθμης,

$$\mathbf{N}(\alpha) = \prod_{i=1}^{n} \alpha^{(i)} \ .$$

Παρατηρούμε τα εξής:

1. Για κάθε $\sigma \in \mathcal{G}(\mathbb{L}/\mathbb{Q}), \sigma(\omega) \in \{\omega_1, ..., \omega_n\}$ και, αντιστρόφως, για κάθε ω_i, υπάρχει $\sigma \in \mathcal{G}(\mathbb{L}/\mathbb{Q})$, τέτοιο ώστε $\sigma(\omega) = \omega_i$.

   Πράγματι, το στοιχείο $\sigma(\omega)$ είναι ρίζα του $f(x)$, αφού $f(\omega) = 0$. Αντιστρόφως, είδαμε αμέσως πριν από τη σχέση (1.1) ότι, για κάθε δείκτη i, υπάρχει $\mathbb{Q}$-ισομορφισμός $\sigma_i : \mathbb{Q}(\omega) \longrightarrow \mathbb{Q}(\omega_i)$, που στέλνει το ω στο ω_i. Με στερεότυπες τεχνικές της Θεωρίας Σωμάτων, αυτός ο ισομορφισμός επεκτείνεται σε αυτομορφισμό $\tilde{\sigma}$ του $\mathbb{L}$ και αυτό είναι το ζητούμενο $\sigma \in \mathcal{G}(\mathbb{L}/\mathbb{Q})$.

2. Αν $\sigma_1, \sigma_2 \in \mathcal{G}(\mathbb{L}/\mathbb{Q})$ τότε $\sigma_1\mathcal{G}(\mathbb{L}/\mathbb{K}) = \sigma_2\mathcal{G}(\mathbb{L}/\mathbb{K}) \Leftrightarrow \sigma_1(\omega) = \sigma_2(\omega)$

   Πράγματι, αυτό προκύπτει αμέσως από την παρατήρηση ότι, αφού $\mathbb{K} = \mathbb{Q}(\omega)$, έχουμε $\sigma_2^{-1} \cdot \sigma_1 \in \mathcal{G}(\mathbb{L}/\mathbb{K}) \Leftrightarrow \sigma_2^{-1} \cdot \sigma_1(\omega) = \omega$.

3. $\mathbf{N}(\alpha) = \prod_\sigma \sigma(\alpha)$, όπου το σ διατρέχει ένα πλήρες σύστημα εκπροσώπων μέσα από το σύνολο $\mathcal{G}(\mathbb{L}/\mathbb{Q})/\mathcal{G}(\mathbb{L}/\mathbb{K})$.

   Αυτό προκύπτει από προφανή συνδυασμό των δύο πρώτων παρατηρήσεων.

Έστω $\mathbb{M} = \mathbb{Q}(\alpha)$. Εφαρμόζουμε το Λήμμα 1.1.19 για την αλυσσίδα ομάδων

$$\mathcal{G}(\mathbb{L}/\mathbb{Q}) > \mathcal{G}(\mathbb{L}/\mathbb{M}) > \mathcal{G}(\mathbb{L}/\mathbb{K}) \ .$$

Είναι

$$|\mathcal{G}(\mathbb{L}/\mathbb{M})| : |\mathcal{G}(\mathbb{L}/\mathbb{K})| = [\mathbb{K} : \mathbb{M}] = [\mathbb{K} : \mathbb{Q}] : [\mathbb{M} : \mathbb{Q}] = n : d \ .$$

Άρα, σε κάθε $\sigma\mathcal{G}(\mathbb{L}/\mathbb{M})$ αντιστοιχούν ακριβώς $\nu = \frac{n}{d}$ το πλήθος σύμπλοκα $\sigma_1\mathcal{G}(\mathbb{L}/\mathbb{K})$, $\ldots, \sigma_\nu\mathcal{G}(\mathbb{L}/\mathbb{K})$ τέτοια ώστε $\sigma_i\mathcal{G}(\mathbb{L}/\mathbb{M}) = \sigma\mathcal{G}(\mathbb{L}/\mathbb{M})$. Αυτό σημαίνει ότι τα σ, που εμφανίζονται στο (3), μπορούμε να τα ομαδοποιήσουμε ανά ν, έτσι ώστε

$$\mathbf{N}(\alpha) = \left(\prod_\sigma \sigma(\alpha) \right)^{\frac{n}{d}}$$

σ διατρέχει ένα πλήρες σύστημα εκπροσώπων μέσα από το σύνολο $\mathcal{G}(\mathbb{L}/\mathbb{Q})/\mathcal{G}(\mathbb{L}/\mathbb{M})$. Το πλήθος των παραγόντων στο $\prod_\sigma \sigma(\alpha)$ είναι ίσο με

$$|\mathcal{G}(\mathbb{L}/\mathbb{Q})| : |\mathcal{G}(\mathbb{L}/\mathbb{M})| = [\mathbb{M} : \mathbb{Q}] = d \, .$$

Επίσης, αν $\sigma_1\mathcal{G}(\mathbb{L}/\mathbb{M}) \neq \sigma_2\mathcal{G}(\mathbb{L}/\mathbb{M})$ τότε $\sigma_1(\alpha) \neq \sigma_2(\alpha)$. Άρα, τα $\sigma(\alpha)$, που εμφανίζονται στο γινόμενο αυτό, είναι όλα διαφορετικά μεταξύ τους και το πλήθος τους είναι d. Συνεπώς, αυτά τα $\sigma(\alpha)$ δεν είναι παρά τα $\alpha_1, \ldots, \alpha_d$, αφού κάθε $\sigma(\alpha)$ πρέπει να είναι ρίζα του $g(x)$. Συμπέρασμα:

$$\mathbf{N}(\alpha) = (\alpha_1\alpha_2 \cdots \alpha_d)^{\frac{n}{d}} = \{(-1)^d \cdot \text{ σταθερός όρος του } g(x)\}^{\frac{n}{d}} \, .$$

Αν ο α είναι ακέραιος, οπότε ο σταθερός όρος του $g(x)$ είναι ρητός ακέραιος, τότε άμεση συνέπεια της τελευταίας σχέσης είναι ότι $\mathbf{N}(\alpha) \in \mathbb{Z}$.

1.2 Αριθμητικά Σώματα Μονοσήμαντης Ανάλυσης

Ορισμός 1.2.1 *Λέμε ότι στο $\mathbb{K}$ (ακριβέστερα, στον δακτύλιο $\mathcal{O}_\mathbb{K}$ των ακεραίων του $\mathbb{K}$) έχουμε* **μονοσήμαντη ανάλυση**, *αν κάθε μη μηδενικός ακέραιος του $\mathbb{K}$, που δεν είναι μονάδα, αναλύεται σε γινόμενο πρώτων παραγόντων, κατά μοναδικό τρόπο· θεωρούμε ότι η σειρά των παραγόντων δεν παίζει ρόλο, και πρώτοι, που είναι συνεταιρικοί, δεν εννοούνται ως διαφορετικοί.*

Θεώρημα 1.2.2 *Στο δακτύλιο $\mathcal{O}_\mathbb{K}$ των ακεραίων του $\mathbb{K}$ υποθέτω ότι*

- (E_1) *Υπάρχει συνάρτηση $\mathbf{v} : \mathbb{K} \to \mathbb{Q}$ με $\mathbf{v}(xy) = \mathbf{v}(x)\mathbf{v}(y) \forall x, y \in \mathbb{K}$ και $\forall x \in \mathcal{O}, x \neq 0$ το $|\mathbf{v}(x)|$ είναι ακέραιος ≥ 1.*
- (E_2) *Αν γ, γ_1 ακέραιοι με $\gamma_1 \neq 0$ υπάρχουν ακέραιοι κ, γ_2 τέτοιοι ώστε*

$$\gamma = \kappa\gamma_1 + \gamma_2 \;\; \mu\varepsilon \;\; \gamma_2 = 0 \;\; \acute{\eta} \;\; |\mathbf{v}(\gamma_2)| < |\mathbf{v}(\gamma_1)|$$

Τότε στον $\mathcal{O}_\mathbb{K}$ ισχύουν τα εξής :

(α΄) Αν οι ακέραιοι γ, γ_1 είναι πρώτοι μεταξύ τους και ο γ_1 διαιρεί το γινόμενο $\beta\gamma$, τότε διαιρεί τον β.

(β΄) Κάθε ανάγωγος είναι πρώτος.

(γ΄) Ο ακέραιος α του $\mathbb{K}$ είναι μονάδα, αν, και μόνο αν, $|\mathbf{v}(\alpha)| = 1$.

(δ΄) Έχουμε μονοσήμαντη ανάλυση σε πρώτους παράγοντες.

Απόδειξη. (α΄) Προφανώς, αρκεί να αποδείξουμε τον ισχυρισμό για γ_1, που δεν είναι μονάδα. Λόγω της (E_2), υπάρχουν ακέραιοι κ, γ_2 έτσι ώστε

$$\gamma = \kappa\gamma_1 + \gamma_2, \;\; \gamma_2 = 0 \;\; \acute{\eta} \;\; |\mathbf{v}(\gamma_2)| < |\mathbf{v}(\gamma_1)|$$

Αποκλείεται όμως $\gamma_2 = 0$ διότι τότε $\gamma_1|\gamma$, που αντιφάσκει στην υπόθεση. Άρα, $\gamma_2 \neq 0$ και η (E_2) εξασφαλίζει την ύπαρξη ακεραίων λ, γ_3 έτσι ώστε

$$\gamma_1 = \lambda\gamma_2 + \gamma_3,\ \gamma_3 = 0 \ \text{ ή } \ |\mathbf{v}(\gamma_3)| < |\mathbf{v}(\gamma_2)| \ .$$

Αν $\gamma_3 \neq 0$, συνεχίζω:

$$\gamma_2 = \mu\gamma_3 + \gamma_4,\ \gamma_4 = 0 \ \text{ ή } \ |\mathbf{v}(\gamma_4)| < |\mathbf{v}(\gamma_3)| \text{ κ.ο.κ.}$$

Η ακολουθία $|\mathbf{v}(\gamma_1)|, |\mathbf{v}(\gamma_2)|, \ldots$ είναι γνησίως φθίνουσα ακολουθία θετικών ακεραίων. Επομένως υπάρχει ένας φυσικός n τέτοιος ώστε $\gamma_{n+1} = 0$, δηλαδή $\gamma_{n-1} = \zeta\gamma_n$, για κάποιο ακέραιο ζ. Όμως, από τις παραπάνω σχέσεις, προχωρώντας διαδοχικά, διαπιστώνουμε εύκολα ότι

$$\text{ΜΚΔ}(\gamma, \gamma_1) = \text{ΜΚΔ}(\gamma_1, \gamma_2) = \text{ΜΚΔ}(\gamma_2, \gamma_3) = \ldots \text{ΜΚΔ}(\gamma_{n-1}, \gamma_n) = \gamma_n \ .$$

Άρα το γ_n μονάδα, αφού οι γ, γ_1 έχουν υποτεθεί πρώτοι μεταξύ τους. Ακόμα $\beta\gamma_n$ =ΜΚΔ$(\beta\gamma, \beta\gamma_1)$ δηλαδή β' =ΜΚΔ$(\beta\gamma, \beta\gamma_1)$ όπου β' ακέραιος συνεταιρικός του β. Προφανώς $\gamma_1|\beta\gamma_1$, ενώ εξ υποθέσεως $\gamma_1|\beta\gamma$. Άρα $\gamma_1|$ΜΚΔ$(\beta\gamma, \beta\gamma_1) = \beta'$, οπότε και $\gamma_1|\beta$.

(β′) Έστω π ανάγωγος, με $\pi|\beta\gamma$. Αν $\mu = \text{ΜΚΔ}(\pi, \gamma)$, τότε $\mu|\pi$ και $\mu|\gamma$. Επειδή ο π είναι ανάγωγος, και ο μ είναι παράγοντάς του, έπεται ότι ο μ είναι μονάδα ή ακέραιος συνεταιρικός του π. Αν ο μ είναι μονάδα, οι π, γ είναι πρώτοι μεταξύ τους οπότε, λόγω του (α′), η σχέση $\pi|\beta\gamma$ δίνει $\pi|\beta$. Αν ο μ είναι συνεταιρικός του π, τότε $\pi|\mu\cdot$ όμως $\mu|\gamma$, άρα $\pi|\gamma$. Σε κάθε περίπτωση ο π διαιρεί τουλάχιστον ένα από τους β, γ, επομένως ο π είναι πρώτος.

(γ′) Κατ' αρχάς, $\mathbf{v}(1) = 1$. Πράγματι, έστω $x \in \mathbb{K}$, μη μηδενικό. Τότε $x = x\cdot 1$, άρα, από την (E_1), $\mathbf{v}(x) = \mathbf{v}(x)\mathbf{v}(1)$, δηλαδή $\mathbf{v}(1) = 1$. Αν ο ακέραιος α είναι μονάδα, τότε $\alpha\alpha' = 1$ για κάποιον ακέραιο α', οπότε, από την (E_1), $\mathbf{v}(\alpha)\mathbf{v}(\alpha') = \mathbf{v}(1) = 1$ και οι παράγοντες στο αριστερό μέλος είναι ρητοί ακέραιοι. Άρα, $\mathbf{v}(\alpha) = \pm 1$. Αντιστρόφως, έστω ακέραιος α, τέτοιος ώστε $|\mathbf{v}(\alpha)| = 1$. Εφαρμόζοντας την (E_2), βρίσκουμε ακεραίους β, γ, έτσι ώστε $1 = \beta\alpha + \gamma$ με $\gamma = 0$ ή $|\mathbf{v}(\gamma)| < |\mathbf{v}(\alpha)|$. Επειδή $|\mathbf{v}(\alpha)| = 1$ και $0 \neq \mathbf{v}(\gamma) \in \mathbb{Z}$, το δεύτερο ενδεχόμενο, προφανώς, αποκλείεται. Άρα $\alpha\beta = 1$, που σημαίνει ότι το α είναι μονάδα.

(δ′) Θα δείξω πρώτα ότι κάθε ακέραιος ξ, που δεν είναι μονάδα, έχει ένα, τουλάχιστον, ανάγωγο διαιρέτη. Πράγματι, ο αριθμός $|\mathbf{v}(\xi)|$ είναι θετικός ρητός ακέραιος. Για κάθε διαιρέτη η του ξ, που δεν είναι μονάδα, ο αριθμός $|\mathbf{v}(\eta)|$ είναι, λόγω της (E_1), θετικός (ρητός) ακέραιος $\leq |\mathbf{v}(\xi)|$. Συνεπώς, υπάρχει διαιρέτης η του ξ, όχι μονάδα, με $|\mathbf{v}(\eta)|$ ελάχιστο. Ο η είναι ανάγωγος, γιατί, σε αντίθετη περίπτωση, $\eta = \mu\nu$ με τους μ, ν ακεραίους, όχι μονάδες. Τότε όμως, από το (γ′), $|\mathbf{v}(\mu)|, |\mathbf{v}(\nu)| > 1$, άρα οι μ, ν είναι διαιρέτες του ξ με $|\mathbf{v}(\mu)|, |\mathbf{v}(\nu)| < |\mathbf{v}(\eta)|$, γεγονός που αντίκειται στην επιλογή του η.

Στη συνέχεια, θα δείξω ότι, κάθε ακέραιος ξ αναλύεται σε πεπερασμένο πλήθος αναγώγων παραγόντων. Πράγματι, αν ο ίδιος ο ξ είναι ανάγωγος, ο ισχυρισμός

ισχύει τετριμμένα. Αν ο ξ δεν είναι ανάγωγος, τότε έχει τουλάχιστον ένα ανάγωγο διαιρέτη η_1. Γράφουμε τότε

$$\xi = \eta_1 \xi_1 \ .$$

Λόγω του (γ'), $|\mathbf{v}(\eta_1)| > 1$, άρα, από τη σχέση $\mathbf{v}(\xi) = \mathbf{v}(\eta_1)\mathbf{v}(\xi_1)$, έπεται $|\mathbf{v}(\xi)| > |\mathbf{v}(\xi_1)|$. Αν ο ακέραιος ξ_1 είναι ανάγωγος, τότε η ζητούμενη ανάλυση του ξ σε ανάγωγους παράγοντες έχει ήδη επιτευχθεί. Διαφορετικά, ο ξ_1 έχει ένα ανάγωγο παράγοντα η_2, οπότε γράφουμε

$$\xi_1 = \eta_2 \xi_2 \ .$$

Όπως πριν, βλέπουμε ότι $|\mathbf{v}(\xi_1)| > |\mathbf{v}(\xi_2)|$. Αν ο ξ_2 είναι ανάγωγος, τότε $\xi = \eta_1\eta_2\xi_2$ είναι η ζητούμενη ανάλυση σε ανάγωγους παράγοντες, διαφορετικά, βρίσκουμε ένα ανάγωγο παράγοντα η_3 του ξ_2, κλπ. Επειδή

$$|\mathbf{v}(\xi)| > |\mathbf{v}(\xi_1)| > |\mathbf{v}(\xi_2)| > \dots$$

είναι φθίνουσα ακολουθία θετικών (ρητών) ακεραίων, η παραπάνω διαδικασία θα σταματήσει ύστερα από πεπερασμένο πλήθος βημάτων. Δηλαδή, υπάρχει κάποιος δείκτης n, έτσι ώστε

$$\xi_{n-1} = \eta_n \xi_n \ ,$$

όπου τώρα, όχι μόνο ο η_n, αλλά και ο ξ_n είναι ανάγωγος. Τότε,

$$\xi = \eta_1\xi_1 = \eta_1\eta_2\xi_2 = \eta_1\eta_2\cdots\eta_{n-1}\xi_{n-1} = \eta_1\eta_2\cdots\eta_n\xi_n \ ,$$

όπου όλοι οι παράγοντες του δεξιώτερου μέλους είναι ανάγωγοι.

