Εφαρμογές

1 Λύση της $x^2+5y^2=6z^\nu$ $\nu=2,3$, όπου $x,5y,6z$ είναι ανά δύο πρώτοι μεταξύ τους.

Η ανάλυση του (2) είναι $(2)=\mathfrak{p}^2$ και το $\mathfrak{p}$ δεν είναι κύριο. Με την βοήθεια του Θ.8, §3, Κεφ.4 φαίνεται εύκολα ότι η δράδα πλαίσεων είναι $\{1,[\mathfrak{p}]\}$. Έχομε τώρα την εξίσωση ιδεωδών

$$(x+y\sqrt{-5})(x-y\sqrt{-5})=(6)(\mathfrak{a})^\nu$$

Έχομε την ανάλυση $(3)=\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1\neq\mathfrak{p}_2$. Επίσης $N(x+y\sqrt{-5})\equiv 0 \pmod 6$, $N(x-y\sqrt{-5})\equiv 0\pmod 6$. Ειδικώτερα, έπεται ότι $(x+y\sqrt{-5})\equiv 0\pmod{\mathfrak{p}}$, $(x-y\sqrt{-5})\equiv 0\pmod{\mathfrak{p}}$, ενώ $\mathfrak{p}^2=(2)\nmid(x\pm y\sqrt{-5})$. Εύκολα φαίνεται τώρα ότι $(x+y\sqrt{-5},\ x-y\sqrt{-5})=\mathfrak{p}_i$, δηλαδή $(x\pm y\sqrt{-5})=\mathfrak{p}\mathfrak{p}_i\mathfrak{a}^\nu$.
Επειδή $N(1\pm\sqrt{-5})=6$ και $(1+\sqrt{-5})$, $(1-\sqrt{-5})$ είναι πρώτοι μεταξύ τους, έπεται ότι $(1+\sqrt{-5})=\mathfrak{p}\mathfrak{p}_1$ και $(1-\sqrt{-5})=\mathfrak{p}\mathfrak{p}_2$ ή αντιστρόφως.
Ας υποθέσομε χωρίς βλάβη της γενικότητος το πρώτο. Τότε
$(x\pm y\sqrt{-5})=(1+\sqrt{-5})\mathfrak{a}^\nu$. Από εδώ φαίνεται ότι $[\mathfrak{a}^\nu]=1$; άρα, αν $\nu=3$, τότε, από το Θ.10 (ii), §3, Κεφ.4, έπεται ότι $[\mathfrak{a}]=1$. Συνεπώς, θέτομε $\mathfrak{a}=(m+n\sqrt{-5})$, δηλαδή $(x\pm y\sqrt{-5})=(1+\sqrt{-5})(m+n\sqrt{-5})^3$ (ιδεωδη). Επειδή οι μόνες ενάδες είναι ±1, και το ±1 μπορεί ν' απορροφηθεί από τον κύβο, καταλήγομε, τελικά, στην

$$x\pm y\sqrt{-5}=(1+\sqrt{-5})(m+n\sqrt{-5})^3,$$

από όπου τα x,y. Επίσης $6z^3=N(x\pm y\sqrt{-5})=N(1+\sqrt{-5})N(\mathfrak{a})^3$, άρα $z=N(\mathfrak{a})=N(m+n\sqrt{-5})=m^2+5n^2$.
Αν $\nu=2$ διακρίνομε δύο περιπτώσεις:
α) $[\mathfrak{a}]=1$. Τότε εργαζόμαστε όπως πριν.
β) $[\mathfrak{a}]=\mathfrak{p}$. Τότε, από την $(x\pm y\sqrt{-5})=(1+\sqrt{-5})\mathfrak{a}^2$ έχομε $\mathfrak{p}^2(x\pm y\sqrt{-5})=(1+\sqrt{-5})(\mathfrak{p}\mathfrak{a})^2$. Είναι $[\mathfrak{p}\mathfrak{a}]=1$, άρα θέτομε $\mathfrak{p}\mathfrak{a}=(m+n\sqrt{-5})$. Επίσης $\mathfrak{p}^2=(2)$, άρα

$$(2)(x\pm y\sqrt{-5})=(1+\sqrt{-5})(m+n\sqrt{-5})^2,$$ από όπου

$$x\pm y\sqrt{-5}=\pm\frac{1+\sqrt{-5}}{2}(m+n\sqrt{-5})^2$$

και βρίσκομε τα x,y. Το z βρίσκεται, όπως στην περίπτωση $\nu=3$:
$6z^2=N(x\pm y\sqrt{-5})=\frac{6}{4}N(m+n\sqrt{-5})^2$, άρα $4z^2=m^2+5n^2$ και
$z=\pm(m^2+5n^2)/2$.

Αναγκαία και ικανή συνθήκη για να γράφεται ο πρώτος p με τη μορφή $2x^2+5y^2$ $(x,y>0)$ είναι $p \equiv 7,13,23,37 \pmod{40}$.

Έστω $p = 2x^2+5y^2$, $x,y>0$. Τότε ο p είναι περιττός, άρα ο y είναι περιττός, οπότε $p \equiv 5+2x^2 \equiv 5$ ή $7 \pmod 8$. Επίσης, $2x^2 \equiv p \pmod 5$, άρα $(2p/5) = +1$. Έπεται ότι $(p/5) = -1$, δηλ. $p \equiv 2$ ή $3 \pmod 5$. Από τις $p \equiv 5$ ή $7 \pmod 8$ και $p \equiv 2$ ή $3 \pmod 5$ έπεται ότι $p = 7, 13, 23, 37 \pmod{40}$.

Αντιστρόφως. Έστω $p \equiv 7,13,23,37 \pmod{40}$. Τότε εργαζόμαστε στο $\mathbb{Q}(\sqrt{-10})$. Η διακρίνουσα είναι -40 και $(-40/p) = (-10/p) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}\left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right) = -\left(\frac{\pm 2}{5}\right) = 1$.

Συνεπώς, Θ.14, §8, Κεφ 3, ο p αναλύεται ως εξής: $(p) = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$. Επίσης $(2) = \mathfrak{p}_2^2$. Τέλος, εύκολα φαίνεται ότι ο αριθμός κλάσεων είναι 2 και $[\mathfrak{p}_2] \neq 1$. Συνεπώς, η ομάδα κλάσεων είναι $\{1, [\mathfrak{p}_2]\}$. Αν $[\mathfrak{p}] = 1$, τότε $\mathfrak{p} = (a+b\sqrt{-10})$, άρα $p = N(\mathfrak{p}) = a^2+10b^2 \equiv a^2 \pmod 5$, άρα $p \equiv \pm 1 \pmod 5$, που αντίκειται στην υπόθεση. Συνεπώς $[\mathfrak{p}] = [\mathfrak{p}_2]$, άρα $[\mathfrak{p}\mathfrak{p}_2] = 1$. Θέτομε $\mathfrak{p}\mathfrak{p}_2 = (a+b\sqrt{-10})$, οπότε $2p = N(\mathfrak{p}\mathfrak{p}_2) = a^2+10b^2$. Έπεται ότι $a = 2a_1$ και $p = 2a_1^2+5b^2$.

3. Ο νόμος τετραγωνικής αντιστροφής.

Έστω $K = \mathbb{Q}(\sqrt{d})$, $d \neq 1$, ελεύθερος τετραγώνου και A ο δακτύλιος των ακεραίων του K. Τα κάθε ιδεώδες $\mathfrak{a}$ του A, έστω $\mathfrak{a}'$ το (συζυγές) ιδεώδες που αποτελείται από τα συζυγή στοιχεία του A. Λόγω της αμφιμονοσήμαντης, επί απεικόνισης

$$A/\mathfrak{a} \ni x + \mathfrak{a} \longrightarrow x' + \mathfrak{a}' \in A/\mathfrak{a}'$$

έπεται ότι $N(\mathfrak{a}) = \operatorname{card} A/\mathfrak{a} = \operatorname{card} A/\mathfrak{a}' = N(\mathfrak{a}')$.

Τα πρώτα ιδεώδη του p κατατάσσονται σε τρεις κατηγορίες:

Έστω $\mathfrak{p}$ ο ρητός πρώτος που $\mathfrak{p} \mid p$.

1η κατηγορία $N(\mathfrak{p}) = p$, αλλά $\mathfrak{p}^2 \neq (p)$.

2η κατηγορία $\mathfrak{p}^2 = (p)$.

3η κατηγορία $\mathfrak{p} = (p)$.

Τα πρώτα ιδεώδη $\mathfrak{p}$ της $1^{ης}$ κατηγορίας έχουν την ιδιότητα $\mathfrak{p} \neq \mathfrak{p}'$, όπότε $(p) = \mathfrak{p}\mathfrak{p}'$. Για τα ιδεώδη της $2^{ης}$ και $3^{ης}$ κατηγορίας έχομε $\mathfrak{p} = \mathfrak{p}'$.

Πράγματι, έστω $\mathfrak{p}$ ιδεώδες της $1^{ης}$ κατηγορίας. Έστω ~~η διακρίνουσα~~ μοναδική βάση $\delta = \sqrt{d}$ ή $(1+\sqrt{d})/2$, ανάλογα με το αν $d \not\equiv 1$, ή $d \equiv 1 \pmod 4$. Τότε $1, \delta$ αποτελούν ακέραια βάση. Έστω $m + n\delta \in \mathfrak{p}$. Τότε $m + n\delta' \in \mathfrak{p}'$. Αν ήταν $\mathfrak{p} = \mathfrak{p}'$ τότε: $n(\delta - \delta') \in \mathfrak{p}$, δηλ. $\mathfrak{p} \mid n(\delta - \delta')$. Το $\delta - \delta'$ διαιρεί τη διακρίνουσα του K. Συνεπώς, αν το $\mathfrak{p}$ διαιρούσε το $\delta - \delta'$, θα διαιρούσε και τη διακρίνουσα του K, άρα θα ήταν της $2^{ας}$ κατηγορίας, άτοπο. Άρα $\mathfrak{p} \nmid (\delta - \delta')$, όπότε $\mathfrak{p} \mid n$ και, συνεπώς, λόγω της $\mathfrak{p} \mid m + n\delta$, $\mathfrak{p} \mid m$. Τότε όμως $p \mid n$ και $p \mid m$ άρα $m + n\delta \in (p)$. Συμπέρασμα: $\mathfrak{p} \subseteq (p)$. Όμως ισχύει και $(p) \subseteq \mathfrak{p}$ ($\mathfrak{p} \mid (p)$), άρα $\mathfrak{p} = (p)$, άτοπο. Έτσι, $\mathfrak{p} \neq \mathfrak{p}'$. Όμως $N(\mathfrak{p}') = N(\mathfrak{p}) = p$, όπότε το $\mathfrak{p}'$ είναι πρώτο ιδεώδες $\neq \mathfrak{p}$ με norm p, άρα $\mathfrak{p}' \mid p$, όπότε $(p) = \mathfrak{p}\mathfrak{p}'$.

Έστω τώρα ότι το $\mathfrak{p}$ είναι της $2^{ης}$ κατηγορίας. Αν ήταν $\mathfrak{p}' \neq \mathfrak{p}$, τότε, όπως πριν θα έπρεπε ο p να έχει δυο διαφορετικούς πρώτους διαιρέτες, άτοπο. Τέλος, ότι για τους πρώτους $\mathfrak{p}$ της $3^{ης}$ κατηγορίας ισχύει $\mathfrak{p}' = \mathfrak{p}$, είναι προφανές.

β) Αν $p \equiv 1 \pmod 4$, τότε η $X^2 - pY^2 = -4$ είναι επιλύσιμη.

Εργαζόμαι στο $K = \mathbb{Q}(\sqrt{p})$. Η διακρίνουσα είναι p. Θεωρώ μια ενάδα η, τέτοια ώστε $\eta \neq \pm 1$ (η εξίσωση του Pell $u^2 - pv^2 = 1$ έχει λύση!) και η η να μην είναι $\pm$ δύναμη άλλης ενάδας. Αν $N(\eta) = -1$ και θέσω $\eta = (a + b\sqrt{p})/4$, τότε $a^2 - pb^2 = -4$, όπότε τελείωσα. Έστω τώρα ότι $N(\eta) = +1$. (*) Γράφω $\eta = \frac{\gamma}{\gamma'}$ για κάποιο ακέραιο γ (π.χ. $\gamma = 1 + \eta$). Αν το (γ) έχει ένα πρώτο διαιρέτη της $3^{ης}$ κατηγορίας, τότε απλοποιώ το κλάσμα γ/γ', άρα μπορώ να υποθέσω εξ αρχής ότι τα $(\gamma), (\gamma')$ δεν έχουν πρώτο διαιρέτη της $3^{ης}$ κατηγορίας. Έστω $\mathfrak{p}$ πρώτος διαιρέτης του (γ) της $1^{ης}$ κατηγορίας. Τότε ο ρητός πρώτος q που διαιρείται από το $\mathfrak{p}$ είναι $\neq p$, και $(q) = \mathfrak{p}\mathfrak{p}'$. Όμως $\mathfrak{p}' \mid (\gamma') = (\gamma)$, άρα $\mathfrak{p} \mid (\gamma)$, $\mathfrak{p}' \mid (\gamma)$, $\mathfrak{p} \neq \mathfrak{p}'$, όπότε $(q) \mid (\gamma)$ άρα $q \mid \gamma$ (στο A) όπότε $q \mid \gamma'$. Έτσι, το κλάσμα γ/γ' σημαίνει απλοποίηση, όπότε

(*) όπότε θα οδηγηθώ σε άτοπο.

μπορούμε να υποθέσουμε ἐξ ἀρχῆς ὅτι τό (γ) δέν ἔχει πρώτο διαιρέτη οὔτε τῆς $1^{ης}$ κατηγορίας. Ἡ μόνη δυνατότητα πού μένει εἶναι νά ἔχει τό (γ) διαιρέτη τῆς $2^{ης}$ κατηγορίας. Ὁ μοναδικός τέτοιος διαιρέτης εἶναι ὁ $(\sqrt{p})$. Συνεπῶς, $(\gamma)=(\sqrt{p})$ ἤ $(\gamma)=A$. Ἰσοδύναμα, $\gamma=\varepsilon\sqrt{p}$, ἤ $\gamma=\varepsilon$, ἀντιστοίχως, ὅπου ε ἑκάδα. Στήν πρώτη περίπτωση $\eta=\gamma/\gamma'=\varepsilon\sqrt{p}/-\varepsilon'\sqrt{p}=-\varepsilon/\varepsilon'=-\varepsilon^2/\varepsilon\varepsilon'=\pm\varepsilon^2$, ἐνῶ στή δεύτερη $\eta=\varepsilon/\varepsilon'=\varepsilon^2/\varepsilon\varepsilon'=\pm\varepsilon^2$. Καί στίς δύο περιπτώσεις ἤρθαμε σέ ἀντίφαση μέ τήν ἐκλογή τοῦ η.

β) Ἄν $p\equiv 1 \pmod 4$ τότε ἡ $X^2-pY^2=-1$ εἶναι ἐπιλύσιμη. Λόγῳ τοῦ (β) ὑπάρχουν $u,v\in\mathbb{Z}$ τ.ὥ. $u^2-pv^2=-4$. Ἄν ὁ v εἶναι ἄρτιος τότε καί ὁ u εἶναι ἄρτιος καί τελειώσαμε. Διαφορετικά uv περιττός ὁπότε $p\equiv 5 \pmod 8$. Ἀφ' ἑτέρου, $N\left(\frac{u+v\sqrt{p}}{2}\right)^3=-1$, ὁπότε ἀρκεῖ νά δείξουμε ὅτι τό $\left(\frac{u+v\sqrt{p}}{2}\right)^3$ εἶναι τῆς μορφῆς $A+B\sqrt{p}$, $A,B\in\mathbb{Z}$. Ἀλλά αὐτό εἶναι ἄμεση συνέπεια τῆς σχέσης $p\equiv 5 \pmod 8$.

γ) $(-1/p)=(-1)^{\frac{p-1}{2}}$ γιά κάθε περιττό πρῶτο p.

Ἄν $p\equiv 1 \pmod 4$, τότε, λόγῳ τοῦ (γ), ἡ $X^2-pY^2=-1$ εἶναι ἐπιλύσιμη. Εἰδικώτερα ἡ $x^2\equiv -1 \pmod p$ εἶναι ἐπιλύσιμη, ἄρα $(-1/p)=1$. Ἀντιστρόφως, ἄν $(-1/p)=1$ τότε τό t^2+1 ἀναλύεται $\bmod p$ σέ δύο διαφορετικούς παράγοντες ἄρα στό $\mathbb{Q}(\sqrt{-1})$ ὁ p ἀναλύεται: $(p)=\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1\neq\mathfrak{p}_2$. Στό σῶμα αὐτό ὁ ἀριθμός κλάσεων εἶναι 1, ὁπότε θέτομε $\mathfrak{p}_1=(a+b\sqrt{-1})$. Τότε $p=N(\mathfrak{p}_1)=a^2+b^2\equiv 1 \pmod 4$.

Ἄρα $(-1/p)=1 \iff p\equiv 1 \pmod 4$, πού ἰσοδυναμεῖ μέ τήν ἐκφώνηση.

δ) Ἔστω $K=\mathbb{Q}(\sqrt{p})$ μέ p πρῶτο $\equiv 1 \pmod 4$ ἤ $K=\mathbb{Q}(\sqrt{-p})$ μέ p πρῶτο $\equiv 3 \pmod 4$. Τότε ὁ ἀριθμός κλάσεων τοῦ K εἶναι περιττός.

Θά ὑποθέσω ὅτι ὁ ἀριθμός κλάσεων εἶναι ἄρτιος καί θά ὁδηγηθῶ σέ ἄτοπο. Ἄν εἶναι ἄρτιος θεωρῶ μιά κλάση $A\neq 1$, μέ $A^2=1$.

Έστω $A=[\mathfrak{a}]$ και $A'=[\mathfrak{a}']$. Επειδή, γενικά, κάθε πρώτο ιδεώδες πολ/σιασμένο επί το συζυγές του δίνει κύριο ιδεώδες ($\beta\lambda\cdot(\alpha)$), έπεται ότι $\mathfrak{a}\mathfrak{a}'$ είναι κύριο ιδεώδες. Άρα $[\mathfrak{a}][\mathfrak{a}']=1$. Επίσης $[\mathfrak{a}]^2=[\mathfrak{a}^2]=A^2=1$, δηλαδή $[\mathfrak{a}]=[\mathfrak{a}']$, δηλ. $A=A'$ ενώ $A\neq 1$. Λόγω της $\mathfrak{a}\sim\mathfrak{a}'$ έπεται ότι υπάρχουν ακέραιοι α,β του K τέτοιοι ώστε $(\alpha)\mathfrak{a}=(\beta)\mathfrak{a}'$. Άρα $N((\alpha))N(\mathfrak{a})=N((\beta))N(\mathfrak{a}')$, δηλαδή $N((\alpha))=N((\beta))$ και, συνεπώς, $N(\alpha)=\pm N(\beta)$.

Έστω $N(\alpha)=N(\beta)$. Τότε υπάρχει ακέραιος γ τ.ώ. $\frac{\alpha}{\beta}=\frac{\gamma}{\gamma'}$ (π.χ. $\gamma=\beta'(\alpha+\beta)$ αν $\beta\neq-\alpha$ και $\gamma=\sqrt{\pm p}$ αν $\beta=-\alpha$).

Απ' τη σχέση $\alpha\mathfrak{a}=\beta\mathfrak{a}'$ έχομε διαδοχικά: $\alpha\gamma'\mathfrak{a}=\beta\gamma'\mathfrak{a}'$, $\beta\gamma\mathfrak{a}=\beta\gamma'\mathfrak{a}'$, $\gamma\mathfrak{a}=\gamma'\mathfrak{a}'$. Θέτοντας $\gamma\mathfrak{a}=\mathfrak{b}\in A$, συμπεραίνομε ότι $\mathfrak{b}=\mathfrak{b}'$. Αν, πάλι, $N(\alpha)=-N(\beta)$, τότε ένα απ' τα δύο στοιχεία α,β έχει αρνητική norm δηλαδή, ανάγκη, $K=\mathbb{Q}(\sqrt{p})$. Εξ υποθέσεως, τότε, $p\equiv 1\pmod 4$ άρα, λόγω του (γ), υπάρχει ενάδα η με $N(\eta)=-1$. Παίρνοντας λοιπόν από έτερου $\mathfrak{a}\mathfrak{a}=\beta\mathfrak{a}'=\beta\eta\,\mathfrak{a}'$ και τώρα $N(\alpha)=N(\beta\eta)$, άρα μπορούμε να δουλέψομε όπως και πριν και να καταλήξομε στο ίδιο συμπέρασμα: Υπάρχει $\mathfrak{b}\in A$, $\mathfrak{b}=\mathfrak{b}'$. Θεωρώντας τη σχέση $\mathfrak{b}=\mathfrak{b}'$ μπορούμε ν' απαλείψομε τους πρώτους διαιρέτες της $3^{\text{ης}}$ κατηγορίας, επίσης, αν $\mathfrak{p}$ είναι πρώτος της $1^{\text{ης}}$ κατηγορίας τ.ώ. $\mathfrak{p}\mid\mathfrak{b}$ και $\mathfrak{p}\mathfrak{p}'=(q)$ $(q\neq p)$ τότε $\mathfrak{p}'\mid\mathfrak{b}'=\mathfrak{b}$, άρα $\mathfrak{p}\mathfrak{p}'\mid\mathfrak{b}$ δηλαδή $(q)\mid\mathfrak{b}$. Τότε $(q)\mid\mathfrak{b}'$, άρα η σχέση $\mathfrak{b}=\mathfrak{b}'$ απλοποιείται περαιτέρω. Συνεπώς, μπορούμε να καταλήξομε τελικά σε μια σχέση $\mathfrak{b}=\mathfrak{b}'$, όπου $\mathfrak{b}\in A$ και το $\mathfrak{b}$ ή ταυτίζεται με το δακτύλιο A ή, αν έχει πρώτο διαιρέτη, αυτός είναι της $2^{\text{ης}}$ κατηγορίας, δηλαδή διαιρεί τη διακρίνουσα του K. Η διακρίνουσα όμως έχει αριθμώς ένα πρώτο διαιρέτη τον $\sqrt{\pm p}$, δηλαδή, σ' αυτή την περίπτωση $\mathfrak{b}=(\sqrt{\pm p})$. Έτσι, σε κάθε περίπτωση το $\mathfrak{b}$ είναι κύριο, δηλαδή $A=[\mathfrak{b}]=1$, άτοπο.

β) Αν p,q είναι διαφορετικοί πρώτοι, $p\equiv q\equiv -1\pmod 4$ και $(p)=\mathfrak{p}_1^2$, $(q)=\mathfrak{p}_2^2$, τότε τα $\mathfrak{p}_1,\mathfrak{p}_2$ είναι κύρια.

στο $\mathbb{Q}(\sqrt{pq})$

Πρώτα παρατηρώ ότι δεν υπάρχει ενάδα με norm -1. Αν υπήρχε,

τότε η $x^2 - pq y^2 = -4$ θα είχε λύση, άρα η $x^2 \equiv -4 \pmod p$ θα είχε, επίσης, λύση. Όμως $p \equiv 3 \pmod 4$, οπότε έρχόμαστε σε αντίφαση με το (δ). Επιλέγω τώρα μία έναδα $\eta \neq \pm 1$ στο σώμα $\mathbb{Q}(\sqrt{pq})$, τέτοια ώστε $\eta \neq \pm$ δύναμη έναδας. Θέτω $\eta = \alpha/\alpha'$ για κάποιο ακέραιο α (π.χ. $\alpha = 1+\eta$), όπότε $(\alpha) = (\alpha')$. Μπορώ, όπως αριβώς στο τέλος της απόδειξης του (ε), να υποθέσω ότι το (α) δεν έχει πρώτο διαιρέτη της 1ης ή 3ης κατηγορίας. Συνεπώς, έχω τις έξης πιθανές περιπτώσεις μόνο:

i) $(\alpha) = A$, ii) $(\alpha) = \mathfrak{p}_1$, iii) $(\alpha) = \mathfrak{p}_2$, iv) $(\alpha) = \mathfrak{p}_1\mathfrak{p}_2$.

Οι περιπτώσεις (i) και (iv) δίνουν αντιστοίχως $\alpha = \varepsilon$, $\alpha = \varepsilon\sqrt{pq}$, όπου ε έναδα, όπότε $\eta = \alpha/\alpha' = \varepsilon/\varepsilon' = \varepsilon^2/\varepsilon\varepsilon' = \varepsilon^2$ και $\eta = \alpha/\alpha' = \varepsilon\sqrt{pq}/(-\varepsilon'\sqrt{pq}) = -\varepsilon/\varepsilon' = -\varepsilon^2$, αντιστοίχως. Και στις δύο περιπτώσεις έρχόμαστε σε αντίφαση με την εκλογή του η. Μένουν λοιπόν οι περιπτώσεις (ii) και (iii), όπότε ένα τουλάχιστον από τα $\mathfrak{p}_1, \mathfrak{p}_2$ είναι κύριο. Όμως $\mathfrak{p}_1\mathfrak{p}_2 = (\sqrt{pq})$, οπότε και τα δύο πρέπει να είναι κύρια.

ε) Αν p, q είναι διαφορετικοί πρώτοι, $p \equiv q \equiv -1 \pmod 4$ τότε η $px^2 - qy^2 = \pm 4$ είναι επιλύσιμη για τουλάχιστον μία εκλογή του προσήμου στο δεξιό μέλος.

Πράγματι, λόγω του (δ) υπάρχουν $a, b \in \mathbb{Z}$ τ.ώ. $\mathfrak{p}_1 = \left(\frac{a+b\sqrt{pq}}{2}\right)$, όπου $N(\mathfrak{p}_1) = p$. Τότε $p = \pm\frac{a^2 - b^2pq}{4}$, άρα $a = pa_1$, $a_1 \in \mathbb{Z}$ και $\pm 4 = pa_1^2 - qb^2$.

ζ) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, για κάθε περιττό πρώτο p.

Ισοδύναμα: $(2/p) = +1$ αν και μόνο αν $p \equiv \pm 1 \pmod 8$. Έστω $p \equiv \pm 1 \pmod 8$. Θέτω $p^* = p$ ή $-p$, έτσι ώστε $p^* \equiv 1 \pmod 8$ και δουλεύω στο $\mathbb{Q}(\sqrt{p^*})$. Στο σώμα αυτό το (2) αναλύεται: $(2) = \mathfrak{p}\mathfrak{p}_1$ $(\mathfrak{p} \neq \mathfrak{p}_1)$. Επίσης, λόγω του (ε), ο αριθμός κλάσεων h είναι περιττός. Θέτω $\mathfrak{p}^h = (\alpha)$, άρα $2^h = \pm N(\alpha)$. Αν $p^* < 0$

το' — απορλείεται. Άν $p^* > 0$ τότε $p^* = p$ και, λόγω του (γ), υπάρχει έναδα η με' $N(\eta) = -1$. Στην συνέχεια θέτω $\beta = \alpha$ άν $p^* < 0$ και $\beta = \eta\alpha$ άν $p^* > 0$, όπότε $N(\beta) = 2^h$. Το' $N(\beta)$ είναι της μορφής $(x^2 - p^* y^2)/4$, όπότε $2^{h+2} = x^2 - p^* y^2 \equiv x^2 \pmod p$. Επειδή ό $h+2$ είναι περιττός έπεται ότι $(2/p) = +1$. Αντιστρόφως, ζέστω $(2/p) = +1$. Τότε το $t^2 - 2$ αναλύεται modulo p, άρα στο' $\mathbb{Q}(\sqrt{2})$ ό p αναλύεται: $(p) = \mathfrak{p}\mathfrak{p}_1$ $(\mathfrak{p} \neq \mathfrak{p}_1)$. Σ' αυτό το' σώμα όλα τα' ιδεώδη είναι κύρια, όπότε θέτομε $\mathfrak{p} = (a + b\sqrt{2})$. Τότε $p = N(\mathfrak{p}) = \pm(a^2 - 2b^2) \equiv \pm 1 \pmod 8$.

β) Νόμος της τετραγωνικής αντιστροφής.

Στα παρακάτω το' p συμβολίζει πρώτο $\equiv 1 \pmod 4$. Τα' q, q_1 συμβολίζουν πρώτους $\equiv -1 \pmod 4$ και τα' r, r_1 οποιουσδήποτε περιττούς πρώτους. Ο νόμος της τετραγωνικής αντιστροφής διατυπώνεται ισοδύναμα ως έξης: $(r/p) = (p/r)$ και $(q/q_1) = -(q_1/q)$. Για τον τυχόντα περιττό' πρώτο r θα' γράφομε r^* για να συμβολίσομε εκείνον απ' τους $r, -r$ ό οποίος είναι $\equiv 1 \pmod 4$.

(i) $(r^*/r_1) = 1 \Rightarrow (r_1/r) = 1$.

Πράγματι, $(r^*/r_1) = 1 \Rightarrow$ το' $t^2 + r_1$ αναλύεται στο $\mathbb{Q}(\sqrt{r^*})$, τότε $(r_1) = \mathfrak{p}\mathfrak{p}_1$ $(\mathfrak{p} \neq \mathfrak{p}_1)$ στο' σώμα αυτό'. Επίσης, ό αριθμός κλάσεων h είναι περιττός, λόγω του (ε). Τότε, ακριβώς όπως στο (η) δείχνομε ότι υπάρχει ακέραιος β τέτοιος ώστε $\mathfrak{p}^h = (\beta)$ και $N(\beta) = r_1^h$. Συνεπώς, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $x^2 - r^* y^2 = 4r_1^h$. Άρα $4r_1^h \equiv x^2 \pmod r$, και επειδή ό h είναι περιττός, $(r_1/r) = 1$.

(ii) $(p/r) = (r/p)$.

Αρκεί να δείξω ότι $(p/r) = 1 \iff (r/p) = 1$.

Πράγματι, $(p/r) = 1 \overset{p=p^*}{\Rightarrow} (p^*/r) = 1 \overset{(i)}{\Rightarrow} (r/p) = 1$.

Επίσης $(r/p) = 1 \overset{p \equiv 1(4)}{\Rightarrow} (\pm r/p) = 1 \Rightarrow (r^*/p) = 1 \overset{(i)}{\Rightarrow} (p/r) = 1$.

(iii) $(q/q_1) = -(q_1/q)$.

Λόγω του (ζ) υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $\pm 4 = qx^2 - q_1 y^2$, άρα $4\mu \equiv qx^2 \pmod{q_1}$, όπου $\mu \in \{1, -1\}$. Τότε $(q/q_1) = (\mu/q_1) = \mu$ (*).

Επίσης, $4\mu = -q_1 y^2 \pmod q$, άρα $(-q_1/q) = (\mu/q) = \mu$, δηλ. $(q_1/q) = -\mu$. Απ' την (*) έχομε τώρα το' αποδεικτέο.

Η εξίσωση του Fermat $x^3+y^3=z^3$, $xyz\neq 0$ είναι αδύνατη.

Δουλεύω στο $\mathbb{Q}(\omega)$, $\omega=(-1+\sqrt{-3})/2$ ($\omega^3=1$) και αποδεικνύω γενικώτερα ότι η

$$\alpha^3+\beta^3+\varepsilon\lambda^{3n}\gamma^3=0, \quad \alpha\beta\gamma\not\equiv 0 \pmod{\lambda} \qquad (1)$$

όπου α,β,γ ακέραιοι του $\mathbb{Q}(\omega)$, ε ένα από τα $\pm 1, \pm\omega, \pm\omega^2$, $\lambda=\omega-1$ (= ο μοναδικός πρώτος διαιρέτης του 3*) και $n\geq 0$ (ακέραιος), είναι αδύνατη. Στο $\mathbb{Q}(\omega)$ ο αριθμός κλάσεων είναι 1.

Λήμμα. Αν ο ακέραιος $\alpha\not\equiv 0 \pmod{\lambda}$ τότε είναι $\alpha^3\equiv \pm 1 \pmod{\lambda^4}$.