Άρα, καταλήξαμε στο συμπέρασμα ότι κάθε ακέραιος του $\mathbb{K}$ αναλύεται σε ανάγωγους παράγοντες. Λόγω του (β'), συμπεραίνομε ότι κάθε ακέραιος του $\mathbb{K}$ αναλύεται σε *πρώτους* παράγοντες.

Θα δείξω τώρα τη μοναδικότητα αυτής της ανάλυσης, αν (1) παραβλέψω τη σειρά γραφής των πρώτων παραγόντων και (2) θεωρήσω συνεταιρικούς πρώτους παράγοντες ως, κατ' ουσίαν, όχι διαφορετικούς. Πράγματι, έστω ότι έχω δύο αναλύσεις του ξ :

$$\pi_1\pi_2\dots\pi_r = \xi = \rho_1\rho_2\dots\rho_s \tag{1.2}$$

Υποθέτω χωρίς βλάβη της γενικότητας $r \leq s$. Ο πρώτος π_1 διαιρεί το γινόμενο $\rho_1\rho_2\dots\rho_s$ οπότε διαιρεί τουλάχιστον ένα από τους $\rho_1, \rho_2, \dots, \rho_s$. Υποθέτω (αλλαζοντας την αρίθμηση των ρ_i, αν χρειαστεί) ότι $\pi_1|\rho_1$. Επειδή και ο ρ_1 είναι πρώτος έχω $\rho_1 = \epsilon_1\pi_1,\ \epsilon_1$ μονάδα και η (1.2) γίνεται

$$\pi_2\dots\pi_r = \epsilon_1\rho_2\dots\rho_s \ .$$

Επαναλαμβάνοντας το παραπάνω επιχείρημα για καθένα από τα $\pi_2, \dots, \pi_r$ θα καταλήξω στη σχέση

$$1 = \epsilon_1\epsilon_2\dots\epsilon_r\rho_{r+1}\rho_{r+2}\dots\rho_s \ ,$$

όπου οι παράγοντες $\rho_{r+1}, \ldots, \rho_s$ υπάρχουν μόνο αν $r > s$. Αυτή η περίπτωση αποκλείεται όμως, γιατί η παραπάνω σχέση δείχνει ότι καθένας από αυτούς τους παράγοντες ρ_j είναι διαιρέτης του 1, άρα είναι μονάδα του $\mathbb{K}$. Αυτό έρχεται σε αντίφαση με τον ορισμό του πρώτου. □

Ορισμός 1.2.3 *Όταν ένα σώμα $\mathbb{K}$ ικανοποιείτις συνθήκες (E_1) και (E_2) του θεωρήματος 1.2.2 χαρακτηρίζεται* **ευκλείδειο**.

Πρόταση 1.2.4 *Η στάθμη $\mathbf{N}$ είναι απεικόνιση του $\mathbb{K}$ στο $\mathbb{Q}$, που ικανοποιεί τη συνθήκη (E_1). Όσον αφορά στην (E_2), αυτή είναι ισοδύναμη με την*

- (E_3). *Αν $\delta \in \mathbb{K}$, τότε υπάρχει $\kappa \in \mathcal{O}$ έτσι ώστε $|\mathbf{N}(\delta - \kappa)| < 1$.*

Απόδειξη. Ο πρώτος ισχυρισμός προκύπτει αμέσως από τις Προτάσεις 1.1.7 και 1.1.8.

Υποθέτουμε τώρα ότι ισχύει η συνθήκη (E_3). Έστω $\gamma, \gamma_1 \in \mathcal{O}$ με $\gamma_1 \neq 0$. Για $\delta = \gamma/\gamma_1$, η (E_3) λέει ότι υπάρχει ακέραιος κ έτσι ώστε $|\mathbf{N}\left(\frac{\gamma}{\gamma_1} - \kappa\right)| < 1$. Θέτουμε $\gamma_2 = \gamma - \kappa\gamma_1$, οπότε, έχουμε διαδοχικά:

$$\begin{aligned} \gamma_2 &= \gamma_1 \left(\frac{\gamma}{\gamma_1} - \kappa\right) , \\ |\mathbf{N}(\gamma_2)| &= |\mathbf{N}(\gamma_1)| \, |\mathbf{N}\left(\frac{\gamma}{\gamma_1} - \kappa\right)| , \\ |\mathbf{N}(\gamma_2)| &< |\mathbf{N}(\gamma_1)| \cdot 1 = |\mathbf{N}(\gamma_1)| . \end{aligned}$$

Αντιστρόφως, υποθέτουμε ότι ισχύει η συνθήκη (E_2). Έστω $\delta \in \mathbb{K}$. Για κατάλληλο $\omega \in \mathbb{K}$, $\mathbb{K} = \mathbb{Q}(\omega)$. Για κατάλληλο $\nu \in \mathbb{Z}$, ο $\alpha = \nu\delta$ είναι ακέραιος [3]. Εφαρμόζουμε τη συνθήκη (E_2) για τα α, ν, οπότε, συμπεραίνουμε ότι υπάρχουν ακέραιοι κ, γ_2 έτσι ώστε

$$\alpha = \kappa\nu + \gamma_2 \;\text{ με }\; |\mathbf{N}(\gamma_2)| < |\mathbf{N}(\nu)| = \nu^2 ,$$

όπου, στην τελευταία ισότητα έγινε χρήση της Πρότασης 1.1.7 Ο ακέραιος κ ικανοποιεί τη συνθήκη (E_3). Πράγματι

$$\nu^2 > |\mathbf{N}(\gamma_2)| = |\mathbf{N}(\alpha - \kappa\nu)| = |\mathbf{N}(\nu\delta - \kappa\nu)| \; = |\mathbf{N}(\nu)\mathbf{N}(\delta - \kappa)| = \nu^2 |\mathbf{N}(\delta - \kappa)| ,$$

άρα $|\mathbf{N}(\delta - \kappa)| < 1$.

□

[3] Πράγματι, αν $g(\omega) = 0$, $g(x) \in \mathbb{Z}[x]$ και c είναι ο συντελεστής του μεγιστοβαθμίου όρου του $g(x)$, τότε, εύκολα βλέπει κανείς ότι $c\omega \in \mathcal{O}_{\mathbb{K}}$. Αν τώρα θέσουμε $\delta = \frac{a_0}{b_0} + \frac{a_1}{b_1}\omega + \frac{a_2}{b_2}\omega^2 + \ldots$ με τα $a_i, b_i \in \mathbb{Z}$, και b είναι το ΕΚΠ των b_i, τότε μπορούμε ως ν να πάρουμε το $c^{d-1}b$ όπου d ο βαθμός του $g(x)$.

Ο συνδυασμός των προτάσεων 1.2.2 και 1.2.4 μας δίνει μία χρήσιμη ικανή συνθήκη για να διαπιστώνουμε ότι σε ένα αριθμητικό σώμα $\mathbb{K}$ ισχύει η μονοσήμαντη ανάλυση. Εφαρμογή θα δούμε στο τέλος της Παραγράφου 1.4.

Για την επίλυση διοφαντικών εξισώσεων, συνήθως, καταφεύγουμε σε παραγοντοποίηση, στην οποία υπεισέρχονται ακέραιοι ενός αριθμητικού σώματος $\mathbb{K}$. Τότε, πολύ χρήσιμη αποδεικνύεται η εξής

Πρόταση 1.2.5 *Έστω ότι στους ακεραίους $\mathcal{O}$ ενός σώματος $\mathbb{K}$ ισχύει η μονοσήμαντη ανάλυση σε πρώτους παράγοντες. Αν ισχύει μια σχέση της μορφής $\alpha\beta = \gamma^n$, με $\alpha, \beta, \gamma \in \mathcal{O}$ και ΜΚΔ$(\alpha, \beta) = 1$, τότε $\alpha = \epsilon'\gamma'^n$ και $\beta = \epsilon''\gamma''^n$ όπου $\epsilon', \epsilon'' \in E(\mathbb{K})$, $\gamma', \gamma'' \in \mathcal{O}$ με ΜΚΔ$(\gamma', \gamma'') = 1$, $\epsilon'\epsilon'' = 1$ και $\gamma'\gamma'' = \gamma$.*

Απόδειξη. Έστω $\alpha = \alpha_1^{r_1}\alpha_2^{r_2}...\alpha_k^{r_k}$, $\beta = \beta_1^{s_1}\beta_2^{s_2}...\beta_m^{s_m}$, $\gamma = \gamma_1^{t_1}\gamma_2^{t_2}...\gamma_l^{t_l}$
οι αναλύσεις των α, β, γ σε πρώτους.
Επειδή οι α, β είναι πρώτοι μεταξύ τους, $\alpha_i \neq \beta_j \ \ \forall i = 1, 2, \ldots, k$,
$j = 1, 2, \ldots, m$. Η σχέση $\alpha\beta = \gamma^n$ δίνει :

$$\alpha_1^{r_1}\alpha_2^{r_2}...\alpha_k^{r_k}\beta_1^{s_1}\beta_2^{s_2}...\beta_m^{s_m} = \gamma_1^{nt_1}\gamma_2^{nt_2}...\gamma_l^{nt_l} \tag{1.3}$$

Λόγω της μονοσήμαντης ανάλυσης, $k + m = l$, ενώ οι πρώτοι που εμφανίζονται στις δύο αναλύσεις, είναι συνεταιρικοί. Αλλάζοντας τη σειρά των $\gamma_1, \gamma_2, \ldots, \gamma_l$, αν χρειαστεί, έχουμε:

$$\alpha_i^{r_i} = \epsilon_i\gamma_i^{nt_i} \ \ i = 1, 2, \ldots, k \ \text{ και } \ \beta_j^{s_j} = \epsilon_j\gamma_j^{nt_j} \ \ j = k+1, k+2, \ldots, k+m$$

$$\text{Άρα } \ \alpha = \epsilon_1\gamma_1^{nt_1}\epsilon_2\gamma_2^{nt_2}...\epsilon_k\gamma_k^{nt_k} \ \text{ και } \ \beta = \epsilon_{k+1}\gamma_{k+1}^{nt_{k+1}}\epsilon_{k+2}\gamma_{k+2}^{nt_{k+2}}...\epsilon_{k+m}\gamma_{k+m}^{nt_{k+m}}$$

$$\text{Δηλαδή } \ \alpha = \epsilon'(\gamma_1^{t_1}\gamma_2^{t_2}...\gamma_k^{t_k})^n \ \text{ και } \ \beta = \epsilon''(\gamma_{k+1}^{t_{k+1}}\gamma_{k+2}^{t_{k+2}}...\gamma_{k+m}^{t_{k+m}})^n.$$

Άρα $\alpha = \epsilon'\gamma'^n$, $\beta = \epsilon''\gamma''^n$ με $\gamma'\gamma'' = \gamma$ και $\epsilon'\epsilon'' = 1$ λόγω της σχέσης (1.3).

Η Πρόταση αυτή είναι απαραίτητο εργαλείο στις Παραγράφους 2.1 και 2.2.

Πρόταση 1.2.6 *Έστω ότι στους αλγεβρικούς ακεραίους ενός σώματος ισχύει η μονοσήμαντη ανάλυση σε πρώτους παράγοντες. Αν ισχύει μια σχέση της μορφής $\alpha\beta = \delta\gamma^n$ με $\alpha, \beta, \gamma, \delta \in \mathcal{O}$ και ΜΚΔ$(\alpha, \beta) = 1$ τότε $\alpha = \delta'\epsilon'\gamma'^m$ και $\beta = \delta''\epsilon''\gamma''^n$ όπου $\epsilon', \epsilon'' \in E(\mathbb{K}), \gamma', \gamma'' \in \mathcal{O}$, ΜΚΔ$(\delta'\gamma', \delta''\gamma'') = 1$ και $\epsilon'\epsilon'' = 1$, $\delta'\delta'' = \delta$, $\gamma'\gamma'' = \gamma$.*

Η απόδειξη είναι ανάλογη με αυτή της προηγούμενης πρότασης.

1.3 Όταν δεν ισχύει η μονοσήμαντη ανάλυση

Στην παράγραφο αυτή θα δούμε τι γίνεται στην περίπτωση που ο δακτύλιος των αλγεβρικών ακεραίων ενός σώματος, δεν είναι δακτύλιος μονοσήμαντης ανάλυσης. Αναγκαίο, είναι, να θυμηθούμε ορισμούς και να δούμε κάποιους νέους.

- Διαιρετότητα ιδεωδών. Εξ ορισμού $\mathfrak{b}|\mathfrak{a} \Leftrightarrow \mathfrak{b} \supseteq \mathfrak{a}$.
- ΜΚΔ ιδεωδών. Ορισμός ανάλογος του 1.1.12 όπου τα $\alpha, \beta, \delta, \delta'$ αντικαθίστανται από ιδεώδη του $\mathcal{O}_{\mathbb{K}}$.

Ορισμός 1.3.1 *Έστω $\mathfrak{a}$ ιδεώδες του $\mathcal{O}_{\mathbb{K}}$. Το $\mathfrak{a}$ λέγεται* **πρώτο**, *αν ισχύει η συνεπαγωγή :*

$$\alpha, \beta \in \mathcal{O}_{\mathbb{K}} \ \text{και} \ \alpha\beta \in \mathfrak{a} \ \Rightarrow \ \alpha \in \mathfrak{a} \ \text{ή} \ \beta \in \mathfrak{a}$$

Χαρακτηριστική ιδιότητα των πρώτων ιδεωδών, ανάλογη με αυτή των πρώτων αριθμών :

Αν $\mathfrak{p}$ πρώτο ιδεώδες, $\mathfrak{a}, \mathfrak{b}$ ιδεώδη και $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$ τότε $\mathfrak{p}|\mathfrak{a}$ ή $\mathfrak{p}|\mathfrak{b}$

Ορισμός 1.3.2 *Έστω $\mathfrak{a} \subseteq \mathbb{K}, \quad \mathfrak{a} \neq \langle 0 \rangle$. Το $\mathfrak{a}$ λέγεται* **κλασματικό ιδεώδες** *του $\mathbb{K}$, αν ικανοποιούνται όλες οι παρακάτω ιδιότητες*
(α΄) Αν $a_1, a_2 \in \mathfrak{a}$ τότε $a_1 - a_2 \in \mathfrak{a}$
(β΄) Αν $\lambda \in \mathcal{O}_{\mathbb{K}}$ και $a \in \mathfrak{a}$ τότε $\lambda a \in \mathfrak{a}$
(γ΄) Υπάρχει $\delta \in \mathcal{O}_{\mathbb{K}}, \delta \neq 0$ τέτοιο ώστε $\delta\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{K}}$

Για τα ιδεώδη του $\mathcal{O}_{\mathbb{K}}$ θα χρησιμοποιούμε τον όρο «ακέραια ιδεώδη». Προφανώς κάθε ακέραιο ιδεώδες είναι κλασματικό. Σ' αυτή την παράγραφο, όταν λέμε «ιδεώδες», εννοούμε «κλασματικό ιδεώδες», εν γένει.

Ορισμός 1.3.3 *Ένα ιδεώδες $\mathfrak{a}$ λέγεται* **κύριο** *αν $\mathfrak{a} = \alpha \cdot \mathcal{O}_{\mathbb{K}}$ για κάποιο $\alpha \in \mathbb{K}$.*

Συχνά χρησιμοποιούμε τον συμβολισμό $\langle\alpha\rangle$ αντί $\alpha \cdot \mathcal{O}_{\mathbb{K}}$. Επίσης, συχνά γράφουμε $\mathfrak{b}|\alpha$ και εννοούμε $\mathfrak{b}|\langle\alpha\rangle$.