Πράγματι, ας θέσω $\alpha=m+n\omega\equiv m+n \pmod{\lambda}$. Τότε $\alpha=\mu+\beta\lambda$, όπου $\mu\in\{1,-1\}$ και β ακέραιος του $\mathbb{Q}(\omega)$. Άρα $\alpha^3=\mu+3\beta\lambda+3\mu\beta^2\lambda^2+\beta^3\lambda^3\equiv\mu+(3\beta\lambda+\beta^3\lambda^3) \pmod{\lambda^4}$. Είναι $3=-\lambda^2\omega^2$, άρα $3\beta\lambda+\beta^3\lambda^3=-\beta\lambda^3\omega^2+\beta^3\lambda^3=\lambda^3\beta(\beta-\omega)(\beta+\omega)$. Όπως είδαμε στην αρχή, κάθε ακέραιος του $\mathbb{Q}(\omega)$ είναι ισοδύναμος mod λ με κάποιο ρητό ακέραιο, δηλαδή $\beta\equiv 0$ ή 1, ή $-1 \pmod{\lambda}$. Άρα $\beta(\beta-\omega)(\beta+\omega)\equiv 0 \pmod{\lambda}$ και συνεπώς $3\beta\lambda+\beta^3\lambda^3\equiv 0 \pmod{\lambda^4}$. Άρα $\alpha^3\equiv\mu \pmod{\lambda^4}$. ∎

Επανέρχομαι στη (1): Αν ήταν $n=0$, δηλαδή $\alpha\beta\gamma\not\equiv 0 \pmod{\lambda}$, θα είχαμε $\pm 1\pm 1\pm\varepsilon\equiv 0 \pmod{\lambda^4}$. Έδω $\varepsilon=\pm 1, \pm\omega, \pm\omega^2$, δηλαδή η τελευταία ισοτιμία είναι αδύνατη. Άρα $n\neq 0$. Ανάλογα αποδεικνύεται ότι αν $n=1$. Συνεπώς $n\geq 2$. Προφανώς μπορούμε να υποθέσουμε ότι τα α,β,γ, είναι ανά δύο πρώτα μεταξύ τους. Γράφω την (1) $(\alpha+\beta)(\alpha+\beta\omega)(\alpha+\beta\omega^2)=\varepsilon\lambda^{3n}(-\gamma)^3$. Εύκολα φαίνεται ότι οι 3 παράγοντες στο αριστερό μέλος έχουν, ανά δύο, μκδ το λ. Ένας, ακριβώς, διαιρείται διά του λ^{3n-2}. Ισχυρίζομαι ότι, χωρίς βλάβη της γενικότητας, αυτός ο παράγων είναι ο $\alpha+\beta$. Γιατί, αν π.χ. ήταν ο $\alpha+\beta\omega$, τότε θα έθετα $\beta'=\beta\omega$ και θα έγραφα την εξίσωση ως $(\alpha+\beta')(\alpha+\beta'\omega)(\alpha+\beta'\omega^2)=\varepsilon\lambda^{3n}(-\gamma)^3$ με $\alpha+\beta'\equiv 0 \pmod{\lambda^{3n-2}}$. Θέτω λοιπόν $\alpha+\beta=\lambda^{3n-2}\delta_1^3\varepsilon_1$, $\alpha+\beta\omega=\lambda\delta_2^3\varepsilon_2$, $\alpha+\beta\omega^2=\lambda\delta_3^3\varepsilon_3$, όπου $\delta_1\delta_2\delta_3=\gamma$ και $\varepsilon_1\varepsilon_2\varepsilon_3=-\varepsilon$. Η σχέση $(\alpha+\beta)+\omega(\alpha+\beta\omega)+\omega^2(\alpha+\beta\omega^2)=0$ συνεπάγεται την $\varepsilon_3\omega^2\delta_3^3+\varepsilon_2\omega\delta_2^3+\varepsilon_1\lambda^{3n-3}\delta_1^3=0$, άρα για κάποιες ενάδες $\varepsilon_4,\varepsilon_5$ ισχύει $\delta_3^3+\varepsilon_4\delta_2^3+\varepsilon_5\lambda^{3(n-1)}\delta_1^3=0$. Ειδικώτερα, $\pm 1\pm\varepsilon_4\equiv 0 \pmod{\lambda^3}$, άρα $\varepsilon_4=\pm 1$ και $\delta_3^3+(\pm\delta_2)^3+\varepsilon_5\lambda^{3(n-1)}\delta_1^3=0$, εξίσωση όμοια με την (1). Έχω όμως κάθοδο ως προς το n, δηλαδή η εξίσωση είναι αδύνατη.

* $(3)=\lambda^2$

Ορ. Το κυκλοτομικό πολυώνυμο τάξεως m.
Εξ ορισμού είναι το πολυώνυμο του οποίου οι ρίζες είναι οι αρχικές m-τάξεως ρίζες του 1 (με πολλαπλότητα ένα ή παραπάνω). Το συμβολίζω $F_m(t)$. Είναι προφανές ότι, αν $d_1 \neq d_2$ τότε τα $F_{d_1}(t)$ και $F_{d_2}(t)$ δεν έχουν κοινή ρίζα. Αφ' ετέρου, αν $d|m$, τότε όλες οι ρίζες του $F_d(t)$ είναι ρίζες του t^m-1, οπότε και όλες οι ρίζες του $\prod_{d|m} F_d(t)$ είναι ρίζες του t^m-1. Αντιστρόφως, αν ζ είναι ρίζα του t^m-1 τότε θεωρώ το ελάχιστο $d \geq 1$ τ.ώ. $\zeta^d-1=0$. Προφανώς $d|m$ και η ζ είναι d-τάξεως αρχική ρίζα του 1, οπότε είναι ρίζα του $F_d(t)$. Συμπεραίνω:

$$t^m-1 = \prod_{d|m} F_d(t).$$

Επειδή $F_1(t)=t-1$, έπεται επαγωγικά, λόγω της $F_m(t)=\dfrac{t^m-1}{\prod_{\substack{d|m \\ d<m}} F_d(t)}$

ότι $\underline{F_m(t) \in \mathbb{Z}[t]}$ για κάθε m. $\underline{\text{Θα δείξουμε, επιπλέον, ότι το } F_m(t) \text{ είναι ανάγωγο στο } \mathbb{Q}[t].}$ Έστω p πρώτος. Αν $f(t)=a_0t^\nu+\dots+a_{\nu-1}t+a_\nu \in \mathbb{Z}[t]$, θέτουμε $\hat{f}(t)=\hat{a}_0t^\nu+\dots+\hat{a}_{\nu-1}t+a_\nu \in \mathbb{F}_p[t]$, όπου $\hat{a}_i=a_i+p\mathbb{Z}$. Η απεικόνιση $\mathbb{Z}[t] \ni f(t) \longmapsto \hat{f}(t) \in \mathbb{F}_p[t]$ είναι ομομορφισμός και, επιπλέον $(\hat{f}(t))^p=\hat{f}(t^p)$. Τώρα θέτουμε $h(t)=t^m-1$ και ξέρουμε ήδη ότι $F_m(t) \mid h(t)$ (στο $\mathbb{Z}[t]$), οπότε $\hat{F}_m(t) \mid \hat{h}(t)$ (στο $\mathbb{F}_p[t]$). Έστω ότι $(p,m)=1$. Τότε τα $\hat{h}(t), \hat{h}'(t)$ είναι πρώτα μεταξύ τους, άρα το $\hat{h}(t)$ έχει μόνο απλές ρίζες. Συνεπώς, αν $(p,m)=1$ τότε το $\hat{F}_m(t)$ έχει απλές ρίζες. Έστω τώρα ζ μια ρίζα του $F_m(t)$ και $\phi(t) \in \mathbb{Z}[t]$ το ελάχιστο πολυώνυμο της ζ πάνω από το $\mathbb{Q}$. Μένει να δείξουμε ότι $F_m(t)=\phi(t)$. Προφανώς, $\phi(t) \mid F_m(t)$ άρα μένει να δείξουμε ότι οποιαδήποτε ρίζα του $F_m(t)$ είναι ρίζα του $\phi(t)$. Θέτουμε $F_m(t)=\phi(t)\cdot g(t)$ (1). Αν $(p,m)=1$ τότε ζ^p είναι m-τάξεως αρχική ρίζα του 1. Ισχύει $g(\zeta^p) \neq 0$. Πραγματικά στην αντίθετη περίπτωση θα θέσουμε $G(t)=g(t^p)$. Τότε $G(\zeta)=0$, άρα $\phi(t) \mid G(t)$ (στο $\mathbb{Z}[t]$) και έστω $G(t)=\phi(t)\cdot q(t)$. Τότε $\hat{\phi}(t)\hat{q}(t)=\hat{G}(t)=\hat{g}(t^p)=(\hat{g}(t))^p$. Πάρε ένα μη σταθερό, ανάγωγο στο $\mathbb{F}_p[t]$ παράγοντα του $\hat{\phi}(t)$, έστω $\hat{\psi}(t)$. Τότε $\hat{\psi}(t) \mid \hat{g}(t)$ άρα, λόγω της (1), $\hat{\psi}(t)^2 \mid \hat{F}_m(t)$ άτοπο, αφού είδαμε πριν ότι το $\hat{F}_m(t)$ δεν έχει πολλαπλή ρίζα.

Το συμπέρασμα είναι λοιπόν ότι για κάθε πρώτο p, $(p,m)=1$, είναι $g(\zeta^p)\neq 0$ άρα, λόγω της $F_m(\zeta^p)=0$ και της (1), $\phi(\zeta^p)=0$. Άρα, το ελάχιστο πολυώνυμο της ζ^p είναι πάλι το $\phi(t)$. Κάνοντας τους ίδιους συλλογισμούς, αλλά με το ζ^p στη θέση του ζ, συμπεραίνομε ότι για p' πρώτο, $(p',m)=1$ είναι $\phi(\zeta^{pp'})=0$. Επαγωγικά βλέπομε ότι για κάθε a άκεραιο ≥ 1, $(a,m)=1$ ο ζ^a είναι ρίζα του $\phi(t)$. Επειδή κάθε ρίζα του $F_m(t)$ είναι της μορφής ζ^a με $a\geq 1$, $(a,m)=1$, συμπεραίνομε ότι όλες οι ρίζες του $F_m(t)$ είναι και ρίζες του $\phi(t)$, όπότε $F_m(t)=\phi(t)$.

6. Στο p-τάξεως κυκλοτομικό σώμα $\mathbb{Q}(\zeta)$ όλες-όλες οι ρίζες του 1 είναι οι $\pm\zeta^a$, $a=0,1,2,\ldots,p-1$.
Δηλαδή, συμφωνα με τους συμβολισμούς της §5, Κεφ.4, έχομε ν' αποδείξομε ότι $W=\langle -\zeta\rangle$: Έστω ότι η τάξη της W είναι m, Η W είναι κυκλική. Έστω $W=\langle\eta\rangle$. Τότε το η είναι m-τάξεως αρχική ρίζα του 1, και το ελάχιστο πολυώνυμο του η είναι το κυκλοτομικό πολυώνυμο $F_m(t)$ βαθμού $\phi(m)$. Λόγω της σχέσης $\mathbb{Q}(\eta)\subseteq\mathbb{Q}(\zeta)$ συμπεραίνομε ότι $\phi(m)\mid p-1$. Επίσης η $\langle -\zeta\rangle$ είναι υποομάδα της W πεπερασμένης τάξης $2p$, άρα $2p\mid m$. Θέτομε $m=2^r p^s m_1$ όπου $r,s\geq 1$ και $(m_1,2p)=1$. Τότε $\phi(m)=2^{r-1}p^{s-1}(p-1)\phi(m_1)$ και λόγω της $\phi(m)\mid p-1$, έπεται ότι $r=1$, $s=1$, $m_1=1$. Άρα $m=2p$, η τάξη της W είναι, συνεπώς, $2p$ άρα $W=\langle -\zeta\rangle$, αφού η $\langle -\zeta\rangle$ έχει τάξη $2p$.

7. Το λήμμα του Kummer: Στο $\mathbb{Q}(\zeta)$ (βλ. 6) κάθε ενάδα είναι γινόμενο μιας δυνάμης του ζ επί μια πραγματική ενάδα.

Έστω $\sigma_i(\zeta)=\zeta^i$ $(i=1,\ldots,p-1)$. Έστω $\varepsilon=a_0+a_1\zeta+\cdots+a_{p-2}\zeta^{p-2}=r(\zeta)$ μια ενάδα. Θεωρούμε την ενάδα $\bar{\varepsilon}=r(\zeta^{-1})=r(\zeta^{p-1})$ και στη συνέχεια την $\mu=\varepsilon/\bar{\varepsilon}$. Οι άλλοι συζυγείς του μ είναι οι $\sigma_i(\mu)$ $(i=1,\ldots,p-1)$, άρα οι $r(\zeta^i)/r(\zeta^{-i})$, συνεπώς $|\sigma_i(\mu)|=\left|r(\zeta^i)/\overline{r(\zeta^i)}\right|=1$.
Λόγω του λήμματος *, §5, Κεφ.4, $\mu\in W$ άρα, απ' το 6., $\mu=\pm\zeta^a$. Πρώτα δ' αποκλείσομε το πρόσημο $-$. Αν ίσχυε,

τότε $\varepsilon = -\zeta^a \cdot \bar{\varepsilon}$. Αν δέσομε, ως συνήθως, $\lambda = 1-\zeta$, τότε $\zeta \equiv 1 \pmod{\lambda}$ και $\varepsilon \equiv -\bar{\varepsilon} \pmod{\lambda}$. Όμως $\varepsilon \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{\lambda}$, δηλαδή $\varepsilon \equiv b \pmod{\lambda}$ για κάποιο $b \in \mathbb{Z}$. Αναλόγως, $\bar{\varepsilon} \equiv a_0 + a_1 + \cdots + a_{p-2} \equiv b \pmod{\lambda}$. Όμως $\varepsilon \equiv -\bar{\varepsilon} \pmod{\lambda}$ δηλαδή $2b \equiv 0 \pmod{\lambda}$. Συνεπώς $b \equiv 0 \pmod{\lambda}$ δηλαδή και $b \equiv 0 \pmod{p}$ (στο $\mathbb{Z}$). Τότε $\varepsilon \equiv b \equiv 0 \pmod{\lambda}$, άτοπο, αφού το ε είναι ενάδα. Συμπεραίνομε, λοιπόν, ότι $\mu = \zeta^a$, δηλ. $\varepsilon = \zeta^a \cdot \bar{\varepsilon}$. Θεωρούμε εώρα $c \in \mathbb{Z}$ τ.ώ. $2c \equiv a \pmod{p}$, δηλαδή $\zeta^a = \zeta^{2c}$ και τώρα $\varepsilon = \zeta^{2c} \cdot \bar{\varepsilon}$, άρα $\varepsilon \zeta^{-c} = \zeta^c \cdot \bar{\varepsilon} = \overline{(\varepsilon \zeta^{-c})}$. Δηλ. $\varepsilon \zeta^{-c} = \eta \in \mathbb{R}$ και $\varepsilon = \zeta^c \cdot \eta$, ό.έ.δ.

Η πρώτη περίπτωση της εξίσωσης του Fermat $x^p + y^p = z^p$.

Εδώ υποθέτομε ότι $p > 3$, αφού η περίπτωση $p = 3$ έχει εξεταστεί στο 4. Εξ ορισμού, η πρώτη περίπτωση είναι εκείνη κατά την οποία κανένα από τα x, y, z δεν είναι διαιρετό διά p. Προφανώς, μπορούμε δίχως βλάβη της γενικότητος να υποθέσομε τα x, y, z πρώτα ανά δύο. Η εξίσωση γίνεται

$$(x+y)(x+y\zeta)(x+y\zeta^2) \cdots (x+y\zeta^{p-1}) = z^p \quad (1)$$

Λόγω της υπόθεσης είναι $z \not\equiv 0 \pmod{\lambda}$, δηλαδή όλοι οι παράγοντες $x + y\zeta^i$, $i = 0, \ldots, p-1$ είναι πρώτοι προς τον λ. Τότε, φαίνεται πολύ εύκολα ότι ανά δύο είναι πρώτοι μεταξύ τους. Τότε η (1) μάς πηγαίνει σε μιά εξίσωση ιδεωδών από την οποία παίρνομε

$$(x + y\zeta) = \alpha^p \text{ για κάποιο ιδεώδες } \alpha. \quad (2)$$

Υποθέτομε τώρα ότι ο p είναι κανονικός πρώτος, δηλ. ότι είναι πρώτος προς τον αριθμό κλάσεων του $\mathbb{Q}(\zeta)$. Τότε, από τη (2) έπεται ότι τα α είναι κύρια, έστω (α) και η (2) ταυτίζεται με την

$$x + y\zeta = \varepsilon \alpha^p, \text{ όπου } \varepsilon \text{ ενάδα} \quad (3).$$

Αν $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, τότε

$$\alpha^p \equiv a_0^p + a_1^p \zeta^p + \cdots + a_{p-2}^p \zeta^{p(p-2)} \equiv a_0 + a_1 + \cdots + a_{p-2} = b \pmod{p},$$

με $b \in \mathbb{Z}$. Επίσης, λόγω του 7. μπορούμε να δέσομε $\varepsilon = \zeta^s \cdot \eta$, όπου $\eta \in \mathbb{R}$. Τότε, από την (3), $x + y\zeta \equiv \zeta^s \cdot \eta \cdot b \pmod{p}$, άρα $\zeta^{-s}(x + y\zeta) \equiv \eta b \pmod{p}$. Παίρνομε την συζυγή σχέση $\zeta^s(x + y\zeta^{-1}) \equiv \eta b \pmod{p}$, δηλαδή

$\zeta^{-s}(x+y\zeta) \equiv \zeta^{s}(x+y\zeta^{-1}) \pmod p$ ή

$$x\zeta^{s} + y\zeta^{s-1} - x\zeta^{-s} - y\zeta^{1-s} \equiv 0 \pmod p \qquad (4)$$

Ἂν τὸ ἀριστερὸ μέλος εἶναι γραμμένο στὴν κανονικὴ μορφή, δηλ. ἂν τὰ s; $s-1$, $-s$, $1-s$ εἶναι ἀντίστοιχα mod p καὶ κανένα δὲν εἶναι ἰσοϋπόλοιπο μὲ $p-1$ modulo p, τότε ἡ (4) συνεπάγεται ὅτι οἱ συντελεστὲς $x, y, -x, -y$ εἶναι $\equiv 0 \pmod p$, ἄτοπο.

Ἂς ὑποθέσουμε τώρα ὅτι ἕνας ἀπ' τοὺς ἐκθέτες εἶναι $\equiv p-1 \pmod p$. Ἔστω π.χ. ὅτι $s \equiv p-1 \pmod p$. Τότε $s-1 \equiv p-2$, $-s \equiv 1$, $1-s \equiv 2 \pmod p$. Ἐπειδὴ $p>3$, οἱ ἐκθέτες εἶναι ἀνισοϋπόλοιποι mod p, ὁπότε ἡ κανονικὴ μορφὴ τοῦ ἀριστεροῦ μέλους τῆς (4) εἶναι

$$x(-1-\zeta-\cdots-\zeta^{p-2}) + y\zeta^{p-2} - x\zeta - y\zeta^{2} \equiv -x - 2x\zeta - (x+y)\zeta^{2} - x\zeta^{3} - \cdots - (\cdots)\zeta^{p-2}$$

καὶ λόγῳ τῆς (4) πρέπει ὅλοι οἱ συντελεστὲς νὰ εἶναι $\equiv 0 \pmod p$. Εἰδικώτερα, $x \equiv 0 \pmod p$, ἄτοπο. Ἀναλόγα ἐργαζόμαστε ἂν κάποιος ἀπ' τοὺς ἄλλους ἐκθέτες εἶναι $\equiv p-1 \pmod p$.

Μένει ἡ περίπτωση κατὰ τὴν ὁποία δύο ἀπ' τοὺς ἐκθέτες εἶναι ἰσοϋπόλοιποι mod p. Ἔχομε τὶς ἑξῆς 6 περιπτώσεις: $s \equiv s-1$, $s \equiv -s$, $s \equiv 1-s$, $s-1 \equiv -s$, $s-1 \equiv 1-s$, $-s \equiv 1-s \pmod p$. Ἡ 1η καὶ ἡ 6η περίπτωση ἀποκλείονται ἀμέσως. Ἡ 2η καὶ ἡ 5η δίνουν $s \equiv 0, 1 \pmod p$ ἀντιστοίχως ἄρα $s-1 \equiv p-1$ ἢ $-s \equiv p-1 \pmod p$ καὶ ἐρχόμαστε στὴν προηγούμενη περίπτωση, κατὰ τὴν ὁποία ἕνας ἐκθέτης ἦταν $\equiv p-1 \pmod p$. Μένει ἡ 3η καὶ ἡ 4η περίπτωση, ποὺ δίνουν $s \equiv (p+1)/2$ καὶ ἡ (4) γίνεται τότε $(x-y)\zeta^{\frac{p+1}{2}} + (y-x)\zeta^{\frac{p-1}{2}} \equiv 0 \pmod p$. Ἐπειδὴ $(p+1)/2 \not\equiv (p-1)/2 \pmod p$, ἕπεται ὅτι $x-y \equiv 0 \pmod p$. Ἂν εἴχαμε θεωρήσει τὴν ἐξίσωση τοῦ Fermat ὡς $x^p + (-z)^p = (-y)^p$, θὰ καταλήγαμε, ὁμοίως, στὴν $x+z \equiv 0 \pmod p$, ὁπότε, τελικά, $x \equiv y \equiv -z \pmod p$. Ὅμως $x+y \equiv x^p + y^p = z^p \equiv z \pmod p$, ἄρα $-2z \equiv z \pmod p$ καὶ $3z \equiv 0 \pmod p$. Ἐπειδὴ $p>3$, ἕπεται ὅτι $z \equiv 0 \pmod p$ κι ἔτσι ὁδηγηθήκαμε σὲ ἄτοπο.

Συμπέρασμα. Ἡ 1η περίπτωση τῆς ἐξίσωσης τοῦ Fermat $x^p + y^p = z^p$ εἶναι ἀδύνατη στὴν περίπτωση ποὺ ὁ p εἶναι κανονικὸς πρώτος.

9. Στο $Q(\sqrt[3]{6})$ δεμελιώδης μονάδα είναι η $\varepsilon = 1 - 6\sqrt[3]{6} + 3\sqrt[3]{36}$

Έστω $\theta = \sqrt[3]{6}$. Οι αλγεβρικοί συζυγείς του θ είναι $\theta\omega$, $\theta\omega^2$ όπου $\omega = (-1+\sqrt{-3})/2$. Για τυχόν $\alpha \in Q(\theta)$, συμβολίζομε τους συζυγείς του α που αντιστοιχούν στους ισομορφισμούς $\theta \to \theta\omega$, $\theta \to \theta\omega^2$ με α' και α'', αντιστοίχως. Έτσι, ειδικώτερα, $\theta' = \theta\omega$ και $\theta'' = \theta\omega^2$. Σύμφωνα με το θεώρημα του Dirichlet στο $Q(\sqrt[3]{6})$ έχομε μια δεμελιώδη ενάδα, ενώ οι ρίζες του 1 που περιέχονται στο $Q(\sqrt[3]{6})$ είναι ± 1. Αρκεί να δείξομε ότι το ε δεν είναι της μορφής $\pm \eta^\nu$ με $\nu > 1$. Παρατηρούμε ότι αν $\varepsilon = -\eta^\nu$, το $-$ μπορεί ν' "απορροφηθεί" από το η^ν, αν ο ν είναι περιττός. Αν ο ν είναι άρτιος, το $-$ αποκλείεται διότι $\varepsilon > 0$. Συνεπώς, θ' αποκλείσομε τη σχέση $\varepsilon = \eta^\nu$, $\nu > 1$. Έστω ότι ίσχυε μια τέτοια σχέση και $\eta = a + b\theta + c\theta^2$, όπου $a, b, c \in \mathbb{Z}$ (σύμφωνα με το Θ. 12, §3, Κεφ. 1 μια ακέραια βάση είναι η $(1, \theta, \theta^2)$. Τότε

$$\begin{pmatrix} 1 & \theta & \theta^2 \\ 1 & \theta' & \theta'^2 \\ 1 & \theta'' & \theta''^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} \varepsilon^{1/\nu} \\ \varepsilon'^{1/\nu} \\ \varepsilon''^{1/\nu} \end{pmatrix},$$

σύστημα το οποίο προκύπτει από τις σχέσεις $\varepsilon = \eta^\nu$, $\varepsilon' = \eta'^\nu$, $\varepsilon'' = \eta''^\nu$. Οι ν-οστές ρίζες δεν είναι, φυσικά, μονοσήμαντα ορισμένες, όμως αυτό δεν έχει σημασία, όπως θα δούμε. Λύνοντας το σύστημα βρίσκομε

$$c = \frac{1}{\sqrt{D_\theta}} \{ (\theta'' - \theta')\varepsilon^{1/\nu} + (\theta - \theta'')\varepsilon'^{1/\nu} + (\theta' - \theta)\varepsilon''^{1/\nu} \}, \qquad (1)$$

όπου D_θ είναι η διακρίνουσα του θ (η οποία ισούται με το τετράγωνο της ορίζουσας του 3×3 πίνακα στο αριστερό μέλος). Αναλόγως,

$$b = \frac{1}{\sqrt{D_\theta}} \{ \theta(\theta'' - \theta')\varepsilon^{1/\nu} + \theta'(\theta - \theta'')\varepsilon'^{1/\nu} + \theta''(\theta' - \theta)\varepsilon''^{1/\nu} \}. \qquad (2)$$

Είναι, $|\theta| = |\theta'| = |\theta''| = \sqrt[3]{6}$, $|\theta'' - \theta'| = |\theta - \theta'| = |\theta - \theta''| = \sqrt{3}\sqrt[3]{6}$,

$|\sqrt{D_\theta}| = \sqrt{|D_\theta|} = 18\sqrt{3}$, $|\varepsilon'| = |\varepsilon''|$.

Συνεπώς, από τις (1) και (2)

$$|c| < \frac{1}{18\sqrt{3}}\sqrt{3}\sqrt[3]{6}\{|\varepsilon|^{1/\nu}+2|\varepsilon'|^{1/\nu}\} < \frac{\sqrt[3]{6}}{18}\{1+2|\varepsilon'|^{1/\nu}\}$$

και, αναλόγως, $|b| < \frac{\sqrt[3]{36}}{18}\{1+2|\varepsilon'|^{1/\nu}\}$.

Είναι $|\varepsilon'| \leq 326.991$, δπότε αν $\nu \geq 10$ τότε $|c|<1$, $|b|<1$, δηλ. $b=c=0$ και $\eta = \alpha \in \mathbb{Q}$. Επειδή το η είναι ενάδας, έπεται ότι $\eta = \pm 1$, άτοπο. Συνεπώς, μένει ν' αποκλείσουμε την σχέση

$$\varepsilon = \eta^{\nu} \quad \text{για} \quad \nu \leq 10 \ , \qquad (3)$$

δπότε αρκεί ν' αποκλεισθεί η (3) για $\nu = 2, 3, 5, 7$.

Αναλύοντας το 11 σε πρώτα ιδεώδη του $\mathbb{Q}(\sqrt[3]{6})$, σύμφωνα με το Θ11, §7, Κεφ. 3, βλέπουμε ότι έχει ένα πρώτο διαιρέτη $\mathfrak{p}_{11} = (\theta+3, 11)$. Τότε $\theta \equiv -3 \pmod{\mathfrak{p}_{11}}$, δπότε κάθε αλγ. ακέραιος του $\mathbb{Q}(\theta)$ είναι ισοδύναμος mod $\mathfrak{p}_{11}$ με έναν ρητόν ακέραιο. Αμέσως υπολογίζουμε ότι $\varepsilon \equiv 2 \pmod{\mathfrak{p}_{11}}$. Έστω ότι $\eta \equiv n \pmod{\mathfrak{p}_{11}}$, $n \in \mathbb{Z}$. Τότε η (3) συνεπάγεται την

$2 \equiv n^{\nu} \pmod{\mathfrak{p}_{11}}$. Επειδή και στα δύο μέλη έχουμε ρητούς ακεραίους, έπεται ότι $2 \equiv n^{\nu} \pmod{11}$ (Προτιμία στο $\mathbb{Z}$!) άρα $\operatorname{ind} 2 \equiv \nu \operatorname{ind} n \pmod{10}$, δηλ. $1 \equiv \nu \operatorname{ind} n \pmod{10}$, δπότε αποκλείεται να είναι $\nu = 2$ ή 5.

Με αναλογο τρόπο αποκλείουμε την περίπτωση $\nu = 3$ (εδώ $\theta \equiv -2 \pmod{\mathfrak{p}_7}$) και την περίπτωση $\nu = 7$ ($\theta \equiv 4 \pmod{\mathfrak{p}_{29}}$).

10. Στο $\mathbb{Q}(\sqrt[3]{6})$ ο αριθμός κλάσεων είναι 1.

Διατηρώ το συμβολισμό του 9. Σύμφωνα με το Θ.8, §3, Κεφ 4 κάθε κλάση περιέχει ένα ακέραιο ιδεώδες $\mathfrak{b}$ τ.ώ.

$$N(\mathfrak{b}) \leq \frac{2}{\pi}\sqrt{27 \cdot 6^2}$$

(η διακρίνουσα του $\mathbb{Q}(\sqrt[3]{6})$ είναι $-27 \cdot 6^2$, σύμφωνα με το Θ.12, §3, Κεφ. 1), άρα $N(\mathfrak{b}) \leq 19$.

Αρκεί να δείξουμε ότι όλα τα ιδεώδη με norm πρώτο ≤ 19 είναι κύρια:

Είναι φανερό ότι $N(2-\theta) = 2$ άρα $(2-\theta) = \mathfrak{p}_2$. Παρατηρώ ότι $(2-\theta)^3 = 2(1-6\theta+3\theta^2) = 2\varepsilon$, άρα $(2) = \mathfrak{p}_2^3$. Έτσι το

μοναδικό ιδεώδες με norm 2 είναι το $\mathfrak{p}_2$ και είναι κύριο.
Σύμφωνα με το Θ.15, §2, Κεφ.3 υπάρχει ένα μόνο ιδεώδες $\mathfrak{p}_3$ με norm 3. Αφ' ετέρου $N((\theta)) = 6$, δηλαδή $(\theta) = \mathfrak{p}_2\mathfrak{p}_3$ και συνεπώς το $\mathfrak{p}_3$ είναι κύριο. Για τους πρώτους 5, 7, 11, 13, 17, 19 θα κάνουμε χρήση του Θ.11, §7, Κεφ.3: Η ανάλυση του (5) δείχνει ότι υπάρχει ακριβώς ένα πρώτο ιδεώδες $\mathfrak{p}_5$ με norm 5. Αφ' ετέρου $N(-1+\theta) = 5$, άρα $\mathfrak{p}_5 = (-1+\theta)$. Για το 7 έχουμε:
$(7) = \mathfrak{p}_7 \cdot \mathfrak{p}_7' \cdot \mathfrak{p}_7''$, όπου $\mathfrak{p}_7 = (\theta+1, 7) = (1+\theta)$,
$\mathfrak{p}_7' = (\theta+2, 7)$, $\mathfrak{p}_7'' = (\theta-3, 7)$. Όμως $N(2+\theta) = 14$, άρα $(2+\theta) = \mathfrak{p}_2\mathfrak{p}_7'$, δηλαδή το $\mathfrak{p}_7'$ είναι κύριο. Επίσης $N(-3+\theta) = -21$, άρα $(-3+\theta) = \mathfrak{p}_3 \cdot \mathfrak{p}_7''$, δηλαδή και το $\mathfrak{p}_7''$ είναι κύριο.
Το (11) έχει ακριβώς ένα πρωτοβάθμιο πρώτο διαιρέτη $\mathfrak{p}_{11} = (3+\theta, 11)$. Επειδή $N(3+\theta) = 33$, πρέπει $(3+\theta) = \mathfrak{p}_{11}\mathfrak{p}_3$, άρα το $\mathfrak{p}_{11}$ είναι κύριο. Τα (13) και (19) δεν αναλύονται, άρα δεν υπάρχουν ιδεώδη με norm 13 ή 19. Τέλος, τα μοναδικά ιδεώδη με norm 17 είναι τα $\mathfrak{p}_{17} = (\theta-5, 17)$ και $N(\theta-5) = 7 \cdot 17$. Είναι $\theta - 5 \equiv 0 \pmod{\mathfrak{p}_7'}$, άρα $(\theta-5) = \mathfrak{p}_7' \cdot \mathfrak{p}_{17}$, δηλαδή το $\mathfrak{p}_{17}$ είναι κύριο.

II. Η εξίσωση $x^3 + 6y^3 = 10z^3$ είναι αδύνατη.

Προφανώς μπορούμε να υποθέσουμε ότι οι x, y, z ($x \not\equiv 0 \pmod 3$) είναι ανά δύο πρώτοι μεταξύ τους. Τότε, ειδικώτερα, είναι $y \not\equiv 0 \pmod 5$, γ περιττός ($= \text{περιττός}$), $z \not\equiv 0 \pmod 3$. Δουλεύουμε στο $\mathbb{Q}(\theta)$, $\theta = \sqrt[3]{6}$. Η εξίσωση γράφεται
(1) $(x+\theta y)(x^2 - y\theta + y^2\theta^2) = 10z^3$. Έστω $\mathfrak{p}$ κοινός πρώτος διαιρέτης των $(x+\theta y)$, $(x^2 - y\theta + y^2\theta^2) = ((x+\theta y)^2 - 3\theta xy)$. Τότε $\mathfrak{p} \mid 3\theta xy$. Αν $\mathfrak{p} \mid y$ τότε $\mathfrak{p} \mid x$ άρα θα ήταν $(x, y) > 1$ (στο $\mathbb{Z}$), άτοπο. Άρα $\mathfrak{p} \mid (3\theta x) = \mathfrak{p}_3^4 \mathfrak{p}_2 (x)$. Αν $\mathfrak{p} = \mathfrak{p}_3$ τότε $x + \theta y \equiv 0 \pmod{\mathfrak{p}_3}$, άρα $z \equiv 0 \pmod{\mathfrak{p}_3}$, που αντίκειται στη σχέση $z \not\equiv 0 \pmod 3$. Αν $\mathfrak{p} \neq \mathfrak{p}_2$, τότε $\mathfrak{p} \mid x$ και $\mathfrak{p} \nmid \theta$ άρα (λόγω της $\mathfrak{p} \mid x + \theta y$) $\mathfrak{p} \mid y$, δηλαδή τα x, y δεν θα ήταν πρώτα μεταξύ τους. Συνεπώς, η μόνη δυνατότητα είναι $\mathfrak{p} = \mathfrak{p}_2$. Επειδή $N(x+\theta y) = 10z^3$ και z περιττός, έπεται ότι $\mathfrak{p}_2 \mid x + \theta y$ αλλά $\mathfrak{p}_2^2 \nmid x + \theta y$. Επίσης $N(x^2 - y\theta + y^2\theta^2) = (x^3 + 6y^3)^2 = 100z^3$ άρα $\mathfrak{p}_2^2 \mid x^2 - y\theta + y^2\theta^2$. Συνεπώς, λόγω

της (1), $\dfrac{(x+\theta y)}{\rho_2}\,\dfrac{(x^2-\theta y+y^2\theta^2)}{\rho_2^{\,2}} = \rho_5\,\rho_5'\,(z)^3$. (2)

Οι παράγοντες στο αριστερό μέλος είναι πρώτοι μεταξύ τους.
Επίσης, $\rho_5 = (-1+\theta)$, $\rho_5' = \left(\dfrac{5}{-1+\theta}\right) = (1+\theta+\theta^2)$, $N(\rho_5)=5$, $N(\rho_5')=25$

~~[illegible]~~

~~[illegible]~~

Προφανώς αποκλείεται $\rho_5 \mid x+\theta y$ και $\rho_5' \mid x+\theta y$, διότι αυτό θα σήμαινε $x+\theta y \equiv 0 \pmod 5$, οπότε $x \equiv y \equiv 0 \pmod 5$. Επίσης ένας τουλάχιστον απ' τους ρ_5, ρ_5' πρέπει να διαιρεί το $x+\theta y$ διότι $N(x+\theta y) = 10z^3 \equiv 0 \pmod 5$. Συνεπώς απ' τη (2) έπεται

$$(x+\theta y) = \rho_2\,\rho_5\,\alpha^3 \quad ή \quad (x+\theta y) = \rho_2\,\rho_5'\,\alpha^3$$

Άρα

$$(x+\theta y) = (2-\theta)(-1+\theta)\alpha^3 \quad ή \quad (x+\theta y) = (2-\theta)(1+\theta+\theta^2)\alpha^3.$$

Ας θέσουμε $\alpha = (u+v\theta+w\theta^2)$, οπότε (βλ. 9.), (λόγω του 10.)

$$x+\theta y = \pm\varepsilon^j(2-\theta)(-1+\theta)(u+v\theta+w\theta^2)^3 \quad ή \quad \pm\varepsilon^j(2-\theta)(1+\theta+\theta^2)(u+v\theta+w\theta^2)^3, \qquad j\in\mathbb{Z} \quad (3)$$

Παρατηρούμε τώρα ότι $\varepsilon = 1-6\theta+3\theta^2 \equiv 1 \pmod 3$, ενώ $(u+v\theta+w\theta^2)^3 \equiv u^3+v^3\theta^3+w^3\theta^6 \equiv u+6v+36w \equiv u \pmod 3$.