Παρατήρηση. Έστω $a, b \in \mathbb{K}$. Τότε

$$\langle a\rangle = \langle b\rangle \ \Leftrightarrow \ \text{υπάρχει μονάδα} \ \epsilon \ \text{τέτοια ώστε} \ a = \epsilon \cdot b$$

Ορισμός 1.3.4 *Αν $\mathfrak{a}, \mathfrak{b}$ ιδεώδη, το γινόμενο $\mathfrak{a}\mathfrak{b}$ ορίζεται ως εξής :*

$$\mathfrak{a}\mathfrak{b} = \{\sum{}' a_i b_i, \quad a_i \in \mathfrak{a}, \ b_i \in \mathfrak{b}\}$$

όπου το $\sum'$ δηλώνει πεπερασμένο άθροισμα.

Αν $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ιδεώδη του $\mathbb{K}$, ισχύουν ακόμα τα εξής :

- Το $\mathfrak{a}\mathfrak{b}$ είναι ιδεώδες του $\mathbb{K}$.
- $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$
- $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$
- $\mathcal{O}_{\mathbb{K}} \cdot \mathfrak{a} = \mathfrak{a} \cdot \mathcal{O}_{\mathbb{K}} = \mathfrak{a}$ (δηλαδή $\mathcal{O}_{\mathbb{K}}$ μοναδιαίο ιδεώδες)

- Για κάθε ιδεώδες $\mathfrak{a}$ του $\mathbb{K}$ υπάρχει ιδεώδες $\mathfrak{a}'$ στο $\mathbb{K}$, (το αντίστροφο του $\mathfrak{a}$), τέτοιο ώστε $\mathfrak{a} \cdot \mathfrak{a}' = \mathfrak{a}' \cdot \mathfrak{a} = \mathcal{O}_{\mathbb{K}}$

Επομένως,

Πρόταση 1.3.5 *Το σύνολο των ιδεωδών του $\mathbb{K}$ αποτελεί αντιμεταθετική ομάδα, την οποία συμβολίζομε με $I_{\mathbb{K}}$. Το σύνολο των κυρίων ιδεωδών του $\mathbb{K}$,*

$$H_{\mathbb{K}} = \{a\mathcal{O}_{\mathbb{K}} : a \in \mathbb{K}^*\}$$

είναι κανονική υποομάδα της $I_{\mathbb{K}}$.

Ορισμός 1.3.6 *Ορίζουμε την ομάδα πηλίκο*

$$\mathcal{K} = I_{\mathbb{K}}/H_{\mathbb{K}}$$

η οποία λέγεται **ομάδα κλάσεων ιδεωδών**.

Θεώρημα 1.3.7 *Η ομάδα $\mathcal{K}$ είναι πεπερασμένη και η τάξη της, που συμβολίζεται με $h_{\mathcal{K}}$, λέγεται* **αριθμός κλάσεων ιδεωδών** *του $\mathcal{K}$.*

Θεώρημα 1.3.8 *Ο δακτύλιος $O_{\mathbb{K}}$ είναι δακτύλιος μονοσήμαντης ανάλυσης αν και μόνο αν $h_{\mathcal{K}} = 1$.*

Ακόμα και όταν ο δακτύλιος $\mathcal{O}_{\mathbb{K}}$ δεν είναι δακτύλιος μονοσήμαντης ανάλυσης, είναι **δακτύλιος του Dedekind**. Δηλαδή κάθε ιδεώδες αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών. Ειδικότερα στην περίπτωση των τετραγωνικών σωμάτων ισχύει το εξής :

Θεώρημα 1.3.9 *Θεωρούμε το τετραγωνικό σώμα $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, όπου d όχι τέλειο τετράγωνο. Αν D η διακρίνουσα του σώματος [4] , $\mathcal{O}_{\mathbb{K}}$ ο δακτύλιος των αλγεβρικών ακεραίων και p ρητός πρώτος τότε :*

- $\langle p \rangle = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ *αν και μόνο αν* $\left(\frac{D}{p}\right) = 1$
  όπου τα $\mathfrak{p}_1, \mathfrak{p}_2$ είναι πρώτα ιδεώδη του $\mathcal{O}_{\mathbb{K}}$ και $\mathfrak{a} \neq \mathfrak{b}$
- $\langle p \rangle = \mathfrak{p}^2$ *αν και μόνο αν* $\left(\frac{D}{p}\right) = 0$
  όπου το $\mathfrak{p}$ είναι πρώτο ιδεώδες του $\mathcal{O}_{\mathbb{K}}$
- $\langle p \rangle = \mathfrak{p}$ *αν και μόνο αν* $\left(\frac{D}{p}\right) = -1$
  όπου το $\mathfrak{p}$ είναι πρώτο ιδεώδες του $\mathcal{O}_{\mathbb{K}}$

[4] Η διακρίνουσα D του σώματος $\mathbb{Q}(\sqrt{d})$, είναι

$$D = \begin{cases} 4d & \text{αν } d \equiv 2,3 \pmod 4 \\ d & \text{αν } d \equiv 1 \pmod 4 \end{cases}$$

Το σύμβολο που εμφανίζεται στο προηγούμενο θεώρημα ονομάζεται **σύμβολο του Kronecker**, αποτελεί γενίκευση του συμβόλου Legendre και ορίζεται ως εξής
Αν $p \neq 2$ και $p \not| D$, ταυτίζεται με το σύμβολο Legendre
Αν $p|D$, $\left(\frac{D}{p}\right) = 0$
Αν $D \equiv 1 \pmod 4$, $\left(\frac{D}{p}\right) = \left(\frac{2}{D}\right)$ όπου το $\left(\frac{2}{D}\right)$είναι το σύμβολο του Jacobi.

Πρόταση 1.3.10 *Έστω $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ ιδεώδη του $\mathbb{K}$. Αν τα $\mathfrak{a}, \mathfrak{b}$ είναι πρώτα μεταξύ τους, η σχέση $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{d}\mathfrak{c}^n$ συνεπάγεται ότι $\mathfrak{a} = \mathfrak{d}_1 \cdot {\mathfrak{c}_1}^n$, $\mathfrak{b} = \mathfrak{d}_2 \cdot {\mathfrak{c}_2}^n$ όπου τα $\mathfrak{d}_1, \mathfrak{d}_2$ είναι πρώτα μεταξύ τους, τα $\mathfrak{c}_1, \mathfrak{c}_2$ είναι πρώτα μεταξύ τους, και $\mathfrak{d}_1 \cdot \mathfrak{d}_2 = \mathfrak{d}$, $\mathfrak{c}_1 \cdot \mathfrak{c}_2 = \mathfrak{c}$.*

Στην επίλυση των διοφαντικών εξισώσεων θα χρειαστούμε τα εξής λήμματα :

Λήμμα 1.3.11 *Αν $x, y \in \mathbb{Z}$ και $\mathfrak{a}$ ιδεώδες με $\mathfrak{a} \neq \mathcal{O}_{\mathbb{K}}$, $\mathfrak{a}|\langle x \rangle$ και $\mathfrak{a}|\langle y \rangle$, τότε οι x, y δεν είναι πρώτοι μεταξύ τους στο $\mathbb{Z}$.*

Λήμμα 1.3.12 *Έστω $\mathfrak{d}, \mathfrak{d}'$ ιδεώδη, τέτοια ώστε*

$$\mathfrak{d} = \langle m, a + b\omega \rangle, \quad \mathfrak{d}' = \langle m, a + b\omega' \rangle$$

όπου $m \in \mathbb{Z}$, $a + b\omega$ ακέραιος του $\mathbb{K}$ και $a + b\omega'$ ο συζυγής του. Αν $\mathfrak{d}| \ \langle x + y\omega \rangle$ τότε $\mathfrak{d}'| \ \langle x + y\omega' \rangle$ όπου $x + y\omega'$ το συζυγές του $x + y\omega$.

Απόδειξη. $\mathfrak{d}|\langle x + y\omega \rangle \ \Rightarrow \ x + y\omega \in \mathfrak{d} \ \Rightarrow$

$$x + y\omega = \nu \cdot m + \mu \cdot (a + b\omega), \quad \mu, \nu \in \mathcal{O}_{\mathbb{K}}$$

Παίρνω τη συζυγή της τελευταίας σχέσης :

$$x + y\omega' = \nu \cdot m + \mu \cdot (a + b\omega')$$

Δηλαδή $x + y\omega \in \mathfrak{d}'$ άρα $\mathfrak{d}'|\langle x + y - 2\omega y \rangle$. □

1.4 Αριθμητική σε τετραγωνικά σώματα

Εξειδικεύουμε τα συμπεράσματα του 1 στα τετραγωνικά σώματα.

Θεωρούμε το $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, όπου d όχι τέλειο τετράγωνο. Το ελάχιστο πολυώνυμο του d πάνω από το $\mathbb{Q}$ είναι το $f(x) = x^2 - d$. Επομένως μια βάση για την επέκταση $\mathbb{K}/\mathbb{Q}$ αποτελείται από τα $1, \sqrt{d}$.

Θεώρημα 1.4.1 *Έστω $d \in \mathbb{Z}$, $d \neq 1$ ελεύθερος τετραγώνου. Οι αλγεβρικοί ακέραιοι του $\mathbb{Q}(\sqrt{d})$ είναι το σύνολο $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ όπου $\omega = \sqrt{d}$, αν $d \equiv 2, 3 \pmod 4$ ή $\omega = (1 + \sqrt{d})/2$, αν $d \equiv 1 \pmod 4$.*

Απόδειξη. *Περίπτωση α΄* : $d \equiv 1 \pmod 4$.

Έστω $\lambda \in \mathbb{Z}[\omega]$. Τότε

$$\lambda = a + b(1+\sqrt{d})/2, \quad \text{για κάποια } a, b \in \mathbb{Z} ,$$

και έχω, διαδοχικά, τις σχέσεις

$$\begin{aligned} 2a + b + b\sqrt{d} &= 2\lambda , \\ (2\lambda - 2a - b)^2 &= b^2 d , \\ \lambda^2 + (-b-2a)\lambda + a^2 + ab + \frac{1-d}{4}b^2 &= 0 . \end{aligned}$$

Έπεται ότι το λ είναι αλγεβρικός ακέραιος, γιατί $d \equiv 1 \pmod 4$ οπότε το $(1-d)/4 \in \mathbb{Z}$. Θα δείξω ότι και κάθε αλγεβρικός ακέραιος του $\mathbb{Q}(\sqrt{d})$ ανήκει στο $\mathbb{Z}[\omega]$.

Έστω $\lambda \in \mathbb{Q}(\sqrt{d})$ αλγεβρικός ακέραιος. Τότε μπορώ να υποθέσω ότι είναι της μορφής

$$\lambda = \frac{a+b\sqrt{d}}{c} \quad \text{όπου} \quad a, b, c \in \mathbb{Z}, \quad c > 0, \text{και } \text{ΜΚΔ}(a,b,c) = 1$$

$$\lambda = \frac{a+b\sqrt{d}}{c} \Rightarrow (c\lambda - a)^2 = b^2 d$$

$$\Rightarrow \lambda^2 - 2\frac{a}{c}\lambda + \frac{a^2 - b^2 d}{c^2}$$

Επειδή λ αλγεβρικός ακέραιος έχω ότι $\dfrac{2a}{c}, \dfrac{a^2-b^2d}{c^2} \in \mathbb{Z}$ δηλαδή

$$c|2a \quad \text{και} \quad c^2 | a^2 - b^2 d$$

Έστω $D = \text{ΜΚΔ}(a,c)$. Τότε $D^2|c^2$ άρα $D^2|a^2 - b^2 d$. Και αφού $D^2|a^2$ έχω ότι $D^2|b^2 d$. Ισχυριζόμαστε ότι $D = 1$. Πράγματι, έστω p πρώτος διαιρέτης του D. Τότε $p^2|D^2$ αλλά και $D^2|b^2 d$ οπότε $p^2|b^2 d$. Ο d είναι ελεύθερος τετραγώνου άρα $p|b^2$ δηλαδή $p|b$. Άτοπο γιατί $\text{ΜΚΔ}(a,b,c) = 1$.

Επειδή $c|2a$ και $\text{ΜΚΔ}(c,a) = 1$ έχουμε ότι $c|2$ οπότε $c = 1$ ή $c = 2$.

Αν $c = 1$: $\lambda = a + b\sqrt{d}$ ενώ $\omega = (1+\sqrt{d})/2$ άρα $\lambda = a + b(2\omega - 1) = a' + b'\omega$ $a', b' \in \mathbb{Z}$. Δηλαδή $\lambda \in \mathbb{Z}[\omega]$.

Αν $c = 2$: Αν a άρτιος, $4|a^2$ και επειδή $4|a^2 - b^2 d$ έχω $4|b^2 d$. Αφού $\text{ΜΚΔ}(a,b,c) = 1$, ο b είναι περιττός. Έπεται ότι $4 \not| b^2$ και άρα $4|d$. Άτοπο γιατί d ελεύθερος τετραγώνου. Άρα a περιττός και $a^2 \equiv 1 \pmod 4$ όμως $a^2 - b^2 d \equiv 0 \pmod 4$ και παίρνω $b^2 \equiv 1 \pmod 4$ που σημαίνει b περιττός. Έτσι

$$\lambda = \frac{a+b\sqrt{d}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2} = a' + b\frac{1+\sqrt{d}}{2} \quad a', b \in \mathbb{Z}$$

Δηλαδή $\lambda \in \mathbb{Z}[\omega]$.

Περίπτωση β΄ : $d \equiv 2, 3 \pmod 4$.

Έστω $\lambda \in Z[\omega]$. Τότε $\lambda = a + b\sqrt{d} \Longrightarrow (\lambda - a)^2 = b^2 d \Rightarrow \lambda^2 - 2a\lambda + a^2 - b^2 d = 0$ οπότε λ αλγεβρικός ακέραιος.

Έστω $\lambda \in \mathbb{Q}(\sqrt{d})$, αλγεβρικός ακέραιος. Τότε

$$\lambda = \frac{a+b\sqrt{d}}{c} \text{ όπου } a,b,c \in \mathbb{Z}, \quad c>0, \text{ και ΜΚΔ}(a,b,c)=1.$$

Ομοίως με πριν καταλήγω στο ότι $c=1$ ή $c=2$.

Αν $c=1$ προφανώς $\lambda \in \mathbb{Z}[\omega]$.

Αν $c=2$: αν a άρτιος φτάνω σε άτοπο (όπως στην προηγούμενη περίπτωση). Αν a περιττός, $a^2 \equiv 1 \pmod 4$ όμως $4|(a^2-b^2d)$ άρα $a^2 \equiv b^2d \pmod 4$ και έχουμε $b^2d \equiv 1 \pmod 4$ (1). Τότε και ο b είναι περιττός αλλιώς a^2-b^2d περιττός και έτσι $4 \not| \ (a^2-b^2d)$. Άτοπο. Άρα $b^2 \equiv 1 \pmod 4$ (2). Από τις (1), (2) έχω ότι $d \equiv 1 \pmod 4$, άτοπο. □

Θεώρημα 1.4.2 *Έστω $d \in \mathbb{Z}$, $d \neq 1$ ελεύθερος τετραγώνου.*

- *Έστω $d<0$. Τότε, για την ομάδα $E(\mathbb{Q}(\sqrt{d}))$ των μονάδων του $\mathbb{Q}(\sqrt{d})$ ισχύει*

$$E(\mathbb{Q}(\sqrt{d})) = \begin{cases} \langle \sqrt{-1} \rangle & \text{αν } d=-1 \\ \langle \frac{1+\sqrt{-3}}{2} \rangle & \text{αν } d=-3 \\ \langle -1 \rangle & \text{αν } d<-4 \end{cases}$$

- *Έστω $d>1$ και ω όπως στην εκφώνηση του Θεωρήματος 1.4.1. Τότε,*

$$E(\mathbb{Q}(\sqrt{d})) = \langle -1, u+v\omega \rangle ,$$

όπου u,v θετικοί ακέραιοι, οι οποίοι ορίζονται ως εξής: Άν $d \equiv 2,3 \pmod 4$, τότε $|u^2-dv^2|=1$ και $u+v\sqrt{d}$ ελάχιστο. Άν $d \equiv 1 \pmod 4$, τότε $|u^2+uv+\frac{1-d}{4}v^2|=1$ και $u+v\sqrt{d}$ ελάχιστο.

Απόδειξη. Έστω $\epsilon \in \mathbb{Q}(\sqrt{d})$ ακέραιος. Το ϵ είναι μονάδα αν και μόνο αν $\mathbf{N}(\epsilon)=\pm 1$. Διακρίνουμε περιπτώσεις :

Αν $d \equiv 2,3 \pmod 4$, τότε $\epsilon = a+b\sqrt{d}$, $a,b \in \mathbb{Z}$. Έχουμε λοιπόν :
$\mathbf{N}(\epsilon)=\pm 1 \ \Rightarrow \ a^2-db^2=\pm 1 \ \overset{-d>0}{\Rightarrow} \ a^2-db^2=1$. Άρα
για $d=-1$, $a=0$ και $b=\pm 1$ ή $b=0$ και $a=\pm 1$, οπότε $E(\mathbb{Q}(\sqrt{-1}))=\langle \sqrt{-1} \rangle$
για $d \geq -2$, $a=\pm 1$ και $b=0$, οπότε $E(\mathbb{Q}(\sqrt{d}))=\{\pm 1\}$

Αν $d \equiv 1 \pmod 4$, τότε $\epsilon = a+b(1+\sqrt{d})/2$, $a,b \in \mathbb{Z}$. Άρα $\mathbf{N}(\epsilon)=\pm 1 \ \Rightarrow$ $(a+b/2)^2-d\cdot b^2/4=\pm 1 \ \overset{-d>0}{\Rightarrow} \ (a+b/2)^2-d\cdot b^2/4=1$. Άρα
για $d=-3$, $b=0$ και $a=\pm 1$ ή $a=0$ και $b=\pm 1$ ή $b=1$ και $a=-1$ ή $b=-1$ και $a=1$, οπότε $E(\mathbb{Q}(\sqrt{-3}))=\langle \frac{1+\sqrt{-3}}{2} \rangle$
για $d<-3$, $b=0$ και $a=\pm 1$, οπότε $E(\mathbb{Q}(\sqrt{d}))=\{\pm 1\}$

Έστω τώρα $d>1$. Από τη Θεωρία των πραγματικών Τετραγωνικών Σωμάτων είναι γνωστό ότι υπάρχει μία μονάδα $\epsilon = u+v\omega$, με $u,v>0$, η λεγόμενη **θεμελιώδης μονάδα** του τετραγωνικού σώματος, τέτοια ώστε, κάθε άλλη μονάδα του να είναι της μορφής $\pm\epsilon^\nu$, $\nu \in \mathbb{Z}$, δηλαδή να ανήκει στην ομάδα $\langle -1, \epsilon \rangle$.

Από την Πρόταση 1.1.10, $|\mathbf{N}(\epsilon)| = 1$, άρα

$$|u^2 - dv^2| = 1 \text{ στην περίπτωση } d \equiv 2, 3 \pmod 4 ,$$

$$|u^2 + uv + \frac{1-d}{4}| = 1 \text{ στην περίπτωση } d \equiv 1 \pmod 4 .$$

Μένει να δείξουμε ότι το ζεύγος (u, v) αποτελεί την ελάχιστη θετική λύση $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ της εξίσωσης $|x^2 - dy^2| = 1$ ή $|x^2 + xy + \frac{1-d}{4}y^2| = 1$, αντιστοίχως. Πράγματι, αν (x, y) είναι λύση της αντίστοιχης εξίσωσης, τότε $|\mathbf{N}(x + y\omega)| = 1$, άρα (Πρόταση 1.1.10) το στοιχείο $x + y\omega$ είναι μονάδα και, συνεπώς, σύμφωνα με τη προαναφερθείσα Θεωρία, έχουμε

$$x + y\omega = \pm\epsilon^\nu = \pm(u + v\omega)^\nu .$$

Αν, επιπλέον, υποτεθεί ότι $x, y > 0$, τότε φαίνεται εύκολα ότι, στο δεξιό μέλος της παραπάνω σχέσης ισχύει το θετικό πρόσημο και $\nu > 0$. Γράφοντας γενικά

$$(u + v\omega)^n = u_n + v_n\omega , \ n \in \mathbb{Z} ,$$

διαπιστώνουμε αμέσως τις αναδρομικές σχέσεις

$$u_{n+1} = uu_n + dvv_n \text{ και } v_{n+1} = uv_n + vu_n \text{ αν } d \equiv 2, 3 \pmod 4$$

$$u_{n+1} = uu_n + \frac{d-1}{4}vv_n \text{ και } v_{n+1} = uv_n + vu_n + vv_n \text{ αν } d \equiv 1 \pmod 4 ,$$

απ' όπου γίνεται φανερό, αναδρομικά, ότι $u_n > u$ και $v_n > v$ για κάθε $n > 1$. Σύμφωνα με ό,τι δείξαμε παραπάνω, όμως, $x + y\omega = u_\nu + v_\nu\omega$ με $\nu \geq 1$. Άρα, αν η λύση (x, y) δεν ταυτίζεται με την (u, v), τότε, κατ' ανάγκη, είναι μεγαλύτερη.

□

Θεώρημα 1.4.3 *Τα μιγαδικά τετραγωνικά σώματα* $\mathbb{Q}(\sqrt{d})$ $d = -1, -2, -3, -7, -11$ *είναι ευκλείδεια και συνεπώς, σε αυτά ισχύει η μονοσήμαντη ανάλυση. Δεν υπάρχουν άλλα ευκλείδεια μιγαδικά τετραγωνικά σώματα.*

Απόδειξη. Θεωρούμε το τετραγωνικό σώμα $\mathbb{Q}(\sqrt{d})$ για το οποίο ισχύουν οι προϋποθέσεις της πρότασης 1.2.4. Άρα ισχύει η μονοσήμαντη ανάλυση σε πρώτους παράγοντες, και η πρόταση (E_3) ως ισοδύναμη της (E_2).
Έστω $\delta = r + s\sqrt{d}$ $r, s \in \mathbb{Q}$ τυχαίο στοιχείο του $\mathbb{Q}(\sqrt{d})$. Λόγω της (E_3) υπάρχει ακέραιος κ έτσι ώστε $\mathbf{N}(\delta - \kappa) < 1$ [5].

Αν $d \equiv 2, 3 \pmod 4$, ο κ είναι της μορφής

$$\kappa = x + y\sqrt{d} \ x, y \in \mathbb{Z}$$

[5] Η συνάρτηση $\mathbf{N}$, στην περίπτωση των μιγαδικών τετραγωνικών σωμάτων παίρνει μη αρνητικές τιμές.

$$\begin{array}{c}\text{Άρα } \mathbf{N}(\delta-\kappa)=(r-x)^2-d(s-y)^2\\ \text{δηλαδή } (r-x)^2-d(s-y)^2<1\end{array} \tag{1.4}$$

Επιλέγω $r=s=1/2$. Τότε, οπωσδήποτε,

$$|x-r|=|x-1/2|\leq 1/2 \text{ και } |y-s|=|y-1/2|\leq 1/2$$

οπότε η σχέση (1.4) γίνεται $1/4+1/4(-d)<1$ από την οποία $-d<3$, άρα $d=-1,-2$.

Αν $d\equiv 1 \pmod 4$ ο κ είναι της μορφής

$$\kappa=x+y\frac{1+\sqrt{d}}{2}\ x,y\in\mathbb{Z}$$

Άρα,
$$1>\mathbf{N}(\delta-\kappa)=(r-x-\frac{y}{2})^2-d(s-\frac{y}{2})^2 \tag{1.5}$$

Επιλέγουμε $r=s=1/4$, οπότε

$$|r-x-\frac{y}{2}|=|\frac{1}{4}-x-\frac{y}{2}|\leq\frac{1}{4} \quad \text{και} \quad |s-\frac{y}{2}|=|\frac{1}{4}-\frac{y}{2}|\leq\frac{1}{4}$$

και από την (1.5) $1/16+1/16(-d)<1$. Ισχύει όμως και ότι $d\equiv 1 \pmod 4$ οπότε $d=-3,-7,-11$.

Αντιστρόφως, για κάθε μία από τις τιμές του d, που εμφανίζονται στην εκφώνηση, το αντίστοιχο σώμα $\mathbb{Q}(\sqrt{d})$ είναι ευκλείδειο (με $\mathbf{v}$ τη στάθμη $\mathbf{N}$), διότι ικανοποιείται η συνθήκη (E_3) της Πρότασης 1.2.4. Αυτό διαπιστώνεται ως εξής :

Αν $d\equiv 2,3 \pmod 4$ και $\delta=r+s\sqrt{d}$ τότε αρκεί να επιλέξω $\kappa=x+y\sqrt{d}$ με τους $x,y\in\mathbb{Z}$ τους πλησιέστερους ακέραιους των r,s αντιστοίχως.

Αν $d\equiv 1 \pmod 4$ και $\delta=r+s\sqrt{d}=r+is\sqrt{|d|}$, τότε επιλέγω το

$$\kappa=x+y\omega=x+\frac{y}{2}+iy\sqrt{|d|}$$

ώστε οι $x,y\in\mathbb{Z}$ να ικανοποιούν τις σχέσεις

$$|2s-y|\leq\frac{1}{2} \text{ και } |r-x-\frac{y}{2}|\leq\frac{1}{2}$$

Τότε, διαπιστώνεται εύκολα ότι

$$\mathbf{N}(\delta-\kappa)=(r-x-\frac{y}{2})^2+|d|(s-\frac{y}{2})^2$$

και από την επιλογή των x,y έπεται ότι

$$\mathbf{N}(\delta-\kappa)\leq\frac{1}{4}+|d|\frac{1}{16}\leq\frac{1}{4}+\frac{11}{16}=\frac{15}{16}<1$$

□

Αποτελεί ικανή συνθήκη, για να ισχύει η μονοσήμαντη ανάλυση σε κάποιο σώμα $\mathbb{K}$, το να είναι το $\mathbb{K}$ ευκλείδειο. Δεν είναι όμως και αναγκαία. Έτσι εκτός

από τα $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$ τα οποία βρήκα προηγουμένως, η μονοσήμαντη ανάλυση ισχύει και σε άλλα τετραγωνικά μιγαδικά σώματα. Αυτά είναι τα $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$. Σχετικά πρόσφατα αποδείχθηκε ότι εκτός από τα παραπάνω εννέα μιγαδικά τετραγωνικά σώματα δεν υπάρχουν άλλα (μιγαδικά τετραγωνικά), στα οποία να ισχύει η μονοσήμαντη ανάλυση.(A.Baker, 1966 και H.M.Stark, 1967). Όσον αφορά στα πραγματικά τετραγωνικά σώματα ισχύει το :

Θεώρημα 1.4.4 *Τα πραγματικά τετραγωνικά σώματα* $\mathbb{Q}(\sqrt{d})$ $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$ *είναι ευκλείδεια και συνεπώς σε αυτά ισχύει η μονοσήμαντη ανάλυση. Δεν υπάρχουν άλλα ευκλείδεια πραγματικά τετραγωνικά σώματα.*

Η απόδειξη του θεωρήματος είναι πολύ δύσκολη ($Chatland$ και $Davenport$, 1950).

Κεφάλαιο 2

Επίλυση Διοφαντικών Εξισώσεων

2.1 Η εξίσωση $\xi^3 + \eta^3 + \zeta^3 = 0$

Δουλεύουμε στο σώμα $\mathbb{Q}(\sqrt{-3})$ όπου σύμφωνα με το θεώρημα 1.4.3 ισχύει η μονοσήμαντη ανάλυση.

- Θέτουμε $\rho = (-1 + \sqrt{-3})/2$ και $\lambda = 1 - \rho$. Τότε $\mathbf{N}(\lambda) = 3$ οπότε ο λ είναι πρώτος λόγω του θεωρήματος 1.1.16.

- Σύμφωνα με το θεώρημα 1.4.2, οι μονάδες του $\mathbb{Q}(\sqrt{-3})$ είναι οι $\{\pm 1, \pm\rho, \pm\rho^2\}$.

- Ο λ είναι συνεταιρικός με τον $\sqrt{-3}$ αφού $\lambda = \rho^2\sqrt{-3}$.

- Η ανάλυση του 3 σε πρώτους παράγοντες είναι $3 = -\rho^2 \cdot \lambda^2$.

Λήμμα 2.1.1 *Οι ακέραιοι του σώματος είναι ισοδύναμοι* $\bmod \lambda$ *με έναν από τους* $0, 1$ *και* -1.

Απόδειξη. Αν $a \in \mathbb{Z}$ τότε $a \equiv 0, 1, -1 \pmod 3$. Έχουμε έτσι διαδοχικά τις σχέσεις :

$$\begin{gathered} a \equiv j \pmod 3, \quad j = 0, 1, -1 \\ 3|a - j \quad j = 0, 1, -1 \text{ στο } \mathbb{Z} \\ 3|a - j \quad j = 0, 1, -1 \text{ στο } \mathbb{Q}(\sqrt{-3}) \\ \text{Άρα } \lambda|a - j \text{ δηλαδή } a \equiv j \pmod \lambda \end{gathered}$$

Αν $\alpha = a + b\rho \;\; a, b \in \mathbb{Z}$ ακέραιος στο $\mathbb{Q}(\sqrt{-3})$ τότε :

$$\alpha = a + b\rho = a + b(1 - \lambda) = a + b - b\lambda \equiv a + b \pmod \lambda$$

Επειδή όμως $a + b \equiv j \pmod \lambda$ όπου $j = 0, 1, -1$ έχουμε ότι $\alpha \equiv 0, 1, -1 \pmod \lambda$.

Λήμμα 2.1.2 *Αν α ακέραιος στο $\mathbb{Q}(\sqrt{-3})$ που δεν διαιρετός δια λ, τότε $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$.*

Απόδειξη. Αφού ο α δεν είναι διαιρετός δια λ, $\alpha \equiv \pm 1 \pmod{\lambda}$. Άρα $\alpha \mp 1 = \lambda\beta$ όπου β ακέραιος. Έτσι

$$\begin{aligned}
\alpha^3 &= \beta^3\lambda^3 \pm 3\beta^2\lambda^2 + 3\beta\lambda \pm 1 \Rightarrow \\
\alpha^3 &= \beta^3\lambda^3 \mp \lambda^2\rho^2\beta^2\lambda^2 - \lambda^2\rho^2\beta\lambda \pm 1 \Rightarrow \\
\alpha^3 &= \beta^3\lambda^3 \mp \rho^2\beta^2\lambda^4 - \rho^2\beta\lambda^3 \pm 1 \Rightarrow \\
\alpha^3 \mp 1 &= \lambda^3(\beta^3 - \rho^2\beta) \mp \rho^2\beta^2\lambda^4 \Rightarrow \\
\alpha^3 \mp 1 &\equiv \lambda^3(\beta^3 - \rho^2\beta) \pmod{\lambda^4} \Rightarrow \\
\alpha^3 \pm 1 &\equiv \lambda^3(\beta^3 - (1 - 2\lambda + \lambda^2)\beta) \pmod{\lambda^4} \Rightarrow \\
\alpha^3 \pm 1 &\equiv \lambda^3\beta^3 - \lambda^3\beta + 2\lambda^4\beta - \lambda^5\beta \pmod{\lambda^4} \Rightarrow \\
\alpha^3 \pm 1 &\equiv \lambda^3(\beta^3 - \beta) \pmod{\lambda^4} \qquad (2.1)
\end{aligned}$$

Για το β έχω $\beta \equiv 0, 1, -1 \pmod{\lambda}$ και έτσι $\beta^3 \equiv \beta \pmod{\lambda}$. Δηλαδή η διαφορά $\beta^3 - \beta$ είναι πάντοτε διαιρετή δια λ οπότε η σχέση (2.1) γίνεται $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$.