Άρα απ' τις (3),
$$x+\theta y \equiv \pm(2-\theta)(-1+\theta)u \equiv u-u\theta^2$$
$$ή \equiv \pm(2-\theta)(1+\theta+\theta^2)u \equiv -u+u\theta+u\theta^2 \pmod 3$$

Τότε $x\equiv u,\ y\equiv 0,\ 0\equiv -u$
ή $x\equiv -u,\ y\equiv u,\ 0\equiv u$ $\pmod 3$

Και στις δύο περιπτώσεις $x\equiv 0 \pmod 3$, άτοπο.

σύστημα γεννητόρων ($\Phi \neq \varnothing$ διότι $\{0\} \in \Phi$). Ἐξ ὑποθέσεως ὡς ἡ Φ ἔχει maximal στοιχεῖα, ἔστω F. Γιά κάθε $x \in E$ τό $F + Rx$ ἀνήκει στή Φ καί περιέχει τό F, ἄρα, κατ' ἀνάγκη, ταυτίζεται μέ τό F. Ἀλλά $F + Rx = F$ σημαίνει ὅτι $x \in F$. Συμπεραίνομε λοιπόν ὅτι $E \subseteq F$ καί, ἐκ κατασκευῆς τῆς Φ, $F \subseteq E$. Ἄρα $E = F \in \Phi$, ὅπότε τό E ἔχει πεπερασμένο σύστημα γεννητόρων.

(β) $\Rightarrow$ (γ): Ἔστω $(M_n)_{n \geq 0}$ μιά αὔξουσα ἀκολουθία ὑπο-modules τοῦ M. Θά δείξομε ὅτι αὐτή εἶναι σταθερή. Θεωροῦμε τό $E = \bigcup_{n \geq 0} M_n$, τό ὁποῖο εἶναι ὑπο-module τοῦ M καί, συνεπῶς, ἐξ ὑποθέσεως, ἔχει ἕνα πεπερασμένο σύστημα γεννητόρων $x_1, \ldots, x_q$. Ἀλλά τότε, ἀφοῦ ἡ $(M_n)_{n \geq 0}$ εἶναι αὔξουσα, θά ὑπάρχει $n_0 \geq 0$ τέτοιο ὥστε $x_1, \ldots, x_q \in M_{n_0}$, ὅπότε $M_{n_0} = E$. Ἄρα, γιά κάθε $n \geq n_0$, $M_{n_0} \subseteq M_n \subseteq E = M_{n_0}$, δηλ. $M_n = M_{n_0}$, πού ἀποδεικνύει τόν ἰσχυρισμό μας.

(γ) $\Rightarrow$ (α): Ἔστω Φ μιά μή κενή οἰκογένεια ὑπο-modules τοῦ M, ἡ ὁποία δέν ἔχει maximal στοιχεῖο. Θά ὁδηγηθοῦμε σέ ἀντίφαση: Πράγματι, κάτι τέτοιο θά σήμαινε ὅτι γιά κάθε $E \in \Phi$ ὑπάρχει ἕνα module ἀπ' τή Φ, ἔστω $f(E)$, τό ὁποῖο περιέχει γνησίως τό E. Δηλαδή, ὑπάρχει μιά ἀπεικόνιση $f : \Phi \longrightarrow \Phi$ τέτοια ὥστε $f(E) \supsetneq E$.

Μιά καί ἡ Φ δέν εἶναι κενή, ἐκλέγομε τυχόν $E_0 \in \Phi$ καί ὁρίζομε ἀναδρομικά $E_{n+1} = f(E_n)$, $n = 0, 1, 2, \ldots$. Ἀλλά τότε ἡ $(E_n)_{n \geq 0}$ εἶναι μιά γνησίως αὔξουσα ἀκολουθία ὑπο-modules τοῦ M καί, συνεπῶς, δέν εἶναι δυνατόν νά εἶναι σταθερή, ἀντιφάσκοντας ἔτσι στήν ὑπόθεση.

<u>Ὁρισμός</u>. Ἔστω R δακτύλιος καί M ἕνα R-module τό ὁποῖο ἱκανοποιεῖ μιά ἀπ' τίς ἰσοδύναμες συνθῆκες τοῦ θεωρήματος 1. Τό M λέγεται module τῆς Noether (πρός τιμήν τῆς Emmy Noether). Ὁ δακτύλιος R λέγεται δακτύλιος τῆς Noether ἄν, θεωρούμενος ὡς R-module

είναι module της Noether.

Θεώρημα 2. Κάθε κύριος δακτύλιος είναι δακτύλιος της Noether.

Απόδειξη. Έστω R κύριος δακτύλιος. Τά R-υπο-modules του R είναι, ακριβώς, τά ιδεώδη του R και, εξ υποθέσεως, καθένα διαθέτει πεπερασμένο σύστημα γεννητόρων (ένα γεννήτορα), δ.έ.δ.

Θεώρημα 3. Έστω R ένας δακτύλιος, M ένα R-module και M' ένα υπο-module του M. Για να είναι τό M module της Noether πρέπει και άρκει τά M' και M/M' να είναι modules της Noether.

Απόδειξη. Έστω ότι τό M είναι module της Noether. Θεωρούμε ένα υπο-module M' του M. Η τυχούσα μή κενή οικογένεια υπο-modules του M' μπορεί να θεωρηθεί ως οικογένεια υπο-modules του M, άρα έχει maximal στοιχείο. Συνεπώς τό M' είναι module της Noether. Όσον αφορά στό M/M', είναι απλό να 'δεί κανείς ότι τά υπο-modules αυτού του module είναι ακριβώς τά "πηλίκα" E/M', όπου E ⊇ M' είναι υπο-module του M. Άν, λοιπόν, Φ είναι μιά μή κενή οικογένεια υπο-modules του M/M', τότε σ' αυτήν αντιστοιχεί μιά μή κενή οικογένεια Ψ υπο-modules του M, η οποία προκύπτει άν "διώξομε τόν παρονομαστή M'". Δηλαδή,

$$\Phi \ni E/M' \longmapsto E \in \Psi \quad , \quad M' \subseteq E \subseteq M$$

E υπο-module του M.

Η Ψ, ως οικογένεια υπο-modules του M έχει maximal στοιχείο, έστω M_0. Ο ισχυρισμός τώρα είναι ότι τό module $M_0/M' \in \Phi$ είναι maximal στοιχείο του Φ. Πράγματι, υποθέτοντας τό αντίθετο, άς θεωρήσομε $M_1/M' \in \Phi$, τέτοιο ώστε $M_1/M' \supsetneq M_0/M'$. Τότε, για κάθε $x \in M_0$,

$x+M' \in M_1/M'$, ἄρα ὑπάρχει $y \in M_1$ τέτοιο ὥστε $x+M'=y+M'$. Ἄρα $x \in y+M' \subseteq M_1$ καί, συνεπῶς, $M_0 \subseteq M_1$. Ἐπειδή $M_1 \in \Psi$ καί τό M_0 εἶναι maximal στοιχεῖο τῆς Ψ, ἔπεται ὅτι $M_0 = M_1$, γεγονός πού ἀντιβαίνει στή σχέση $M_1/M' \neq M_0/M'$. Ἀντιστρόφως, ἄς ὑποθέσουμε ὅτι τό M' εἶναι ὑπο-module τοῦ R-module M καί τό M', καθώς καί τό M/M' εἶναι modules τῆς Noether. Θ' ἀποδείξουμε ὅτι καί τό M εἶναι module τῆς Noether, δείχνοντας ὅτι ἱκανοποιεῖ τή συνθήκη (μ) τοῦ θεωρήματος 1: Ἔστω $(E_n)_{n\geq 0}$ αὔξουσα ἀκολουθία ὑπο-modules τοῦ M. Τότε ἡ $(E_n \cap M')_{n\geq 0}$ εἶναι αὔξουσα ἀκολουθία ὑπο-modules τοῦ M', ἄρα εἶναι σταθερή, ἔστω ἀπ' τό δείκτη n_1 καί μετά. Ἐπίσης ἡ ἀκολουθία $\{(E_n+M')/M'\}_{n\geq 0}$ εἶναι αὔξουσα ἀκολουθία ὑπο-modules τοῦ M/M'. ἄρα εἶναι σταθερή ἀπό τό δείκτη n_2, ἔστω, καί μετά. Θέτουμε $n_0 = \max\{n_1, n_2\}$ καί θα' δείξουμε ὅτι $E_n = E_{n_0}$ γιά κάθε $n \geq n_0$. Προφανῶς, ἀρκεῖ νά δείξουμε ὅτι $E_{n_0+1} \subseteq E_{n_0}$. Ἔστω λοιπόν $x \in E_{n_0+1}$. Ἀπ' τή σχέση $(E_{n_0+1}+M')/M' = (E_{n_0}+M')/M'$ συμπεραίνουμε ὅτι ἄν πάρουμε κυρίως $m_1 \in M'$ θα' ἔχουμε $x+m_1 = y+m_2$ γιά κατάλληλα $y \in E_{n_0}$ καί $m_2 \in M'$. Συνεπῶς τό στοιχεῖο $x-y = m_2-m_1$ ἀνήκει συχρόνως στό E_{n_0+1} καί στό M' ἄρα στό $E_{n_0+1} \cap M' = E_{n_0} \cap M'$. Ἔστι $x-y \in E_{n_0}$, ἀπ' ὅπου $x \in E_{n_0}$, ὅ.ἐ.δ.

Θεώρημα 4. Ἔστω R δακτύλιος καί $E_1, \dots, E_m$ R-modules τῆς Noether. Τότε, τό R-module $\prod_{i=1}^{m} E_i$ εἶναι module τῆς Noether.

Ἀπόδειξη. Ἀρκεῖ ν' ἀποδείξουμε τό θεώρημα γιά $m=2$: Τό E_1 εἶναι ἰσόμορφο μέ τό $E_1 \times \{0\}$, πού εἶναι ὑπο-module τοῦ $E_1 \times E_2$. Τό module $(E_1 \times E_2)/(E_1 \times \{0\})$ εἶναι ἰσόμορφο μέ τό E_2 (μέσω τῆς ἀπεικόνισης $(E_1 \times E_2)/(E_1 \times \{0\}) \ni (x_1, x_2) + (E_1 \times \{0\}) \longrightarrow x_2 \in E_2$). Ἐφαρμόζοντας, λοιπόν, τό θεώρημα 3 μέ τό $E_1 \times E_2$ στή θέση τοῦ M καί τό $E_1 \times \{0\}$ στή θέση τοῦ M', συμπεραίνουμε ὅτι

τό $E_1 \times E_2$ εἶναι module τῆς Noether.

Θεώρημα 5. Ἔστω R δακτύλιος τῆς Noether καί M ἕνα R-module μέ πεπερασμένο σύστημα γεννητόρων. Τότε τό M εἶναι module τῆς Noether.

Ἀπόδειξη. Ἔστω $e_1, \dots, e_m$ ἕνα σύστημα γεννητόρων τοῦ M. Θεωροῦμε τόν ἐπιμορφισμό τῶν R-modules

$$R^m \ni (x_1, \dots, x_m) \xrightarrow{\Phi} x_1 e_1 + \dots + x_m e_m \in M$$

Σύμφωνα μέ τό Θεώρημα 4 τό R^m εἶναι module τῆς Noether, ἄρα καί τό $R^m/\mathrm{Ker}\Phi$ εἶναι module τῆς Noether, ἀπ' τό Θεώρημα 3. Ἀλλά τό $R^m/\mathrm{Ker}\Phi$ εἶναι ἰσόμορφο μέ τό M, ὅ. ἐ. δ.

Τέλος, ἔχομε τό βασικό συμπέρασμα αὐτοῦ τοῦ κεφαλαίου:

Θεώρημα 6. Ἄν τό K εἶναι ἕνα ἀριθμητικό σῶμα καί A δ. δακτύλιος τῶν ἀκεραίων του, τότε ὁ A εἶναι δακτύλιος τῆς Noether.

Ἀπόδειξη.* Ὁ $\mathbb{Z}$, ὡς κύριος δακτύλιος, εἶναι δακτύλιος τῆς Noether (Θεώρημα 2). Ὁ A εἶναι $\mathbb{Z}$-module μέ πεπερασμένο σύστημα γεννητόρων (Θεώρημα 9, Κεφάλαιο 1), ἄρα $\mathbb{Z}$-module τῆς Noether (Θεώρημα 5). Ἔστω τώρα Φ μιά μή κενή οἰκογένεια A-ὑπο-modules τοῦ A (ὁ A θεωρεῖται τώρα ὡς A-module), δηλαδή ἡ Φ εἶναι μή κενή οἰκογένεια ἰδεωδῶν τοῦ A καί τό ἰδεώδη τοῦ A εἶναι εἰδική περίπτωση $\mathbb{Z}$-ὑπο-modules τοῦ $\mathbb{Z}$-module A, τό ὁποῖο, ὅπως εἴπαμε παραπάνω, εἶναι module τῆς Noether. Ἄρα ἡ Φ ἔχει maximal στοιχεῖο, ἄρα ὁ A, θεωρούμενος ὡς A-module, εἶναι module τῆς Noether, δηλαδή, ἐξ ὁρισμοῦ, εἶναι δακτύλιος τῆς Noether.

* Γιά μιά διαφορετική ἀπόδειξη βλ. σελ. 20α

Άλλη απόδειξη του Θεωρήματος 6

Είναι καλό ν' αποδειχθεί το έξης λήμμα: Αν R είναι δακτύλιος του δακτυλίου A, τότε κάθε A-module είναι και R-module. Επιπλέον, αν το A-module M, θεωρούμενο ως R-module είναι module της Noether, τότε και το A-module είναι της Noether.

(Απόδειξη του λήμματος με χρήση του Θεωρήματος 1(γ))

Ερχόμαστε τώρα στην κυρίως απόδειξη. Ο $\mathbb{Z}$ είναι δακτύλιος Noether (Θεώρημα 2) και ο A είναι $\mathbb{Z}$-module με πεπερασμένο σύστημα γεννητόρων (Θεώρημα 3, Κεφ. 1) άρα, ο A είναι $\mathbb{Z}$-module Noether (Θεώρημα 5). Από το παραπάνω λήμμα είναι και A-module Noether, δηλ. δακτύλιος Noether.

ΚΕΦΑΛΑΙΟ 3
Η Αριθμητική των ιδεωδών

1. Πρώτα και maximal ιδεώδη

Έστω A δακτύλιος και $\mathfrak{p} \neq A$ ιδεώδες του A. Θεωρούμε γνωστή την ισοδυναμία των παρακάτω συνθηκών, οι οποίες χαρακτηρίζουν πότε το $\mathfrak{p}$ είναι πρώτο ιδεώδες:

α) Αν a, b είναι ιδεώδη του A και $ab \subseteq \mathfrak{p}$, τότε $a \subseteq \mathfrak{p}$ είτε $b \subseteq \mathfrak{p}$.

β) Αν $x, y \in A$ και $xy \in \mathfrak{p}$ τότε $x \in \mathfrak{p}$ είτε $y \in \mathfrak{p}$.

γ) Το σύνολο $A - \mathfrak{p}$ είναι κλειστό ως προς τον πολλαπλασιασμό.

δ) Ο δακτύλιος $A/\mathfrak{p}$ είναι ακέραια περιοχή.

Θεωρούμε, επίσης, γνωστή την ισοδυναμία των παρακάτω συνθηκών, οι οποίες χαρακτηρίζουν πότε τα $\mathfrak{p}$ είναι maximal ιδεώδες:

α) Το $\mathfrak{p}$ δεν περιέχεται γνησίως σε κανένα ιδεώδες του A διαφορετικό από το A.

β) Ο δακτύλιος $A/\mathfrak{p}$ είναι σώμα.

Συμπεραίνομε λοιπόν ότι κάθε maximal ιδεώδες είναι πρώτο. Το αντίστροφο δεν ισχύει, εν γένει, όπως φαίνεται αν πάρομε $A = \mathbb{Z}[t]$ και $\mathfrak{p} = (t)$, οπότε το (t) είναι, προφανώς, πρώτο ιδεώδες, όχι όμως και maximal, αφού $(t) \subsetneq (t) + (c) \subsetneq \mathbb{Z}[t]$, αν $c \in \mathbb{Z} - \{0\}$.

<u>Λήμμα 1</u>. Αν A' είναι υποδακτύλιος του δακτυλίου A και το $\mathfrak{p}$ είναι πρώτο ιδεώδες του A, τότε το $\mathfrak{p} \cap A'$ είναι πρώτο ιδεώδες του A'.

Απόδειξη. Υπάρχει ένας προφανής δομομορφισμός $A' \longrightarrow A/\mathfrak{p}$ (σύνθεση των δομομορφισμών $A' \to A$, $A \to A/\mathfrak{p}$) με πυρήνα το $A' \cap \mathfrak{p}$. Άρα ο δακτύλιος $A'/A' \cap \mathfrak{p}$ είναι

ισόμορφος μ' έναν δακτύλιο του $A/\mathfrak{p}$, άρα είναι ακέραια περιοχή, δ.ε.δ.

Λήμμα 2. Άν ένας δακτύλιος της Noether δέν είναι σώμα, τότε περιέχει ένα maximal (άρα και πρώτο) ιδεώδες, μή μηδενικό.

Απόδειξη. Έστω A ένας τέτοιος δακτύλιος. Επιλέγομε ένα $a \in A$, $a \neq 0$, το οποίο δέν έχει αντίστροφο στόν A. Τότε $(a) \subsetneq A$, άρα ή οικογένεια $\Phi = \{ I \text{ ιδεώδες του } A : (a) \subseteq I \subsetneq A \}$ είναι μή κενή, άρα έχει ένα maximal στοιχείο, έστω m. Προφανώς το m είναι maximal ιδεώδες του A και μή μηδενικό, δ.ε.δ.

Λήμμα 3 Άν ή ακέραια περιοχή A είναι δακτύλιος της Noether, τότε κάθε ιδεώδες $\neq (0)$ περιέχει ένα μή μηδενικό γινόμενο πρώτων ιδεωδών. (Υποτίθεται ότι ή A δέν είναι σώμα).

Απόδειξη. Έστω Φ ή οικογένεια των μή μηδενικών ιδεωδών του A, για τά οποία δέν αληθεύει ή συνθήκη του λήμματος. Άν $\Phi \neq \phi$, έστω m το maximal στοιχείο της Φ. Το m δέν είναι πρώτο γιατί, άν ήταν, δέν θ' ανήκε στη Φ (αφού θα' περιείχε ένα μή μηδενικό γινόμενο πρώτων ιδεωδών : το ίδιο το m). Επίσης $m \neq A$, αφού το ιδεώδες A περιέχει κάποιο μή μηδενικό πρώτο ιδεώδες (Λήμμα 2) και, συνεπώς, δέν ανήκει στη Φ. Άρα, υπάρχουν $a, b \in A$, τέτοια ώστε $a \notin m$, $b \notin m$ και $ab \in m$. Επειδή τά $m+(a)$ και $m+(b)$ περιέχουν γνησίως το m, είναι αδύνατον ν' ανήκουν στή Φ, δπότε $m+(a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_\nu$, $m+(b) \supseteq \mathfrak{p}_{\nu+1} \cdots \mathfrak{p}_\mu$, όπου στα δεξιά μέλη έχομε μή μηδενικά γινόμενα πρώτων ιδεωδών. Τότε, $m = (m+(a)) \cdot (m+(b)) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_\nu \mathfrak{p}_{\nu+1} \cdots \mathfrak{p}_\mu$ και το τελευταίο γινόμενο ιδεωδών δέν είναι μηδενικό, αφού ο A είναι ακέραια περιοχή. Η τελευταία σχέση, όμως, έρχεται σε αντίφαση μέ την $m \in \Phi$, άρα $\Phi = \phi$, δ.ε.δ.

2. Κλασματικά ἰδεώδη.

Ὁρισμός. Ἔστω A ἀκέραια περιοχή καί K τό σῶμα πηλίκων της. Τό $I \subseteq K$ λέγεται κλασματικό ἰδεώδες τῆς A ἄν εἶναι A-υπο-module τοῦ K μέ τήν ἐπιπλέον ἰδιότητα ὅτι ὑπάρχει $d \in A$, $d \neq 0$ τέτοιο ὥστε $d \cdot I \subseteq A$ (δηλαδή, τά στοιχεῖα τοῦ I ἔχουν κοινό παρονομαστή ἀπ' τό A). Ἰσοδύναμα, τό $I \subseteq K$ λέγεται κλασματικό ἰδεώδες τοῦ A, ἄν $\exists\, d \in A$, $d \neq 0$, τέτοιο ὥστε τό dI νά εἶναι ἰδεώδες τοῦ A, ὑπό τήν συνήθη ἔννοια.

α) Μιά σημαντική κατηγορία κλασματικῶν ἰδεωδῶν τῆς A εἶναι τά ἰδεώδη $(\gamma) = \{\alpha\gamma \,/\, \alpha \in A\}$, ὅπου $\gamma \in K$. Τά ἰδεώδη αὐτῆς τῆς μορφῆς λέγονται κύρια (κλασματικά) ἰδεώδη τῆς A.

β) Τά μέ τή συνηθισμένη ἔννοια ἰδεώδη τῆς A εἶναι, προφανῶς, κλασματικά ἰδεώδη τῆς A, τά ὁποῖα, συνήθως, χαρακτηρίζονται "ἀκέραια ἰδεώδη τῆς A" (ἐδῶ, ὡς κοινό παρονομαστή μποροῦμε νά πάρουμε τό $1 \in A$).

γ) Κάθε A-υπο-module τοῦ K, πού ἔχει πεπερασμένο πλῆθος γεννητόρων, εἶναι κλασματικό ἰδεώδες τῆς A, διατί ὁ κοινός παρονομαστής τῶν γεννητόρων εἶναι καί κοινός παρονομαστής ὅλων τῶν στοιχείων αὐτοῦ τοῦ module.

δ) Ἄν ὁ A εἶναι δακτύλιος τῆς Noether, τότε ἰσχύει καί τό ἀντίστροφο: δηλαδή, κάθε κλασματικό ἰδεώδες I, θεωρούμενο ὡς A-module ἔχει πεπερασμένο πλῆθος γεννητόρων. Διατί, ἄν $dI \subseteq A$, τότε $I \subseteq d^{-1}A$ καί τά A-modules $d^{-1}A$ καί A εἶναι ἰσόμορφα. Ἄρα τό I εἶναι A-υπο-module ἑνός A-module τῆς Noether καί, συνεπῶς, ἔχει πεπερασμένο σύστημα γεννητόρων (Θεώρημα 1(β), Κεφάλαιο 2).

ε) Τό ἄθροισμα καί τό γινόμενο δύο (ἤ περισσοτέρων) κλασματικῶν ἰδεωδῶν τῆς A δρίζεται κατ' ἀναλογία πρός τό ἄθροισμα καί τό γινόμενο τῶν ἀκεραίων ἰδεωδῶν τῆς A. Ἄν τά I, I' εἶναι κλασματικά ἰδεώδη τῆς A, τό ἴδιο ἰσχύει καί γιά τά $I \cap I'$, $I + I'$, $I \cdot I'$, διατί, ἄν d, d' εἶναι οἱ κοινοί παρονομαστές τῶν d, d', ἀντιστοίχως, τότε τά

$I \cap I'$, $I + I'$, $I \cdot I'$ ἔχουν ὡς κοινό παρονομαστή τό dd'.

5.) Τό σύνολο τῶν μή μηδενικῶν κλασματικῶν ἰδεωδῶν τῆς A ἀποτελεῖ, ἐφοδιασμένο μέ τόν πολλαπλασιασμό, ἕνα ἀντιμεταθετικό μονοειδές.

3. Ἡ μονότροπη ἀνάλυση τῶν μή μηδενικῶν ἰδεωδῶν ἑνός δακτυλίου τοῦ Dedekind σέ γινόμενο πρώτων ἰδεωδῶν.

Ὁρισμός. Ὁ δακτύλιος A λέγεται δακτύλιος τοῦ Dedekind, ἄν εἶναι τῆς Noether, ἀκέραια κλειστός καί κάθε πρῶτο μή μηδενικό ἀκέραιο ἰδεῶδες τοῦ A εἶναι maximal.

Θεώρημα 1. Ὁ δακτύλιος τῶν ἀκεραίων ἑνός ἀριθμητικοῦ σώματος εἶναι δακτύλιος τοῦ Dedekind.

Ἀπόδειξη. Ἔστω K ἀριθμητικό σῶμα καί A ὁ δακτύλιος τῶν ἀκεραίων του. Ὁ A εἶναι ἀκέραια κλειστός (Θεώρημα 6, Κεφάλαιο 1) καί δακτύλιος τῆς Noether (Θεώρημα 6, Κεφάλαιο 2). Ἔστω τώρα πρῶτο ἰδεῶδες $\mathfrak{p} \neq (0)$ τοῦ A. Ἔστω $x \in \mathfrak{p}$, $x \neq 0$. Ἀφοῦ $x \in A$, θά ἰσχύει μιά σχέση τῆς μορφῆς $x^m = a_{m-1}x^{m-1} + \dots + a_1 x + a_0$, $a_0 \neq 0$. Λύνοντας ὡς πρός a_0 βλέπομε ὅτι $a_0 \in (x) \cap \mathbb{Z} \subseteq \mathfrak{p} \cap \mathbb{Z}$, ἄρα $\mathfrak{p} \cap \mathbb{Z} \neq (0)$. Ἐπιπλέον τό $\mathfrak{p} \cap \mathbb{Z}$ εἶναι πρῶτο ἰδεῶδες τοῦ $\mathbb{Z}$ (Λῆμμα 1), ἄρα θά εἶναι τῆς μορφῆς $p\mathbb{Z}$ μέ $p \in \mathbb{Z}$ πρῶτο ἀριθμό. Μποροῦμε τώρα νά ἐμφυτεύσομε τό σῶμα $\mathbb{Z}/p\mathbb{Z}$ στό δακτύλιο $A/\mathfrak{p}$ μέσῳ τῆς ἀπεικόνισης

$$\mathbb{Z}/p\mathbb{Z} \ni a + p\mathbb{Z} \longrightarrow a + \mathfrak{p} \in A/\mathfrak{p} .$$

Ἔτσι, μποροῦμε νά θεωρήσομε τό σῶμα $\mathbb{Z}/p\mathbb{Z}$ ὑποδακτύλιο τοῦ δακτυλίου $A/\mathfrak{p}$ καί παρατηροῦμε ὅτι ὅλα τά στοιχεῖα τοῦ $A/\mathfrak{p}$ εἶναι ἀκέραια πάνω ἀπ' τό $\mathbb{Z}/p\mathbb{Z}$ (ἀφοῦ ὅλα τά στοιχεῖα τοῦ A εἶναι ἀκέραια πάνω ἀπ' τό $\mathbb{Z}$), ἄρα ὁ $A/\mathfrak{p}$ εἶναι σῶμα, βάσει τοῦ ἑπομένου γενικοῦ λήμματος: Ἄν τό σῶμα S εἶναι ὑποδακτύλιος τοῦ δακτυλίου R καί

, όλα τα στοιχεία του R είναι αλγεβρικά πάνω απ' το S, τότε ο R είναι σώμα : Πράγματι, αρκεί να δείξομε ότι το τυχόν $x \in R - \{0\}$ έχει αντίστροφο. Θεωρούμε την επέκταση $S(x)$ του S, η οποία είναι πεπερασμένη, εξ υποθέσεως. Τότε, ο γραμμικός μετασχηματισμός του διανυσματικού χώρου $S(x)$, που ορίζεται : $S(x) \ni y \longrightarrow xy \in S(x)$, ως αμφιμονοσήμαντος είναι και "επί" ($S(x)$ είναι πεπερασμένης διάστασης S-διανυσματικός χώρος). Ειδικώτερα, υπάρχει $y \in S(x)$ ($\acute{\alpha}\rho\alpha\ y \in R$) τέτοιο ώστε $xy = 1$, ό.έ.δ.

Στα παρακάτω και μέχρι το τέλος της §3, ο A θα είναι ένας δακτύλιος του Dedekind, αλλ' όχι σώμα ακέραια περιοχή, και K το σώμα πηλίκων του. Οι έννοιες μη μηδενικό πρώτο ιδεώδες και maximal ιδεώδες είναι τώρα ισοδύναμες.

<u>Θεώρημα 2</u>. Κάθε μη μηδενικό πρώτο ακέραιο ιδεώδες του A είναι αντιστρεπτό στο μονοειδές των μη μηδενικών κλασματικών ιδεωδών του A. (Στο μονοειδές αυτό, η μονάδα είναι το ιδεώδες A).

Απόδειξη. Έστω $\mathfrak{p} \neq (0)$ πρώτο ιδεώδες του A και

$$\mathfrak{p}' = \{x \in K : x\mathfrak{p} \subseteq A\} \qquad (1)$$

Το $\mathfrak{p}'$ είναι A-υπο-module του K και για τυχόν $d \in \mathfrak{p} - \{0\}$ ισχύει $d\mathfrak{p}' \subseteq A$, όπότε το $\mathfrak{p}'$ είναι ένα κλασματικό ιδεώδες του A. Αρκεί λοιπόν ν' αποδείξομε ότι $\mathfrak{p} \cdot \mathfrak{p}' = A$. Απ' την (1) είναι φανερό ότι $\mathfrak{p} \cdot \mathfrak{p}' \subseteq A$ καθώς και $A \subseteq \mathfrak{p}'$, άρα $\mathfrak{p} = A \cdot \mathfrak{p} \subseteq \mathfrak{p}'\mathfrak{p} \subseteq A$. Όμως το $\mathfrak{p}$ είναι maximal οπότε $\mathfrak{p}' \cdot \mathfrak{p} = A$ είτε $\mathfrak{p}' \cdot \mathfrak{p} = \mathfrak{p}$. Αρκεί ν' αποκλείσομε την τελευταία σχέση. Έστω λοιπόν ότι αυτή ίσχυε. Τότε, για τυχόν $x \in \mathfrak{p}'$ θα είχαμε $x\mathfrak{p} \subseteq \mathfrak{p}$ και επαγωγικά $x^n\mathfrak{p} \subseteq \mathfrak{p}$ ($n = 1, 2, \ldots$), άρα ο δακτύλιος $A[x]$ είναι ένα κλασματικό ιδεώδες του A (ως κοινό παρονομαστή των στοιχείων του αρκεί να πάρομε οποιοδήποτε μη μηδενικό στοιχείο του $\mathfrak{p}$), άρα ο $A[x]$ είναι ένα A-module με πεπερασμένο σύστημα γεν-

νητόρων (§2, (δ)), δπότε τό x είναι ἀκέραιο πάνω ἀπ' τόν A (Θεώρημα 1, κεφάλαιο 1). Ἐπειδή ὁ A εἶναι ἀλγεβρικά κλειστός, ἕπεται ὅτι $x \in A$, καί μιά καί τό $x \notin p'$ εἶναι τυχαῖο, $p' \subseteq A$, ἄρα $p' = A$. Μένει νά δείξομε ὅτι ἡ τελευταία ἰσότητα εἶναι ἀδύνατη. Ἔστω ὅτι ἴσχυε κι ἄς θεωρήσομε $a \notin p = \{0\}$. Ἀπ' τό Λῆμμα 3, τό (a) περιέχει ἕνα μή μηδενικό γινόμενο $p_1 p_2 \cdots p_n$ πρώτων ἰδεωδῶν καί, δίχως βλάβη τῆς γενικότητας, ἄς ὑποθέσομε ὅτι τό n εἶναι τό ἐλάχιστο δυνατό. Ἔχομε τώρα $p \supseteq (a) \supseteq p_1 \cdots p_n$, ἄρα, ἀφοῦ τό p εἶναι πρῶτο, ἕνα τοὐλάχιστον ἀπ' τά $p_1, \ldots, p_n$ περιέχεται στό p. Ἔστω $p_1 \subseteq p$. Τό p_1 εἶναι maximal, ἄρα $p_1 = p$. Ἄς θέσομε $b = p_2 \cdots p_n$ (ἐννοεῖται ὅτι $b \neq A$ ἄν $n = 1$).

Τότε $(a) \supseteq p \cdot b$, ἐνῶ $(a) \not\supseteq b$, λόγῳ τῆς ἐκλογῆς τοῦ n (ἄν $b = A$, τότε $(a) \supseteq p$, δηλ. $(a) = p$ καί σ' αὐτή τήν περίπτωση ἀντίστροφο τοῦ p εἶναι, προφανῶς, τό κλασματικό ἰδεῶδες $(\frac{1}{a}) = \frac{1}{a} A$). Ἄρα ὑπάρχει $b \in b$ τέτοιο ὥστε $b \notin (a)$. Ὅμως $(a) \supseteq p \cdot (b)$, ἄρα $bp \subseteq (a)$, δπότε καί $ba^{-1} p \subseteq A$. Ἀπ' τήν (1) τότε, $ba^{-1} \in p'$. Ἀφ' ἑτέρου, $b \notin (a)$ δπότε $ba^{-1} \notin A$, ἄρα ἀποκλείεται νά ἰσχύει $p' = A$, ὅ.ἐ.δ.