Θεώρημα 2.1.3 *Η εξίσωση $\xi^3 + \eta^3 + \zeta^3 = 0$ δεν έχει μη τετριμμένες, ακέραιες λύσεις.*

Απόδειξη. Υποθέτουμε ότι υπάρχουν ακέραιοι ξ, η, ζ $\xi\eta\zeta \neq 0$, τέτοιοι ώστε

$$\xi^3 + \eta^3 + \zeta^3 = 0 \qquad (2.2)$$

Αν κάποιος πρώτος π διαιρεί δύο από τους ξ, η, ζ τότε θα διαιρεί και τον τρίτο. Επομένως μπορούμε να υποθέσουμε ότι οι ακέραιοι ξ, η, ζ είναι πρώτοι ανά δύο. Αν κανένας από τους ξ, η, ζ δεν είναι διαιρετός δια $\lambda = 1 - \rho$, από το λήμμα 2.1.2, ισχύει η σχέση $\pm 1 \pm 1 \pm 1 \equiv 0 \pmod{\lambda^4}$
Αυτό όμως είναι αδύνατο να συμβεί. Έτσι, τουλάχιστον ένας από τους ξ, η, ζ - έστω ο ζ - είναι διαιρετός δια λ. Επειδή οι ξ, η, ζ είναι πρώτοι ανά δύο, ο λ δεν διαιρεί τους ξ, η. Θέτουμε $\zeta = \lambda^n\gamma$ $n \geq 1$ και γ ακέραιος, μη διαιρετός δια λ.
Η εξίσωση (2.2) γίνεται $\xi^3 + \eta^3 + \lambda^{3n}\gamma^3 = 0$. Θεωρούμε όμως την πιο γενική εξίσωση

$$\xi^3 + \eta^3 + \epsilon\lambda^{3n}\gamma^3 = 0 \qquad (2.3)$$

όπου ϵ μονάδα του $\mathbb{Q}(\sqrt{-3})$ και $\xi, \eta, \gamma, \lambda$ ακέραιοι πρώτοι ανά δύο.
Θα δείξουμε ότι αυτή δεν έχει μη τετριμμένη λύση. Αν είχε θα επιλέγαμε κάποια με ελάχιστο δυνατό n. Λόγω του λήμματος 2.1.2 η σχέση (2.3) δίνει

$$\pm 1 \pm 1 \pm \epsilon\lambda^{3n} \equiv 0 \pmod{\lambda^4}$$

όπου τα τρία πρόσημα είναι ανεξάρτητα.
Οι περιπτώσεις $\pm 2 \pm \epsilon\lambda^{3n} \equiv 0 \pmod{\lambda^4}$ αποκλείονται διότι συνεπάγονται τη σχέση $\lambda | 2$ άρα $\mathbf{N}(\lambda) | \mathbf{N}(2)$ δηλαδή $3|4$, άτοπο. Άρα, για να ισχύει η τελευταία σχέση,

πρέπει $\lambda^{3n}\equiv 0 \pmod{\lambda^4}$ δηλαδή $n\geq 2$.
Οι ακέραιοι $\alpha_1=\xi+\eta,\ \alpha_2=\xi+\rho\eta,\ \alpha_3=\xi+\rho^2\eta$ είναι ισοδύναμοι $\bmod\lambda$. [1]
Τα $1,\rho,\rho^2$ είναι ρίζες της εξίσωσης $x^3-1=0$. Έτσι στη σχέση
$x^3-1=(x-1)(x-\rho)(x-\rho^2)$ η αντικατάσταση $x\leftarrow\frac{-\xi}{\eta}$ δίνει : $\xi^3+\eta^3=\alpha_1\alpha_2\alpha_3$ και λόγω της (2.3), $\epsilon\lambda^{3n}\gamma^3=-\alpha_1\alpha_2\alpha_3$
Δηλαδή ο λ διαιρεί το γινόμενο $\alpha_1\alpha_2\alpha_3$ και επειδή είναι πρώτος, διαιρεί τουλάχιστον ένα από τους $\alpha_1,\alpha_2,\alpha_3$. Οι $\alpha_1,\ \alpha_2,\ \alpha_3$ όμως, είναι ισοδύναμοι $\bmod\lambda$ άρα $\alpha_1\equiv\alpha_2\equiv\alpha_3\equiv 0 \pmod{\lambda}$.
Οι ακέραιοι $\beta_1=\alpha_1/\lambda,\beta_2=\alpha_2/\lambda,\beta_3=\alpha_3/\lambda$ είναι πρώτοι ανά δύο [2]. Έτσι $\xi^3+\eta^3=\lambda^3\beta_1\beta_2\beta_3$ οπότε από τη σχέση (2.3), $\beta_1\beta_2\beta_3+\epsilon\lambda^{3(n-1)}\gamma^3=0$. Δηλαδή ο λ^{3n-3} διαιρεί το $\beta_1\beta_2\beta_3$ και επειδή οι β_1,β_2,β_3 είναι πρώτοι ανά δύο, ένας ακριβώς από αυτούς διαιρείται από το λ^{3n-3}.
Υποθέτουμε ότι αυτός είναι ο β_1, διότι η εξίσωση (2.3) δεν αλλάζει αν το η αντικατασταθεί από τον $\eta\rho$ ή $\eta\rho^2$. Λόγω της πρότασης 1.2.5 θα έχουμε :

$$\beta_1=\epsilon_1\lambda^{3n-3}\zeta_1^3,\ \beta_2=\epsilon_2\eta_1^3,\ \beta_3=\epsilon_3\xi_1^3$$

όπου $\epsilon_1,\epsilon_2,\epsilon_3$ μονάδες του $\mathbb{Q}(\sqrt{-3})$ και ζ_1,η_1,ξ_1 ακέραιοι πρώτοι ανά δύο, μη διαιρετοί δια λ. Ισχύει

$$\rho^2\beta_3+\rho\beta_2+\beta_1=0 \tag{2.4}$$

διότι,

$$(-1-\rho)\frac{\alpha_3}{\lambda}+\rho\frac{\alpha_2}{\lambda}+\frac{\alpha_1}{\lambda}=$$
$$\frac{1}{\lambda}((-1-\rho)(\xi+\rho^2\eta)+\rho(\xi+\rho\eta)+\xi+\eta)=0$$

Αντικαθιστώντας τις παραπάνω τιμές των β_1,β_2,β_3 στη σχέση (2.4) έχουμε :

$$\rho^2\epsilon_3\xi_1^3+\rho\epsilon_2\eta_1^3+\epsilon_1\lambda^{3n-3}\zeta_1^3=0$$

δηλαδή,

$$\xi_1^3+\epsilon_4\eta_1^3+\epsilon_5\lambda^{3n-3}\zeta_1^3=0 \tag{2.5}$$

Επειδή $n\geq 2$ και κανένας από τους ξ_1,η_1 δεν είναι διαιρετός δια λ, λόγω του λήμματος 2.1.2 έχουμε $\pm1\pm\epsilon_4\equiv 0 \pmod{\lambda^3}$. Έτσι $\epsilon_4=\pm1$ και η εξίσωση (2.5) γίνεται

$$\xi_1^3+(\pm\eta_1)^3+\epsilon_5\lambda^{3(n-1)}\zeta_1^3=0$$

Η τελευταία εξίσωση είναι της ίδιας μορφής με τη (2.3) και έχει λύση, αφού έχει και η (2.3). Όμως ο εκθέτης του λ είναι μικρότερος απ¨ ότι στη (2.3). Αντίφαση με την υπόθεση.

---

[1] $\alpha_1\equiv\xi+\eta \pmod{\lambda}$, $\alpha_2=\xi+(1-\lambda)\eta\equiv\xi+\eta \pmod{\lambda}$ και $\alpha_3=\xi+(1-\lambda)^2\eta\equiv\xi+\eta \pmod{\lambda}$

[2] Αν οι β_1,β_2 διαιρούνται από τον ίδιο πρώτο π, τότε οι $\beta_1-\beta_2=\eta$, $\lambda\beta_1-\beta_1+\beta_2=\xi$ θα διαιρούνται από τον π. Άτοπο γιατί είναι πρώτοι μεταξύ τους. Ομοίως δείχνουμε ότι οι β_1,β_3 και β_2,β_3 είναι πρώτοι μεταξύ τους.

2.2 Η εξίσωση $x^2 + 7 = 2^n$ των Ramanujan - Nagell

Σε αυτή την παράγραφο θα αποδείξουμε το

Θεώρημα 2.2.1 *Η εξίσωση $x^2 + 7 = 2^n$ έχει ακέραιες λύσεις $(\pm x, n)$ τις*

$$(1, 3),\ (3, 4),\ (5, 5),\ (11, 7),\ (181, 15)$$

και μόνο αυτές.

Θα εργαστούμε στο σώμα $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, όπου, σύμφωνα με το θεώρημα 1.4.3 ισχύει η μονοσήμαντη ανάλυση.

- Δακτύλιος των ακεραίων του $\mathbb{K}$ είναι ο
$$\mathcal{O}_{\mathbb{K}} = \{a + b\omega,\ \ a, b \in \mathbb{Z}\} \text{ όπου } \omega = \frac{1 + \sqrt{-7}}{2}$$
- Το συζυγές του ω είναι το $\omega' = \dfrac{1 - \sqrt{-7}}{2}$
- Από το θεώρημα 1.4.2 ξέρουμε ότι οι μονάδες του σώματος είναι οι $\{\pm 1\}$
- Στάθμη του τυπικού στοιχείου $a + b\omega \in \mathbb{Q}(\sqrt{-7})$,
$$\mathbf{N}(a + b\omega) = a^2 + ab + 2b^2$$
- Η ανάλυση του 2 σε πρώτους είναι
$$2 = \left(\frac{1 + \sqrt{-7}}{2}\right)\left(\frac{1 - \sqrt{-7}}{2}\right)$$

  Πράγματι, έστω $2 = (a + b\omega)(c + d\omega)$. Τότε $\mathbf{N}(2) = \mathbf{N}(a + b\omega)\mathbf{N}(c + d\omega)$ Άρα $a^2 + ab + 2b^2 = 2$ και $c^2 + cd + 2d^2 = 2$ Έτσι έχουμε $b = 1, a = -1$ ή $b = 1, a = 0$ ή $b = -1, a = 0$ ή $b = -1, a = 1$ και $c = -1, d = 1$ ή $c = 0, d = 1$ ή $c = 1, d = -1$ ή $c = 0, d = -1$. Επιλέγω εκείνα τα ζεύγη $(a, b), (c, d)$ που ικανοποιούν την $2 = (a+b\omega)(c+d\omega)$, δηλαδή $(a, b) = (0, 1)$ και $(c, d) = (1, -1)$. Τα $(1 + \sqrt{-7})/2, (1 - \sqrt{-7})/2$ είναι πρώτοι, σύμφωνα με την πρόταση 1.1.16, διότι η στάθμη τους είναι πρώτος.

Απόδειξη θεωρήματος. Έστω x, n ακέραιοι, έτσι ώστε

$$x^2 + 7 = 2^n \tag{2.6}$$

Προφανώς ο x είναι περιττός, και υποθέτουμε ότι είναι θετικός.
Αν ο n είναι άρτιος, ισχύει η σχέση :

$$(2^{n/2} - x)(2^{n/2} + x) = 7$$

από την οποία

$$2^{n/2}-x=1 \text{ και } 2^{n/2}+x=7$$

Προσθέτοντας κατά μέλη, έχουμε : $2\cdot 2^{n/2}=8$. Άρα $n=4$ και $x=3$.

Αν ο n είναι περιττός, προφανώς $n>1$. Για $n=3$, έχουμε $x=1$. Υποθέτουμε $n>3$.
Ο x είναι περιττός, οπότε $x=2k+1 \Rightarrow x^2+7=4k^2+4k+8$. Ο x^2+7 είναι διαιρετός δια 4, οπότε θέτοντας $m=n-2$ η εξίσωση (2.6) γράφεται :

$$\frac{x^2+7}{4}=2^m \text{ δηλαδή}$$

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)=\left(\frac{1+\sqrt{-7}}{2}\right)^m\left(\frac{1-\sqrt{-7}}{2}\right)^m$$

Το δεξιό μέλος της τελευταίας ισότητας είναι μια παραγοντοποιήση σε πρώτους. Οι πρώτοι $(1+\sqrt{-7})/2, (1-\sqrt{-7})/2$ δεν γίνεται να διαιρούν ταυτόχρονα τους $(x+\sqrt{-7})/2, (x-\sqrt{-7})/2$ [3] οπότε οι τελευταίοι είναι πρώτοι μεταξύ τους. Έτσι, σύμφωνα με την πρόταση 1.2.5

$$\frac{x+\sqrt{-7}}{2}=\pm\left(\frac{1+\sqrt{-7}}{2}\right)^m \text{ και } \frac{x-\sqrt{-7}}{2}=\pm\left(\frac{1-\sqrt{-7}}{2}\right)^m$$

ή $$\frac{x+\sqrt{-7}}{2}=\pm\left(\frac{1-\sqrt{-7}}{2}\right)^m \text{ και } \frac{x-\sqrt{-7}}{2}=\pm\left(\frac{1+\sqrt{-7}}{2}\right)^m$$

Σε όλες τις περιπτώσεις, αφαιρώντας κατά μέλη παίρνουμε :

$$\pm\sqrt{-7}=\left(\frac{1+\sqrt{-7}}{2}\right)^m-\left(\frac{1-\sqrt{-7}}{2}\right)^m$$

Όμως το θετικό πρόσημο δεν γίνεται να εμφανίζεται. Πράγματι, θέτουμε $(1+\sqrt{-7})/2=a,\ (1-\sqrt{-7})/2=b$. Προφανώς, $a\cdot b=2$ ενώ η σχέση

$$\sqrt{-7}=\left(\frac{1+\sqrt{-7}}{2}\right)^m-\left(\frac{1-\sqrt{-7}}{2}\right)^m \text{ συνεπάγεται } a^m-b^m=a-b$$

Έτσι, $a^2=(1-b)^2=1-2b+b^2=1-ab^2+b^2\equiv 1 \pmod{b^2}$. Τότε, επειδή ο m είναι περιττός, $a^m=a\cdot a^{m-1}=a\cdot(a^2)^{\frac{m-1}{2}}\equiv a \pmod{b^2}$. Άρα $a^m-b^m\equiv a \pmod{b^2}$. Άτοπο γιατί $a^m-b^m=a-b$.

Άρα $-\sqrt{-7}=\left(\frac{1+\sqrt{-7}}{2}\right)^m-\left(\frac{1-\sqrt{-7}}{2}\right)^m$ και έχουμε :

$$-\sqrt{-7}=\frac{1}{2^m}((1+\sqrt{-7})^m-(1-\sqrt{-7})^m) \Leftrightarrow$$

[3] Αν ο $(1+\sqrt{-7})/2$ διαιρεί τους $(x+\sqrt{-7})/2, (x-\sqrt{-7})/2$, θα διαιρεί και τη διαφορά τους : $(1+\sqrt{-7})/2|\sqrt{-7} \Rightarrow \mathbf{N}((1+\sqrt{-7})/2)|\mathbf{N}(\sqrt{-7}) \Rightarrow 2|7$, άτοπο

$$-2^{m-1} = \binom{m}{1} + \binom{m}{3}(\sqrt{-7})^2 + ... + \binom{m}{m}(\sqrt{-7})^{m-1} \Leftrightarrow$$
$$-2^{m-1} = \binom{m}{1} - \binom{m}{3}7 + ... + \binom{m}{2k+1}(-7)^k + ... + \binom{m}{m}(-7)^{\frac{m-1}{2}}$$
$$\text{άρα } 2^{m-1} + m \equiv 0 \pmod 7 \tag{2.7}$$

Το $m \in \mathbb{Z}$ έχει περίοδο 7 mod 7 και το 2^{m-1} έχει περίοδο 3 mod 7. Το άθροισμά τους έχει περίοδο ίση με το ΕΚΠ$[3,7] = 21$. Επομένως οι λύσεις της (2.7)είναι

$$m \equiv 3 \pmod{21} \text{ ή } m \equiv 5 \pmod{21} \text{ ή } m \equiv 13 \pmod{21}$$

Επειδή ο m είναι περιττός [4], έχω τελικά ότι

$$m \equiv 3 \pmod{42} \text{ ή } m \equiv 5 \pmod{42} \text{ ή } m \equiv 13 \pmod{42}$$

Οι τιμές $m = 3, 5, 13$ δίνουν αποδεκτές λύσεις. Θα δείξουμε ότι είναι αδύνατον να υπάρξει λύση $m \equiv 13 \pmod{42}$, $m \neq 13$.
Έστω m λύση της (2.6) με $m \equiv 13 \pmod{42}$, $m \neq 13$. Έστω ακόμα

$$ord_7(m-13) = l$$

Επειδή $2^{6\cdot 7^l} \equiv 1 \pmod{7^{l+1}}$ [5] έχουμε $2^{m-13} \equiv 1 \pmod{7^{l+1}}$ και άρα

$$2^{m-1} \equiv 2^{12} \pmod{7^{l+1}} \tag{2.8}$$

Λόγω του λήμματος 2.2.2 ισχύει

$$\binom{m}{k}7^{\frac{k-3}{2}} \equiv \binom{13}{k}7^{\frac{k-3}{2}} \pmod{7^l} \quad k = 3,5,7,9,11,13$$

$$\text{Άρα } \binom{m}{k}7^{\frac{k-1}{2}} \equiv \binom{13}{k}7^{\frac{k-1}{2}} \pmod{7^{l+1}} \quad k = 3,5,7,9,11,13 \tag{2.9}$$

Επειδή

$$-2^{m-1} = \binom{m}{1} - \binom{m}{3}7 + ... + \binom{m}{2k+1}(-7)^k + ... + \binom{m}{m}(-7)^{\frac{m-1}{2}}$$

έχουμε

$$2^{m-1} + \binom{m}{1} - \binom{m}{3}7 + ... + \binom{m}{2k+1}(-7)^k + ... + \binom{m}{m}(-7)^{\frac{m-1}{2}} \equiv 0 \pmod{7^{l+1}}$$

[4] $m \equiv 3 \pmod{21} \Rightarrow m-3 = 21\cdot k$, $k \in \mathbb{Z}$. Ο $m-3$ είναι άρτιος, άρα $m-3 = 2\cdot l\cdot 21$, $l \in \mathbb{Z} \Rightarrow m \equiv 3 \pmod{42}$. Ομοίως τα υπόλοιπα.

[5] ΜΚΔ$(2,7) = 1$ άρα ΜΚΔ$(2,7^{l+1}) = 1$ και έτσι $2^{6\cdot 7^{l+1}} \equiv 1 \pmod{7^{l+1}}$

Όμως $\binom{m}{2k+1}7^k = \frac{m(m-1)...(m-13)...(m-2k+1)}{(2k+1)!}7^k \equiv 0 \pmod{7^{l+1}}$

για $2k+1>13$ διότι $ord_7(2k+1)! < k$ [6] Έτσι η τελευταία σχέση γίνεται

$$2^{m-1} + \binom{m}{1} - \binom{m}{3}7 + ... + \binom{m}{13}7^6 \equiv 0 \pmod{7^{l+1}}$$

οπότε λόγω των σχέσεων (2.8), (2.9)

$$2^{12} + m - \binom{13}{3}7 + ... + \binom{13}{13}7^6 \equiv 0 \pmod{7^{l+1}}$$

Επομένως $m-13 \equiv 0 \pmod{7^{l+1}}$, άτοπο γιατί $ord_7(m-13)=l$.

Ομοίως δείχνουμε ότι δεν γίνεται να έχουμε λύση m της (2.6), $m \equiv 3 \pmod{42}$, $m \neq 3$, ούτε λύση $m \equiv 5 \pmod{42}$, $m \neq 5$. (Η απόδειξη είναι πολύ ευκολότερη από άποψη υπολογισμών)
Οι τιμές $m=3,5,13$ μας δίνουν τις λύσεις $(x,n)=(x,m+2)=(5,5),(11,7),(181,15)$ της αρχικής εξίσωσης.

□

Χρησιμοποιήσαμε το

Λήμμα 2.2.2 *Έστω ότι οι M,N,m,a,ν είναι ακέραιοι και $m \equiv a \pmod{N}$. Υποθέτουμε ότι για κάθε πρώτο διαιρέτη p του N ισχύει $ord_p(\nu!) \leq ord_p(M)$. Τότε*

$$\binom{m}{\nu}M \equiv \binom{a}{\nu}M \pmod{N}$$

Απόδειξη. Έστω $d=$ΜΚΔ$(\nu!,N)$. Τότε $\nu! = k\cdot d$ όπου ΜΚΔ$(k,N)=1$.

$$\binom{m}{\nu}M = \frac{m(m-1)\dots(m-\nu+1)}{\nu!}M = \frac{m(m-1)\dots(m-\nu+1)}{k}\cdot\frac{M}{d}$$

Λόγω, όμως, της σχέσης $m \equiv a \pmod{N}$ έχουμε

$$m(m-1)\dots(m-\nu+1) \equiv a(a-1)\dots(a-\nu+1) \pmod{N} \Rightarrow$$

$$\frac{1}{k}m(m-1)\dots(m-\nu+1) \equiv \frac{1}{k}a(a-1)\dots(a-\nu+1) \pmod{N} \Rightarrow$$

[6] Πράγματι $ord_7(2k+1)! = \left[\frac{2k+1}{7}\right]+\left[\frac{2k+1}{7^2}\right]+\left[\frac{2k+1}{7^3}\right]+... < \frac{2k+1}{7}+\frac{2k+1}{7^2}+\frac{2k+1}{7^3}+... = \frac{2k+1}{6} < k$ αφού $\frac{2k+1}{6} < k \Leftrightarrow 4k-1>0 \Leftrightarrow k>1$ το οποίο ισχύει

$$\frac{1}{k}m(m-1)\dots(m-\nu+1)\frac{M}{d} \equiv \frac{1}{k}a(a-1)\dots(a-\nu+1)\frac{M}{d} \pmod{N} \Rightarrow$$

$$\binom{m}{\nu}M \equiv \binom{a}{\nu}M \pmod{N}$$

□

2.3 Η εξίσωση $X^2 - 17Y^2 = Z^3$

Θεωρούμε το τετραγωνικό σώμα $\mathbb{K} = \mathbb{Q}(\sqrt{17})$ όπου σύμφωνα με το θεώρημα 1.4.4 ισχύει η μονοσήμαντη ανάλυση.

- Ο δακτύλιος των ακεραίων του σώματος είναι
$$\mathcal{O}_{\mathbb{K}} = \{a + b\omega \; a, b \in \mathbb{Z}\} \text{ όπου } \omega = \frac{1+\sqrt{17}}{2}$$
- Ελάχιστο πολυώνυμο του ω
$$x^2 - x - 4$$
- Το συζυγές του ω είναι το
$$\omega' = \frac{1-\sqrt{17}}{2}$$
- Στάθμη του τυπικού στοιχείου $a + b\omega \in \mathbb{K}$ είναι
$$\mathbf{N}(a + b\omega) = a^2 + ab - 4b^2$$
- Θεμελιώδης μονάδα
$$\epsilon = 5 - 2\omega, \;\; \mathbf{N}(5 - 2\omega) = -1$$
- Η ανάλυση του 2 σε πρώτους είναι
$$2 = (-2 + \omega)(1 + \omega)$$
Πράγματι, οι $-2 + \omega, \;\; 1 + \omega$ είναι πρώτοι γιατί η στάθμη τους είναι πρώτος.
- Το συζυγές του $-2 + \omega$ είναι το
$$-2 + \frac{1-\sqrt{17}}{2} = -1 - \omega$$

Εύρεση όλων των ακεραίων λύσεων της εξίσωσης

$$x^2 - 17y^2 = z^3 \text{ με ΜΚΔ}(x, 17y) = 1 \tag{2.10}$$

Έστω x, y, z ακέραιοι, τέτοιοι ώστε να ικανοποιούν την εξίσωση (2.10). Τότε :

$$(x - \sqrt{17}y)(x + \sqrt{17}y) = z^3 \tag{2.11}$$

$$\text{Αν } d = \text{ΜΚΔ}(x - \sqrt{17}y, x + \sqrt{17}y), \quad \text{τότε}$$

$$d|2 \cdot \text{ΜΚΔ}(x, \sqrt{17}y) \tag{2.12}$$

Οι x, y είναι πρώτοι μεταξύ τους στο $\mathbb{Q}(\sqrt{17})$ [7], και επομένως οι $x, \sqrt{17}y$ είναι πρώτοι μεταξύ τους στο ίδιο σώμα [8]. Επομένως η σχέση (2.12) συνεπάγεται ότι $d|2$.

Έστω $d = -2 + \omega$. Τότε $x + \sqrt{17}y = (-2 + \omega)(a + b\omega)$ $a, b \in \mathbb{Z}$.
Παίρνοντας συζυγή έχουμε ότι $x - \sqrt{17}y = -(1 + \omega)(a + b\omega')$. Άρα ο $(x - \sqrt{17}y)$ εκτός από τον πρώτο $-2 + \omega$, διαιρείται επίσης, και από τον πρώτο $1 + \omega$, οπότε $(-2 + \omega)(1 + \omega) = 2|x - \sqrt{17}y$. Ομοίως $2|x + \sqrt{17}y$ που αντίκειται στην υπόθεση $d = -2 + \omega$.

Ομοίως αποκλείουμε τη περίπτωση $d = 1 + \omega$, και μας μένουν οι περιπτώσεις $d = 1$ ή $d = 2$.

Αν $d = 1$, λόγω της πρότασης 1.2.5, η σχέση (2.11) μας δίνει

$$(x + \sqrt{17}y) = (m + n\omega)^3(5 - 2\omega)^k, \quad \text{άρα}$$

$$(x - y + 2y\omega) = (m + n\omega)^3(5 - 2\omega)^k$$

Αν $k \equiv 0 \pmod 3$, τότε $(x - y + 2y\omega) = (m + n\omega)^3$, άρα

$$x = -\frac{13}{2}n^3 + \frac{27}{2}n^2m - \frac{3}{2}nm^2 + m^3$$

$$y = -\frac{5}{2}n^3 + \frac{3}{2}n^2m - \frac{3}{2}nm^2$$

$$z = m^2 - mn - 4n^2$$

Επειδή οι x, y είναι ακέραιοι πρώτοι μεταξύ τους, πρέπει $\text{ΜΚΔ}(m, 2n) = 1$. Ακόμα $\text{ΜΚΔ}(x, 17) = 1$ οπότε πρέπει $-13n^3 + 27n^2m - 3nm^2 + 2m^3 \not\equiv 0 \pmod{17}$ απ'

[7] Αν κάποιος πρώτος π του $\mathbb{Q}(\sqrt{17})$ διαιρεί τους x, y τότε : $\mathbf{N}(\pi)|\mathbf{N}(x)$ και $\mathbf{N}(\pi)|\mathbf{N}(y)$. Δηλαδή $\mathbf{N}(\pi)|x^2$ και $\mathbf{N}(\pi)|y^2$. Όμως $\mathbf{N}(\pi) \neq 1$, οπότε υπάρχει ρητός πρώτος που διαιρεί τους x, y. Άτοπο γιατί οι x, y είναι πρώτοι μεταξύ τους στο $\mathbb{Z}$.

[8] Σύμφωνα με τη πρόταση 1.1.16, ο $\sqrt{17}$ είναι πρώτος στο $\mathbb{Q}(\sqrt{17})$, διότι η στάθμη του είναι πρώτος. Αφού οι x, y είναι πρώτοι μεταξύ τους, κανένας από τους πρώτους που εμφανίζονται στην κανονική ανάλυση του x, δεν εμφανίζεται στην κανονική ανάλυση του y. Αν οι $x, \sqrt{17}y$ δεν είναι πρώτοι μεταξύ τους στο $\mathbb{Q}(\sqrt{17})$, τότε ο $\sqrt{17}$ εμφανίζεται στην κανονική ανάλυση του x. Άρα $\sqrt{17}|x$ δηλαδή $x = \sqrt{17} \cdot (a + b\omega)$. Παίρνοντας συζυγή έχουμε ότι $x = -\sqrt{17} \cdot (a + b\omega')$.
Από τις δύο τελευταίες σχέσεις παίρνουμε ότι $17|x^2$ δηλαδή $17|x$. Άτοπο γιατί οι $x, 17y$ είναι πρώτοι μεταξύ τους στο $\mathbb{Z}$.

όπου $n \not\equiv 2m \pmod{17}$.

Αν $k \equiv 1 \pmod 3$, τότε $(x - y + 2y\omega) = (m + n\omega)^3(5 - 2\omega)$, άρα

$$x = -\frac{33}{2}n^3 + \frac{57}{2}n^2m - \frac{39}{2}nm^2 + 4m^3$$
$$y = \frac{7}{2}n^3 - \frac{15}{2}n^2m + \frac{9}{2}nm^2 - m^3$$
$$z = 4n^2 - nm - m^2$$

ΜΚΔ$(m, 2n) = 1$, $n \not\equiv 2m \pmod{17}$

Αν $k \equiv 2 \pmod 3$, τότε $(x - y + 2y\omega) = (m + n\omega)^3(5 - 2\omega)^2$, άρα

$$x = -\frac{251}{2}n^3 + \frac{483}{2}n^2m - \frac{309}{2}nm^2 + 33m^3$$
$$y = \frac{61}{2}n^3 - \frac{117}{2}n^2m + \frac{75}{2}nm^2 - 8m^3$$
$$z = -4n^2 + nm + m^2$$

ΜΚΔ$(m, 2n) = 1$, $n \not\equiv -2m \pmod{17}$

Αν $d = 2 : x - \sqrt{17}y \equiv x - y \pmod 2$ και $x + \sqrt{17}y \equiv x + y \pmod 2$, διότι $\sqrt{17} = 2\omega + 1$. Άρα οι x, y είναι περιττοί [9] .
Επειδή $2|x - \sqrt{17}y,\ x + \sqrt{17}y$, η σχέση (2.11) μας δίνει ότι $2|z$ και γράφεται ως εξής διαδοχικά :

$$\begin{aligned}(x - \sqrt{17}y)(x + \sqrt{17}y) &= 2^3{z_1}^3 \\ \frac{x - \sqrt{17}y}{2} \cdot \frac{x + \sqrt{17}y}{2} &= 2{z_1}^3 \\ \left(\frac{x + y}{2} - \omega y\right)\left(\frac{x - y}{2} + \omega y\right) &= 2{z_1}^3\end{aligned}$$

Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $x + y \equiv 2 \pmod 4$, οπότε $x - y \equiv 0 \pmod 4$.

$\omega \equiv -1 \pmod{1+\omega}$ και $y, \frac{x+y}{2} \equiv 1 \pmod 2$ άρα $y, \frac{x+y}{2} \equiv 1 \pmod{1+\omega}$

Έτσι $\frac{x+y}{2} - \omega y \equiv 1 - (-1) \cdot 1 = 2 \equiv 0 \pmod{1+\omega}$.

Συνεπώς, $\frac{x+y}{2} - \omega y = (1 + \omega)(m + n\omega)^3(5 - 2\omega)^k$

όπου, όπως και στην προηγούμενη περίπτωση, αρκεί να θεωρήσουμε τις τιμές $k = 0, 1, 2$. Για κάθε μια από αυτές τις τιμές, βρίσκουμε οικογένεια λύσεων συναρτήσει των παραμέτρων m, n.

[9] $2|x - y, 2|x + y$ και $(x, y) = 1$

2.4 Η εξίσωση $X^2+5=2Y^3$

Δουλεύουμε στο σώμα $\mathbb{K}=\mathbb{Q}(\sqrt{-5})$.

- Ο δακτύλιος των ακεραίων του σώματος είναι
$$\mathcal{O}_{\mathbb{K}}=\{a+b\sqrt{-5},\ \ a,b\in\mathbb{Z}\}$$
- Από το θεώρημα 1.4.2 γνωρίζουμε ότι μονάδες του σώματος είναι οι $\{\pm 1\}$.
- Ο αριθμός κλάσεων ιδεωδών είναι 2. Αυτό διαπιστώνεται από πίνακες ή με τη βοήθεια του υπολογιστικού πακέτου Pari.
- Η ανάλυση του $\langle 2\rangle$, σύμφωνα με το θεώρημα 1.3.9 είναι
$$\langle 2\rangle=\mathfrak{p}_1{}^2,\ \ \text{όπου}\ \ \mathfrak{p}_1\ \ \text{είναι πρώτο ιδεώδες, όχι κύριο}$$

Θεώρημα 2.4.1 *Η εξίσωση $x^2+5=2y^3$ έχει λύσεις (x,y) τις $(-7,3),(7,3)$.*

Απόδειξη. Έστω x,y έτσι ώστε να ικανοποιούν τη

$$x^2+5=2y^3 \tag{2.13}$$

Προφανώς ο x είναι περιττός, ενώ η σχέση (2.13) γράφεται :

$$\begin{gathered}(x-\sqrt{-5})(x+\sqrt{-5})=2y^3\ \ \text{οπότε}\\ \langle x-\sqrt{-5}\rangle\langle x+\sqrt{-5}\rangle=\langle 2\rangle\langle y\rangle^3\end{gathered} \tag{2.14}$$

Έστω $\mathfrak{p}$ πρώτο ιδεώδες, κοινός διαιρέτης των $\langle x-\sqrt{-5}\rangle,\langle x+\sqrt{-5}\rangle$.

$$\begin{aligned}\mathfrak{p}|\ \langle x-\sqrt{-5}\rangle\ &\Rightarrow\ \langle x-\sqrt{-5}\rangle\subseteq\mathfrak{p}\ \Rightarrow\ x-\sqrt{-5}\in\mathfrak{p}\\ \mathfrak{p}|\ \langle x+\sqrt{-5}\rangle\ &\Rightarrow\ \langle x+\sqrt{-5}\rangle\subseteq\mathfrak{p}\ \Rightarrow\ x+\sqrt{-5}\in\mathfrak{p}\end{aligned}$$

Άρα $2x\in\mathfrak{p}\ \Rightarrow\ \langle 2x\rangle\subseteq\mathfrak{p}\ \Rightarrow\ \mathfrak{p}|\ \langle 2x\rangle$.
Αν $\mathfrak{p}\not|\langle 2\rangle$ τότε [10] $\mathfrak{p}|\ \langle x\rangle$, και λόγω της (2.14) $\mathfrak{p}|\ \langle y\rangle^3$ δηλαδή $\mathfrak{p}|\ \langle y\rangle$. Έτσι από το λήμμα 1.3.11 έχουμε ότι οι x,y δεν είναι πρώτοι μεταξύ τους στο $\mathbb{Z}$. Άτοπο.
Άρα κάθε πρώτος διαιρέτης $\mathfrak{p}$, των $\langle x-\sqrt{-5}\rangle,\langle x+\sqrt{-5}\rangle$ διαιρεί το $\langle 2\rangle$.

$$\begin{gathered}\langle 2\rangle|\ \langle x-\sqrt{-5}\rangle\langle x+\sqrt{-5}\rangle\ \ \text{και}\ \ \mathfrak{p}_1|\ \langle 2\rangle\ \ \text{άρα}\\ \mathfrak{p}_1|\ \langle x-\sqrt{-5}\rangle\ \ \text{ή}\ \ \mathfrak{p}_1|\ \langle x+\sqrt{-5}\rangle\end{gathered}$$

Στην πραγματικότητα, αν το $\mathfrak{p}_1$ διαιρεί κάποιο από τα $\langle x-\sqrt{-5}\rangle$, $\langle x+\sqrt{-5}\rangle$ θα διαιρεί και το άλλο. [11] Άρα

$$\text{ΜΚΔ}(\langle x-\sqrt{-5}\rangle,\langle x+\sqrt{-5}\rangle)=\mathfrak{p}_1$$

[10] Επειδή το $\mathfrak{p}$ είναι πρώτο ιδεώδες.
[11] Αν π.χ. $\mathfrak{p}_1|\langle x+\sqrt{-5}\rangle$ τότε $\langle x+\sqrt{-5}\rangle\subseteq\mathfrak{p}_1\ \Rightarrow\ x+\sqrt{-5}\in\mathfrak{p}_1$ Όμως $\mathfrak{p}_1|\ \langle 2\rangle$ άρα $\langle 2\rangle\subseteq\mathfrak{p}_1\ \Rightarrow\ 2\sqrt{-5}\in\mathfrak{p}_1$. Άρα $x-\sqrt{-5}\in\mathfrak{p}_1\ \Rightarrow\ \langle x-\sqrt{-5}\rangle\subseteq\mathfrak{p}_1\ \Rightarrow\ \mathfrak{p}_1|\ \langle x-\sqrt{-5}\rangle$.