Σύμφωνα μέ τό Θεώρημα 2, γιά ἕνα μή μηδενικό πρῶτο (ἀκέραιο) ἰδεῶδες p τοῦ A ἔχει νόημα ἡ ἔκφραση $p^{-n} \stackrel{\text{ορ}}{=} (p^{-1})^n$ $(n = 1, 2, 3, \ldots)$. Ἐπίσης, ὁρίζομε $p^0 = A$. Τώρα εἴμαστε σέ θέση ν' ἀποδείξομε τό θεμελιῶδες

<u>Θεώρημα 3.</u> Ἔστω P τό σύνολο τῶν μή μηδενικῶν πρώτων ἰδεωδῶν τοῦ A. Τότε:
α) Κάθε μή μηδενικό κλασματικό ἰδεῶδες a τοῦ A ἀναλύεται μονότροπα σέ γινόμενο πρώτων ἰδεωδῶν (παραβλέποντας τή διάταξη στό γινόμενο):

$$a = \prod_{p \in P} p^{\nu_p(a)}, \quad \nu_p(a) \in \mathbb{Z}, \qquad (2)$$

ὅπου οἱ ἐκθέτες $\nu_p(\alpha)$ εἶναι σχεδὸν ὅλοι μηδέν.

β) Τὸ μονοειδὲς τῶν μὴ μηδενικῶν πλασματικῶν ἰδεωδῶν τοῦ A εἶναι ἀβελιανὴ ὁμάδα ὡς πρὸς τὸν πολλαπλασιασμό.

Ἀπόδειξη(α) Ἔστω d ὁ κοινὸς παραγοντὴς τῶν στοιχείων τοῦ α. Τότε $d\alpha \subseteq A$, ἄρα $\alpha = d\alpha \cdot (d^{-1}) = d\alpha \cdot (d)^{-1}$ καὶ τὰ $d\alpha$, (d) εἶναι ἀκέραια ἰδεώδη τοῦ A. Συνεπῶς, ἀρκεῖ ν' ἀποδείξουμε τὸν ἰσχυρισμὸ (α) στὴν περίπτωση κατὰ τὴν ὁποία τὰ α εἶναι ἀκέραιο ἰδεώδες. Σ' αὐτὴ τὴν περίπτωση, ἔστω Φ ἡ οἰκογένεια τῶν μὴ μηδενικῶν ἀκεραίων ἰδεωδῶν τοῦ A, τὰ ὁποῖα δὲν εἶναι ἴσα μὲ κάποιο γινόμενο μὴ μηδενικῶν πρώτων ἰδεωδῶν τοῦ A κι ἂς ὑποθέσουμε τὴ Φ μὴ κενή. Τότε ἡ Φ θὰ ἔχει κάποιο maximal σ' αὐτὴν στοιχεῖο α. Εἶναι $\alpha \neq A$, διότι ὁ ἰσχυρισμὸς (α) ἀληθεύει γιὰ $\alpha = A$ (σ' αὐτὴν τὴν περίπτωση ὅλα τὰ $\nu_p(\alpha)$ εἶναι μηδὲν στὴ (2)). Θεωροῦμε ἐπίσης τὴν οἰκογένεια Ψ τῶν μὴ τετριμμένων (ἀκεραίων) ἰδεωδῶν τοῦ A, ποὺ περιέχουν τὸ α καὶ ἔστω γιὰ ἕνα maximal στὴν Ψ στοιχεῖο. Τὸ p εἶναι, προφανῶς, maximal καὶ μεταξὺ τῶν ἀκεραίων ἰδεωδῶν τοῦ A, ἄρα εἶναι πρῶτο, μὴ μηδενικό. Ἔστω p' τὸ ἀντίστροφο (πλασματικό) ἰδεώδες τοῦ p (Θεώρημα 2). Ἐξ ὑποθέσεως $\alpha \subseteq p$, ἄρα $\alpha p' \subseteq p \cdot p' = A$. Ἐπίσης $A = p \cdot p' \subseteq p \cap p' \subseteq p'$, ἄρα $\alpha = \alpha A \subseteq \alpha p'$. Συνεπῶς

$$\alpha \subseteq \alpha p' \subseteq A \qquad (3)$$

Ἐπίσης

$$\alpha \neq \alpha p' \qquad (4)$$

Πράγματι, ἂν δὲν ἴσχυε ἡ (4), τότε, γιὰ $x \in p'$ καὶ $n = 1, 2, \ldots$, θὰ εἴχαμε $x^n \alpha \subseteq \alpha$ καὶ θὰ συμπεραίναμε (ὅπως καὶ στὴν ἀπόδειξη τοῦ θεωρήματος 2) ὅτι $x \in A$ καὶ, κατ' συνέπεια, $p' = A$, ὅπότε $p = pA = pp' = A$, ποὺ ἀντίκειται στὴν ὑπόθεση ὅτι τὸ p δὲν εἶναι τετριμμένο. Ἀπ' τὶς (3) καὶ (4), τώρα, καὶ τὸ γεγονὸς ὅτι τὸ α εἶναι maximal στὴ Φ, συμπεραίνουμε ὅτι $\alpha p' \notin \Phi$, ἄρα ὑπάρχουν $p_1, \ldots, p_n \in P$ εἰς τρόπον ὥστε

$\alpha = \alpha p' = p_1 \cdots p_n$, άρα $\alpha = \alpha p' p = p_1 \cdots p_n p$, άτοπο αφού $\alpha \in \Phi$.
Συνεπώς αποδείχτηκε η δυνατότητα ανάλυσης όπως στη σχέση (2).
Για τη μοναδικότητα αυτής της ανάλυσης: Έστω ότι είχαμε δύο αναλύσεις του ίδιου κλασματικού ειδεώδους

$$\prod_{p \in P} p^{\nu_p} = \prod_{p \in P} p^{\nu'_p}, \text{ όπότε } \prod_{p \in P} p^{\nu_p - \nu'_p} = A$$

Αν δεν ήταν όλοι οι εκθέτες $\nu_p = \nu'_p$ μηδέν, τότε θα είχαμε, χωρίζοντας τους θετικούς από τους αρνητικούς εκθέτες, μια σχέση της μορφής

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} = p_{r+1}^{\alpha_{r+1}} \cdots p_k^{\alpha_k},$$

όπου $p_1, \ldots, p_k \in P$, $r \geq 1$, $k \geq r$, $\alpha_1, \ldots, \alpha_k > 0$ και τα $p_1, \ldots, p_k$ διαφορετικά ανά δύο (αν $k = r$ το δεξιό μέλος εννοείται ίσο με A). Τότε το p_1 περιέχει το δεξιό μέλος, άρα ένα τουλάχιστον πρώτο ιδεώδες από τα $p_{r+1}, \ldots, p_k$ (αν το δεξιό μέλος ισούται με A, τότε $p_1 \supseteq A$), λ.χ. το p_{r+1}.
Αλλά το p_{r+1} είναι maximal άρα $p_1 = p_{r+1}$ (αντιστοίχως, $p_1 = A$), άτοπο.

β) Η (2) δείχνει ότι το αντίστροφο του α είναι το ιδεώδες

$$\prod_{p \in P} p^{-\nu_p(\alpha)},$$

γεγονός που αποδεικνύει και τον ισχυρισμό (β).

Ο.Ε.Δ.

Αναφερόμενοι στο συμβολισμό του θεωρήματος 3, έχομε τις παρακάτω χρήσιμες προτάσεις:

α) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$

$$\nu_p(a^{-1}) = -\nu_p(a)$$

Η απόδειξη είναι προφανής.

β) Τό α εἶναι ἀκέραια ἰδεώδες ἄν καί μόνο ἄν
$v_p(\alpha) \geq 0 \quad \forall\, p \in P$

Πράγματι, ἄν τό α εἶναι ἀκέραιο ἰδεώδες, τότε, ὅπως εἴδαμε στήν ἀπόδειξη τοῦ θεωρήματος 3, τό α γράφεται ὡς γινόμενο μή μηδενικῶν πρώτων ἰδεωδῶν, ἄρα $v_p(\alpha) \geq 0 \quad \forall\, p \in P$
Τό ἀντίστροφο εἶναι φανερό.

γ) $\alpha \subseteq \beta \iff v_p(\alpha) \geq v_p(\beta) \quad \forall\, p \in P.$

Πράγματι, $\alpha \subseteq \beta \iff \alpha \cdot \beta^{-1} \subseteq A \overset{(4)}{\iff} v_p(\alpha\beta^{-1}) \geq 0 \quad \forall\, p \in P$
$\overset{(\alpha')}{\iff} v_p(\alpha) - v_p(\beta) \geq 0 \quad \forall\, p \in P.$

δ) $v_p(\alpha+\beta) = \min(v_p(\alpha), v_p(\beta))$

Ἔστω $n_p = \min(v_p(\alpha), v_p(\beta))$. Ἀπό τό (γ) γίνεται φανερό ὅτι τό τ περιέχει καί τό α καί τό β ἄν καί μόνο ἄν $v_p(\tau) \leq n_p$. Ἄρα, τό ἐλάχιστο (ὡς πρός τή διάταξη $\subseteq$) ἰδεώδες πού περιέχει τά α καί β συγχρόνως εἶναι τό

$\prod_{p \in P} p^{n_p}$. Ἀφ' ἑτέρου, τό ἐλάχιστο ἰδεώδες πού περιέχει τά α καί β εἶναι τό $\alpha+\beta$, ὅπότε $v_p(\alpha+\beta) = n_p \quad \forall\, p \in P$

ε) $v_p(\alpha \cap \beta) = \max(v_p(\alpha), v_p(\beta))$

Ἡ ἀπόδειξη εἶναι ἐντελῶς ἀνάλογη μέ τοῦ (δ), ἄν λάβομε ὑπ' ὄψη ὅτι τό $\alpha \cap \beta$ εἶναι τό μέγιστο ἰδεώδες, πού περιέχεται συγχρόνως στά α καί β.

4. Norm ιδεώδους

Σ' αυτή την παράγραφο K είναι ένα αριθμητικό σώμα, $[K:\mathbb{Q}]=n$ και A ο δακτύλιος των ακεραίων του K. Για $x\in K$ συμβολίζουμε με $N(x)$ την $N_{K/\mathbb{Q}}(x)$.

<u>Θεώρημα 4</u>. Άν $x\in A-\{0\}$, τότε $|N(x)|=\operatorname{card} A/(x)$.

Απόδειξη. Ο A, θεωρούμενος ως $\mathbb{Z}$-module, έχει μιά βάση $e_1,\dots,e_n$, έστω. (δηλ. $e_1,\dots,e_n$ είναι μιά ακέραια βάση του K). Το ιδεώδες (x) θεωρούμενο επίσης ως $\mathbb{Z}$-module έχει μιά βάση, αποτελούμενη από n στοιχεία, λόγω του ισομορφισμού $A\ni a\longrightarrow ax\in(x)$. Η βάση αυτή του (x) μπορεί να επιλεγεί τέτοια ώστε να είναι της μορφής $m_1e_1,\dots,m_ne_n$, όπου $m_1,\dots,m_n$ θετικοί ακέραιοι. Τότε οι δακτύλιοι $A/(x)$ και $\prod_{i=1}^{n}\mathbb{Z}/m_i\mathbb{Z}$ καθίστανται ισόμορφοι μέσω της έξης απεικονίσεως:

$$A/(x)\ni a_1e_1+\dots+a_ne_n+(x)\longrightarrow(a_1+m_1\mathbb{Z},\dots,a_n+m_n\mathbb{Z})\in\prod_{i=1}^{n}\mathbb{Z}/m_i\mathbb{Z}.$$

Απ' αυτόν τον ισομορφισμό προκύπτει, ειδικώτερα, ότι

$$\operatorname{card} A/(x)=m_1\dots m_n.$$

Θεωρούμε τώρα την γραμμική απεικόνιση u μεταξύ των $\mathbb{Z}$-modules A και (x), που ορίζεται απ' την σχέση $u(e_i)=m_ie_i$ $(i=1,\dots,n)$. Η u έχει ορίζουσα $\det u=m_1\dots m_n$. Επίσης, παρατηρούμε ότι $xe_1,\dots,xe_n$ είναι μιά άλλη βάση του $\mathbb{Z}$-module (x), άρα υπάρχει ένας αυτομορφισμός v αυτού του module, τέτοιος ώστε $v(m_ie_i)=xe_i$ $(i=1,\dots,n)$ και η ορίζουσα $\det v$ αυτού του αυτομορφισμού πρέπει να είναι ±1. Η απεικόνιση $v\circ u:A\to A$ απεικονίζει το e_i στό xe_i άρα είναι ο περιορισμός της απεικόνισης "πολλαπλασιασμός επί x στό K", της οποίας η ορίζουσα $\det(v\circ u)$ είναι,

ἐξ ὁρισμοῦ, $N(x)$. Συνεπῶς, $|N(x)| = |\det(u_{ij}u)| = |\det u| \cdot |\det u| =$
$= m_1 \cdot \ldots \cdot m_n = \operatorname{card} A/(x)$, δ' ἃ ἔδει δ.

Ὁρισμός. Ἔστω $\mathfrak{a}$ μὴ μηδενικὸ ἀκέραιο ἰδεῶδες τοῦ A. Τότε ὀνομάζομε *norm* τοῦ $\mathfrak{a}$ καὶ συμβολίζομε μὲ $N(\mathfrak{a})$ τὸν πληθάριθμο $A/\mathfrak{a}$.

α) Εἶναι $N(\mathfrak{a})$ πεπερασμένος ἀριθμός.
Πράγματι, ἔστω $a \in \mathfrak{a} - \{0\}$. Τότε $(a) \subseteq \mathfrak{a}$, ἄρα ἂν $x, y \in A$ καὶ $x + \mathfrak{a} \neq y + \mathfrak{a}$, ἕπεται ὅτι καὶ $x + (a) \neq y + (a)$. Αὐτὸ σημαίνει ὅτι τὰ διαφορετικὰ στοιχεῖα τοῦ $A/\mathfrak{a}$ εἶναι, τὸ πολύ, ὅσα καὶ τοῦ $A/(a)$. Ὅμως τὸ σύνολο $A/(a)$ εἶναι πεπερασμένο βάσει τοῦ θεωρήματος 4.
β) Ἂν τὰ $\mathfrak{a}$ εἶναι κύρια ἰδεώδη τοῦ A, $\mathfrak{a} = (a)$, τότε
$$N((a)) = |N(a)|$$
Διότι, ἐξ ὁρισμοῦ, $N((a)) = \operatorname{card} A/(a) = |N(a)|$, βάσει τοῦ θεωρήματος 4.

Θεώρημα 5. Ἂν $\mathfrak{a}, \mathfrak{b}$ εἶναι μὴ μηδενικὰ ἀκέραια ἰδεώδη τοῦ A, τότε $N(\mathfrak{a}\cdot\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$.

Ἀπόδειξη. Προφανῶς, ἀρκεῖ ν' ἀποδείξομε τὸ θεώρημα στὴν περίπτωση ποὺ $\mathfrak{b} = \mathfrak{p}$ (= πρῶτα, ἄρα καὶ maximal, ἰδεώδη $\neq (0)$).
Εἶναι $\mathfrak{a}\mathfrak{p} \subseteq \mathfrak{a}$ καὶ θεωρώντας τὰ ἰδεώδη $\mathfrak{a}\mathfrak{p}$ καὶ $\mathfrak{a}$ ὡς (προσθετικὲς) ὑποομάδες τῆς ὁμάδας A ἔχομε*
$$\operatorname{card} A/\mathfrak{a}\mathfrak{p} = \operatorname{card} A/\mathfrak{a} \cdot \operatorname{card} \mathfrak{a}/\mathfrak{a}\mathfrak{p}.$$
Συνεπῶς, ἀρκεῖ ν' ἀποδείξομε ὅτι
$$\operatorname{card} \mathfrak{a}/\mathfrak{a}\mathfrak{p} = \operatorname{card} A/\mathfrak{p}.$$
Πρὸς τοῦτο παρατηροῦμε πρῶτα ὅτι τὸ $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ εἶναι ἕνας διανυσματικὸς χῶρος πάνω ἀπὸ τὸ σῶμα $A/\mathfrak{p}$, μὲ τὶς ἑξῆς πράξεις: Ἂν $x, y \in \mathfrak{a}$ καὶ $\lambda \in A$ τότε ὁρίζομε
$$(x + \mathfrak{a}\mathfrak{p}) + (y + \mathfrak{a}\mathfrak{p}) = (x + y) + \mathfrak{a}\mathfrak{p} \qquad (1)$$
$$(\lambda + \mathfrak{p}) \cdot (x + \mathfrak{a}\mathfrak{p}) = \lambda x + \mathfrak{a}\mathfrak{p} \qquad (2)$$

Η πρόσθεση, προφανώς, είναι καλά ορισμένη. Όσον αφορά στον πολ/σιασμό, έστω ότι $\lambda+\rho=\lambda'+\rho$ και $x+\alpha\rho=x'+\alpha\rho$ $(\lambda,\lambda'\in A,\ x,x'\in\alpha)$. Τότε $\lambda-\lambda'\in\rho$ και $x-x'\in\alpha\rho$, δηπότε $\lambda x-\lambda'x'=\lambda x-\lambda x'+\lambda x'-\lambda'x'=\lambda(x-x')+x'(\lambda-\lambda')$ $\in\alpha\rho$, άρα $\lambda x+\alpha\rho=\lambda'x'+\alpha\rho$.

Τα αξιώματα των διανυσματικών χώρων επαληθεύονται εύκολα στην περίπτωσή μας. Ας εξετάσουμε τώρα τι ιδιότητες έχουν οι υπόχωροι του διανυσματικού χώρου $\alpha/\alpha\rho$: Θα πρέπει να είναι σύνολα της μορφής $V/\alpha\rho$, όπου $V\subseteq\alpha$, τέτοια ώστε:

α) $\alpha\rho\in V/\alpha\rho$, άρα $\alpha\rho\subseteq V$. Συνεπώς

$$\alpha\rho\subseteq V\subseteq\alpha \tag{3}$$

β) Το $V/\alpha\rho$ είναι κλειστό ως προς την πρόσθεση, που ορίζεται απ' την (1), άρα το V είναι κλειστό ως προς την πρόσθεση του A.

γ) Αν $\lambda+\rho\in A/\rho$ και $x+\alpha\rho\in V/\alpha\rho$ τότε, λόγω της (2), πρέπει $\lambda x+\alpha\rho\in V/\alpha\rho$, άρα $\lambda x\in V$. Δηλαδή $\lambda\in A$ και $x\in V\Longrightarrow\lambda x\in V$.

Λόγω των (β) και (γ) το V είναι ένα ακέραιο ιδεώδες του A, άρα, απ' την πρόταση γ της §3 και την (3),

$$\nu_{\rho'}(\alpha\rho)\geqslant\nu_{\rho'}(V)\geqslant\nu_{\rho'}(\alpha),\quad\forall\,\rho'\in P \tag{4}$$

ενώ το αριστερώτερο μέλος ίσούται (πρόταση α, §3) με $\nu_{\rho'}(\alpha)+\nu_{\rho'}(\rho)=\nu_{\rho'}(\alpha)$ ή $\nu_{\rho'}(\alpha)+1$, αναλόγως αν $\rho'\neq\rho$ ή $\rho'=\rho$, αντιστοίχως. Συνεπώς η (4) λέει ότι $V=\alpha$ ή $V=\alpha\rho$, άρα οι υπόχωροι $V/\alpha\rho$ είναι μόνο οι τετριμμένοι, δηλαδή όλος ο χώρος $\alpha/\alpha\rho$ ή ο μηδενόχωρος $\{\alpha\rho\}$. Κατ' ανάγκη τότε, ο διανυσματικός χώρος $\alpha/\alpha\rho$ είναι μονοδιάστατος, άρα έχει πληθάριθμο ίσο με τον πληθάριθμο του σώματος πάνω απ' το οποίο ορίζεται. Δηλαδή

$\operatorname{card}\alpha/\alpha\rho=\operatorname{card}A/\rho$, ό.έ.δ.

5. Διαιρετότητα στά ἀκέραια ἰδεώδη τοῦ δακτυλίου ἀκεραίων ἑνός ἀριθμητικοῦ σώματος.

Σ' αὐτή τήν παράγραφο K εἶναι ἕνα ἀριθμητικό σῶμα καί A ὁ δακτύλιος τῶν ἀκεραίων τοῦ K. Λέγοντας ἁπλῶς "ἰδεώδες" θά ἐννοοῦμε "ἀκέραιο ἰδεῶδες τοῦ A".

Ὁρισμός. Λέμε ὅτι τό ἰδεῶδες $\alpha \neq (0)$ διαιρεῖ τό ἰδεῶδες β (συμβολικά, $\alpha | \beta$) ἄν $\alpha \supseteq \beta$. Ἰσοδύναμες ἐκφράσεις: Τό α εἶναι διαιρέτης τοῦ β ἤ τό β εἶναι διαιρετό ἀπ' τό α. Ἄν $x \in A$, γράφομε $\alpha | x$ ἤ $x \equiv 0 (\mathrm{mod}\, \alpha)$ ἐννοώντας $\alpha | (x)$, δηλ $x \in \alpha$.

Χρήσιμες προτάσεις: Στίς παρακάτω προτάσεις τά ἰδεώδη, πού ἐμφανίζονται ὡς διαιρέτες, ὑποτίθενται μή μηδενικά.

α) $\alpha | \beta$ ἄν καί μόνο ἄν ὑπάρχει ἰδεῶδες τ τέτοιο ὥστε $\beta = \alpha \cdot \tau$.

Πράγματι, $\alpha | \beta \Rightarrow \alpha \supseteq \beta \Rightarrow \beta \alpha^{-1} \subseteq A$. Ἄρα τό ἰδεῶδες $\tau = \beta \alpha^{-1}$ εἶναι ἀκέραιο καί $\beta = \alpha \cdot \tau$. Ἀντίστροφα, $\beta = \alpha \cdot \tau \Rightarrow \beta \subseteq \alpha \Rightarrow \alpha | \beta$.

β) $\alpha | (0)$ καί $A | \alpha$ γιά ὅλα τά μή μηδενικά ἰδεώδη α.

Ἡ ἀπόδειξη εἶναι προφανής.

γ) $\alpha | \beta \Leftrightarrow \nu_{\mathfrak{p}}(\alpha) \leq \nu_{\mathfrak{p}}(\beta)$ γιά κάθε μή μηδενικό πρῶτο ἰδεῶδες $\mathfrak{p}$.

Ἡ ἀπόδειξη εἶναι ἄμεση συνέπεια τῆς πρότασης γ, §3.

δ) Οἱ μόνοι διαιρέτες τοῦ μή μηδενικοῦ πρώτου ἰδεώδους $\mathfrak{p}$ εἶναι οἱ A καί $\mathfrak{p}$.

Πράγματι, τό $\mathfrak{p}$ εἶναι maximal.

ε) $\alpha | \beta$ καί $\beta | \alpha \Rightarrow \alpha = \beta$,

$\alpha | \alpha$,

$\alpha | \beta$ καί $\beta | \tau \Rightarrow \alpha | \tau$.

Οἱ ἰσχυρισμοί αὐτοί εἶναι ἄμεσες συνέπειες τοῦ ὁρισμοῦ.

ε) $\mathfrak{a} \mid \mathfrak{b} \Rightarrow N(\mathfrak{a}) \mid N(\mathfrak{b})$.

Πράγματι, ἀπ' τὴν (α) ἔχομε ὅτι $\mathfrak{a} \mid \mathfrak{b} \Rightarrow \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{x}$ γιά κάποιο ἰδεῶδες $\mathfrak{x}$. Ἄρα $N(\mathfrak{b}) = N(\mathfrak{a} \cdot \mathfrak{x}) = N(\mathfrak{a}) \cdot N(\mathfrak{x})$, σύμφωνα μέ τό θεώρημα 5.

Ὁρισμός. Μέγιστος κοινός διαιρέτης (ΜΚΔ) τῶν ἰδεωδῶν $\mathfrak{a}, \mathfrak{b}$ (συμβολικά $(\mathfrak{a}, \mathfrak{b})$) εἶναι τό μέγιστο (ὑπό τήν ἔννοια τῆς διάταξης $\mid$ ἤ, ἰσοδύναμα, τό ἐλάχιστο ὑπό τήν ἔννοια τῆς διάταξης $\subseteq$) ἰδεῶδες, πού διαιρεῖ τά $\mathfrak{a}$ καί $\mathfrak{b}$ συγχρόνως. Εἶναι φανερό ὅτι

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$$

ζ) Ἄν ὁ $\mathfrak{x}$ εἶναι κοινός διαιρέτης τῶν $\mathfrak{a}, \mathfrak{b}$, τότε $\mathfrak{x} \mid (\mathfrak{a}, \mathfrak{b})$. Εἰδικώτερα, ἄν ὁ $\mathfrak{x}$ εἶναι κοινός διαιρέτης τῶν κυρίων ἰδεωδῶν $(a), (b)$, τότε $\mathfrak{x} \mid (a \pm b)$.

Ὁ πρῶτος ἰσχυρισμός προκύπτει ἀμέσως ἀπ' τόν ὁρισμό. Ὅσον ἀφορᾶ στό δεύτερο, $\mathfrak{x} \mid (a), (b) \Rightarrow \mathfrak{x} \mid ((a), (b)) \Rightarrow$ $\mathfrak{x} \supseteq (a) + (b) \supseteq (a \pm b) \Rightarrow \mathfrak{x} \mid (a \pm b)$.

Ὁρισμός. Ἐλάχιστο κοινό πολλαπλάσιο (ΕΚΠ) τῶν ἰδεωδῶν $\mathfrak{a}, \mathfrak{b}$ (συμβολικά $[\mathfrak{a}, \mathfrak{b}]$) εἶναι τό ἐλάχιστο (ὑπό τήν ἔννοια τῆς διάταξης $\mid$ ἤ, ἰσοδύναμα, τό μέγιστο ὑπό τήν ἔννοια τῆς διάταξης $\subseteq$) ἰδεῶδες, πού διαιρεῖται συγχρόνως ἀπ' τά $\mathfrak{a}$ καί $\mathfrak{b}$. Εἶναι φανερό ὅτι

$$[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a} \cap \mathfrak{b}.$$

η) $[\mathfrak{a}, \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cdot \mathfrak{b}$

Πράγματι, ἀρκεῖ νά δείξομε ὅτι γιά κάθε μή μηδενικό πρῶτο ἰδεῶδες $\mathfrak{p}$ ἰσχύει $\nu_{\mathfrak{p}}([\mathfrak{a}, \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b})) = \nu_{\mathfrak{p}}(\mathfrak{a} \cdot \mathfrak{b})$:

Εἶναι $\nu_{\mathfrak{p}}([\mathfrak{a}, \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b})) = ((\alpha), \S 3)\ \nu_{\mathfrak{p}}([\mathfrak{a}, \mathfrak{b}]) + \nu_{\mathfrak{p}}((\mathfrak{a}, \mathfrak{b})) =$

$= \nu_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) + \nu_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = ((\delta), (\varepsilon), \S 3)\ \max\{\nu_{\mathfrak{p}}(\mathfrak{a}), \nu_{\mathfrak{p}}(\mathfrak{b})\} +$

$+ \min\{\nu_{\mathfrak{p}}(\mathfrak{a}), \nu_{\mathfrak{p}}(\mathfrak{b})\} = \nu_{\mathfrak{p}}(\mathfrak{a}) + \nu_{\mathfrak{p}}(\mathfrak{b}) = ((\alpha), \S 3)\ \nu_{\mathfrak{p}}(\mathfrak{a} \cdot \mathfrak{b})$.

θ) $(\alpha, \beta) = A \iff$ ὁ μόνος κοινὸς διαιρέτης τῶν α, β εἶναι ὁ A. Στὴν περίπτωση αὐτὴ τὰ α, β χαρακτηρίζονται πρῶτα μεταξύ τους.

Ἔστω $(\alpha, \beta) = A$. Ἂν ὁ τ εἶναι κοινὸς διαιρέτης τῶν α, β, τότε, ἀπὸ τὴ (ζ), $\tau \mid A$, δηλαδὴ $\tau \geq A$, ἄρα $\tau = A$. Τὸ ἀντίστροφο ἰσχύει ἐξ ὁρισμοῦ τοῦ ΜΚΔ.

ι) Ἂν τὰ α, β εἶναι πρῶτα μεταξύ τους, τότε $[\alpha, \beta] = \alpha\beta$. Πράγματι, αὐτὸ ἰσχύει λόγῳ τῆς (η).

ια) Ἂν $\alpha \mid \beta\tau$ καὶ τὰ α, β εἶναι πρῶτα μεταξύ τους, τότε $\alpha \mid \tau$.

Ἀπόδειξη: Ἀρκεῖ, σύμφωνα μὲ τὴ (γ), γιὰ κάθε μὴ μηδενικὸ πρῶτο ἰδεῶδες ρ νὰ δείξουμε ὅτι ἰσχύει $\nu_\rho(\alpha) \leq \nu_\rho(\tau)$. Ὅμως, ἐξ ὑποθέσεως, $\nu_\rho(\alpha) \leq \nu_\rho(\beta\tau) = \nu_\rho(\beta) + \nu_\rho(\tau)$. Ἂν $\nu_\rho(\alpha) > 0$, τότε $\nu_\rho(\beta) = 0$, λόγῳ τῆς ὑπόθεσης στὰ α, β, ἄρα $\nu_\rho(\alpha) \leq \nu_\rho(\tau)$. Ἂν, πάλι, $\nu_\rho(\alpha) = 0$ τότε, προφανῶς, $\nu_\rho(\alpha) \leq \nu_\rho(\tau)$.

ιβ) Ἂν τὰ α, β εἶναι πρῶτοι μεταξύ τους διαιρέτες τοῦ τ, τότε $\alpha\beta \mid \tau$.

Πράγματι, ἀπὸ τὸν ὁρισμὸ τοῦ ΕΚΠ, $[\alpha, \beta] \mid \tau$ καὶ τώρα, ἀπὸ τὴ (ι), $\alpha\beta \mid \tau$.

ιγ) Ἂν τὸ ρ εἶναι μὴ μηδενικὸ πρῶτο ἰδεῶδες τότε, γιὰ κάθε ἰδεῶδες α, $\rho \mid \alpha$ εἴτε τὸ ρ εἶναι πρῶτο πρὸς τὸ α.

Ἔστω ὅτι $\rho \nmid \alpha$. Οἱ μόνοι διαιρέτες τοῦ ρ εἶναι τὰ A καὶ ρ, λόγῳ τοῦ (δ), ἄρα ὁ μόνος κοινὸς διαιρέτης τῶν ρ καὶ α εἶναι τὸ A.

ιδ) Ἂν $a, b \in A$, $a \neq 0$ τότε ἰσχύει:

$$a \mid b \ (\text{στὸν } A) \iff (a) \mid (b)$$

Πράγματι, ἂν $a \mid b$, τότε $b = ac$ γιά κάποιο $c \in A$, ἄρα

$(b)=(a\cdot c)=(a)(c)$, δηλαδή $(a)\mid(b)$. Αντιστρόφως, $(a)\mid(b) \Rightarrow (a)\supseteq(b) \Rightarrow b\in(a) \Rightarrow b=ac$ για κάποιο $c\in A \Rightarrow a\mid b$.

Ορισμός. Το $\varepsilon\in A-\{0\}$ χαρακτηρίζεται ως ένάδα του A (ή και ένάδα του K) άν $\varepsilon^{-1}\in A$. Δυό μή μηδενικά στοιχεία του A χαρακτηρίζονται συνεταιρικά άν υπάρχει ένάδα ε του A, τέτοια ώστε τό ένα στοιχείο να ισούται με τό άλλο πολ/σιασμένο επί ε.

Οί ένάδες του A, προφανώς, αποτελούν πολλαπλασιαστική ομάδα. Επίσης, η συνεταιρικότητα είναι μιά σχέση ισοδυναμίας στό σύνολο $A-\{0\}$.

Θεώρημα 6. Έστω ότι $a, b\in A-\{0\}$. Τότε, $(a)=(b)$, άν και μόνο άν τά a, b είναι συνεταιρικά. Ειδικώτερα, $(a)=A$ άν και μόνο άν τό a είναι ένάδα του A.

Απόδειξη. Άν $(a)=(b)$, τότε $(a)\mid(b)$ και $(b)\mid(a)$, άρα, από την πρόταση (ιδ) $a\mid b$ και $b\mid a$. Τότε τό $\varepsilon=ba^{-1}$ και τό $\varepsilon^{-1}=ab^{-1}$ ανήκουν και τά δύο στόν A, άρα τό ε είναι ένάδα του A· επιπλέον $b=a\varepsilon$. Αντιστρόφως, άν $b=a\varepsilon$ και τό ε είναι ένάδα του A, τότε $b\mid a$ και $a\mid b$, άρα, από την πρόταση (ιδ), $(b)\mid(a)$ και $(a)\mid(b)$. Τότε, από την πρόταση (ε), $(a)=(b)$. Ο δεύτερος ισχυρισμός του θεωρήματος είναι φανερός, άν παρατηρήσουμε ότι $A=(1)$ και τά στοιχεία του A τά συνεταιρικά με τό 1 είναι, ακριβώς, οί ένάδες του A.

6. Ανάλυση ενός ρητού πρώτου σε γινόμενο πρώτων ιδεωδών ενός αριθμητικού σώματος.

Επεξήγηση της επικεφαλίδας: Σ' αυτή την παράγραφο θεωρούμε ένα αριθμητικό σώμα K, $[K:\mathbb{Q}]=n$ και A το δακτύλιο των ακεραίων του K. Αν p είναι ρητός πρώτος, τότε αυτός δρίζει ένα κύριο ιδεώδες στο A, το Ap, το οποίο συμβολίζουμε (p) για απλούστευση των συμβολισμών (αντιθέτως, το κύριο ιδεώδες που παράγει το p στο $\mathbb{Z}$ θα συμβολίζουμε $p\mathbb{Z}$). Το (p) ως ακέραιο ιδεώδες του A, θα έχει μια κανονική ανάλυση

$$(p)=\prod_{i=1}^{m}\mathfrak{p}_i^{e_i},\quad \mathfrak{p}_i\neq\mathfrak{p}_j \text{ αν } i\neq j,\quad e_i\geq 1\ (i=1,\dots,m), \tag{1}$$

σύμφωνα με το Θεώρημα 3. Για απλούστευση στη διατύπωση και μεγαλύτερη παραστατικότητα λέμε ότι στην (1) έχουμε την κανονική ανάλυση του p σε πρώτα ιδεώδη του K. Τέλος, λέγοντας πρώτο ιδεώδες, εννοούμε μη μηδενικό πρώτο ιδεώδες του A. Το σύνολο αυτών των ιδεωδών, όπως και στην §3, συμβολίζουμε με P.

<u>Θεώρημα 7.</u> Για κάθε $\mathfrak{p}_i$ στην (1) ισχύει $\mathfrak{p}_i\cap\mathbb{Z}=p\mathbb{Z}$. Αντίστροφα, αν $\mathfrak{p}\in P$ και $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$, τότε $\mathfrak{p}=\mathfrak{p}_i$ για κάποιο $i\in\{1,\dots,m\}$.

Απόδειξη$^{\circledast}$ $p\mathbb{Z}\subseteq(p)=\prod_{i=1}^{m}\mathfrak{p}_i^{e_i}\subseteq\mathfrak{p}_i$, για κάθε i, άρα $p\mathbb{Z}\subseteq\mathfrak{p}_i\cap\mathbb{Z}$. Αντίστροφα, έστω $x\in\mathfrak{p}_i\cap\mathbb{Z}$, δηλαδή $(x)\subseteq\mathfrak{p}_i$, $\mathfrak{p}_i\mid(x)$, άρα ((6), §5) $N(\mathfrak{p}_i)\mid N((x))$.

Όμως $N((x))=$ ((β), σελ. 31) $|N(x)|=|x^n|$, αφού $x\in\mathbb{Z}$, ενώ $N(\mathfrak{p}_i)\mid N((p))$ και $N((p))=|N(p)|=p^n$. Συνεπώς, ο αριθμός $N(\mathfrak{p}_i)$ είναι δύναμη του p και διαιρεί το x^n, ενώ

$^{\circledast}$ Ακολουθεί άλλη απόδειξη στη σελ. 37α.

Άλλη απόδειξη του Θεωρήματος 7.

Συμφωνα με το Λήμμα 1, §1, το $p_i \cap \mathbb{Z}$ είναι πρώτο ιδεώδες του $\mathbb{Z}$, άρα της μορφής $q\mathbb{Z}$, όπου q ρητός πρώτος. Μα' άλλου, $p \in (p) \subseteq p_i$, άρα $p \in p_i \cap \mathbb{Z} = q\mathbb{Z}$ και, συνεπώς $p = q$.

Έστω τώρα ότι $p \in P$ και $p \cap \mathbb{Z} = p\mathbb{Z}$. Τότε $(p) \subseteq p_i$, άρα $v_p((p)) \geq 1$, και είναι δυνατόν να συμβαίνει μόνο όταν το p συμπίπτει με κάποιο p_i, από εκείνα που εμφανίζονται στο δεξιό μέλος της (1).

$N(\mathfrak{p}_i) \neq 1$ ($N(\mathfrak{p}_i) = 1 \Rightarrow \operatorname{card} A/\mathfrak{p}_i = 1 \Rightarrow \mathfrak{p}_i = A$, ἄτοπο), ἄρα $p | x$ (στό $\mathbb{Z}$), δηλαδή $x \in p\mathbb{Z}$.

Ἔστω τώρα ὅτι $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ μιά κάποια $\mathfrak{p} \in P$. Ἂν $\omega_1, \dots, \omega_n$ εἶναι μιά ἀκέραια βάση τοῦ K, τότε κάθε στοιχεῖο τοῦ (p) θά εἶναι τῆς μορφῆς $(m_1 \omega_1 + \cdots + m_n \omega_n)p$, $m_i \in \mathbb{Z}$ $(i = 1, \dots, n)$. Ὅμως, γιά κάθε $i = 1, \dots, n$, $m_i p \in p\mathbb{Z} \subseteq \mathfrak{p}$, ἄρα τό παραπάνω στοιχεῖο ἀνήκει στό $\mathfrak{p}$. Συνεπῶς $(p) \subseteq \mathfrak{p}$, δηλ. $\mathfrak{p} | (p)$ καί, λόγῳ τῆς (1) καί τοῦ θεωρήματος 3, $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$, ὅ.ἔ.δ.

Λόγῳ τῆς σχέσης $\mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$ φαίνεται εὔκολα ὅτι ἡ ἀπεικόνιση

$$\mathbb{Z}/p\mathbb{Z} \ni x + p\mathbb{Z} \longrightarrow x + \mathfrak{p}_i \in A/\mathfrak{p}_i$$

εἶναι ἕνας μονομορφισμός. Συνεπῶς, μποροῦμε νά θεωρήσομε τό σῶμα $A/\mathfrak{p}_i$ ὡς ἐπέκταση τοῦ $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ γιά κάθε $i = 1, \dots, m$. Ἡ ἐπέκταση αὐτή εἶναι πεπερασμένης διάστασης. Πράγματι, ἂν $b_1, \dots, b_n$ εἶναι μιά ἀκέραια βάση τοῦ K τότε, εἶναι προφανές ὅτι τά $b_1 + \mathfrak{p}_i, \dots, b_n + \mathfrak{p}_i$ παράγουν τό $A/\mathfrak{p}_i$ πάνω ἀπ' τό $\mathbb{F}_p$, ἄρα ἡ διάσταση τοῦ διανυσματικοῦ χώρου $A/\mathfrak{p}_i$ πάνω ἀπ' τό $\mathbb{F}_p$ εἶναι $\leq n$.

Ὁρισμός. Ἡ πεπερασμένη διάσταση, ἔστω f_i, τῆς ἐπέκτασης $A/\mathfrak{p}_i : \mathbb{F}_p$ λέγεται βαθμός τοῦ $\mathfrak{p}_i$. Ὁ θετικός ἀκέραιος e_i, ὁ ὁποῖος ἐμφανίζεται ὡς ἐκθέτης τοῦ $\mathfrak{p}_i$ στήν (1), λέγεται δείκτης διακλάδωσης τοῦ $\mathfrak{p}_i$.

Ὁ παραπάνω ὁρισμός ἀναφέρεται σέ ἰδεώδη $\mathfrak{p} \in P$, τά ὁποῖα ἐμφανίζονται στήν κανονική ἀνάλυση κάποιου πρώτου $p \in \mathbb{Z}$. Τό παρακάτω θεώρημα μᾶς ἐξασφαλίζει ὅτι κάθε ἰδεώδες $\mathfrak{p} \in P$ ἔχει τήν ἰδιότητα νά ἐμφανίζεται στήν κανονική ἀνάλυση κάποιου πρώτου $p \in \mathbb{Z}$.

Θεώρημα 8. Για κάθε $p \in P$ υπάρχει ακριβώς ένας πρώτος $p \in \mathbb{Z}$, τέτοιος ώστε $p \mid (p)$ και, συνεπώς, το p εμφανίζεται στην κανονική ανάλυση του p σε πρώτα ιδεώδη. Αν f είναι ο βαθμός του p, τότε $N(p) = p^f$.

Απόδειξη. Το A/p είναι σώμα και, μάλιστα, πεπερασμένο (βλ. ορισμό και (α) στη σελ. 31). Έστω p η χαρακτηριστική αυτού του σώματος. Θα δείξουμε ότι $p \mid (p)$ ή, ισοδύναμα, ότι $p \supseteq (p)$. Πράγματι, αν $ap \in (p)$, $a \in A$, τότε, αφού η χαρακτηριστική του A/p είναι p, έχουμε $p(a+p) = p$, δηλαδή $ap \in p$.
Έστω τώρα ότι $p \mid (q)$, όπου $q \in \mathbb{Z}$, q πρώτος $\neq p$. Υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $px + qy = 1$, οπότε $(px+qy) = A$. Λόγω της πρότασης (ζ), §9, πρέπει $p \mid (px+qy)$, δηλαδή, $p = A$, άτοπο.
Τέλος, έστω f ο βαθμός του p. Εξ ορισμού, αυτό σημαίνει ότι η επέκταση $A/p : \mathbb{F}_p$ είναι βαθμού f. Αλλά τότε, αφού το $\mathbb{F}_p$ έχει p στοιχεία, το A/p θα έχει p^f στοιχεία. Άρα, $N(p) = \operatorname{card} A/p = p^f$, ό.έ.δ.

Θεώρημα 9. Αν ο $p \in \mathbb{Z}$ είναι πρώτος και η κανονική ανάλυση του σε πρώτα ιδεώδη του K δίνεται στην (1), τότε $e_1 f_1 + \cdots + e_m f_m = n$, όπου f_i είναι ο βαθμός του $\mathfrak{p}_i$ $(i = 1, \ldots, m)$ και $n = [K : \mathbb{Q}]$.

Απόδειξη. $N((p)) = N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}) =$ (Θεώρημα 5)

$= N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_m)^{e_m} =$ (Θεώρημα 8) $p^{f_1 e_1} \cdots p^{f_m e_m} =$

$= p^{e_1 f_1 + \cdots + e_m f_m}$.

Αφ' ετέρου $N((p)) =$ ((6), σελ. 31) $|N(p)| = p^n$, ό.έ.δ.

Θεώρημα 10. Αν για τον ακέραιο ιδεώδες $\mathfrak{a}$ ισχύει $N(\mathfrak{a}) = p$, πρώτος, τότε το $\mathfrak{a}$ είναι πρώτο και διαιρεί το (p).

Απόδειξη. Έστω $\alpha = \prod_{i=1}^{m} p_i^{e_i}$ η κανονική ανάλυση του α σε πρώτα ιδεώδη. Τότε (θεωρήματα 5 και 8),

$p = N(\alpha) = \prod_{i=1}^{m} p_i^{e_i f_i}$, όπου p_i είναι ο ρητός πρώτος με την ιδιότητα $p_i | (p_i)$ και f_i ο βαθμός του p_i $(i=1,\dots,m)$. Άλλα τότε, δεδομένου ότι $e_i \geq 1$, $f_i \geq 1$ για κάθε $i=1,\dots,m$, πρέπει $m=1$, $e_1 = f_1 = 1$, άρα $\alpha = p_1$ και $p = p_1$. Αφ' ετέρου, $p_1 | (p_1)$, εξ ορισμού, άρα $\alpha | (p)$, δ.ε.δ.

7. Χρήσιμα θεωρήματα για την κανονική ανάλυση ενός ρητού πρώτου σε πρώτα ιδεώδη ενός αριθμητικού σώματος.

Διατηρούμε το συμβολισμό της §6.

Λήμμα 1. Έστω $p \in P$ και p ο ρητός πρώτος, που διαιρείται από το p (δηλαδή $p | (p)$ · βλ. Θεώρημα 8). Άν $a \in \mathbb{Z}$ τότε, $p | (a) \iff p | a$.

Απόδειξη. Έστω f ο βαθμός του p, δηλ. $N(p) = p^f$ (θεώρημα 8). Επίσης, $N((a)) = (\beta)$, σελ. 31) $|N(a)| = |a|^n$. Άρα, $p | (a) \Rightarrow$ (θεώρημα 5) $N(p) | N((a)) \Rightarrow p^f | |a|^n \Rightarrow p | a$. Αντιστρόφως, $p | a \Rightarrow a \in p\mathbb{Z} =$ (θεώρημα 7) $p \cap \mathbb{Z} \subseteq p$, άρα $(a) \subseteq p$. (Άλλη απόδειξη στη σελ. 40α)

Λήμμα 2. Έστω $p \in P$ και p ο ρητός πρώτος, που διαιρείται από το p. Έστω $e \geq 1$ ο εκθέτης του p στην κανονική ανάλυση του p. Άν $a \in \mathbb{Z}$ και $a \equiv 0 \pmod{p^l}$, ενώ $a \not\equiv 0 \pmod{p^{l+1}}$ $(l \geq 0)$, τότε ο εκθέτης του p στην κανονική ανάλυση του (a) είναι el.

Απόδειξη. $a = \left(\frac{a}{p^l}\right) \cdot p^l = b p^l$, όπου $b \in \mathbb{Z}$, $b \not\equiv 0 \pmod{p}$.

Απλούστερη απόδειξη του Λήμματος 1.

Το p εμφανίζεται στην ανάλυση του (p), άρα
(Θεώρημα Σ) $p \cap \mathbb{Z} = p\mathbb{Z}$. Συνεπώς, αν $a \in \mathbb{Z}$
τότε, $p|a \Leftrightarrow a \in p\mathbb{Z} = p \cap \mathbb{Z} \Leftrightarrow a \in p \Leftrightarrow (a) \subseteq p$
$\Leftrightarrow p|a$

Άρα $(a) = (b)(p)^l$ και, από το λήμμα 1, $p \nmid (b)$. Άρα, ο εκθέτης του p στην κανονική ανάλυση του (a) ισούται με τον εκθέτη του p στην κανονική ανάλυση του $(p)^l$, που είναι $\in l$.

Λήμμα 3. Έστω $K = \mathbb{Q}(\theta)$, $\theta \in A$ και ο δείκτης του θ δεν διαιρείται από το ρητό πρώτο p. Τότε κάθε $a \in A$ είναι ισοδύναμο modulo p με κάποιο στοιχείο του $\mathbb{Z}[\theta]$.

Απόδειξη. Έστω k ο δείκτης του θ. Εξ ορισμού, k είναι η τάξη της (προσθετικής) ομάδας $A/\mathbb{Z}[\theta]$. Άρα, $k(a + \mathbb{Z}[\theta]) = \mathbb{Z}[\theta]$, που σημαίνει ότι $ka \in \mathbb{Z}[\theta]$. Αφ' ετέρου, υπάρχει $k' \in \mathbb{Z}$, τέτοιο ώστε $kk' \equiv 1 \pmod p$. Θέτομε $ka = b \in \mathbb{Z}[\theta]$, οπότε $a \equiv k'ka = k'b \pmod p$, δ.ε.δ.

Λήμμα 4. Έστω $K = \mathbb{Q}(\theta)$, $\theta \in A$, p ρητός πρώτος και $\mathfrak{p} \in P$ τέτοιο ώστε $\mathfrak{p} \mid (p)$. Άν ο δείκτης του θ δεν διαιρείται από τον p τότε $A/\mathfrak{p} = \mathbb{F}_p(\hat\theta)$, όπου $\hat\theta = \theta + \mathfrak{p}$. Μια βάση της επέκτασης $A/\mathfrak{p} : \mathbb{F}_p$ είναι η $1, \hat\theta, \dots, \hat\theta^{f-1}$, όπου f ο βαθμός του $\mathfrak{p}$.

Απόδειξη. Έν γένει, άν $a \in A$ θα συμβολίζομε με $\hat a$ την κλάση $a + \mathfrak{p} \in A/\mathfrak{p}$. Στη σελίδα 38 είδαμε ότι υπάρχει μια ισόμορφη εμφύτευση του $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ στο $A/\mathfrak{p}$, η οποία ταυτίζει, για $x \in \mathbb{Z}$, την κλάση $x + p\mathbb{Z} \in \mathbb{F}_p$ με την κλάση $\hat x$. Συνεπώς, για $x \in \mathbb{Z}$, η κλάση $\hat x$ θεωρείται στοιχείο του $\mathbb{F}_p$. Έστω τώρα $a \in A$. Τότε, λόγω του λήμματος 3, υπάρχουν $x_0, \dots, x_{n-1} \in \mathbb{Z}$ και $b \in A$ έτσι ώστε $a = x_0 + x_1\theta + \dots + x_{n-1}\theta^{n-1} + pb$, άρα $\hat a = a + \mathfrak{p} = x_0 + x_1\theta + \dots + x_{n-1}\theta^{n-1} + \mathfrak{p} =$

$$= (x_0 + \mathfrak{p}) + (x_1 + \mathfrak{p})(\theta + \mathfrak{p}) + \dots + (x_{n-1} + \mathfrak{p})(\theta + \mathfrak{p})^{n-1} =$$
$$= \hat x_0 + \hat x_1 \cdot \hat\theta + \dots + \hat x_{n-1} \cdot \hat\theta^{n-1}.$$

Συνεπώς, $A/\mathfrak{p} \subseteq \mathbb{F}_p(\hat\theta)$. Αντιστρόφως, επειδή $\hat\theta \in A/\mathfrak{p}$ και $\mathbb{F}_p \subseteq A/\mathfrak{p}$, θα έχομε $\mathbb{F}_p(\hat\theta) \subseteq A/\mathfrak{p}$, άρα $A/\mathfrak{p} = \mathbb{F}_p(\hat\theta)$. Εξ ορισμού, f είναι ο βαθμός της επέκτασης $A/\mathfrak{p} : \mathbb{F}_p$, άρα $f = [\mathbb{F}_p(\hat\theta) : \mathbb{F}_p]$ και,

συνεπῶς, τά $1, \hat{\theta}, \dots, \hat{\theta}^{f-1}$ εἶναι βάση τῆς ἐν λόγῳ ἐπέκτασης.
ὅ.ἐ.δ

Ἔστω $g(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_m t^m \in \mathbb{Z}[t]$. Συμβολίζω με $\hat{g}(t) = \hat{a}_0 + \hat{a}_1 t + \hat{a}_2 t^2 + \dots + \hat{a}_m t^m \in \mathbb{F}_p[t]$.

Λῆμμα 5. Μέ τίς ὑποθέσεις κ.λ.π. τοῦ λήμματος 4:
Ἄν $h(t) \in \mathbb{Z}[t]$ καί $\phi(t) \in \mathbb{Z}[t]$ εἶναι τέτοιο ὥστε τό $\hat{\phi}(t) \in \mathbb{F}_p[t]$ εἶναι τό ἐλάχιστο πολυώνυμο τοῦ $\hat{\theta}$ πάνω ἀπό τό $\mathbb{F}_p$ τότε,
$$h(\theta) \equiv 0 \pmod{p} \iff \hat{\phi}(t) \mid \hat{h}(t).$$

Ἀπόδειξη. Ἄν $h(\theta) \equiv 0 \pmod{p}$, τότε $\hat{h}(\hat{\theta}) = \hat{0}$. Ἑπομένως, τά πολυώνυμα $\hat{h}(t)$ καί $\hat{\phi}(t)$ τοῦ $\mathbb{F}_p[t]$ ἔχουν κοινή ρίζα, ἐνῶ τό δεύτερο εἶναι, ἐξ ὑποθέσεως, ἀνάγωγο πάνω ἀπό τό $\mathbb{F}_p$. Συνεπῶς $\hat{\phi}(t) \mid \hat{h}(t)$.
Ἀντιστρόφως, ἔστω $\hat{h}(t) = \hat{\phi}(t) \cdot \hat{\psi}(t)$, ὅπου $\psi(t) \in \mathbb{Z}[t]$. Τότε, $\hat{h}(\hat{\theta}) = \hat{\phi}(\hat{\theta}) \cdot \hat{\psi}(\hat{\theta}) = \hat{0}$, ἄρα $h(\theta) \in \mathfrak{p}$, πού σημαίνει $h(\theta) \equiv 0 \pmod{p}$.

Λῆμμα 6. Μέ τίς ὑποθέσεις κ.λ.π. τοῦ λήμματος 4:
Ἔστω $\phi(t) \in \mathbb{Z}[t]$, τέτοιο ὥστε $\phi(\theta) \equiv 0 \pmod{p}$ καί τό $\hat{\phi}(t) \in \mathbb{F}_p[t]$ εἶναι ἀνάγωγο. Τότε $(\phi(\theta), p) = \mathfrak{p}$ (ὅπου, γράφοντας $(\phi(\theta), p)$ ἐννοοῦμε $((\phi(\theta)), (p))$).

Ἀπόδειξη. Ἔστω $(\phi(\theta), p) = \mathfrak{a}$. Θά δείξομε πρῶτα ὅτι τό $\mathfrak{a}$ εἶναι πρῶτο*: Ἔστω $b_1 b_2 \in \mathfrak{a}$, $b_1, b_2 \in A$. Τότε, τό λῆμμα 3 μᾶς ἐπιτρέπει νά γράψομε $b_i = h_i(\theta) + p c_i$, $h_i(\theta) \in \mathbb{Z}[\theta]$, $c_i \in A$ $(i = 1, 2)$. Ἄρα $b_1 b_2 = h_1(\theta) h_2(\theta) + \text{πολ/σιο τοῦ } p$, ἀπ' ὅπου $h_1(\theta) h_2(\theta) \in \mathfrak{a}$. Ἀφ' ἑτέρου, ~~$p \mid \mathfrak{a}$~~ $p \mid \mathfrak{a}$ καί, συνεπῶς, $h_1(\theta) h_2(\theta) \in \mathfrak{p}$, δηλαδή $h_1(\theta) h_2(\theta) \equiv 0 \pmod{p}$. Ἀπό τό λῆμμα 5 τότε, $\hat{\phi}(t) \mid \hat{h}_1(t) \cdot \hat{h}_2(t)$, ἄρα τό $\hat{\phi}(t)$ διαιρεῖ (στό $\mathbb{F}_p[t]$) ἕνα τουλάχιστον ἀπό τά $\hat{h}_1(t), \hat{h}_2(t)$. Ἔστω

* Ἐπειδή $p \mid \phi(\theta) \Rightarrow p \mid p$, ἔχομε $p \mid \mathfrak{a}$, ἄρα $\mathfrak{a} \neq A$.

$\hat{\phi}(t) \mid \hat{h}_1(t)$ καὶ ἂν θέσωμε $h_1(t) = \phi(t)\cdot\psi(t) + p\cdot g(t)$, ὅπου $\psi(t), g(t) \in \mathbb{Z}[t]$. Τότε, $h_1(\theta) = \phi(\theta)\cdot\psi(\theta) + p\cdot g(\theta)$ καὶ ἐπειδὴ $\alpha \mid \phi(\theta), p$, συμπεραίνομε ὅτι $\alpha \mid h_1(\theta)$ ἄρα καὶ $\alpha \mid h_1(\theta) + pc_1 = b_1$, δηλαδὴ $b_1 \in \alpha$. Ἔτσι, λοιπόν, τὸ α εἶναι πρῶτο. Ὅμως εἴδαμε πρὶν ὅτι $p \mid \alpha$, δηλαδὴ $p \supseteq \alpha$ καὶ, ἐπειδὴ τὸ α εἶναι maximal, συμπεραίνομε ὅτι $\alpha = p$, ὅ.ἐ.δ.

<u>Θεώρημα 11</u>. Ἔστω $K = \mathbb{Q}(\theta)$, $\theta \in A$ καὶ ὁ δείκτης τοῦ θ δὲν διαιρεῖται ἀπὸ τὸν πρῶτο $p \in \mathbb{Z}$. Ἔστω $g(t) \in \mathbb{Z}[t]$ τὸ ἐλάχιστο πολυώνυμο τοῦ θ πάνω ἀπὸ τὸ $\mathbb{Q}$. Ἀναλύομε τὸ $\hat{g}(t) \in \mathbb{F}_p[t]$ (βλ. ἀμέσως πρὶν τὸ λῆμμα 5) σὲ ἀνάγωγα πολυώνυμα τοῦ $\mathbb{F}_p[t]$:

$$\hat{g}(t) = \hat{\phi}_1(t)^{e_1} \cdots \hat{\phi}_m(t)^{e_m},$$

ὅπου $\phi_1(t), \ldots, \phi_m(t) \in \mathbb{Z}[t]$, μὲ συντελεστὴ μεγιστοβαθμίου ὅρου 1, $\hat{\phi}_1(t), \ldots, \hat{\phi}_m(t) \in \mathbb{F}_p[t]$ ἀνάγωγα, διαφορετικὰ ἀνὰ δύο καὶ $e_i \geq 1$ $(i = 1, \ldots, m)$. Τέλος, ἔστω $f_i = \deg \phi_i$ $(i = 1, \ldots, m)$. Τότε ἡ κανονικὴ ἀνάλυση τοῦ p σὲ πρῶτα ἰδεώδη τοῦ K εἶναι

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}, \quad (p, \phi_i(\theta)) = \mathfrak{p}_i \quad (i = 1, \ldots, m),$$

ὅπου τὰ (διαφορετικὰ ἀνὰ δύο) πρῶτα μὴ μηδενικὰ ἰδεώδη $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ ἔχουν, ἀντιστοίχως, βαθμοὺς $f_1, \ldots, f_m$.

Ἀπόδειξη. Ἔστω $\mathfrak{p} \in P$ ἕνα ἰδεῶδες ποὺ ἐμφανίζεται στὴν κανονικὴ ἀνάλυση τοῦ p. Ἀπὸ τὴν $g(\theta) = 0$ ἕπεται ὅτι $\hat{g}(\hat{\theta}) = \hat{0} \in \mathbb{F}_p(\hat{\theta}) = (\text{λῆμμα 4})\ A/\mathfrak{p}$, ἄρα $\hat{\phi}_1(\hat{\theta})^{e_1} \cdots \hat{\phi}_m(\hat{\theta}) = \hat{0}$, ὁπότε ὑπάρχει ἕνα $i \in \{1, \ldots, m\}$ τέτοιο ὥστε $\hat{\phi}_i(\hat{\theta}) = \hat{0} \in A/\mathfrak{p}$, δηλαδὴ

$$\phi_i(\theta) \equiv 0 \pmod{\mathfrak{p}}. \tag{1}$$

Ἰσχυρισμός: Δὲν ὑπάρχει $\phi_j(t)$, $j \in \{1, \ldots, m\}$, $j \neq i$ τέτοια ὥστε $\phi_j(\theta) \equiv 0 \pmod{\mathfrak{p}}$. Γιατὶ μιὰ τέτοια σχέση θὰ συν-

επαγόταν την $\hat{\phi}_j(\hat{\theta}) = \hat{0}$ και, απ' το λήμμα 5 τότε, την $\hat{\phi}_i(t) \mid \hat{\phi}_j(t)$ άρα και την $\hat{\phi}_i(t) = \hat{\phi}_j(t)$, αφού τα $\hat{\phi}_i(t)$, $\hat{\phi}_j(t)$ είναι ανάγωγα, με συντελεστή μεγιστοβαθμίου όρου 1.

Συμπεραίνομε, λοιπόν, ότι υπάρχει μια αμφιμονοσήμαντη απεικόνιση απ' τα ιδεώδη $\mathfrak{p} \in P$, που διαιρούν το (p), στο σύνολο $\{\phi_1(t), \dots, \phi_m(t)\}$, τέτοια ώστε, αν $\mathfrak{p} \longmapsto \phi_i(t)$ τότε να ικανοποιείται η (1) αρα η $\mathfrak{p} = (\phi_i(\theta), p)$ (λόγω του λήμματος 6).

Συνεπώς, αν $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ είναι όλα τα διαφορετικά πρώτα ιδεώδη που διαιρούν το (p), θα είναι $r \leq m$ και μπορούμε να τα θεωρήσομε έτσι αριθμημένα, ώστε

$$(\phi_i(\theta), p) = \mathfrak{p}_i \quad (i = 1, \dots, r). \tag{2}$$

$$(\phi_i(\theta), p) = A \quad (i = r+1, \dots, m \text{ αν } r < m). \tag{3}$$

Τώρα, απ' το λήμμα 4, $A/\mathfrak{p}_i = \mathbb{F}_p(\theta + \mathfrak{p}_i)$ και, λόγω της $\mathfrak{p}_i \mid (\phi_i(\theta))$, $\hat{\phi}_i(\theta + \mathfrak{p}_i) = \hat{0}\ (= \mathfrak{p}_i)$ με το $\hat{\phi}_i(t) \in \mathbb{F}_p[t]$ ανάγωγο βαθμού f_i. Άρα $[\mathbb{F}_p(\theta + \mathfrak{p}_i) : \mathbb{F}_p] = f_i$ και, συνεπώς, $[A/\mathfrak{p}_i : \mathbb{F}_p] = f_i$. Εξ ορισμού του βαθμού του $\mathfrak{p}_i$, η τελευταία σχέση λέει ότι

$$\text{βαθμός του } \mathfrak{p}_i = f_i \quad (i = 1, \dots, r). \tag{4}$$

Μένει ν' αποδείξομε ότι

$$r = m \text{ και } \nu_{\mathfrak{p}_i}((p)) = e_i \quad (i = 1, \dots, m). \tag{5}$$

Έστω $\nu_{\mathfrak{p}_i}((p)) = e_i'$ $(i = 1, \dots, r)$. Έχομε

$$\phi_1(\theta)^{e_1} \dots \phi_m(\theta)^{e_m} \equiv g(\theta) = 0 \pmod{p} \quad (\text{η ισοτιμία στον } A).$$

Άρα, $e_i' = \nu_{\mathfrak{p}_i}((p)) \leq \nu_{\mathfrak{p}_i}(\phi_1(\theta)^{e_1} \dots \phi_m(\theta)^{e_m}) \overset{(2),(3)}{=} \nu_{\mathfrak{p}_i}(\phi_i(\theta)^{e_i})$

$$= e_i \cdot \nu_{\mathfrak{p}_i}(\phi_i(\theta)).$$

Άρα

$$e_i' \leq e_i \cdot \nu_{\mathfrak{p}_i}(\phi_i(\theta)) \quad (i = 1, \dots, r)$$

Αν $\nu_{\mathfrak{p}_i}((\phi_i(\theta))) = 1$, τότε $e_i' \leq e_i$. Αν $\nu_{\mathfrak{p}_i}((\phi_i(\theta))) > 1$ τότε, (λόγω της (2)) $\nu_{\mathfrak{p}_i}((p)) = 1$, άρα $e_i' = 1 \leq e_i$. Σε κάθε περίπτωση, λοιπόν, έχομε

$$e_i' \leq e_i \quad (i = 1, \ldots, r). \tag{6}$$

Άφ' ετέρου, από την ανάλυση του $\hat{g}(t)$ σε ανάγωγα πολυώνυμα του $\mathbb{F}_p[t]$ (εκφώνηση του θεωρήματος) έχομε $n = \deg g = \deg \hat{g} = \sum_{i=1}^{r} e_i' f_i'$, ενώ από το θεώρημα 9 και την (4), $n = \sum_{i=1}^{m} e_i f_i$. Τώρα, οι σχέσεις $\sum_{i=1}^{m} e_i f_i = \sum_{i=1}^{r} e_i' f_i'$, $r \leq m$ και (6) αποδεικνύουν την (5), ό.έ.δ.

Ορισμός. Ένα πολυώνυμο $t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{Z}[t]$ λέγεται πολυώνυμο του Eisenstein ως προς τον πρώτο $p \in \mathbb{Z}$ αν $p \mid a_i$, $i = 0, 1, \ldots, n-1$ και $p^2 \nmid a_0$.

Τα πολυώνυμα του Eisenstein είναι ανάγωγα πάνω από το $\mathbb{Q}$, όπως αποδεικνύεται εύκολα, με στοιχειώδη μέσα.

Θεώρημα 12. Έστω $K = \mathbb{Q}(\theta)$ και το θ είναι ρίζα ενός πολυωνύμου του Eisenstein ως προς τον πρώτο p. Τότε, η κανονική ανάλυση του p σε πρώτα ιδεώδη του K είναι της μορφής $(p) = \mathfrak{p}^n$, $n = [K:\mathbb{Q}]$.

Απόδειξη. Έστω $t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{Z}[t]$ το πολυώνυμο του Eisenstein ως προς p, του οποίου ρίζα είναι το θ. Τότε

$$\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0 = 0 \tag{1}$$

Έστω

$$(p) = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}$$

η κανονική ανάλυση του p σε πρώτα ιδεώδη του K και f_i ο βαθμός του $\mathfrak{p}_i$ $(i = 1, \ldots, m)$. Τότε (θεώρημα 9),

$$\sum_{i=1}^{m} e_i f_i = n \qquad (2)$$

Η σχέση $a_j \equiv 0 \pmod p$ $(j=0,\dots,n-1)$ συνεπάγεται ότι $a_j \equiv 0 \pmod{\mathfrak{p}_i}$ $(i=1,\dots,m,\ j=0,\dots,n-1)$ και, συνεπώς $\theta \equiv 0 \pmod{\mathfrak{p}_i}$ $(i=1,\dots,m)$. Επίσης, επειδή $p \mid a_0$ αλλά $p^2 \nmid a_0$, έχομε (λήμμα 2, §7) $\nu_{\mathfrak{p}_i}(a_0) = e_i$ $(i=1,\dots,m)$.

Τώρα, λόγω της (2), $e_i \le n$. Αν $e_i = n$, τότε έχομε τελειώσει. Έστω, λοιπόν, ότι $e_i < n$. Τότε, στην (1), κάθε όρος $a_{n-k}\theta^{n-k}$ $(k=1,\dots,n-1)$ διαιρείται από το $\mathfrak{p}_1^{e_1+1}$. Επίσης, το θ^n διαιρείται από το $\mathfrak{p}_1^n$, άρα διαιρείται από το $\mathfrak{p}_1^{e_1+1}$. Συνεπώς, $a_0 = -a_1\theta - \dots - a_{n-1}\theta^{n-1} - \theta^n \equiv 0 \pmod{\mathfrak{p}_1^{e_1+1}}$, που αντιβαίνει στη σχέση $\nu_{\mathfrak{p}_1}(a_0) = e_1$, δ' ε.δ.

<u>Ορισμός</u>. Ο πρώτος $p \in \mathbb{Z}$ λέμε ότι διακλαδώνεται στο K αν υπάρχει ιδεώδες $\mathfrak{p} \in P$, τέτοιο ώστε $\mathfrak{p}^2 \mid p$.