και από τη σχέση (2.13) παίρνω διαδοχικά

$$\langle x-\sqrt{-5}\rangle\langle x+\sqrt{-5}\rangle = \mathfrak{p}_1{}^2\langle y\rangle^3$$
$$\frac{\langle x+\sqrt{-5}\rangle}{\mathfrak{p}_1}\cdot\frac{\langle x-\sqrt{-5}\rangle}{\mathfrak{p}_1} = \langle y\rangle^3$$

Έτσι, λόγω της Πρότασης 1.3.10

$$\frac{\langle x+\sqrt{-5}\rangle}{\mathfrak{p}_1} = \mathfrak{a}^3 \;\Rightarrow\; \langle x+\sqrt{-5}\rangle = \mathfrak{p}_1\mathfrak{a}^3$$

Ο αριθμός κλάσεων ιδεωδών είναι 2. Μεταφέροντας λοιπόν την τελευταία σχέση σε κλάσεις ισοδυναμίας έχουμε

$$\mathbf{1} = [\mathfrak{p}_1][\mathfrak{a}]^3 \overset{[\mathfrak{a}]^2=1}{\Rightarrow} \quad \mathbf{1} = [\mathfrak{p}_1][\mathfrak{a}] \;\Rightarrow\; [\mathfrak{p}_1\mathfrak{a}] = \mathbf{1}$$

Άρα το $\mathfrak{p}_1\mathfrak{a}$ είναι κύριο ιδεώδες, δηλαδή $\mathfrak{p}_1\mathfrak{a} = \langle m+n\sqrt{-5}\rangle$. Έχουμε λοιπόν διαδοχικά

$$\begin{aligned}
\langle x+\sqrt{-5}\rangle &= \mathfrak{p}_1\mathfrak{a}^3,\\
\mathfrak{p}_1{}^2\langle x+\sqrt{-5}\rangle &= (\mathfrak{p}_1\mathfrak{a})^3,\\
\langle 2\rangle\langle x+\sqrt{-5}\rangle &= \langle m+n\sqrt{-5}\rangle^3,\\
2(x+\sqrt{-5}) &= \pm(m+n\sqrt{-5})^3,\\
2(x+\sqrt{-5}) &= (m+n\sqrt{-5})^3
\end{aligned}$$

$$\text{Άρα } x=\frac{m^3-15m^2n^2}{2} \text{ και } 2=n(3m^2-5n^2)$$

Οπότε $n=-1$ και $m=\pm1$ και παίρνουμε τις λύσεις $(x,y)=(\pm7,3)$.

2.5 Η εξίσωση $X^2-145Y^2=-111Z^6$

Εργαζόμαστε στο σώμα $\mathbb{K}=\mathbb{Q}(\sqrt{145})=\mathbb{Q}(\omega)$, όπου

$$\omega=\frac{1+\sqrt{145}}{2}\,.$$

- Ελάχιστο πολυώνυμο του ω
$$x^2-x-36$$
- Δεύτερος συζυγής του ω
$$\omega'=1-\omega=\frac{1-\sqrt{145}}{2}$$

- Δακτύλιος των ακεραίων του $\mathbb{K}$

$$\mathcal{O}_{\mathbb{K}} = \{a + b\omega, \quad a, b \in \mathbb{Z}\}$$

- Στάθμη του τυπικού στοιχείου $a + b\omega \in \mathbb{K}$

$$\mathbf{N}(a + b\omega) = a^2 + ab - 36b^2$$

- Θεμελιώδης μονάδα του σώματος $\mathbb{K}$

$$\epsilon = 11 + 2\omega, \quad \mathbf{N}(\epsilon) = -1$$

- Ομάδα κλάσεων ιδεωδών του $\mathbb{K}$

$$\langle g \rangle \cong \mathbb{Z}_4 \ , \quad \text{όπου } g \text{ είναι το ιδεώδες } \langle 2, 1 + \omega \rangle$$

Την τελευταία πληροφορία σχετικά με την ομάδα κλάσεων ιδεωδών μας πήραμε μέσω του αριθμοθεωρητικού πακέτου PARI, ακολουθώντας την εξής διαδικασία :

$$\begin{aligned} f &= x^2 - x - 36 \\ bnf &= \texttt{bnfinit}(f) \\ bnfcls &= \texttt{bnfclassunit}(f) \\ g &= bnfcls[5,][1][3][1] \end{aligned}$$

$$\texttt{idealtwoelt}(bnf, g)$$

Στο δεξιό μέλος της εξίσωσής μας εμφανίζεται ο αριθμός $111 = 3 \cdot 37$, οπότε είναι απαραίτητο να γνωρίζουμε την ανάλυση των $3, 37$ σε ιδεώδη του $\mathbb{K}$. Επίσης, όπως θα δούμε παρακάτω, θα μας χρειασθεί και η ανάλυση του 2. Με την εντολή

$$\texttt{idealprimedec}(bnf, p)$$

όπου p ρητός πρώτος, το PARI επιτυγχάνει την ανάλυση του p σε πρώτα ιδεώδη του $\mathbb{K}$. Έτσι, βρήκαμε

$$\langle 2 \rangle = \mathfrak{p}_2\mathfrak{p}_2' \ , \ \mathfrak{p}_2 = \langle 2, 1 + \omega \rangle = g \ , \ \mathfrak{p}_2' = \langle 2, 2 + \omega \rangle = \langle 2, 1 + \omega' \rangle$$

$$\langle 3 \rangle = \mathfrak{p}_3\mathfrak{p}_3' \ , \ \mathfrak{p}_3 = \langle 3, 2 + \omega \rangle \ , \ \mathfrak{p}_3' = \langle 3, 3 + \omega \rangle = \langle 3, 2 + \omega' \rangle$$

$$\langle 37 \rangle = \mathfrak{p}_{37}\mathfrak{p}_{37}' \ , \ \mathfrak{p}_{37} = \langle 37, 10 + \omega \rangle \ , \ \mathfrak{p}_{37}' = \langle 37, -11 + \omega \rangle = \langle 37, 10 + \omega' \rangle$$

Παρατήρηση. Οι δεξιώτερες ισότητες σε κάθε μία από τις τρεις τελευταίες γραμμές, σε συνδυασμό με το Λήμμα 1.3.12 συνεπάγονται ότι, αν $\mathfrak{p} \in \{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_{37}\}$ και $\mathfrak{p} | \langle a + b\omega \rangle$, τότε $\mathfrak{p}' | \langle a + b\omega' \rangle$.

Θα μας χρειασθεί, επίσης, να ξέρουμε σε ποιά κλάση ιδεωδών ανήκει καθένα από τα παραπάνω ιδεώδη. Η εντολή του PARI

$$\texttt{bnfisprincipal}(bnf, g)$$

όπου $\mathfrak{p}$ είναι ένα οποιοδήποτε από τα παραπάνω ιδεώδη, μας δίνει τις εξής σχέσεις:

$$\begin{aligned}
\mathfrak{p}_2' &= \langle \frac{1}{2} + \frac{1}{8}\omega \rangle \mathfrak{p}_2^3 \\
\mathfrak{p}_3 &= \langle -\frac{1}{2} + \frac{1}{8}\omega \rangle \mathfrak{p}_2^3 \\
\mathfrak{p}_3' &= \langle -3 + \frac{1}{2}\omega \rangle \mathfrak{p}_2 \\
\mathfrak{p}_{37} &= \langle 5 + \frac{1}{2}\omega \rangle \mathfrak{p}_2 \\
\mathfrak{p}_{37}' &= \langle \frac{1}{2} + \frac{3}{8}\omega \rangle \mathfrak{p}_2^3
\end{aligned}$$

Επίλυση της διοφαντικής εξίσωσης

$$x^2 - 145y^2 = -111z^6 \ , \ x, y, z \in \mathbb{Z}, \text{ΜΚΔ}(x, 145y) = 1 \ . \tag{2.15}$$

Η σχέση (2.15) δίνει $(x - \sqrt{145}y)(x + \sqrt{145}y) = -3 \cdot 37z^6$. Περνούμε σε ιδεώδη:

$$\langle x - \sqrt{145}y \rangle \langle x + \sqrt{145}y \rangle = \langle 3 \rangle \langle 37 \rangle \langle z \rangle^6 \ .$$

Λόγω των αναλύσεων των ιδεωδών, που παράγονται από τα 3 και 37, η τελευταία γίνεται

$$\langle x - \sqrt{145}y \rangle \langle x + \sqrt{145}y \rangle = \langle x - y + 2y\omega \rangle \langle x + y - 2y\omega \rangle = \mathfrak{p}_3 \mathfrak{p}_3' \mathfrak{p}_{37} \mathfrak{p}_{37}' \langle z \rangle^6 \tag{2.16}$$

Θέλουμε τώρα να ανακαλύψουμε τους πιθανούς κοινούς διαιρέτες $\mathfrak{d}$ των παραγόντων του αριστερού μέλους. Έστω $\mathfrak{d}$ κοινός διαιρέτης των $\langle x - \sqrt{145}y \rangle, \langle x + \sqrt{145}y \rangle$. Έχουμε, διαδοχικά,

$$\begin{gathered}
\langle x - \sqrt{145}y \rangle, \langle x + \sqrt{145}y \rangle \subseteq \mathfrak{d} \ , \\
x - \sqrt{145}y \ , \ x + \sqrt{145}y \in \mathfrak{d} \ , \\
2x \in \mathfrak{d} \ \text{ και } \ 2\sqrt{145}y \in \mathfrak{d} \ , \\
\langle 2x \rangle \subseteq \mathfrak{d} \ \text{ και } \ \langle 2\sqrt{145}y \rangle \subseteq \mathfrak{d} \ , \\
\mathfrak{d} | \ \langle 2 \rangle \langle x \rangle \ \text{ και } \ \mathfrak{d} | \ \langle 2 \rangle \langle \sqrt{145} \rangle \ .
\end{gathered}$$

Επειδή τα $\mathfrak{d}, \langle x \rangle$ είναι πρώτα μεταξύ τους [12], $\mathfrak{d} | \langle 2 \rangle$. Άρα,

> Αν ο $\mathfrak{d}$ είναι ο ΜΚΔ των $\langle x - \sqrt{145}y \rangle$ και $\langle x + \sqrt{145}y \rangle$, τότε $\mathfrak{d} \in \{\mathcal{O}, \mathfrak{p}_2, \mathfrak{p}_2', \langle 2 \rangle\}$.

[12] Έστω ότι υπήρχε μη τετριμμένος κοινός διαιρέτης $\mathfrak{b}$ των $\mathfrak{d}, \langle x \rangle$. Επειδή $\mathfrak{d} | \langle x + \sqrt{145}y \rangle$ και $\mathfrak{b} | \mathfrak{d}$, έπεται ότι $\mathfrak{b} | \langle x + \sqrt{145}y \rangle$. Εξ υποθέσεως, $\mathfrak{b} | \ \langle x \rangle$, άρα $\mathfrak{b} | \langle \sqrt{145}y \rangle$, οπότε λόγω του λήμματος 1.3.11 οι $x, 145y$ δεν θα ήταν πρώτοι μεταξύ τους, άτοπο.

Αν από τους x, y **ο ένας είναι άρτιος και ο άλλος περιττός**, τότε, αναγκαστικά, $\mathfrak{d} = \mathcal{O}$ [13] οπότε από τη σχέση (2.16), λόγω και του λήμματος 1.3.12, συμπεραίνουμε ότι ισχύει μία από τις περιπτώσεις

$$\langle x - y + 2y\omega \rangle = \mathfrak{p}_3\mathfrak{p}_{37} \text{ ή } \mathfrak{p}_3\mathfrak{p}'_{37} \text{ ή } \mathfrak{p}'_3\mathfrak{p}_{37} \text{ ή } \mathfrak{p}'_3\mathfrak{p}'_{37} \, .$$

Παρατηρούμε τώρα ότι η αλλαγή προσήμου στο y, η οποία δεν αλλάζει ουσιαστικά τις λύσεις της αρχικής εξίσωσης, μετατρέπει το $\langle x - y + 2y\omega \rangle$ στο $\langle x + y - 2y\omega \rangle = \langle x - y + 2y\omega' \rangle$. Αν αυτό συνδυαστεί με το Λήμμα 1.3.12, βγαίνει το συμπέρασμα ότι, στις παραπάνω διαζευκτικές περιπτώσεις, μπορούμε να θεωρήσουμε, χωρίς βλάβη της γενικότητας, μόνο εκείνες στις οποίες εμφανίζεται το $\mathfrak{p}_3$. Έτσι,

$$\langle x - y + 2\omega y \rangle = \mathfrak{p}_3\mathfrak{p}_{37}\mathfrak{a}^6 \tag{2.17}$$
$$\langle x - y + 2\omega y \rangle = \mathfrak{p}_3\mathfrak{p}'_{37}\mathfrak{a}^6 \tag{2.18}$$

για κάποιο ακέραιο ιδεώδες $\mathfrak{a}$.

Αν οι x, y **είναι και οι δύο περιττοί**, ο z είναι άρτιος, έστω$z = 2z_1$ και η σχέση (2.16) γίνεται

$$\langle \frac{x-y}{2} + \omega y \rangle \langle \frac{x+y}{2} - \omega y \rangle = \mathfrak{p}_3\mathfrak{p}'_3\mathfrak{p}_{37}\mathfrak{p}'_{37}\mathfrak{p}_2^4{\mathfrak{p}'_2}^4 \langle z_1 \rangle^6 \tag{2.19}$$

Οι παράγοντες στο αριστερό μέλος είναι πρώτοι μεταξύ τους [14] Κατ' αναλογίαν με πρίν, μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι αριστερώτερος παράγων διαιρείται από το $\mathfrak{p}_2$. Έτσι η σχέση (2.19) συνεπάγεται μία από τις παρακάτω σχέσεις

$$\langle \frac{x-y}{2} + \omega y \rangle = \mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}_{37}\mathfrak{a}^6 \tag{2.20}$$
$$\langle \frac{x-y}{2} + \omega y \rangle = \mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}'_{37}\mathfrak{a}^6 \tag{2.21}$$
$$\langle \frac{x-y}{2} + \omega y \rangle = \mathfrak{p}_2^4\mathfrak{p}'_3\mathfrak{p}_{37}\mathfrak{a}^6 \tag{2.22}$$
$$\langle \frac{x-y}{2} + \omega y \rangle = \mathfrak{p}_2^4\mathfrak{p}'_3\mathfrak{p}'_{37}\mathfrak{a}^6 \tag{2.23}$$

για κάποιο ακέραιο ιδεώδες $\mathfrak{a}$.

Προχωρούμε τώρα σε επίλυση κάθε μιας από τις εξισώσεις ιδεωδών, στις οποίες καταλήξαμε.

---

[13] Έστω π.χ. ότι $\mathfrak{d} = \mathfrak{p}_2$ τότε, διαδοχικά, έχομε $\mathfrak{p}_2 | \langle x + \sqrt{145}y \rangle = \langle x - y + 2\omega y \rangle$, $\mathfrak{p}_2 | \langle x - y \rangle$, $x - y \in \mathfrak{p}_2$, $x - y = 2a + b(1 + \omega)$ για κάποια $a, b \in \mathbb{Z}$, άρα $x - y = 2a$, άτοπο. Ανάλογα αποκλείονται οι περιπτώσεις $\mathfrak{d} = \mathfrak{p}'_2, \langle 2 \rangle$.