<u>Θεώρημα 13</u>. Ο πρώτος $p \in \mathbb{Z}$ διακλαδώνεται στο K αν και μόνο αν διαιρεί τη διακρίνουσα του K.

<u>Απόδειξη</u>. Θα αποδείξομε το θεώρημα στην ειδική, αρκετά συνήθη περίπτωση κατά την οποία $K = \mathbb{Q}(\theta)$ για κάποιο θ του οποίου ο δείκτης δεν διαιρείται από τον p. Έστω, τότε, $g(t) \in \mathbb{Z}[t]$ το ελάχιστο πολυώνυμο του θ πάνω από το $\mathbb{Q}$. Θεωρούμε το $\bar{g}(t) \in \mathbb{F}_p[t]$ (βλ. πριν από το λήμμα 5) και έστω η ανάλυση του $\bar{g}(t)$ σε ανάγωγα του $\mathbb{F}_p[t]$ όπως στην εκφώνηση του θεωρήματος 11. Σύμφωνα με εκείνο το θεώρημα, ο p διακλαδώνεται αν και μόνο αν ένα τουλάχιστον e_i είναι >1, δηλ. αν και μόνο αν το $\bar{g}(t)$ έχει μια πολλαπλή ρίζα, που ισοδυναμεί με το ότι το $g(t)$ έχει τουλάχιστον δύο ρίζες ίσοδύναμες mod p. Αυτό σημαίνει ότι η διακρίνουσα του θ $\left(= \prod_{i \ne j}(\theta_i - \theta_j)^2\right.$, όπου θ_i, $i=1,2,\dots$ είναι οι ρίζες του $g(t)$) είναι $\equiv 0 \pmod p$. Αλλά

ἡ διακρίνουσα τοῦ θ εἶναι ≡0 (mod p) ἂν καὶ μόνο ἂν ἡ διακρίνουσα τοῦ K εἶναι ≡0 (mod p), λόγῳ τῆς σχέσεως

Διακρίνουσα τοῦ θ = (δείκτης τοῦ θ)² · διακρίνουσα τοῦ K

καὶ τῆς ὑποθέσεως ὅτι δ p δὲν διαιρεῖ τὸν δείκτη τοῦ θ.

ὅ.ἐ.δ.

8. Ἐφαρμογές

A. Τετραγωνικὰ σώματα

Ἔστω $K=\mathbb{Q}(\theta)$, ὅπου $\theta=\sqrt{d}$, $d\in\mathbb{Z}-\{1\}$ ἐλεύθερος τετραγώνου.

i) $d\equiv 1 \pmod 4$. Τότε ἡ διακρίνουσα τοῦ K εἶναι d (Θεώρημα 11, §3, Κεφάλαιο I) ἐνῶ ἡ διακρίνουσα τοῦ θ εἶναι 4d, ὁπότε ὁ δείκτης τοῦ θ εἶναι 2. Συνεπῶς, γιὰ τὴν ἀνάλυση τῶν περιττῶν πρώτων p μποροῦμε νὰ ἐφαρμόσομε τὸ θεώρημα 11 : Ἂν $p\mid d$ τότε $t^2-d\equiv t^2 \pmod p$, ὁπότε $(p)=\mathfrak{p}^2$, ὅπου τὸ $\mathfrak{p}$ εἶναι πρῶτο ἰδεῶδες, πρώτου βαθμοῦ. Ἂν $p\nmid d$ τότε τὸ t^2-d εἶναι ἀνάγωγο στὸ $\mathbb{F}_p$ ἂν καὶ μόνο ἂν τὸ d εἶναι τετραγωνικὸ ἀνισοϋπόλοιπο modulo p $\left(\left(\frac{d}{p}\right)=-1\right)$ καὶ τότε (p) = πρῶτο ἰδεῶδες βαθμοῦ 2,

ἄρα στὴν ἀντίθετη περίπτωση $\left(\left(\frac{d}{p}\right)=1\right)$ $(p)=\mathfrak{p}_1\mathfrak{p}_2$,

ὅπου $\mathfrak{p}_1\neq\mathfrak{p}_2$ εἶναι πρῶτα ἰδεώδη πρώτου βαθμοῦ.

Ἐρχόμαστε τώρα στὴν ἀνάλυση τοῦ 2. Εἶναι $K=\mathbb{Q}\left(\frac{1+\theta}{2}\right)$ καὶ τὸ ἀκέραιο στοιχεῖο $(1+\theta)/2$ ἔχει διακρίνουσα d, ἄρα δείκτη 1. Ἐφαρμόζομε, λοιπόν, ξανὰ τὸ θεώρημα 11, ὅπου τώρα τὸ ἐλάχιστο πολυώνυμο τοῦ $(1+\theta)/2$ εἶναι τὸ $t^2-t+(1-d)/4$. Ὅμως

$$t^2-t+(1-d)/4 \equiv \begin{cases} t(t-1) \pmod 2, & \text{ἂν } d\equiv 1 \pmod 8 \\ t^2-t+1 \text{ ἀνάγωγο mod 2}, & \text{ἂν } d\equiv 5 \pmod 8. \end{cases}$$

Συνεπῶς τὸ (2) εἶναι γινόμενο δύο διαφορετικῶν πρώτων

πρώτου βαθμού, στην περίπτωση που $d \equiv 1 \pmod 8$, ενώ είναι πρώτο ιδεώδες δεντέρου βαθμού αν $d \equiv 5 \pmod 8$.

ii) $d \equiv 2 \pmod 4$. Σ' αυτή την περίπτωση μια ακέραια βάση του K είναι η $1, \theta$ (Θεώρημα 11, §3, Κεφάλαιο I), άρα το θεώρημα 11 εφαρμόζεται για κάθε πρώτο p. Έτσι, $t^2 - d \equiv t^2 \pmod p$ αν $p \mid d$ (ειδικώτερα, αν $p = 2$), το $t^2 - d$ είναι ανάγωγο $\bmod p$ αν $p \nmid d$ και $\left(\frac{d}{p}\right) = -1$ και, τέλος,

το $t^2 - d$ αναλύεται σε δύο πρωτοβάθμιους παράγοντες $\bmod p$ αν $p \nmid d$ και $\left(\frac{d}{p}\right) = 1$, όπότε βγάζομε τα ανάλογα συμπεράσματα, όπως κάναμε και στην περίπτωση (i).

iii) $d \equiv 3 \pmod 4$. Αυτή η περίπτωση είναι εντελώς ανάλογη με την (ii), μόνο που τώρα $2 \nmid d$. Έχομε όμως $t^2 - d \equiv t^2 + 1 \equiv (t+1)^2 \pmod 2$, άρα $(2) = \mathfrak{p}^2$ για κάποιο πρώτο ιδεώδες $\mathfrak{p}$ πρώτου βαθμού.

Ανακεφαλαιώνοντας, έχομε:

<u>Θεώρημα 14.</u> Στο $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z} - \{1\}$, ελεύθερος τετραγώνου, η ανάλυση των ρητών πρώτων γίνεται ως εξής (με $\deg \mathfrak{p}$ θα συμβολίζομε το βαθμό του πρώτου ιδεώδους $\mathfrak{p}$): Ο p διακλαδώνεται, δηλ.

$$(p) = \mathfrak{p}^2, \quad \deg \mathfrak{p} = 1,$$

αν και μόνο αν $p \mid d$.

Για τον περιττό πρώτο p, αν δεν διαιρεί το d ισχύουν τα εξής:

$(p) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $\deg \mathfrak{p}_1 = \deg \mathfrak{p}_2 = 1$

αν και μόνο αν $\left(\frac{d}{p}\right) = 1$, ενώ

$(p) = \mathfrak{p}$, $\deg \mathfrak{p} = 2$ αν και μόνο αν $\left(\frac{d}{p}\right) = -1$.

Αν ο 2 δεν διαιρεί το d (όπότε, υποχρεωτικώς, $d \equiv 1 \pmod 4$), τότε: $(2) = \mathfrak{p}$, $\deg \mathfrak{p} = 2$, αν $d \equiv 5 \pmod 8$

$(2) = \mathfrak{p}_1 \mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $\deg \mathfrak{p}_1 = \deg \mathfrak{p}_2 = 1$, αν $d \equiv 1 \pmod 8$.

Β. Καθαρῶς κυβικά σώματα

Ἔστω $K=\mathbb{Q}(\theta)$, $\theta=\sqrt[3]{ab^2}>1$, ὅπου a,b θετικοί ἀκέραιοι, ἐλεύθεροι τετραγώνου, πρῶτοι μεταξύ τους. Στά παρακάτω θά κάνομε χρήση τοῦ Θεωρήματος 12, §3, Κεφάλαιο 1.

i) Ἔστω $a^2\not\equiv b^2 \pmod 9$. Τότε, ἡ διακρίνουσα τοῦ K εἶναι $-27a^2b^2$, ἐνῶ ἡ διακρίνουσα τοῦ θ εἶναι $-27a^2b^4$, ἄρα ὁ δείκτης τοῦ θ εἶναι b. Συνεπῶς, ἂν $3\nmid b$ τότε (Θεώρημα 3, §7), ἡ κανονική ἀνάλυση τοῦ 3 θά εἶναι ὅπως ἡ κανονική ἀνάλυση τοῦ t^3-ab^2 modulo 3. Ὅμως, $t^3-ab^2\equiv(t-a)^3 \pmod 3$, ἄρα $(3)=\mathfrak{p}^3$. Ἂν $3\mid b$, τότε $3\nmid a$ καί παρατηροῦμε ὅτι $K=\mathbb{Q}(\theta^2/b)$, τό θ^2/b ἔχει ἐλάχιστο πολυώνυμο t^3-a^2b, διακρίνουσα $-27a^4b^2$ καί δείκτη a. Ἄρα, ἡ κανονική ἀνάλυση τοῦ 3 εἶναι ὅπως ἡ κανονική ἀνάλυση τοῦ t^3-a^2b modulo 3. Ἐπειδή $t^3-a^2b\equiv t^3 \pmod 3$, συμπεραίνομε ὅτι καί πάλι $(3)=\mathfrak{p}^3$.

ii) Ἔστω $a^2\equiv b^2 \pmod 9$. Τότε ἡ διακρίνουσα τοῦ K εἶναι $-3a^2b^2$, ὁπότε (Θεώρημα 13, §7) ὁ 3 διακλαδώνεται. Σύμφωνα μέ τό Θεώρημα 9, §6, οἱ μόνες δυνατές περιπτώσεις εἶναι

$$(3)=\mathfrak{p}^3 \quad \text{ἤ} \quad (3)=\mathfrak{p}_1^2\mathfrak{p}_2\,,\ \mathfrak{p}_1\neq\mathfrak{p}_2\,.$$

Ἂν δείξομε ὅτι τό (3) ἔχει τουλάχιστον δύο διαφορετικούς πρώτους διαιρέτες τότε, κατ' ἀνάγκη, ἰσχύει ἡ δεύτερη περίπτωση. Τήν ὕπαρξη αὐτῶν τῶν δύο πρώτων διαιρετῶν συμπεραίνομε ἂν βροῦμε δύο ἀκεραίους $\alpha,\beta\in K$, τέτοιους ὥστε $N(\alpha)\equiv N(\beta)\equiv 0 \pmod 3$ καί ὁ $\alpha-\beta$ εἶναι πρῶτος πρός τό 3. Πράγματι, ἂν $N(\alpha)\equiv 0 \pmod 3$ τότε, στήν κανονική ἀνάλυση τοῦ α ἐμφανίζεται, κατ' ἀνάγκη, κάποιο πρῶτο ἰδεῶδες $\mathfrak{p}_1$ τοῦ K μέ norm δύναμη τοῦ 3. Ἀναλόγα, στήν κανονική ἀνάλυση τοῦ β ἔχομε ἕνα πρῶτο ἰδεῶδες $\mathfrak{p}_2$ μέ norm δύναμη τοῦ 3. Σύμφωνα μέ τό Θεώρημα 8, §6, πρέπει $\mathfrak{p}_1\mid 3$ καί $\mathfrak{p}_2\mid 3$. Ἂν ἦταν $\mathfrak{p}_1=\mathfrak{p}_2$, τότε

$\mathfrak{p}_1 | \alpha - \beta$, που αντιβαίνει στην υπόθεση για τα $\alpha - \beta$.
Ένα τέτοιο ζευγάρι α και β ακεραίων του K βρίσκεται πάντοτε μεταξύ των $\omega-1, \omega, \omega+1$, όπου $\omega = (1+ab+ab^2/b)/3$ (βλ. Θεώρημα 12, §3, Κεφάλαιο 1). Δηλαδή, μένει ν' αποδείξουμε ότι δύο μεταξύ των ρητών ακεραίων $N(\omega-1)$, $N(\omega)$, $N(\omega+1)$ είναι διαιρετοί από το 3 : Επειδή $K = \mathbb{Q}(\sqrt[3]{(a^2)(b)^2})$ και $a^2 \equiv 1 \equiv b \pmod 3$, μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι $K = \mathbb{Q}(\sqrt[3]{ab^2})$ με $a \equiv b \equiv 1 \pmod 3$. Τότε

$$N(\omega) = \frac{1+ab^2+a^2b-3ab}{27}, \quad N(\omega+1) = -\frac{1-ab}{3} + N(\omega),$$

$$N(\omega-1) = -1 + \frac{1-ab}{3} + N(\omega).$$

Επιπλέον, οι μόνες δυνατότητες modulo 9 για τα a, b είναι:
$a \equiv b \equiv 1$, $a \equiv b \equiv 4$, $a \equiv b \equiv -2 \pmod 9$.
Στην πρώτη περίπτωση, $N(\omega) - N(\omega+1) = (1-ab)/3 \equiv 0 \pmod 3$ και $27 \cdot N(\omega) = 1 + ab^2 + a^2b - 3ab \equiv 0 \pmod{81}$. Άρα, $0 \equiv N(\omega) \equiv N(\omega+1) \pmod 3$. Στη δεύτερη περίπτωση, $N(\omega) - N(\omega-1) = 1 - \frac{1-ab}{3} \equiv 0 \pmod 3$ και $27 \cdot N(\omega) \equiv 0 \pmod{81}$, άρα $0 \equiv N(\omega) \equiv N(\omega-1) \pmod 3$. Στην τρίτη περίπτωση, $N(\omega+1) - N(\omega-1) = 1 - 2\frac{1-ab}{3} \equiv 0 \pmod 3$ και $27 \cdot N(\omega+1) = -8 + ab^2 + a^2b + 6ab \equiv 0 \pmod{81}$, άρα $0 \equiv N(\omega+1) \equiv N(\omega-1) \pmod 3$.
Το τελικό συμπέρασμα, λοιπόν, είναι ότι στην περίπτωση (ii) η κανονική ανάλυση του 3 είναι της μορφής $\mathfrak{p}_1^2 \mathfrak{p}_2$.
Ανακεφαλαιώνοντας, έχομε:

<u>Θεώρημα 15</u>. Στο $\mathbb{Q}(\sqrt[3]{ab^2})$, a, b θετικοί ακέραιοι ελεύθεροι τετραγώνου, πρώτοι μεταξύ τους $(ab^2 > 1)$ η κανονική ανάλυση του 3 σε πρώτα ιδεώδη είναι:

$$(3) = \mathfrak{p}^3 \ , \ \deg \mathfrak{p} = 1 \ , \text{ αν } a^2 \not\equiv b^2 \pmod 9$$

και

$$(3) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2 \ , \ \deg \mathfrak{p}_1 = \deg \mathfrak{p}_2 \ , \text{ αν } a^2 \equiv b^2 \pmod 9.$$

Γ. Ανάλυση των 2, 3, 5, 7 σε γινόμενο πρώτων ιδεωδών του $Q(\theta)$, όπου $\theta^5 = 2$.

Υπολογίζεται ότι η διακρίνουσα του θ είναι $2^4 \cdot 5^5$, άρα οι μόνοι πιθανοί διαιρέτες του δείκτη του θ είναι οι 2 και 5 και, συνεπώς, το θεώρημα 11 της §7 δεν μπορεί να εφαρμοστεί για την ανάλυση αυτών των πρώτων. Παρατηρούμε όμως ότι το ελάχιστο πολυώνυμο του θ, δηλαδή το $t^5 - 2$ είναι πολυώνυμο του Eisenstein ως προς το 2, άρα (θεώρημα 12, §3) θα έχομε

$$(2) = \mathfrak{p}_2^5 \quad , \text{ όπου } N(\mathfrak{p}_2) = 2.$$

Επίσης, $K = Q(\theta - 2)$ και το ελάχιστο πολυώνυμο του $\theta - 2$ είναι το $(t+2)^5 - 2 = t^5 + 10t^4 + 40t^3 + 80t^2 + 80t + 30$, το οποίο είναι πολυώνυμο του Eisenstein ως προς το 5, άρα

$$(5) = \mathfrak{p}_5^5 \quad , \text{ όπου } N(\mathfrak{p}_5) = 5.$$

Για την ανάλυση των 3 και 7 μπορούμε να χρησιμοποιήσομε ασφαλώς το θεώρημα 11, §3. Είναι

$$t^5 - 2 \equiv t^5 + 1 \equiv (t+1)(t^4 - t^3 + t^2 - t + 1) \pmod 3$$

και το τεταρτοβάθμιο πολυώνυμο στο δεξιώτερο μέλος είναι ανάγωγο modulo 3. Συνεπώς,

$$(3) = \mathfrak{p}_3 \cdot \mathfrak{p}_3' \quad , \text{ όπου } N(\mathfrak{p}_3) = 3 \text{ και } N(\mathfrak{p}_3') = 3^4.$$

Τέλος, $t^5 - 2 \equiv (t+3)(t^4 - 3t^3 + 2t^2 + t - 3) \pmod 7$ και το τεταρτοβάθμιο πολυώνυμο είναι ανάγωγο modulo 7. Άρα

$$(7) = \mathfrak{p}_7 \cdot \mathfrak{p}_7' \quad , \text{ όπου } N(\mathfrak{p}_7) = 7 \text{ και } N(\mathfrak{p}_7') = 7^4.$$

Δ. Ανάλυση του 2 και του 83 σε πρώτα ιδεώδη του $Q(\theta)$, όπου $\theta^3 - 7\theta + 10 = 0$.

Παρατηρούμε ότι το $(\theta^2 - \theta + 2)/4$ είναι ακέραιο στοιχείο του $Q(\theta)$ (με υπολογισμό του ελαχίστου πολυωνύμου του) και ακόμη, ότι τα $1, \theta, (\theta^2 - \theta + 2)/4$ αποτελούν βάση με διακρι-

. νουσα -83, συνεπῶς ἀποτελοῦν μιά ἀκέραια βάση τοῦ $Q(\theta)$. Ἡ διακρίνουσα τοῦ θ εἶναι $-16\cdot 83$, ἄρα ὁ δείκτης τοῦ θ εἶναι 4. Δέν μποροῦμε, λοιπόν, νά ἐφαρμόσομε τό θεώρημα 11, §3 γιά τήν ἀνάλυση τοῦ 2. Ὅμως, παρατηροῦμε ὅτι ἄν θέσομε

$$\lambda = \theta + (\theta^2-\theta+2)/4 = (\theta^2+3\theta+2)/4,$$

τότε $\theta = -6+5\lambda-\lambda^2$, ἄρα $Q(\theta)=Q(\lambda)$ καί τό λ ἔχει ἐλάχιστο πολυώνυμο t^3-5t^2+9t-4 καί διακρίνουσα -83. Τό λ ἔχει λοιπόν δείκτη 1 καί τό θεώρημα 11, §3 ἐφαρμόζεται: $t^3-5t^2+9t-4 \equiv t^3+t^2+t = t(t^2+t+1) \pmod 2$. Συνεπῶς,

$$(2) = \mathfrak{p}_2 \cdot \mathfrak{p}_2', \text{ ὅπου } N(\mathfrak{p}_2)=2 \text{ καί } N(\mathfrak{p}_2')=4.$$

Ἐπίσης, $t^3-7t+10 \equiv (t-14)^2(t+28) \pmod{83}$, ἄρα

$$(83) = \mathfrak{p}_{83}^2 \cdot \mathfrak{p}_{83}', \text{ ὅπου } N(\mathfrak{p}_{83}) = N(\mathfrak{p}_{83}') = 83 \text{ καί } \mathfrak{p}_{83} \neq \mathfrak{p}_{83}'.$$

Ε. Ἀνάλυση τῶν πρώτων στό p-τάξεως κυκλοτομικό σῶμα ($p \geq 2$).

Ἔστω ζ ἀρχική p-τάξεως ρίζα τοῦ 1, $K=Q(\zeta)$ καί A ὁ δακτύλιος τῶν ἀκεραίων τοῦ K. Μιά ἀκέραια βάση τοῦ K εἶναι ἡ $1, \zeta, \ldots, \zeta^{p-2}$ (θεώρημα 13, §3, Κεφάλαιο 1). Θέτοντας $\lambda = \zeta - 1$ εἶναι εὔκολο νά δοῦμε ὅτι καί ἡ $1, \lambda, \ldots, \lambda^{p-2}$ εἶναι ἀκέραια βάση τοῦ K. Προφανῶς $K=Q(\lambda)$ καί, ἀφοῦ τό ἐλάχιστο πολυώνυμο τοῦ ζ εἶναι $(t^p-1)/(t-1)$, τό ἐλάχιστο πολυώνυμο τοῦ λ εἶναι $((t+1)^p-1)/t$, δηλαδή εἶναι ἕνα πολυώνυμο τοῦ Eisenstein ὡς πρός τόν πρῶτο p. Συνεπῶς, ἀπ' τό θεώρημα 12, §3, θά εἶναι

$$(p) = \mathfrak{p}^{p-1}, \quad N(\mathfrak{p}) = p. \tag{1}$$

Ἀφ' ἑτέρου, $N((\lambda)) = |N(\lambda)| = p$, ἄρα τό κύριο ἰδεώδες (λ) εἶναι πρῶτο καί διαιρεῖ τό p. Λόγῳ τῆς (1) ὁ p ἔχει μόνο ἕνα πρῶτο διαιρέτη, τόν $\mathfrak{p}$, ὁπότε $\mathfrak{p} = (\lambda)$. Ἄρα

$$(p) = (\lambda)^{p-1}, \quad N((\lambda)) = p \quad (\lambda = \zeta - 1).$$

Ας δούμε τώρα την ανάλυση των πρώτων $p' \neq p$.

Λήμμα. Αν p' είναι ένα πρώτο ιδεώδες, που διαιρεί τον ρητό πρώτο $p' \neq p$, τότε $N(p') \equiv 1 \pmod p$.

Απόδειξη. Για το τυχόν $\alpha \in A$ συμβολίζουμε $\hat{\alpha} = \alpha + p' \in A/p'$. Εξ ορισμού είναι $N(p') = \mathrm{card}(A/p')$. Παρατηρούμε ότι οι κλάσεις $\hat{1}, \hat{\zeta}, \dots, \hat{\zeta}^{p-1}$ είναι διαφορετικές. Πράγματι, έστω $\hat{\zeta}^i = \hat{\zeta}^j$, $0 \leq i < j \leq p-1$. Τότε $\zeta^i - \zeta^j \in p'$, δηλαδή $(\zeta^i - \zeta^j) \subseteq p'$ η, ισοδύναμα, $p' \mid (\zeta^i - \zeta^j) = (\zeta^i)(1 - \zeta^{j-i})$. Τότε $N(p') \mid N(\zeta^i) N(1-\zeta^{j-i}) = N(1-\zeta^{j-i})$. Όμως, το ελάχιστο πολυώνυμο του ζ^{j-i} είναι το $g(t) = t^{p-1} + \dots + t + 1$, δπότε το ελάχιστο πολυώνυμο του $1 - \zeta^{j-i}$ είναι το $g(t+1)$, με σταθερό όρο p. Έτσι, $N(1-\zeta^{j-i}) = p$ και, τότε, αποκλείεται η σχέση $N(p') \mid N(1-\zeta^{j-i})$, αφού $N(p') =$ δύναμη του p'. Έτσι οι κλάσεις $\hat{1}, \hat{\zeta}, \dots, \hat{\zeta}^{p-1}$ αποτελούν υποομάδα τάξης p της πολλαπλασιαστικής ομάδας των μη μηδενικών κλάσεων του A/p', η οποία έχει τάξη $N(p') - 1$. Έπεται ότι $p \mid N(p') - 1$, δ' ε.δ.

Θεώρημα 16. Στο κυκλοτομικό σώμα τάξης $p > 2$, οι ρητοί πρώτοι αναλύονται ως εξής (ζ είναι αρχική ρίζα τάξης p):

i) $(p) = (\zeta - 1)^{p-1}$, $(\zeta - 1)$ πρώτο ιδεώδες βαθμού 1.

ii) Αν $p' \neq p$ και f είναι η τάξη του p' modulo p (= ο ελάχιστος εκθέτης ν τέτοιος ώστε $p'^{\nu} \equiv 1 \pmod p$· ως γνωστόν, $f \mid p-1$), τότε

$$(p') = p'_1 \cdots p'_g \quad , g = (p-1)/f ,$$

όπου, καθένα απ' τα διαφορετικά πρώτα ιδεώδη $p'_1, \dots, p'_g$ είναι βαθμού f.

Απόδειξη. Το (i) έχει ήδη αποδειχθεί στην αρχή του Ε. Έστω τώρα $p' \neq p$ και p' πρώτο ιδεώδες που διαιρεί το p'. Θα δείξουμε ότι ο βαθμός του p' είναι f. Έστω ότι

είναι s. Επειδή $p'^s = N(p') \equiv 1 \pmod{p}$ (λόγω του λήμματος), πρέπει, εξ ορισμού του f, να είναι $s \geq f$. Θα δείξομε τώρα ότι $s \leq f$. Έστω τώρα $\alpha \in A$. Ας γράψομε το α ως εξής:

$$\alpha = \sum_{i=0}^{p-2} a_i \zeta^i \quad , \quad a_i \in \mathbb{Z} \quad , \quad i = 0, \ldots, p-2 \qquad (1)$$

Λόγω των παρακάτω σχέσεων:

$$\zeta^{p'^f} = \zeta \quad (\text{διότι } p'^f \equiv 1 \pmod{p}),$$

$$(\beta+\gamma)^{p'^f} \equiv \beta^{p'^f} + \gamma^{p'^f} \pmod{p'} \text{ για όλα τα } \beta, \gamma \in A$$
(από την ανάπτυξη του διωνύμου του Νεύτωνα),

$$a^{p'^f} \equiv a \pmod{p'} \quad \forall\, a \in \mathbb{Z} \quad (\text{από το μικρό θεώρημα του Fermat}),$$

έπεται, σχηματίζοντας την (1) στη δύναμη p'^f,

$$\alpha^{p'^f} \equiv \alpha \pmod{p'}, \text{ δηλαδή } (\alpha^{p'^f} - \alpha) \subseteq (p') \subseteq p'.$$

Συμπεραίνομε λοιπόν ότι κάθε $\hat{\alpha} \in A/p'$ είναι ρίζα του πολυωνύμου $t^{p'^f} - t \in A/p'[t]$. Όμως, σε οποιοδήποτε σώμα, το πλήθος των ριζών ενός πολυωνύμου είναι, το πολύ, ίσο με το βαθμό του. Κατα συνέπεια, $\operatorname{card} A/p' \leq p'^f$, δηλαδή $p'^s \leq p'^f$ και $s \leq f$. Δείξαμε λοιπόν ότι ο τυχών πρώτος διαιρέτης p' του p' έχει βαθμό f. Επιπλέον ο p' δεν διακλαδώνεται, σύμφωνα με το Θεώρημα 13, §7 (βλ. και Θεώρημα 13, §3, Κεφάλαιο 1) άρα, σύμφωνα με το Θεώρημα 9, §6, το πλήθος των πρώτων διαιρετών p' του p' είναι $(p-1)/f$, ό.ε.δ.

ΚΕΦΑΛΑΙΟ 4

§1. Διακριτές υποομάδες του $\mathbb{R}^n$.

Ορισμός. Μιά προσθετική υποομάδα H του $\mathbb{R}^n$ λέγεται διακριτή ἄν ἡ τομή της μέ ὁποιοδήποτε φραγμένο ὑποσύνολο τοῦ $\mathbb{R}^n$ εἶναι πεπερασμένη (ἤ κενή).

Θεώρημα 1. Οἱ διακριτές υποομάδες τοῦ $\mathbb{R}^n$ εἶναι, ἀκριβῶς, τά $\mathbb{Z}$-modules τοῦ $\mathbb{R}^n$, πού παράγονται ἀπό $r \leq n$ γραμμικῶς ἀνεξάρτητα πάνω στό $\mathbb{R}$ διανύσματα τοῦ $\mathbb{R}^n$.

Ἀπόδειξη. Ἔστω H μιά διακριτή υποομάδα τοῦ $\mathbb{R}^n$ καί $\{e_1,\dots,e_r\}$ ἕνα σύστημα γραμμικῶς ἀνεξαρτήτων πάνω ἀπ' τό $\mathbb{R}$ διανυσμάτων τοῦ H μέ τό r μέγιστο δυνατό. Ἔστω

$$P = \{ \sum_{i=1}^{r} \alpha_i e_i \ , \ 0 \leq \alpha_i \leq 1 \} \subseteq \mathbb{R}^n$$

τό παραλληλεπίπεδο, πού κατασκευάζεται μέ τά $e_1,\dots,e_r$. Τό P εἶναι φραγμένο, ἄρα τό $P \cap H$ εἶναι πεπερασμένο. Ἔστω τώρα ὁποιοδήποτε $x \in H$. Ἐπειδή τό $\{x, e_1,\dots,e_r\}$ ἀποτελεῖται ἀπό $\mathbb{R}$-γραμμικῶς ἐξαρτημένα διανύσματα, θά ἔχομε μιά σχέση τῆς μορφῆς $x = \sum_{i=1}^{r} \lambda_i e_i$, $\lambda_i \in \mathbb{R}$ $(i=1,\dots,r)$.

Γιά κάθε $j \in \mathbb{Z}$ θέτομε

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i \ \in H \ ,$$

ὁπότε $x_j = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i \ \in P$, ἄρα καί $x_j \in P \cap H$ γιά κάθε $j \in \mathbb{Z}$. Ἐπίσης, $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$ καί, ἐπειδή $x_1, e_1,\dots,e_r \in P \cap H$, ἕπεται ὅτι ἡ H εἶναι $\mathbb{Z}$-module, πού παράγεται ἀπ' τό πεπερασμένο σύνολο $P \cap H$.
Ἀφ' ἑτέρου, ἐπειδή $x_j \in P \cap H$ γιά ὅλα τά $j \in \mathbb{Z}$, θά ὑπάρχουν

$j,k \in \mathbb{Z}$, $j \neq k$ τέτοια ώστε $x_j = x_k$, δηλαδή, για κάθε $i=1,\dots,r$ θα έχουμε $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$, άρα $\lambda_i \in \mathbb{Q}$ $(i=1,\dots,r)$. Συνεπώς, κάθε διάνυσμα του H και, ειδικώτερα, του $P \cap H$ είναι γραμμικός συνδυασμός των $e_1,\dots,e_r$ με ρητούς συντελεστές. Έστω d το ΕΚΠ των παρονομαστών των συντελεστών που συναντούμε όταν γράφουμε τα διανύσματα του $P \cap H$ ως γραμμικούς συνδυασμούς των $e_1,\dots,e_r$. Επειδή η H είναι $\mathbb{Z}$-module παραγόμενο απ' τα διανύσματα του $P \cap H$ (όπως είδαμε παραπάνω), έπεται ότι $H \subseteq \frac{1}{d}\mathbb{Z}e_1 + \dots + \frac{1}{d}\mathbb{Z}e_r$.

Άρα το $\mathbb{Z}$-module dH είναι υπο-module του $\sum_{i=1}^{r} \mathbb{Z}\cdot e_i$, δηλαδή υπάρχει μια βάση $f_1,\dots,f_r$ του $\sum_{i=1}^{r} \mathbb{Z}\cdot e_i$ και μη μηδενικοί ακέραιοι $a_1,\dots,a_s$, $s \leq r$ εις τρόπον ώστε τα διανύσματα $a_1f_1,\dots,a_sf_s$ ν' αποτελούν βάση του $\mathbb{Z}$-module dH. Αφ' ετέρου $dH \subseteq \sum_{i=1}^{r} \mathbb{Z}e_i \subseteq H$ και βλέποντας τα

dH, $\sum_{i=1}^{r} \mathbb{Z}e_i$ και H ως αβελιανές δμάδες με βαθμούς s, r και s, αντιστοίχως, συμπεραίνομε ότι $s \leq r \leq s$, άρα $s=r$. Άρα η H είναι το $\mathbb{Z}$-module που παράγεται απ' τα $\frac{a_1}{d}f_1, \dots, \frac{a_r}{d}f_r$ και μένει να δείξομε την ανεξαρτησία αυτών των διανυσμάτων πάνω απ' το $\mathbb{R}$. Αρκεί να δείξομε ότι τα $f_1,\dots,f_r$ είναι $\mathbb{R}$-γραμμικώς ανεξάρτητα: Θέτομε

$f_i = \sum_{j=1}^{r} b_{ij}e_j$, $b_{ij} \in \mathbb{Z}$ $(i=1,\dots,r)$. Αν ίσχυε μια σχέση της μορφής $\sum_{i=1}^{r} \lambda_i f_i = 0$ με $(\lambda_1,\dots,\lambda_r) \in \mathbb{R}^r - \{(0,0,\dots,0)\}$, τότε

$$\sum_{j=1}^{r} \left(\sum_{i=1}^{r} b_{ij}\lambda_i \right) e_j = 0 \quad , \text{άρα} \quad \sum_{i=1}^{r} b_{ij}\lambda_i = 0 \quad (j=1,\dots,r).$$

Το γραμμικό δμογενές σύστημα με πίνακα (b_{ij}) έχει μη τετριμμένη λύση άρα $\det(b_{ij}) = 0$. Η τελευταία σχέση, σε συνδυασμό με το ότι $b_{ij} \in \mathbb{Q}$ $\forall i,j$, συνεπάγονται την

ὑπαρξη ρητῆς λύσης $(\rho_1,\dots,\rho_r)\in\mathbb{Q}^r-\{(0,0,\dots,0)\}$ τοῦ ὁμογενοῦς συστήματος, ποὺ θεωρήσαμε μόλις πρίν. Τότε ὅμως $\sum_{i=1}^{r}\rho_i f_i = 0$ καὶ πολλαπλασιάζοντας ἐπὶ τὸ ΕΚΠ τῶν παρονομαστῶν τῶν ρ_i $(i=1,\dots,r)$ καταλήγομε στὸ συμπέρασμα ὅτι τὰ $f_1,\dots,f_r$ εἶναι $\mathbb{Z}$-γραμμικῶς ἐξαρτημένα, γεγονὸς ποὺ ἀντίκειται στὸν ὁρισμό τους.

Ἀντιστρόφως, ἔστω ὅτι τὰ $e_1,\dots,e_r$ εἶναι $\mathbb{R}$-γραμμικῶς ἀνεξάρτητα διανύσματα τοῦ $\mathbb{R}^n$ καὶ θεωροῦμε τὸ $\mathbb{Z}$-module $H=\mathbb{Z}e_1+\cdots+\mathbb{Z}e_r$. Προφανῶς τὸ H εἶναι ὑποομάδα τῆς προσθετικῆς ὁμάδας $\mathbb{R}^n$ καὶ ἀρκεῖ νὰ δείξομε ὅτι αὐτὴ εἶναι διακριτή. Συμπληρώνομε τὸ $\{e_1,\dots,e_r\}$ μὲ διανύσματα $e_{r+1},\dots,e_n$ (στὴν περίπτωση ποὺ $r<n$) σχηματίζοντας n γραμμικῶς ἀνεξάρτητα διανύσματα τοῦ $\mathbb{R}^n$. Ἀρκεῖ νὰ δείξομε ὅτι ἡ τομὴ τοῦ $M=\mathbb{Z}e_1+\cdots+\mathbb{Z}e_n$ μὲ ὁποιοδήποτε φραγμένο ὑποσύνολο τοῦ $\mathbb{R}^n$ εἶναι πεπερασμένο σύνολο. Πρὸς τοῦτο, ἀρκεῖ πάλι νὰ δείξομε ὅτι ἡ τομὴ τοῦ M μὲ μιὰ ὁποιαδήποτε ἀνοικτὴ σφαῖρα κέντρου $0\in\mathbb{R}^n$ εἶναι πεπερασμένο σύνολο: Θεωροῦμε τὴ βάση $e_1^*,\dots,e_n^*$ τοῦ $\mathbb{R}^n$ ποὺ ὁρίζεται ἀπὸ τὶς σχέσεις:

$$\langle e_i^*, e_j\rangle = \delta_{ij} \qquad 1\le i,j\le n\,.$$

Ἔστω τώρα ἡ σφαῖρα S κέντρου 0 καὶ ἀκτῖνας ℓ καὶ $x\in S\cap M$. Θέτομε $x=a_1e_1+\cdots+a_ne_n$, $a_i\in\mathbb{Z}$ $(i=1,\dots,n)$. Τότε $a_i=\langle x,e_i^*\rangle$ ὁπότε (ἀνισότης Cauchy-Schwarz) $|a_i|=|\langle x,e_i^*\rangle|\le\|x\|\cdot\|e_i^*\|<\ell\cdot\|e_i^*\|$, ὁπότε τὸ a_i μπορεῖ νὰ πάρει πεπερασμένο μόνο πλῆθος ἀκεραίων τιμῶν, γιὰ κάθε $i=1,\dots,n$. Συνεπῶς καὶ τὸ x μόνο πεπερασμένες τιμὲς μπορεῖ νὰ πάρει, ὁπότε τὸ $S\cap M$ εἶναι πεπερασμένο, ὅ.ἐ.δ.

Ὁρισμός. Μιὰ διακριτὴ ὑποομάδα τοῦ $\mathbb{R}^n$, ποὺ παράγεται ἀπὸ n γραμμικῶς ἀνεξάρτητα διανύσματα τοῦ $\mathbb{R}^n$ λέγεται δικτυωτὸ τοῦ $\mathbb{R}^n$.

Σύμφωνα με τον προηγούμενο ορισμό, κάθε δικτυωτό του $\mathbb{R}^n$ είναι της μορφής $\mathbb{Z}e_1+\cdots+\mathbb{Z}e_n$, όπου $\mathcal{E}=\{e_1,\ldots,e_n\}$ είναι μια βάση του $\mathbb{R}^n$. Θα συμβολίζουμε με $P_{\mathcal{E}}$ το παραλληλεπίπεδο $\{\sum_{i=1}^{n}\alpha_i e_i,\ 0\le\alpha_i<1\ (i=1,\ldots,n)\}$ και θα το λέμε θεμελιώδες παραλληλεπίπεδο, που αντιστοιχεί στη βάση $\mathcal{E}$. Είναι προφανές ότι κάθε $x\in\mathbb{R}^n$ είναι ισοδύναμο modulo H με ένα ακριβώς σημείο $y\in P_{\mathcal{E}}$. Δηλαδή, δοθέντος του $x\in\mathbb{R}^n$, υπάρχει ένα ακριβώς $y\in P_{\mathcal{E}}$ τέτοιο ώστε $x-y\in H$.

Στα παρακάτω, αν $A\subseteq\mathbb{R}^n$ είναι μετρήσιμο κατά Lebesgue, θα συμβολίζουμε με $\mu(A)$ το μέτρο (ή όγκο) του A.

<u>Θεώρημα 2.</u> Αν το H είναι δικτυωτό του $\mathbb{R}^n$ και παράγεται απ' τις βάσεις $\mathcal{E}=\{e_1,\ldots,e_n\}$ και $\mathcal{F}=\{f_1,\ldots,f_n\}$, τότε $\mu(P_{\mathcal{E}})=\mu(P_{\mathcal{F}})$.

Απόδειξη. Έχουμε κάποιες σχέσεις

$$f_i=\sum_{j=1}^{n}a_{ij}e_j\ ,\ a_{ij}\in\mathbb{Z}\ \ (j=1,\ldots n),\ i=1,\ldots,n\ .$$

άρα $\mu(P_{\mathcal{F}})=|\det(a_{ij})|\cdot\mu(P_{\mathcal{E}})\ge\mu(P_{\mathcal{E}})$. Λόγω συμμετρίας ισχύει και η αντίστροφη ανισότητα $\mu(P_{\mathcal{E}})\ge\mu(P_{\mathcal{F}})$, απ' όπου το αποδεικτέο.

<u>Ορισμός.</u> Αν το H είναι δικτυωτό του $\mathbb{R}^n$, τότε ο όγκος ενός οποιουδήποτε θεμελιώδους παραλληλεπιπέδου, που αντιστοιχεί σε βάση του H (σύμφωνα με το Θεώρημα 2 είναι ανεξάρτητος της βάσης) συμβολίζεται με $v(H)$ και ονομάζεται θεμελιώδης όγκος του δικτυωτού H.

Θεώρημα 3. Αν H είναι ένα δικτυωτό του $\mathbb{R}^n$ και S ένα μετρήσιμο υποσύνολο του $\mathbb{R}^n$, τέτοιο ώστε $\mu(S) > v(H)$, τότε υπάρχουν $x, y \in S$, $x \neq y$ τέτοια ώστε $x - y \in H$.

Απόδειξη. Έστω $\mathcal{E}$ μιά βάση του δικτυωτού H. Λόγω της μονοσήμαντης ανάλυσης των στοιχείων του $\mathbb{R}^n$ σε άθροισμα ενός στοιχείου του H και ενός του $P_{\mathcal{E}}$ (βλ. πρίν απ' την εκφώνηση του θεωρήματος 2), ισχύει

$$S = \bigcup_{h \in H} (S \cap (h + P_{\mathcal{E}})),$$

όπου τα σύνολα που απαρτίζουν την ένωση στο δεξιό μέλος είναι ανά δύο ξένα. Συνεπώς

$$\mu(S) = \sum_{h \in H} \mu(S \cap (h + P_{\mathcal{E}})) = \sum_{h \in H} \mu((-h + S) \cap P_{\mathcal{E}}) \quad (1$$

(η τελευταία ισότητα είναι συνέπεια του αναλλοίωτου του όγκου κατά τις μεταφορές). Αν ήταν όλα τα σύνολα $(-h + S) \cap P_{\mathcal{E}}$ $(h \in H)$ ξένα ανά δύο, τότε το δεξιώτερο μέλος της (1) θα ήταν $\leq \mu(P_{\mathcal{E}}) = v(H)$, γεγονός που θα ερχόταν σε αντίφαση με την υπόθεση $\mu(S) > v(H)$. Συνεπώς, υπάρχουν $h, h' \in H$, $h \neq h'$ τέτοια ώστε τα σύνολα $(-h + S) \cap P_{\mathcal{E}}$ και $(-h' + S) \cap P_{\mathcal{E}}$ να έχουν μή κενή τομή.

Άρα υπάρχουν $x, y \in S$ τέτοια ώστε $-h + x = -h' + y$, άρα $x - y = h - h' \in H$ και $x - y \neq 0$, ὅ. ἐ. δ.

Θεώρημα 4 (Minkowski) Έστω H δικτυωτό του $\mathbb{R}^n$ και $S \subseteq \mathbb{R}^n$ μετρήσιμο, συμμετρικό ως προς την αρχή και κυρτό. Αν (α) $\mu(S) > 2^n \cdot v(H)$ ή (β) $\mu(S) \geq 2^n \cdot v(H)$ και το S είναι συμπαγές (στην περίπτωση (β) απαιτείται μόνο) τότε το $S \cap H$ περιέχει σημείο διαφορο της αρχής.

Απόδειξη. (α) Παρατηρούμε ότι το $S' = \frac{1}{2}S$ ικανοποιεί την απαίτηση του θεωρήματος 3, άρα υπάρχουν

$$x, y \in S' , \ x \neq y \ , \ x - y \in H . \qquad (1)$$

Στη συνέχεια παρατηρούμε ότι $2x, 2y \in S$ και λόγω συμμετρίας του S ως προς την αρχή, $-2y \in S$. Λόγω κυρτότητος του S και το $\frac{1}{2}(2x + (-2y))$ ανήκει στο S. Δηλαδή, $x - y \in S$ και απ' την (1) τώρα, $x - y \in S \cap H$ και $x - y \neq 0$, ό.ε.δ. (β) Για κάθε $\nu = 1, 2, \ldots$ το $(1 + \frac{1}{\nu})S$ πληροί τις απαιτήσεις του (α) όπότε $(1 + \frac{1}{\nu})S \cap H^* \neq \phi$, όπου $H^* = H - \{0\}$. Αφ' ετέρου, η απεικόνιση

$$\mathbb{R}^n \ni x \longrightarrow (1 + \tfrac{1}{\nu})x \in \mathbb{R}^n$$

είναι διαιομορφισμός, όπότε το $(1 + \frac{1}{\nu})S$ είναι συμπαγές σύνολο, άρα η τομή $(1 + \frac{1}{\nu})S \cap H^*$ είναι πεπερασμένη. Έπίσης, λόγω της κυρτότητος του S, είναι εύκολο να 'δεί κανείς ότι αν $\alpha, \beta \in \mathbb{R}$ και $\alpha < \beta$ τότε $\alpha S \subseteq \beta S$. Άρα, η ακολουθία των μη κενών και πεπερασμένων συνόλων $(1 + \frac{1}{\nu})S \cap H^*$, $\nu = 1, 2, \ldots$, είναι φθίνουσα άρα, κατ' ανάγκη, τελικώς σταθερή, δίστερ' από το δείκτη ν_0, άς πούμε. Μ' άλλα λόγια,

$$\bigcap_{\nu \in \mathbb{N}} \left(H^* \cap (1 + \tfrac{1}{\nu})S\right) = H^* \cap (1 + \tfrac{1}{\nu_0})S \neq \phi$$

Έστω, λοιπόν, $x \in H^* \cap (1 + \frac{1}{\nu_0})S$. Τότε

$$x \in \bigcap_{\nu \in \mathbb{N}} \left(H^* \cap (1 + \tfrac{1}{\nu})S\right) = H^* \bigcap_{\nu \in \mathbb{N}} (1 + \tfrac{1}{\nu})S \ ,$$

όπότε αρκεί να αποδείξομε ότι $\bigcap_{\nu \in \mathbb{N}} (1 + \frac{1}{\nu})S \subseteq S$. Πράγματι, έστω

$y \in \bigcap_{\nu \in \mathbb{N}} (1 + \frac{1}{\nu})S$. Τότε, για κάθε ν υπάρχει $y_\nu \in S$ τέτοιο

ώστε $y = (1 + \frac{1}{\nu})y_\nu$. Επειδή το S είναι φραγμένο σύνολο, $\lim_\nu (y_\nu / \nu) = 0$, άρα $\lim_\nu y_\nu = \lim_\nu (y - y_\nu/\nu) = y$ και τώρα,

λόγω συμπαγείας του S, $y \in S$, ό.ε.δ.

2. Γεωμετρική παράσταση ενός αριθμητικού σώματος.

Έστω K ένα αριθμητικό σώμα βαθμού n. Τότε υπάρχουν ακριβώς n ισομορφες εμφυτεύσεις $\sigma : K \longrightarrow \mathbb{C}$ με την ιδιότητα $\sigma(q) = q \ \forall q \in \mathbb{Q}$. Οι εμφυτεύσεις αυτές μπορεί να' δριοθούν ως εξής. Έστω $K = \mathbb{Q}(\theta)$ και $\phi(t) \in \mathbb{Q}[t]$ το ελάχιστο πολυώνυμο του θ. Το $\phi(t)$ είναι ανάγωγο πάνω απ' το $\mathbb{Q}$ βαθμού n, συνεπώς έχει ακριβώς n διαφορετικές, απλές ρίζες $\theta_1, \dots, \theta_n$. Τότε οι n ισομορφες εμφυτεύσεις $K \longrightarrow \mathbb{C}$ είναι οι

$$\sigma_i : K \to \mathbb{C} \ , \ \sigma_i(\theta) = \theta_i \ , \ \sigma_i(q) = q \ \forall q \in \mathbb{Q} \quad (i = 1, \dots, n).$$

Έστω ότι το $\phi(t)$ έχει s πραγματικές ρίζες και t ζεύγη συζυγών μιγαδικών ριζών, δηλαδή $s + 2t = n$. Στο εξής θα' δηοθέτομε τις ρίζες $\theta_1, \dots, \theta_n$ αριθμημένες ως εξής:

$$\theta_1, \dots, \theta_s \in \mathbb{R} \ , \ \theta_{s+1} \ , \ \theta_{s+2} = \overline{\theta}_{s+1} \ , \ \dots \ , \ \theta_{s+t} \ , \ \theta_{s+2t} = \overline{\theta}_{s+t} \ ,$$

όπου η μπάρα $\overline{\ }$ δηλοί τη μιγαδική συζυγία. Αντιστοίχως, οι ισόμορφες εμφυτεύσεις (τους δηοίους, απλούστερα, άς λέμε ισομορφισμούς) θα' αριθμούνται και θα' συμβολίζονται

$\sigma_1, \dots, \sigma_s$ (πραγματικοί ισομορφισμοί)

$\sigma_{s+1}, \overline{\sigma}_{s+1}, \dots, \sigma_{s+t}, \overline{\sigma}_{s+t}$ (μιγαδικοί ισομορφισμοί).

Τέλος, άν $z = x + iy \in \mathbb{C}$, $x, y \in \mathbb{R}$, συμβολίζομε $Re(z) = x$ και $Im(z) = y$.

Ορισμός. Σε κάθε $\alpha \in K$ αντιστοιχούμε το

$$\sigma(\alpha) = (\sigma_1(\alpha), \dots, \sigma_s(\alpha) ; Re(\sigma_{s+1}(\alpha)), Im(\sigma_{s+1}(\alpha)) ; \dots ; Re(\sigma_{s+t}(\alpha)), Im(\sigma_{s+t}(\alpha)),$$

το δηοίο δνομάζομε γεωμετρική παράσταση του α στο $\mathbb{R}^n$.

Θεώρημα 5. Αν M είναι ένα $\mathbb{Z}$-module του K και $\{x_1,\dots,x_n\}$ είναι μιά βάση του, τότε τό $\sigma(M)$ είναι ένα δικτυωτό του $\mathbb{R}^n$ και

$$v(\sigma(M)) = 2^{-t}\sqrt{|d|}, \qquad (1)$$

όπου d η διακρίνουσα της παραπάνω βάσης.

Απόδειξη. Έξ υποθέσεως $M = \mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$, δπότε $\sigma(M) = \mathbb{Z}\sigma(x_1) + \dots + \mathbb{Z}\sigma(x_n)$, δηλαδή τό $\sigma(M)$ είναι $\mathbb{Z}$-module, πού παράγεται άπ' τά $\sigma(x_1),\dots,\sigma(x_n)$. Άπ' τό Θεώρημα 1 έπεται ότι $\sigma(M)$ είναι διακριτή υποομάδα του $\mathbb{R}^n$, άρα, γιά νά είναι δικτυωτό, αρκεί ν' αποδείξομε ότι τά $\sigma(x_1),\dots,\sigma(x_n)$ είναι γραμμικώς ανεξάρτητα διανύσματα του $\mathbb{R}^n$. Πρός τούτο μελετούμε την ορίζουσα του $n\times n$ πίνακα $\begin{pmatrix}\sigma(x_1)\\ \vdots \\ \sigma(x_n)\end{pmatrix}$. Η απόλυτη τιμή της ορίζουσας αύτης μάς δίνει τον όγκο του θεμελιώδους παραλληλεπιπέδου, πού αντιστοιχεί στη βάση $\{\sigma(x_1),\dots,\sigma(x_n)\}$ του $\mathbb{R}^n$ (είναι βάση, έφ' όσον αποδειχθεί μή μηδενική η παραπάνω ορίζουσα). Η i-οστή γραμμή του θεωρουμένου πίνακα είναι $\sigma_1(x_i),\dots,\sigma_s(x_i), \frac{1}{2}(\sigma_{s+1}(x_i)+\overline{\sigma}_{s+1}(x_i)), \frac{1}{2i}(\sigma_{s+1}(x_i)-\overline{\sigma}_{s+1}(x_i)),\dots$

Για τον υπολογισμό της ορίζουσας ακολουθούμε την εξής διαδικασία: Κάθε στήλη πού έχει συντελεστή $\frac{1}{2i}$ πολλαπλασιάζεται επί i και προστίθεται στην αμέσως προηγούμενη στήλη. Έτσι φτάνομε σέ μιά ορίζουσα, της όποίας η i-οστή γραμμή είναι $\sigma_1(x_i),\dots,\sigma_s(x_i), \sigma_{s+1}(x_i), \frac{1}{2i}(\sigma_{s+1}(x_i)-\overline{\sigma}_{s+1}(x_i)), \sigma_{s+2}(x_i),\dots$.

Πολλαπλασιάζοντας τις στήλες $\begin{pmatrix}\sigma_{s+1}(x_1)\\ \vdots\\ \sigma_{s+1}(x_n)\end{pmatrix},\dots,\begin{pmatrix}\sigma_{s+t}(x_1)\\ \vdots\\ \sigma_{s+t}(x_n)\end{pmatrix}$ επί $-\frac{1}{2i}$, και προσθέτοντας κάθε μία στην αμέσως επόμενή της στήλη, φτάνομε σέ όρίζουσα, της όποίας η i-οστή γραμμή είναι $\sigma_1(x_i),\dots,\sigma_s(x_i), \sigma_{s+1}(x_i), -\frac{1}{2i}\overline{\sigma}_{s+1}(x_i),\dots$,

άρα ίσούται μέ $(-1/2i)^t$, επί την ορίζουσα, πού η i-οστή γραμ-

μή εἶναι : $\sigma_1(x_i), \dots, \sigma_s(x_i), \sigma_{s+1}(x_i), \overline{\sigma}_{s+1}(x_i), \dots, \sigma_{s+t}(x_i), \overline{\sigma}_{s+t}(x_i)$ καί ἡ τελευταία ὁρίζουσα εἶναι d, ὅ. ἔ. δ.

<u>Θεώρημα 6.</u> Ἔστω A ὁ δακτύλιος τῶν ἀκεραίων τοῦ K, d ἡ διακρίνουσα τοῦ K καί $\mathfrak{a}$ ἕνα μή μηδενικό ἀκέραιο ἰδεῶδες τοῦ A. Τότε τά $\sigma(A)$ καί $\sigma(\mathfrak{a})$ εἶναι δικτυωτά τοῦ $\mathbb{R}^n$ καί

$$v(\sigma(A)) = 2^{-t}\sqrt{|d|}\,, \quad v(\sigma(\mathfrak{a})) = 2^{-t}\sqrt{|d|}\cdot N(\mathfrak{a}).$$

Ἀπόδειξη. Ὁ δακτύλιος A εἶναι ἕνα $\mathbb{Z}$-module μέ βάση ἀποτελούμενη ἀπό n στοιχεῖα (Θεώρημα 9, Κεφάλαιο 1, §2). Ἄρα καί τό $\mathfrak{a}$ (ὡς ὑποομάδα τῆς προσθετικῆς ὁμάδας A) θά εἶναι $\mathbb{Z}$-module μέ βάση ἀποτελούμενη ἀπό ὄχι περισσότερα ἀπό n στοιχεῖα. Ἀφ' ἑτέρου, ὑπάρχουν n $\mathbb{Z}$-γραμμικῶς ἀνεξάρτητα στοιχεῖα στό $\mathfrak{a}$ (ἄν π.χ. $x_1, \dots, x_n$ εἶναι ἀνεξάρτητα στοιχεῖα τοῦ A, τότε τά $ax_1, \dots, ax_n$, γιά ὁποιοδήποτε $a \in \mathfrak{a}$, $a \neq 0$, εἶναι n $\mathbb{Z}$-γραμμικῶς ἀνεξάρτητα στοιχεῖα τοῦ $\mathfrak{a}$), ἄρα τό $\mathbb{Z}$-module $\mathfrak{a}$ ἔχει βάση ἀπό n στοιχεῖα. Ἔστω ὅτι $A = \mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$ καί $\mathfrak{a} = \mathbb{Z}y_1 + \dots + \mathbb{Z}y_n$ καί οἱ βάσεις $\{x_1, \dots, x_n\}$ καί $\{y_1, \dots, y_n\}$ τοῦ K ἔχουν διακρίνουσες d καί d', ἀντιστοίχως. Προφανῶς, ἡ διακρίνουσα τοῦ K εἶναι d διότι $\{x_1, \dots, x_n\}$ εἶναι μιά ἀκέραια βάση τοῦ K. Ἀφ' ἑτέρου, λόγῳ τοῦ θεωρήματος τά $\sigma(A)$ καί $\sigma(\mathfrak{a})$ εἶναι δικτυωτά τοῦ $\mathbb{R}^n$ καί $v(\sigma(A)) = 2^{-t}\sqrt{|d|}$ καί $v(\sigma(\mathfrak{a})) = 2^{-t}\cdot\sqrt{|d'|}$. Συνεπῶς, μένει ν' ἀποδείξομε ὅτι $\sqrt{|d'|} = \sqrt{|d|}\cdot N(\mathfrak{a})$: Ἔστω

$$y_i = \sum_{j=1}^{n} c_{ij}x_j\,, \quad c_{ij} \in \mathbb{Z}\ (j=1,\dots,n)\,, \quad i=1,\dots,n \qquad (1)$$

. Τότε $d' = D(y_1, \dots, y_n) = (\det(c_{ij}))^2 \cdot D(x_1, \dots, x_n) = (\det(c_{ij}))^2 \cdot d$. Ἀλλά, ἀπ' τή θεωρία τῶν Ἀβελιανῶν ὁμάδων εἶναι γνωστό ὅτι ἡ σχέση (1) (ἐδῶ θεωροῦμε τήν A ἀβελιανή ὁμάδα, ἐλευθέρα στρέψεως, καί τήν $\mathfrak{a}$ ὑποομάδα της) συνεπάγεται τήν $[A:\mathfrak{a}] = |\det(c_{ij})|$. Ὅμως, ἐξ ὁρισμοῦ $[A:\mathfrak{a}] = N(\mathfrak{a})$, ὅ. ἔ. δ.

3. Η ομάδα των κλάσεων ιδεωδών.

Σ' αυτήν την παράγραφο το K θα είναι ένα αριθμητικό σώμα και A ο δακτύλιος των ακεραίων του. Σύμφωνα με το θεώρημα 3(β), §3, Κεφάλαιο 3, τα μη μηδενικά κλασματικά ιδεώδη του K είναι μια πολλαπλασιαστική αβελιανή ομάδα, στην οποία ορίζομε μια σχέση ισοδυναμίας ως εξής:
Άν τα α, β είναι κλασματικά ιδεώδη του K, όχι (0), τότε
$\alpha \sim \beta \iff$ υπάρχει $\gamma \in K$, τέτοιο ώστε $\beta = (\gamma)\cdot\alpha$.
Την κλάση ισοδυναμίας του α συμβολίζομε με $[\alpha]$. Παρατηρούμε ότι, για κάθε $\gamma \in K$, $[(\gamma)] = [(1)] = [A] := \mathbf{1}$.
Ορίζομε πολλαπλασιασμό κλάσεων ως εξής:

$$[\alpha]\cdot[\beta] = [\alpha\cdot\beta]$$

και είναι προφανές ότι η πράξη αυτή είναι καλά ορισμένη και καθιστά το σύνολο $\{[\alpha] : \alpha \neq (0)$ κλασματικό ιδεώδες του $K\}$ αβελιανή ομάδα, την οποία θα συμβολίζομε G_K και θα λέμε <u>ομάδα κλάσεων ιδεωδών του K</u>. Ο αντικειμενικός σκοπός αυτής της παραγράφου είναι ν' αποδείξομε ότι η G_K είναι πεπερασμένη.

<u>Λήμμα</u>. Έστω H δικτυωτό του $\mathbb{R}^n$, $n = s+2t$ $(s, t \geq 0)$ και $c_1, \ldots, c_{s+t}$ θετικοί αριθμοί τέτοιοι ώστε

$$\prod_{i=1}^{s+t} c_i > \left(\frac{4}{\pi}\right)^t \cdot v(H) \ .$$

Τότε, υπάρχει ένα μη μηδενικό σημείο $(x_1, \ldots, x_s, y_{s+1}, z_{s+1}, \ldots, y_{s+t}, z_{s+t})$ του H, τέτοιο ώστε

$$|x_i| < c_i \ (i = 1, \ldots, s) \text{ και } y_{s+i}^2 + z_{s+i}^2 < c_{s+i} \ (i = 1, \ldots, t) \qquad (1)$$

Απόδειξη. Έστω S το σύνολο των σημείων $(x_1, \ldots, x_s, y_{s+1}, z_{s+1}, \ldots, y_{s+t}, z_{s+t}) \in \mathbb{R}^n$, τα οποία ικανοποιούν τις (1). Αρκεί να δείξομε ότι $S \cap H \neq \{\mathbf{o}\}$. Είναι απλό ν' αποδείξει κανείς ότι το S είναι συμμετρικό ως προς $\mathbf{o}$ και κυρτό.

Ο όγκος του S είναι

$$\mu(S) = \int_S d(x_1, \dots, x_s, y_{s+1}, z_{s+1}, \dots, y_{s+t}, z_{s+t}) =$$

$$= \int_{-c_1}^{c_1} dx_1 \cdots \int_{-c_s}^{c_s} dx_s \cdot \iint_{y_{s+1}^2 + z_{s+1}^2 < c_{s+1}} dy_{s+1}\, dz_{s+1} \cdot \cdots \cdot \iint_{y_{s+t}^2 + z_{s+t}^2 < c_{s+t}} dy_{s+t}\, dz_{s+t} =$$

$$= (2c_1) \cdots (2c_s)(\pi c_{s+1}) \cdots (\pi c_{s+t}) = 2^s \cdot \pi^t \prod_{i=1}^{s+t} c_i >$$

$$> 2^s \cdot \pi^t \cdot \left(\frac{4}{\pi}\right)^t \cdot v(H) = 2^n \cdot v(H),$$

άρα το αποδεικτέο προκύπτει από το Θεώρημα 4, §1, Κεφάλαιο 4.

Έστω $[K:\mathbb{Q}] = n = s + 2t$, όπου τα s και t είναι όπως στην αρχή της §2, και d η διακρίνουσα του K.

<u>Θεώρημα 7.</u> Έστω $\mathfrak{a} \neq (0)$ ακέραιο ιδεώδες. Τότε, υπάρχει $\alpha \in \mathfrak{a}$, $\alpha \neq 0$ τέτοιο ώστε

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t \cdot N(\mathfrak{a}) \cdot \sqrt{|d|}$$

Απόδειξη. Έστω $\varepsilon > 0$. Ορίζουμε τώρα ως εξής τους θετικούς αριθμούς $c_1, \dots, c_{s+t}$:

$$c_i = \left[\left(\frac{2}{\pi}\right)^t \cdot N(\mathfrak{a}) \cdot \sqrt{|d|} + \varepsilon\right]^{1/(s+t)}, \quad i = 1, \dots, s+t.$$

Από το θεώρημα 6, §2, το $\sigma(\mathfrak{a})$ είναι δικτυωτό του $\mathbb{R}^n$ με όγκο $v(\sigma(\mathfrak{a})) = 2^{-t} \cdot N(\mathfrak{a}) \cdot \sqrt{|d|}$. Άρα

$$\prod_{i=1}^{s+t} c_i > \left(\frac{2}{\pi}\right)^t \cdot N(\mathfrak{a}) \cdot \sqrt{|d|} = \left(\frac{4}{\pi}\right)^t v(\sigma(\mathfrak{a})),$$

και το λήμμα συνεπάγεται ότι υπάρχει $\sigma(\alpha) \in S \cap \sigma(\alpha)$, όπου το S είναι όπως και στο λήμμα. Δηλαδή,

$$|\sigma_i(\alpha)| < c_i \quad (i=1,\dots,s), \quad (\mathrm{Re}\,\sigma_{s+i}(\alpha))^2 + (\mathrm{Im}\,\sigma_{s+i}(\alpha))^2 < c_{s+i} \quad (i=1,\dots,t)$$

και οι τελευταίες t ανισότητες ισοδυναμούν με τις

$$|\sigma_{s+i}(\alpha)|^2 \le c_{s+i} \quad (i=1,\dots,t)$$

Τότε, $|N(\alpha)| = |\sigma_1(\alpha)| \cdots |\sigma_s(\alpha)| \cdot |\sigma_{s+1}(\alpha)|^2 \cdots |\sigma_{s+t}(\alpha)|^2 < \prod_{i=1}^{s+t} c_i =$

$$\left(\frac{2}{\pi}\right)^t \cdot N(\alpha) \cdot \sqrt{|d|} + \varepsilon .$$

Άρα, σύμφωνα με τα παραπάνω, για κάθε $\nu = 1, 2, \dots$, υπάρχει $\alpha_\nu \in \alpha$ τέτοιο ώστε $\sigma(\alpha_\nu) \in \sigma(\alpha) \cap S_1$ και

$$|N(\alpha_\nu)| < \left(\frac{2}{\pi}\right)^t \cdot N(\alpha) \cdot \sqrt{|d|} + \frac{1}{\nu} , \qquad (1)$$

όπου S_1 είναι το σύνολο S, παραπάνω, που αντιστοιχεί στην τιμή $\varepsilon = 1$. Επειδή το $\sigma(\alpha)$ είναι δικτυωτό και το S_1 φραγμένο, συμπεραίνουμε ότι η ακολουθία $(\sigma(\alpha_\nu))_\nu$ είναι τελικώς σταθερά, άρα υπάρχει $\nu_0 \in \mathbb{N}$, τέτοιο ώστε $\alpha_{\nu_0} = \alpha_\nu$ για κάθε $\nu \ge \nu_0$. Συνεπώς, λόγω της (1),

$$|N(\alpha_{\nu_0})| < \left(\frac{2}{\pi}\right)^t \cdot N(\alpha) \cdot \sqrt{|d|} + \frac{1}{\nu} \quad \forall\, \nu \ge \nu_0 ,$$

άρα $|N(\alpha_{\nu_0})| \le \left(\frac{2}{\pi}\right)^t \cdot N(\alpha) \cdot \sqrt{|d|}$, δ.ε.δ.

Θεώρημα 8. Κάθε κλάση ιδεωδών περιέχει ένα ακέραιο ιδεώδες $\mathfrak{b}$, τέτοιο ώστε

$$N(\mathfrak{b}) \le \left(\frac{2}{\pi}\right)^t \sqrt{|d|} .$$

Απόδειξη. Έστω $[\tau]$ η δοθείσα κλάση, όπου τ ένα κλασματικό ιδεώδες του K. Υπάρχει $d \in A$ τέτοιο ώστε, τό $\sigma\tau = d\cdot\tau$ να είναι ακέραιο ιδεώδες και $[\sigma] = [\alpha]$. Έστω τώρα $\alpha \in \sigma$ τέτοιο ώστε $|N(\alpha)| \leq (2/\pi)^t N(\sigma)\sqrt{|d|}$ (θεώρημα 7). Τό ιδεώδες $\beta = \alpha\cdot\sigma^{-1}$ είναι ακέραιο, διότι $\beta = (\alpha)\cdot\sigma^{-1} \subseteq \sigma\cdot\sigma^{-1} = A$. Επίσης, $\sigma\beta = (\alpha)$ άρα $N(\sigma)\cdot N(\beta) = N(\sigma\beta) = N((\alpha)) = |N(\alpha)| \leq (2/\pi)^t N(\sigma)\sqrt{|d|}$, απ' όπου η αποδεικτέα.

Θεώρημα 9. Η ομάδα G_K των κλάσεων ιδεωδών του K είναι πεπερασμένη.