[14] Πράγματι, έστω ότι έχουν ένα πρώτο κοινό διαιρέτη. Αυτός πρέπει να διαιρεί το άθροισμα και τη διαφορά των δύο παραγόντων, άρα τα $x, y\sqrt{145}$. Δηλαδή τα $\langle x \rangle, \langle y\sqrt{145} \rangle$ έχουν κοινό πρώτο διαιρέτη $\mathfrak{p}$. Τότε $y\sqrt{145} \in \mathfrak{p}$ άρα $145y \in \mathfrak{p}$ οπότε $\mathfrak{p} | \langle 145y \rangle$. Όμως και $\mathfrak{p} | \langle x \rangle$, άρα, από το λήμμα 1.3.11 οι $x, \sqrt{145}y$ δεν είναι πρώτοι μεταξύ τους στο $\mathbb{Z}$, άτοπο.

- Επίλυση της (2.17).
  Περνούμε σε κλάσεις ιδεωδών:

$$\mathbf{1} = \mathbf{1} \cdot [\mathfrak{p}_2]^3 \cdot [\mathfrak{p}_2] \cdot [\mathfrak{a}]^2 = [\mathfrak{a}]^2$$

  Άρα $[\mathfrak{a}] = [\mathfrak{p}_2^2]$ ή $[\mathfrak{a}] = \mathbf{1}$.

  Αν $[\mathfrak{a}\mathfrak{p}_2^2] = \mathbf{1}$ η σχέση (2.17) γίνεται, διαδοχικά :

$$\begin{aligned} \mathfrak{p}_2^{12}\langle x - y + 2\omega y\rangle &= \langle 17 - 2\omega\rangle(\mathfrak{p}_2^2\mathfrak{a})^6 \\ \langle 65 + 3\omega\rangle\langle x - y + 2\omega y\rangle &= \langle 17 - 2\omega\rangle\langle m + n\omega\rangle^6 \\ x - y + 2\omega y &= \frac{(11 + 2\omega)^\nu(1372 - 181\omega)(m + n\omega)^6}{4096} \ . \end{aligned} \tag{2.24}$$

  Στην τελευταία ισότητα παίρνουμε στάθμες [15], οπότε

$$2^{24}(x^2 - 145y^2) = (-1)^\nu 2^{12} 111(m^2 + mn - 36n^2)^6 \ .$$

  Επειδή το αριστερό μέλος ισούται με $-111z^6$, συμπεραίνομε από την τελευταία ότι ο ν είναι περιττός και

$$z = \frac{m^2 + mn - 36n^2}{4} \ .$$

  Για τις διάφορες τιμές του ν αναπτύσουμε το δεξιό μέλος της (2.24) και λύνουμε ως πρός x, y.

  Για παράδειγμα, κάνοντας χρήση του MAPLE, υπολογίζουμε, για $\nu = 3$,

$$\frac{(11 + 2\omega)^3(1372 - 181\omega)(m + n\omega)^6}{4096} =$$

$$\begin{aligned} &\tfrac{305387}{1024}m^6 + \tfrac{5974101}{512}m^5 n + \tfrac{194779485}{1024}m^4 n^2 + \tfrac{423372555}{256}m^3 n^3 \\ &+\tfrac{8282179125}{1024}m^2 n^4 + \tfrac{10801283013}{512}mn^5 + \tfrac{23477657571}{1024}n^6 \\ &+\omega\left(\tfrac{221263}{4096}m^6 + \tfrac{4328433}{2048}m^5 n + \tfrac{141124185}{4096}m^4 n^2 + \tfrac{306747375}{1024}m^3 n^3\right. \\ &\quad\left.+\tfrac{6000712785}{4096}m^2 n^4 + \tfrac{7825885857}{2048}mn^5 + \tfrac{17010339303}{4096}n^6\right) \ . \end{aligned}$$

  Η υπόλοιπη διαδικασία είναι πολύ απλή: Εξισώνουμε το $x - y$ με το ρητό μέρος του δεξιού μέλους και το $2y$ με τον συντελεστή του ω και βρίσκουμε τα x, y, ενώ το z είναι ήδη υπολογισμένο παραπάνω.

  Είδαμε, λοιπόν, ότι αν καταλήξουμε σε μία σχέση όμοια με την (2.24), ο υπολογισμός των x, y, z μπορεί να θεωρείται δεδομένος. Για τον λόγο αυτό,

[15] Εδώ γίνεται χρήση της εντολής `idealnorm`(bnf, I) (όπου I ιδεώδες ή γεννήτορας ιδεώδους) του PARI.

στις παρακάτω περιπτώσεις θα σταματούμε τη διαδικασία επίλυσης μέχρι να βρούμε σχέση ανάλογη της (2.24).

Αν $[\mathfrak{a}] = \mathbf{1}$ η σχέση (2.17) δίνει, διαδοχικά :

$$\begin{aligned} \langle x - y + 2\omega y\rangle &= \langle 17 - 2\omega\rangle\langle m + n\omega\rangle^6 \,, \\ x - y + 2\omega y &= (11 + 2\omega)^\nu (17 - 2\omega)(m + n\omega)^6 \,, \quad \nu \text{ περιττός} \,. \end{aligned}$$

- Επίλυση της (2.18).
  $\mathbf{1} = \mathbf{1}\cdot[\mathfrak{p}_2]^3\cdot[\mathfrak{p}_2]^3\cdot[\mathfrak{a}]^2 = [\mathfrak{p}_2]^2[\mathfrak{a}]^2$. Άρα $[\mathfrak{a}] = [\mathfrak{p}_2^3]$ ή $[\mathfrak{a}] = [\mathfrak{p}_2]$. Έπεται ότι $[\mathfrak{a}\mathfrak{p}_2] = \mathbf{1}$ ή $[\mathfrak{a}\mathfrak{p}_2'] = \mathbf{1}$.

  Αν $[\mathfrak{a}\mathfrak{p}_2] = \mathbf{1}$ η σχέση (2.18) συνεπάγεται διαδοχικά :

$$\begin{aligned} \mathfrak{p}_2^6\langle x - y + 2\omega y\rangle &= \mathfrak{p}_3\mathfrak{p}_{37}'(\mathfrak{p}_2\mathfrak{a})^6 \,, \\ \langle 64, 43 + \omega\rangle\langle x - y + 2\omega y\rangle &= \langle 111, 26 + \omega\rangle\langle m + n\omega\rangle^6 \,, \\ \langle x - y + 2\omega y\rangle &= \langle \frac{23}{16} - \frac{5}{64}\omega\rangle\langle m + n\omega\rangle^6 \,, \\ x - y + 2\omega y &= \frac{(92 - 5\omega)(11 + 2\omega)^\nu (m + n\omega)^6}{64} \,, \quad \nu \text{ περιττός} \,. \end{aligned}$$

  Αν $[\mathfrak{a}\mathfrak{p}_2'] = \mathbf{1}$ η σχέση (2.18) δίνει διαδοχικά :

$$\begin{aligned} \mathfrak{p}_2'^6\langle x - y + 2\omega y\rangle &= \mathfrak{p}_3\mathfrak{p}_{37}'(\mathfrak{p}_2'\mathfrak{a})^6 \,, \\ \langle 64, 20 + \omega\rangle\langle x - y + 2\omega y\rangle &= \langle 111, 26 + \omega\rangle\langle m + n\omega\rangle^6 \,, \\ \langle x - y + 2\omega y\rangle &= \langle \frac{85}{64} - \frac{1}{64}\omega\rangle\langle m + n\omega\rangle^6 \,, \\ x - y + 2\omega y &= \frac{(85 - \omega)(11 + 2\omega)^\nu (m + n\omega)^6}{64} \,, \quad \nu \text{ περιττός} \,. \end{aligned}$$

- Επίλυση της (2.20).
  $\mathbf{1} = \mathbf{1}\cdot[\mathfrak{p}_2]^3\cdot[\mathfrak{p}_2]\cdot[\mathfrak{a}]^2 = [\mathfrak{a}]^2$, άρα $[\mathfrak{a}] = [\mathfrak{p}_2^2]$ (δηλαδή $[\mathfrak{a}\mathfrak{p}_2^2] = 1$) ή $[\mathfrak{a}] = \mathbf{1}$.

  Αν $[\mathfrak{a}\mathfrak{p}_2^2] = \mathbf{1}$ η σχέση (2.20) δίνει διαδοχικά :

$$\begin{aligned} \mathfrak{p}_2^{12}\langle \frac{x - y}{2} + y\omega\rangle &= \langle 5 - \omega\rangle\langle 17 - 2\omega\rangle\langle m + n\omega\rangle^6 \,, \\ \langle 65 + 3\omega\rangle\langle \frac{x - y}{2} + y\omega\rangle &= \langle 5 - \omega\rangle\langle 17 - 2\omega\rangle\langle m + n\omega\rangle^6 \,, \\ \langle \frac{x - y}{2} + y\omega\rangle &= \langle \frac{59}{64} + \frac{31}{256}\omega\rangle\langle m + n\omega\rangle^6 \,, \\ \frac{x - y}{2} + y\omega &= \frac{(236 + 31\omega)(11 + 2\omega)^\nu (m + n\omega)^6}{256} \,, \quad \nu \text{ περιττός} \,. \end{aligned}$$

  Αν $[\mathfrak{a}] = \mathbf{1}$ η σχέση (2.20) δίνει διαδοχικά:

$$\begin{aligned} \langle \frac{x - y}{2} + y\omega\rangle &= \langle 73 + 11\omega\rangle\langle m + n\omega\rangle^6 \,, \\ \frac{x - y}{2} + y\omega &= (73 + 11\omega)^\nu (m + n\omega)^6 \,, \quad \nu \text{ περιττός} \,. \end{aligned}$$

Στα επόμενα θα είμαστε πιο συνοπτικοί. Κάνοντας πάντα χρήση του PARI, μπορούμε να υπολογίζουμε γινόμενα (συνάρτηση `idealmul`), δυνάμεις (συνάρτηση `idealpow`) και πηλίκα (συνάρτηση `idealdiv`) ιδεωδών.

- Επίλυση της (2.21).
  $\mathbf{1} = \mathbf{1} \cdot [\mathfrak{p}_2]^3 \cdot [\mathfrak{p}_2]^3 \cdot [\mathfrak{a}]^2 = [\mathfrak{p}_2]^2 \cdot [\mathfrak{a}]^2$. Άρα $[\mathfrak{a}] = [\mathfrak{p}_2]$ ή $[\mathfrak{a}] = [\mathfrak{p}_2^3]$. Έπεται ότι $[\mathfrak{a}\mathfrak{p}_2] = \mathbf{1}$ ή $[\mathfrak{a}\mathfrak{p}_2'] = \mathbf{1}$.

  Αν $[\mathfrak{a}\mathfrak{p}_2] = \mathbf{1}$ η σχέση (2.21) γίνεται διαδοχικά :

$$\begin{aligned}
\langle \frac{x-y}{2} + y\omega \rangle &= \frac{\mathfrak{p}_3\mathfrak{p}_{37}'}{\mathfrak{p}_2^2}(\mathfrak{a}\mathfrak{p}_2)^6 \,, \\
\langle \frac{x-y}{2} + y\omega \rangle &= \langle 10 - \frac{7}{4}\omega \rangle \langle m + n\omega \rangle^6 \,, \\
\frac{x-y}{2} + y\omega &= \frac{(40-7\omega)(11+2\omega)^\nu (m+n\omega)^6}{4} \,, \quad \nu \text{ περιττός} \,.
\end{aligned}$$

  Αν $[\mathfrak{a}\mathfrak{p}_2'] = \mathbf{1}$ η σχέση (2.21) δίνει διαδοχικά :

$$\begin{aligned}
\langle \frac{x-y}{2} + y\omega \rangle &= \frac{\mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}_{37}'}{\mathfrak{p}_2'^6}(\mathfrak{a}\mathfrak{p}_2')^6 \,, \\
\langle \frac{x-y}{2} + y\omega \rangle &= \langle \frac{461-89\omega}{64} \rangle \langle m + n\omega \rangle^6 \,, \\
\frac{x-y}{2} + y\omega &= \frac{(461-89\omega)(11+2\omega)^\nu (m+n\omega)^6}{64} \,, \quad \nu \text{ περιττός} \,.
\end{aligned}$$

- Επίλυση της (2.22).
  $\mathbf{1} = \mathbf{1} \cdot [\mathfrak{p}_2] \cdot [\mathfrak{p}_2] \cdot [\mathfrak{a}]^2 = [\mathfrak{p}_2]^2 \cdot [\mathfrak{a}]^2$. Άρα $[\mathfrak{a}] = [\mathfrak{p}_2]$ ($[\mathfrak{a}\mathfrak{p}_2] = \mathbf{1}$) ή $[\mathfrak{a}] = [\mathfrak{p}_2^3]$ ($[\mathfrak{a}\mathfrak{p}_2'] = \mathbf{1}$).

  Αν $[\mathfrak{a}\mathfrak{p}_2] = \mathbf{1}$, η (2.22) δίνει διαδοχικά :

$$\begin{aligned}
\langle \frac{x-y}{2} + y\omega \rangle &= \frac{\mathfrak{p}_3'\mathfrak{p}_{37}}{\mathfrak{p}_2^2}(\mathfrak{a}\mathfrak{p}_2)^6 \,, \\
\langle \frac{x-y}{2} + y\omega \rangle &= \langle 6 - \frac{5}{4}\omega \rangle \langle m + n\omega \rangle^6 \,, \\
\frac{x-y}{2} + y\omega &= \frac{(24-5\omega)(11+2\omega)^\nu (m+n\omega)^6}{4} \,, \quad \nu \text{ περιττός} \,.
\end{aligned}$$

  Αν $[\mathfrak{a}\mathfrak{p}_2'] = \mathbf{1}$ η (2.22) δίνει διαδοχικά :

$$\begin{aligned}
\langle \frac{x-y}{2} + y\omega \rangle &= \frac{\mathfrak{p}_2^4\mathfrak{p}_3'\mathfrak{p}_{37}}{\mathfrak{p}_2'^6}(\mathfrak{a}\mathfrak{p}_2')^6 \,, \\
\langle \frac{x-y}{2} + y\omega \rangle &= \langle \frac{255-67\omega}{64} \rangle \langle m + n\omega \rangle^6 \,, \\
\frac{x-y}{2} + y\omega &= \frac{(255-67\omega)(11+2\omega)^\nu (m+n\omega)^6}{64} \,, \quad \nu \text{ περιττός} \,.
\end{aligned}$$

- Επίλυση της (2.23).
  $\mathbf{1} = \mathbf{1} \cdot [\mathfrak{p}_2] \cdot [\mathfrak{p}_2]^3 \cdot [\mathfrak{a}]^2 = [\mathfrak{a}]^2$. Έπεται ότι $[\mathfrak{a}] = \mathbf{1}$ ή $[\mathfrak{a}] = [\mathfrak{p}_2^2]$ ($[\mathfrak{a}\mathfrak{p}_2^2] = \mathbf{1}$).
  Αν $[\mathfrak{a}] = \mathbf{1}$, η (2.23) δίνει διαδοχικά :

$$\begin{aligned}
\langle \frac{x-y}{2} + y\omega \rangle &= \frac{\mathfrak{p}_2^4 \mathfrak{p}_3' \mathfrak{p}_{37}'}{\mathfrak{p}_2'^6} (\mathfrak{a}\mathfrak{p}_2)^6 \ , \\
\langle \frac{x-y}{2} + y\omega \rangle &= \langle 3 - 7\omega \rangle \langle m + n\omega \rangle^6 \ , \\
\frac{x-y}{2} + y\omega &= (3-7\omega)(11+2\omega)^\nu (m+n\omega)^6 \ , \quad \nu \text{ περιττός} \ .
\end{aligned}$$

  Αν $[\mathfrak{a}\mathfrak{p}_2^2] = \mathbf{1}$, η (2.23) δίνει διαδοχικά :

$$\begin{aligned}
\langle \frac{x-y}{2} + y\omega \rangle &= \frac{\mathfrak{p}_3' \mathfrak{p}_{37}'}{\mathfrak{p}_2^8} (\mathfrak{a}\mathfrak{p}_2^2)^6 \ , \\
\langle \frac{x-y}{2} + y\omega \rangle &= \langle \frac{15}{64} - \frac{29}{256}\omega \rangle \langle m + n\omega \rangle^6 \ , \\
\frac{x-y}{2} + y\omega &= \frac{(60-29\omega)(11+2\omega)^\nu (m+n\omega)^6}{256} \ , \quad \nu \text{ περιττός} \ .
\end{aligned}$$