Απόδειξη. Λόγω του θεωρήματος 8, αρκεί ν' αποδείξομε ότι, δοθέντος ενός φυσικού αριθμού q, υπάρχει, το πολύ, πεπερασμένο πλήθος ακεραίων ιδεωδών β, τέτοιων ώστε $N(\beta) \mid q$. Έχομε $q = N(\beta) = \operatorname{card} A/\beta$, άρα $q(1+\beta) = \beta$, δηλαδή $q \in \beta$, άρα $\beta \mid (q)$, απ' όπου φαίνεται ότι το β ανήκει σ' ένα πεπερασμένο σύνολο (βλ. πρόταση γ, §5, κεφάλαιο 3), ό.ε.δ.

Ορισμός. Η τάξη της ομάδας G_K, η οποία είναι πεπερασμένη, σύμφωνα με το θεώρημα 9, συμβολίζεται με h_K και λέγεται αριθμός κλάσεων ιδεωδών του K.

Θεώρημα 10. Έστω σ ιδεώδες του K (κλασματικό). Τότε, (i) το σ^{h_K} είναι κύριο ιδεώδες.
(ii) Αν το σ^m είναι κύριο ιδεώδες και $(m, h_K) = 1$, τότε το σ είναι κύριο ιδεώδες.

Απόδειξη. Έστω G η πολλαπλασιαστική ομάδα των μη μηδενικών (κλασματικών) ιδεωδών του K και G_0 η υποομάδα των κυρίων ιδεωδών. Προφανώς $G_K \cong G/G_0$ μέσω του ισομορφισμού $G/G_0 \ni \sigma\cdot G_0 \longrightarrow [\sigma] \in G_K$.

Αφού η τάξη της G/G_0 είναι h_K, θά είναι $(\alpha G_0)^{h_K} = G_0$, δηλαδή $\alpha^{h_K} \in G_0$, τό όποίο άποδεικνύει τό (i).
(ii) Έστω $\alpha^m \in G_0$ καί $(m, h_K) = 1$. Θεωροῦμε τούς $u, v \in \mathbb{Z}$ έτσι ώστε $u \cdot h_K + v \cdot m = 1$. Τότε

$\alpha = \alpha^{u \cdot h_K + v \cdot m} = (\alpha^{h_K}) \cdot (\alpha^m)^v$, τό δπαῖο ἀνήκει στην ὑπο-ὁμάδα G_0, λόγῳ τῆς ὑπόθεσης μιά τό α^m καί τοῦ (i).

4. Ἀνάλυση σέ γινόμενο ἀναγώγων παραγόντων.

Οἱ συμβολισμοί τῆς προηγουμένης παραγράφου ἐξακολουθοῦν νά ἰσχύουν.

Ὁρισμός. Τό $\varepsilon \in A - \{0\}$ λέγεται ἑνάδα τοῦ A ἄν $\varepsilon^{-1} \in A$.
Τά στοιχεῖα $\alpha, \beta \in A - \{0\}$ λέγονται συνεταιρικά ἄν ὑπάρχει ἑνάδα ε τοῦ A, τέτοια ὥστε $\beta = \varepsilon \cdot \alpha$.
Τό $\pi \in A$ λέγεται ἀνάγωγο, ἄν οἱ μόνοι διαιρέτες του στό δακτύλιο A εἶναι οἱ ἑνάδες καί τά συνεταιρικά του στοιχεῖα, δίχως τό ἴδιο νά εἶναι ἑνάδα.

Παρατηρήσεις: (i) Οἱ ἑνάδες τοῦ A εἶναι πολλ/σιαστική ὁμάδα. (ii) Ἡ σχέση συνεταιρικότητας στόν A εἶναι ἰσοδυναμία.

Θεώρημα 11. Τό $\varepsilon \in A - \{0\}$ εἶναι ἑνάδα ἄν καί μόνο ἄν $N(\varepsilon) = \pm 1$.

Ἀπόδειξη. Γενικά, γιά κάθε $\alpha \in A - \{0\}$ ἰσχύει $\alpha \mid N(\alpha)$ (ἡ διαιρετότητα στό δακτύλιο A). Πράγματι, ἄν $t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0$ εἶναι τό χαρακτηριστικό πολυώνυμο τοῦ α, τότε $N(\alpha) = (-1)^n c_0$, ἄρα

$$\frac{N(\alpha)}{\alpha} = \frac{(-1)^n c_0}{\alpha} = (-1)^{n+1} \frac{(c_1 \alpha + \cdots + c_{n-1}\alpha^{n-1} + \alpha^n)}{\alpha} =$$

$= (-1)^{n+1}(c_1 + \cdots + c_{n-1}\alpha^{n-2} + \alpha^{n-1}) \in A$, δηλαδή $\alpha \mid N(\alpha)$.
Άν λοιπόν $N(\varepsilon) = \pm 1$, τότε $\varepsilon \mid 1$, πού σημαίνει ότι $\varepsilon^{-1} \in A$, δηλαδή τό ε είναι έναδα τού A.
Άντίστροφα, άν τό ε είναι έναδα τού A, τότε υπάρχει $\varepsilon' \in A$ έτσι ώστε $\varepsilon.\varepsilon' = 1$, άρα $1 = N(1) = N(\varepsilon).N(\varepsilon')$ καί οί $N(\varepsilon), N(\varepsilon')$ είναι ρητοί άκέραιοι (Θεώρημα 8, §2, κεφάλαιο 1). Συνεπώς, $N(\varepsilon) = \pm 1$.

Θεώρημα 12. Στό δακτύλιο A κάθε μή μηδενικό στοιχείο, πού δέν είναι έναδα, άναλύεται (όχι κατ' άνάγκη μονότροπα) σέ γινόμενο άναγώγων στοιχείων τού A.

Άπόδειξη. Έστω $\alpha \in A$ καί $|N(\alpha)| = p$ (πρώτος). Τότε τό α είναι άνάγωγο. Πράγματι, έστω δ διαιρέτης τού α καί $\alpha = \delta.\beta$, $\beta \in A$. Τότε $p = |N(\alpha)| = |N(\delta)|.|N(\beta)|$ καί $|N(\delta)|$, $|N(\beta)|$ είναι ρητοί άκέραιοι, όπότε $|N(\delta)| = 1$ ή p. Στήν πρώτη περίπτωση τό δ είναι έναδα (βάσει τού θεωρήματος 11), ένώ στή δεύτερη, $|N(\beta)| = 1$, τό β είναι έναδα, άρα τό δ είναι συνεταιρικό τού α. Έτσι, άποδείχτηκε ό ίσχυρισμός μας. Τώρα ή άπόδειξη γίνεται πολύ άπλά, μέ έπαγωγή έπί τού φυσικού άριθμού $|N(\alpha)| \geqslant 2$.

Όρισμός. Λέμε ότι στό K ίσχύει ή μονότροπη άνάλυση, άν ή άνάλυση τών μή μηδενικών στοιχείων $\alpha \in A$, τά όποία δέν είναι έναδες, σέ άνάγωγα στοιχεία τού A είναι μονότροπη υπό τήν έξής έννοια: Άν $\alpha = \pi_1 \cdots \pi_s$ καί $\alpha = \pi'_1 \cdots \pi'_r$ είναι άναλύσεις τού α σέ άνάγωγα στοιχεία, τότε $s = r$ καί τά $\pi_1, \ldots, \pi_r$ είναι δυνατόν νά τεθούν σέ 1-1 άντιστοιχία μέ τά $\pi'_1, \ldots, \pi'_r$, έτσι ώστε τά άντίστοιχα στοιχεία νά είναι συνεταιρικά.

Στην ανάλυση $\alpha = \pi_1 \cdots \pi_r$, τυχόν υπάρχοντα συνεταιρικά στοιχεία μπορεί να γίνουν ίσα ύστερα από πολλαπλασιασμό επί κατάλληλη μονάδα. Συνεπώς, μπορούμε να έχομε την ανάλυση του α με τη μορφή

$$\alpha = \pi_1^{e_1} \cdots \pi_m^{e_m}, \quad e_i \geq 1 \quad (i = 1, \ldots, m)$$

όπου τα ανάγωγα $\pi_1, \ldots, \pi_m$ είναι ανά δύο μη συνεταιρικά. Αυτή η ανάλυση, στην περίπτωση σώματος μοναδικής ανάλυσης, είναι μονότροπη υπό την εξής έννοια: Αν

$$\alpha = \pi_1'^{e_1'} \cdots \pi_q'^{e_q'}, \quad e_i' \geq 1 \ (i = 1, \ldots, q)$$

και τα $\pi_1', \ldots, \pi_q'$ είναι ανά δύο μη συνεταιρικά, τότε $m = q$, τα $\pi_1, \ldots, \pi_m$ μπορεί να τεθούν σε 1-1 αντιστοιχία με τα $\pi_1', \ldots, \pi_m'$ έτσι ώστε τα αντίστοιχα να είναι συνεταιρικά και οι εκθέτες των αντιστοίχων να είναι ίσοι.

Παράδειγμα μη μονότροπης ανάλυσης: Στο $K = \mathbb{Q}(\sqrt{-5})$ δεν ισχύει η μονότροπη ανάλυση. Πράγμαι, σ' αυτή την περίπτωση, $A = \mathbb{Z}[\sqrt{-5}]$ (Θεώρημα 11, §3, Κεφάλαιο 1), και οι αριθμοί $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ είναι ανάγωγοι, μη συνεταιρικοί ανά δύο, ενώ $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$. Έτσι ο 6 έχει δύο ουσιωδώς διαφορετικές αναλύσεις σε αναγώγους παράγοντες

Θεώρημα 13. Στο K ισχύει η μονότροπη ανάλυση αν και μόνον αν, για κάθε ανάγωγο $\pi \in A$ αληθεύει η συνεπαγωγή $\pi \mid ab \ (a, b \in A) \Longrightarrow \pi \mid a$ είτε $\pi \mid b$.

Απόδειξη. Αν ισχύει η συνεπαγωγή για κάθε ανάγωγο $\pi \in A$, τότε εργαζόμαστε ακριβώς όπως στην περίπτωση του $\mathbb{Q}$ ($A = \mathbb{Z}$). Στην περίπτωση αυτή ανάγωγα στοιχεία είναι οι ρητοί πρώτοι και η ιδιότητα ($p \mid ab \Rightarrow p \mid a$ είτε $p \mid b$), που χαρακτηρίζει τους ρητούς πρώτους p, είναι η ουσιώδης για τη μονότροπη ανάλυση των ρητών ακεραίων σε γινόμενο πρώτων παραγόντων. Αντίστροφα, αν ισχύει η μονότροπη ανάλυση,

τότε, ἀπό τή σχέση $\pi | ab$, ὅπου τό π εἶναι ἀνάγωγο, συμπεραίνομε ὅτι τό π ἐμφανίζεται στήν ἀνάλυση τοῦ ab σέ ἀνάγωγους παράγοντες ἄρα, κατ' ἀνάγκη, ἐμφανίζεται στήν ἀνάλυση τοῦ a εἴτε τοῦ b, δηλαδή $\pi | a$ εἴτε $\pi | b$.

Λῆμμα. Ἄν $\pi \in A$ καί τό (π) εἶναι πρῶτο ἰδεῶδες τοῦ A, τότε τό π εἶναι ἀνάγωγο. Ἄν ὁ A εἶναι περιοχή κυρίων ἰδεωδῶν, ἰσχύει καί τό ἀντίστροφο.

Ἀπόδειξη. Ἔστω ὅτι τό (π) εἶναι πρῶτο. Ἔστω $a | \pi$, ὁπότε $\pi = ab$ $(a, b \in A)$. Τότε $(\pi) = (a)(b)$ ἄρα, ἐξ ὑποθέσεως, ἕνα ἀπό τά δύο ἰδεώδη τοῦ δεξιοῦ μέλους εἶναι ἴσα μέ A. Ἄν $(a) = A$, τότε (Θεώρημα 6, §5, κεφάλαιο 3) τό a εἶναι ἑνάδα, ἐνῶ ἄν $(b) = A$, τότε τό b εἶναι ἑνάδα, ἄρα τό a εἶναι συνεταιρικό τοῦ π. Συνεπῶς τό π ἔχει μόνο τετριμμένους διαιρέτες, ἄρα εἶναι ἀνάγωγο. Ἀντιστρόφως, ἄς ὑποθέσομε ὅτι ὁ A εἶναι περιοχή κυρίων ἰδεωδῶν καί τό $\pi \in A$ εἶναι ἀνάγωγο. Τότε $(\pi) \neq A$ (διότι ἀλλοιῶς τό π θά ἦταν ἑνάδα· βλ. τήν παραπομπή παραπάνω) ἄρα τό (π) ἔχει κάποιο πρῶτο διαιρέτη $\mathfrak{p}$. Ἐξ ὑποθέσεως $\mathfrak{p} = (\rho)$, $\rho \in A$, ἄρα $(\rho) \supseteq (\pi)$. Τότε $\rho | \pi$ ὁπότε τό ρ εἶναι, εἴτε ἑνάδα, εἴτε συνεταιρικό τοῦ π. Ἡ πρώτη περίπτωση ἀποκλείεται διότι θά σήμαινε ὅτι $\mathfrak{p} = (\rho) = A$, ἐνῶ ἡ δεύτερη σημαίνει ὅτι $(\pi) = (\rho) = \mathfrak{p}$, συνεπῶς τό (π) εἶναι πρῶτο.

Θεώρημα 14. Στό K ἰσχύει ἡ μονότροπη ἀνάλυση ἄν καί μόνο ἄν $h_K = 1$ (γιά τόν ὁρισμό τοῦ h_K βλ. σελίδα 67).

Ἀπόδειξη. Ἔστω ὅτι στό K ἰσχύει ἡ μονότροπη ἀνάλυση. Θέλομε ν' ἀποδείξομε ὅτι $h_K = 1$, δηλαδή ὅτι κάθε ἰδεῶδες (κλασματικό εἴτε ἀκέραιο) τοῦ A εἶναι κύριο. Σύμφωνα μέ τό Θεώρημα 3, §3 τοῦ κεφαλαίου 3, ἀρκεῖ ν' ἀποδείξομε ὅτι κάθε πρῶτο ἰδεῶδες $\mathfrak{p}$ τοῦ A εἶναι κύριο. ξδῶ νά παρεμβληθεῖ τό ☆ τῆς σελίδος 71α Τό (π) εἶναι πρῶτο ἰδεῶδες. Πράγματι, ἔστω $xy \in (\pi)$, $x, y \in A$.

(*) Έστω $\alpha \in \mathfrak{p}$, $\alpha \neq 0$, α όχι ενάδα και $\alpha = \pi_1 \cdots \pi_\nu$ η ανάλυση του α σε ανάγωγους παράγοντες. Επειδή $\pi_1 \cdots \pi_\nu \in \mathfrak{p}$ και το $\mathfrak{p}$ είναι πρώτο, έπεται ότι, για κάποιο δείκτη $i \in \{1, \dots, \nu\}$ είναι $\pi_i \in \mathfrak{p}$. Θέτουμε $\pi_i = \pi$.

Τότε $\pi | xy$ ἄρα (Θεώρημα 13) $\pi | x$ εἴτε $\pi | y$, δηλαδή $x \in (\pi)$, εἴτε $y \in (\pi)$. Συνεπῶς τό (π) εἶναι ἕνα πρῶτα ἰδεώδες πού περιέχεται στό ρ. Ὅμως τό (π), ὡς πρῶτο, εἶναι maximal, ὁπότε $(\pi) = \rho$.

Ἀντιστρόφως, ἔστω $h_K = 1$, πού σημαίνει ὅτι ὅλα τά ἰδεώδη εἶναι κύρια. Ἔστω $\pi \in A$, π ἀνάγωγο καί $\pi | ab$, ὅπου $a, b \in A$. Σύμφωνα μέ τό Θεώρημα 13, ἀρκεῖ ν' ἀποδείξωμε ὅτι $\pi | a$ εἴτε $\pi | b$: Ἀπ' τό λῆμμα, τό (π) εἶναι πρῶτο ἰδεώδες καί, λόγῳ τῆς σχέσεως $(\pi) | (a)(b)$, ἐμφανίζεται στήν κανονική ἀνάλυση τοῦ ἰδεώδους $(a)(b)$. Ἐπειδή στά ἰδεώδη ἰσχύει ἡ μονότροπη ἀνάλυση σέ πρῶτα ἰδεώδη, ἕπεται ὅτι τό (π) πρέπει νά ἐμφανίζεται στήν κανονική ἀνάλυση τοῦ (a) εἴτε τοῦ (b). Συνεπῶς, $\pi | a$ εἴτε $\pi | b$, ὅ.ἐ.δ.

§5. Τό θεώρημα τοῦ Dirichlet γιά τις ἑνάδες.

Ὑποθέτομε τούς συμβολισμούς κ.λ.π. τῆς εἰσαγωγῆς τῆς §2

Λῆμμα. Τό σύνολο τῶν ἑνάδων ε, οἱ ὁποῖες ἱκανοποιοῦν τίς σχέσεις

$$|\sigma_i(\varepsilon)| = 1 \,, \quad 1 \le i \le s+t \tag{1}$$

εἶναι μιά ὑποομάδα W τῆς ὁμάδας τῶν ἑνάδων, ἡ ὁποία ἀποτελεῖται ἀπό ἐκεῖνες τίς ρίζες τῆς μονάδας, πού ἀνῆκαν στό K. Ἡ ὁμάδα W εἶναι κυκλική, ἄρτιας τάξης.

Ἀπόδειξη. Τό $\sigma(W)$ εἶναι μή κενό ($1, -1 \in W$) ὑποσύνολο τοῦ δικτυωτοῦ $\sigma(A)$, φραγμένο λόγῳ τῆς (1), ἄρα πεπερασμένο.

Συνεπῶς τό W εἶναι πεπερασμένο. Ἄν $\varepsilon \in W$, οἱ δυνάμεις τοῦ ε δέν μπορεῖ νά εἶναι ὅλες διαφορετικές, συνεπῶς τό ε εἶναι ρίζα τῆς μονάδας. Ἀντιστρόφως, ἄν τό

$\varepsilon \in K$ εἶναι ρίζα τῆς μονάδας τότε, προφανῶς, ἱκανοποιεῖ τὶς (1), ἄρα τό W ἀποτελεῖται, ἀκριβῶς, ἀπ' τὶς ρίζες τῆς μονάδας, πού ἀνήκουν στό K. Εἶναι προφανές ὅτι τό W εἶναι ὑποομάδα τῆς πολλαπλασιαστικῆς ὁμάδας $K^* (= K - \{0\})$; κάθε ὑποομάδα, ὅμως, τῆς πολλαπλασιαστικῆς ὁμάδας ἑνός σώματος εἶναι κυκλική, ἄρα ἡ W εἶναι κυκλική ὁμάδα καί, μάλιστα, ἄπειρης τάξης, ἀφοῦ περιέχει ὡς ὑποομάδα τήν $\{1, -1\}$, δ.ἐ.δ.

Τώρα θεωροῦμε τήν ἑξῆς γεωμετρική παράσταση τοῦ K^*: Ὁρίζουμε τήν ἀπεικόνιση $L: K^* \longrightarrow \mathbb{R}^{s+t}$ ὡς ἑξῆς:

$$L(x) = (\log|\sigma_1(x)|, \dots, \log|\sigma_s(x)|, \log|\sigma_{s+1}(x)|, \dots, \log|\sigma_{s+t}(x)|).$$

Ἔστω E ἡ ὁμάδα τῶν ἑνάδων τοῦ K.

Ἡ L εἶναι ὁμομορφισμός, ἄρα ἡ $L(E)$ εἶναι ὑποομάδα τῆς προσθετικῆς ὁμάδας $\mathbb{R}^{s+t}$. Ἔστω S φραγμένο ὑποσύνολο τοῦ $\mathbb{R}^{s+t}$. Τότε τό $L(E) \cap S$ εἶναι φραγμένο, ἄρα γιά κάθε $\varepsilon \in E$ μέ $L(\varepsilon) \in L(E) \cap S$, τά $\sigma_1(\varepsilon), \dots, \sigma_{s+t}(\varepsilon)$ εἶναι φραγμένα, ἄρα καί οἱ στοιχειώδεις συμμετρικές παραστάσεις τῶν $\sigma_1(\varepsilon), \dots, \sigma_s(\varepsilon), \sigma_{s+1}(\varepsilon), \overline{\sigma_{s+1}}(\varepsilon), \dots, \sigma_{s+t}(\varepsilon), \overline{\sigma_{s+t}}(\varepsilon)$ εἶναι φραγμένες. Αὐτό σημαίνει ὅτι ὑπάρχει πεπερασμένος ἀριθμός ἐπιλογῶν γιά τό χαρακτηριστικό πολυώνυμο τοῦ ε, ἄρα καί γιά τό ἴδιο τό ε. Συνεπῶς, τό $L(E) \cap S$ εἶναι πεπερασμένο, ὁπότε ἡ $L(E)$ εἶναι διακριτή ὑποομάδα τοῦ $\mathbb{R}^{s+t}$, ἄρα (θεώρημα 1, §1) ἡ $L(E)$ εἶναι $\mathbb{Z}$-module παραγόμενο ἀπό $r \leq s+t$ ἀνεξάρτητα (πάνω ἀπ' τό $\mathbb{R}$) διανύσματα τοῦ $\mathbb{R}^{s+t}$. Ἔστω $L(E) = e_1\mathbb{Z} + \dots + e_r\mathbb{Z}$ καί $L(\varepsilon_i) = e_i$ $(i = 1, \dots, r)$.

Ἂν $\varepsilon \in E$, τότε $L(\varepsilon) = n_1 e_1 + \dots + n_r e_r$, ὅπου $n_1, \dots, n_r \in \mathbb{Z}$, ἄρα $L(\varepsilon) = L(\varepsilon_1^{n_1} \dots \varepsilon_r^{n_r})$ καί, συμφωνα μέ τό λῆμμα, $\operatorname{Ker} L = \{\zeta : \zeta \in K, \text{ρίζα τῆς μονάδος}\}$. Τότε $\varepsilon \varepsilon_1^{-n_1} \dots \varepsilon_r^{-n_r} \in \operatorname{Ker} L$, ἄρα

$$\varepsilon = \zeta \varepsilon_1^{n_1} \dots \varepsilon_r^{n_r}, \quad \zeta \text{ ρίζα τῆς μονάδας} \in K.$$

Τό ὑπόλοιπο αὐτῆς τῆς παραγράφου θά ἔχει ὡς ἀντικειμενικό σκοπό τήν ἀπόδειξη τῆς σχέσης $r = s+t-1$. Ὅταν ἐπιτευχθεῖ αὐτό, θά ἔχουμε ἀποδείξει τό ἑξῆς θεμελιώδες ἀποτέλεσμα:

Θεώρημα 15 (Dirichlet). Υπάρχουν $r=s+t-1$ ενάδες του K έστω $\varepsilon_1,\dots,\varepsilon_r$, τέτοιες ώστε, κάθε ενάδα ε του K να γράφεται μονότροπα με τη μορφή

$$\varepsilon = \zeta \varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}, \qquad (1)$$

όπου $n_1,\dots,n_r\in\mathbb{Z}$ και ζ είναι ρίζα της μονάδας που ανήκει στο K. Ένα σύνολο ενάδων όπως το $\{\varepsilon_1,\dots,\varepsilon_r\}$ λέγεται σύνολο (ή σύστημα) θεμελιωδών ενάδων του K.

Απόδειξη. Όπως είδαμε μόλις πριν από την εκφώνηση του θεωρήματος, αυτό που μένει ν' αποδειχθεί είναι ότι $r=s+t-1$ (ξέρομε ότι $r\le s+t$· παρατηρήστε επίσης ότι η γραμμική ανεξαρτησία των $e_1,\dots,e_r$ εξασφαλίζει το μονότροπο της γραφής (1)).

Έστω $\varepsilon\in E$ τότε (Θεώρημα 11, §4) $\pm 1 = N(\varepsilon) =$

$$= \prod_{i=1}^{s}\sigma_i(\varepsilon)\cdot\prod_{i=1}^{t}\sigma_{s+i}(\varepsilon)\cdot\overline{\sigma}_{s+i}(\varepsilon), \text{ άρα } 1=\prod_{i=1}^{s}|\sigma_i(\varepsilon)|\cdot\prod_{i=1}^{t}|\sigma_{s+i}(\varepsilon)|^2$$

και $\sum_{i=1}^{s}\log|\sigma_i(\varepsilon)| + 2\sum_{i=1}^{t}\log|\sigma_{s+i}(\varepsilon)| = 0$. Άρα το $L(\varepsilon)$ είναι σημείο του υπερεπιπέδου

$$\Pi:\ \sum_{i=1}^{s}t_i + 2\sum_{i=1}^{t}t_{s+i} = 0.$$

Επειδή $L(E)\subseteq\Pi$ και το Π είναι διαστάσεως $s+t-1$, έπεται ότι $r\le s+t-1$. Μένει να δείξομε ότι το $L(E)$ περιέχει τουλάχιστον $s+t-1$ γραμμικώς ανεξάρτητα διανύσματα. Πρώτα παρατηρούμε ότι μια ισομορφία μεταξύ του Π και του $\mathbb{R}^{s+t-1}$ είναι η προβολή $\pi:\Pi\longrightarrow\mathbb{R}^{s+t-1}$ με $\pi(x_1,\dots,x_{s+t-1},x_{s+t}) = (x_1,\dots,x_{s+t-1})$. Αν ήταν $r<s+t-1$ τότε τα $\pi(e_1),\dots,\pi(e_r)$ ($e_i=L(\varepsilon_i)$, $i=1,\dots,r$) θα' παρήγαν ένα γνήσιο υπόχωρο $V=\pi(L(E))$ του $\mathbb{R}^{s+t-1}$, άρα θα' υπήρχε μια γραμμική μορφή $f':\mathbb{R}^{s+t-1}\longrightarrow\mathbb{R}$ τέτοια ώστε $f'|V=0$, δίχως η f' να είναι μηδενική. Τότε, η γραμμική μορφή $f'\circ\pi:\Pi\longrightarrow\mathbb{R}$, δίχως να είναι μηδενική, μηδενίζεται στο $L(E)\subseteq\Pi$. Μένει να δείξομε ότι αυτό είναι

άτοπο, διότι θά συμπεράναμε ότι $r = s+t-1$. Τό άτοπο θά είχε αποδειχθεί άν καταφέρομε νά αποδείξομε ότι γιά κάθε μή μηδενική γραμμική μορφή $f : \Pi \longrightarrow \mathbb{R}$, υπάρχει $\varepsilon \in E$ τέτοια ώστε $f(L(\varepsilon)) \neq 0$. Άπόδειξη αύτου του ίσχυρισμού: Η f είναι της μορφής $f(x_1, \dots, x_{s+t-1}, x_{s+t}) = c_1 x_1 + \dots + c_{s+t-1} x_{s+t-1}$ γιά κάποιους σταθερούς $c_1, \dots, c_{s+t-1} \in \mathbb{R}$. Έπρόκειτο, λοιπόν, $f \circ \pi^{-1} : \mathbb{R}^{s+t-1} \longrightarrow \mathbb{R}$ είναι μιά γραμμική μορφή, άρα υπάρχουν $c_1, \dots, c_{s+t-1} \in \mathbb{R}$ τέτοια ώστε γιά κάθε $(y_1, \dots, y_{s+t-1}) \in \mathbb{R}^{s+t-1}$ να είναι $f \circ \pi^{-1}(y_1, \dots, y_{s+t-1}) = c_1 y_1 + \dots + c_{s+t-1} y_{s+t-1}$. Άρα

γιά $(x_1, \dots, x_{s+t}) \in \Pi$, $f(x_1, \dots, x_{s+t}) = f \circ \pi^{-1}(\pi(x_1, \dots, x_{s+t})) = f \circ \pi^{-1}(x_1, \dots, x_{s+t-1}) = c_1 x_1 + \dots + c_{s+t-1} x_{s+t-1}$. Έπειδή $f \neq 0$, τά $c_1, \dots, c_{s+t-1}$ δέν είναι όλα μηδέν.

Έστω d ή διακρίνουσα του K. Άς επιλέξομε $\alpha \in \mathbb{R}$ τέτοιο ώστε

$$\alpha > 2^n (2\pi)^{-t} \sqrt{|d|} .$$

Γιά οποιοδήποτε $\lambda = (\lambda_1, \dots, \lambda_{s+t-1}) \in \mathbb{R}_{>0}^{s+t-1}$ έστω ό $\lambda_{s+t} \in \mathbb{R}$, πού ορίζεται άπ' τίς συνθήκες

$$\prod_{i=1}^{s} \lambda_i \prod_{i=1}^{t} \lambda_{s+i}^2 = \alpha \quad , \lambda_{s+t} > 0$$

Άς θυμηθούμε ότι τό δικτυωτό $\sigma(A)$ έχει $v(\sigma(A)) = 2^{-t} \sqrt{|d|}$, (θεώρημα ε, §2), όπότε

$$\prod_{i=1}^{s} \lambda_i \cdot \prod_{i=1}^{t} \lambda_{s+i}^2 > 2^n (2\pi)^{-t} \sqrt{|d|} = 2^n \pi^{-t} \cdot v(\sigma(A)) \geq$$

$$\geq \left(\frac{4}{\pi}\right)^t \cdot v(\sigma(A)) ,$$

γιά νά συμπεράνομε, μέ έφαρμογή του λήμματος της §3, ότι υπάρχει $x_\lambda \in A - \{0\}$ μέ $|\sigma_i(x_\lambda)| < \lambda_i$ $(i = 1, \dots, s)$ καί

$|\sigma_{s+i}(x_\lambda)|^2 < \lambda_{s+i}^2$ $(i = 1, \dots, t)$. Τότε

$$1 \leq |N(x_\lambda)| < \alpha \quad \text{(είδικώτερα, } \alpha > 1) \qquad (2)$$

Αφ' ετέρου, για κάθε $i=1,\dots,s$ έχομε

$$|\sigma_i(x_\lambda)| = |N(x_\lambda)| \cdot \prod_{\substack{j=1\\ j\neq i}}^{s} |\sigma_j(x_\lambda)|^{-1} \cdot \prod_{j=1}^{t} |\sigma_{j+s}(x_\lambda)|^{-2} > \prod_{\substack{j=1\\ j\neq i}}^{s} \lambda_j^{-1} \cdot \prod_{j=1}^{t} \lambda_{j+s}^{-2} =$$

$$= \lambda_i \alpha^{-1}.$$

Επίσης, για κάθε $i=1,\dots,t$,

$$|\sigma_{i+s}(x_\lambda)|^2 = |N(x_\lambda)| \prod_{j=1}^{s} |\sigma_j(x_\lambda)|^{-1} \cdot \prod_{\substack{j=1\\ j\neq i}}^{t} |\sigma_{j+s}(x_\lambda)|^{-2} > \prod_{j=1}^{s} \lambda_j^{-1} \cdot \prod_{\substack{j=1\\ j\neq i}}^{t} \lambda_{j+s}^{-2} =$$

$$= \lambda_{i+s}^2 \cdot \alpha^{-1} > \lambda_{i+s}^2 \cdot \alpha^{-2}.$$

Άρα $\lambda_i > |\sigma_i(x_\lambda)| > \lambda_i \alpha^{-1}$ για κάθε $i=1,\dots,s+t$, όπότε

$$0 < \log\lambda_i - \log|\sigma_i(x_\lambda)| < \log\alpha \quad , \ i=1,\dots,s+t$$

Άρα $|f(L(x_\lambda)) - \sum_{i=1}^{s+t-1} c_i \log\lambda_i| = |\sum_{i=1}^{s+t-1} c_i \log|\sigma_i(x_\lambda)| - \sum_{i=1}^{s+t-1} c_i \log\lambda_i| \leq$

$$\leq \sum_{i=1}^{s+t-1} |c_i| (\log\lambda_i - \log|\sigma_i(x_\lambda)|) < \log\alpha \cdot \sum_{i=1}^{s+t-1} |c_i| := \beta$$

Τώρα, για κάθε $\nu\in\mathbb{N}$ διαλέγω $\lambda=\lambda^{(\nu)} = (\lambda_1^{(\nu)},\dots,\lambda_{s+t-1}^{(\nu)}) \in \mathbb{R}_{>0}^{s+t-1}$ τέτοιο ώστε $\sum_{i=1}^{s+t-1} c_i \log\lambda_i^{(\nu)} = 2\beta\nu$. Σύμφωνα με ό,τι αποδείξαμε πρίν, υπάρχει $x_\nu\ (=x_{\chi^{(\nu)}})$ στό $A-\{0\}$ τέτοιο ώστε

$$|f(L(x_\nu)) - \sum_{i=1}^{s+t-1} c_i \log\lambda_i^{(\nu)}| < \beta \quad , \text{δηλαδή } |f(L(x_\nu)) - 2\beta\nu| < \beta.$$

Συνεπώς,

$$(2\nu-1)\beta < f(L(x_\nu)) < (2\nu+1)\beta$$

όπότε για $\nu\neq\mu$ θα είναι $f(L(x_\nu)) \neq f(L(x_\mu))$.
Αφ' ετέρου $|N(x_\nu)| < \alpha$ (πρβλ. (2)) άρα $N((x_\nu)) < \alpha$, όπότε τα ιδεώδη (x_ν), $\nu=1,2,\dots$ είναι πεπερασμένα τό

πλῆθος (διότι στὴν ἀπόδειξη τοῦ θεωρήματος 9, §3 δείξαμε ὅτι πεπερασμένο πλῆθος ἀκεραίων ἰδεωδῶν τοῦ A εἶναι δυνατὸν νὰ ἔχει norm μικρότερη ἀπὸ δοθέντα θετικὸ ἀριθμό). Συνεπῶς, ὑπάρχουν $\mu, \nu \in \mathbb{N}$, $\mu \neq \nu$ τέτοια ὥστε $(x_\mu) = (x_\nu)$ ἄρα (Θεώρημα 6, §5, Κεφάλαιο 3) $x_\mu = \varepsilon \cdot x_\nu$ γιά κάποια ἐνάδα ε ($\varepsilon \in E$). Τότε $f(L(\varepsilon)) = f(L(x_\mu x_\nu^{-1})) = f(L(x_\mu)) - f(L(x_\nu)) \neq 0$, ὅ.ἐ.δ.