Γραμμικες Μορφες Λογαριθμων Αλγεβρικων Αριθμων και Εφαρμογες

Νικόλαος Κατσίπης

Μεταπτυχιακή Εργασία

Επιβλέπων Καθηγητής Ν.Γ. Τζανάκης

Τμήμα Μαθηματικών - Πανεπιστήμιο Κρήτης

Φθινοπωρινό εξάμηνο 2007

έκδοση 31-10-2007

Η μεταπτυχιακή αυτή εργασία κατατέθηκε στο Τμήμα Μαθηματικών της Σχολής Θετικών και Τεχνολογικών Επιστημών του Πανεπιστημίου Κρήτης τον Οκτώβριο του 2007.
Την επιτροπή αξιολόγησης αποτέλεσαν οι:
Γιάννης Αντωνιάδης
Μιχάλης Κουλουντζάκης
Νίκος Τζανάκης.

Περιεχόμενα

Πρόλογος

Υπερβατικός αριθμός είναι ένας μιγαδικός αριθμός, ο οποίος δεν είναι αλγεβρικός, δηλαδή, δεν είναι ρίζα μη μηδενικού πολυωνύμου με ακέραιους συντελεστές. Ο πρώτος υπερβατικός αριθμός κατασκευάστηκε το 1844 από τον J. Liouville, ο οποίος απέδειξε πρώτα ότι κάθε αλγεβρικός αριθμός α ικανοποιεί την εξής ιδιότητα (θεώρημα του Liouville):

> Αν ο βαθμός του αλγεβρικού αριθμού α είναι d, τότε υπάρχει θετική σταθερά C, εξαρτώμενη μόνο από τον α, τέτοια ώστε
>
> $$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^d}\,,$$
>
> για οποιουσδήποτε ακεραίους p, q με $q > 0$.

Ο αριθμός που κατασκεύσε ο Liouville ήταν ο

$$\xi = \sum_{n=1}^{\infty} 10^{-n!}\,,$$

ο οποίος και ονομάστηκε *αριθμός του Liouville*. Ύστερα, το 1873 ο C. Hermite απέδειξε ότι ο e είναι υπερβατικός· το ότι είναι άρρητος είχε αποδειχθεί από τον L. Euler πολύ ενωρίτερα, το 1744. Το 1874 ο G. Cantor απέδειξε με συνολοθεωρητικά επιχειρήματα το ότι "σχεδόν όλοι" οι μιγαδικοί αριθμοί είναι υπερβατικοί. Πρόκειται για θεώρημα ύπαρξης, όχι κατασκευαστικό θεώρημα. Λίγο αργότερα, το 1882, ο F. von Lindemann απέδειξε την υπερβατικότητα του π, δίνοντας και την τελειωτική -αρνητική- απάντηση στο ερώτημα, που έθεσαν πρώτοι οι αρχαίοι Έλληνες, περί του τετραγωνισμού του κύκλου.

Το 1900, ο D. Hilbert, στο διεθνές συνέδριο Μαθηματικών στο Παρίσι, έθεσε τα 23 διάσημα έκτοτε προβλήματα, το έβδομο εκ των οποίων είναι το εξής:

> Πότε ο α^β, για α αλγεβρικό $\neq 0, 1$ και β άρρητο, είναι υπερβατικός;

Το παραπάνω ερώτημα μπορεί να διατυπωθεί με πολλούς ισοδύναμους τρόπους. Μπορούμε λοιπόν, να θέσουμε την παραπάνω ερώτηση και ως εξής: *πότε ένας άρρητος λογάριθμος αλγεβρικού αριθμού με βάση αλγεβρικό αριθμό είναι υπερβατικός;* ή αλλιώς, *πότε ένα πηλίκο φυσικών λογάριθμων αλγεβρικών αριθμών είναι υπερβατικός;* Σχολιάζοντας τότε το 7ο πρόβλημα, ο D. Hilbert εξεφρασε την πεποίθηση του ότι δεν θα λυνόταν πριν την υπόθεση του Riemann ή πριν την απόδειξη του θεωρήματος του Fermat.

Το 7ο πρόβλημα όμως δεν άργησε να λυθεί. Το 1934, οι A.O. Gelfond και Th. Schneider, ανεξάρτητα ο ένας από τον άλλο, απέδειξαν το εξής θεώρημα:

> Για κάθε μη μηδενικούς αλγεβρικούς αριθμούς $\alpha_1, \alpha_2, \beta_1, \beta_2$ με $\log \alpha_1, \log \alpha_2$ γραμμικώς ανεξάρτητους υπέρ το $\mathbb{Q}$, ισχύει ότι $\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0$.

Το θεώρημα αυτό λύνει το 7ο πρόβλημα του Hilbert. Εκείνη τη χρονική περίοδο διατυπώθηκε και η εικασία ότι το θεώρημα των Gelfond-Schneider ισχύει για περισσότερους από δύο λογάριθμους, η οποία και αποδείχθηκε το 1966 από τον A. Baker. Συγκεκριμένα, ο Baker απέδειξε αυτό που σήμερα είναι γνωστό ως *Θεώρημα του Baker* (ομογενής περίπτωση):

> Η γραμμική ανεξαρτησία των $\log \alpha_1, \ldots, \log \alpha_n$ υπέρ το $\mathbb{Q}$ συνεπάγεται τη γραμμική ανεξαρτησία τους υπέρ το $\bar{\mathbb{Q}}$.

Λίγο αργότερα, ο A. Baker απέδειξε και τη μη ομογενή περίπτωση:

> Η γραμμική ανεξαρτησία των $\log \alpha_1, \ldots, \log \alpha_n$ υπέρ το $\mathbb{Q}$ συνεπάγεται τη γραμμική ανεξαρτησία των $1, \log \alpha_1, \ldots, \log \alpha_n$ υπέρ το $\bar{\mathbb{Q}}$.

Περαιτέρω, ο A. Baker πέτυχε να δώσει μη τετριμμένα κάτω φράγματα για τις απόλυτες τιμές μη μηδενικών ομογενών και μη ομογενών γραμμικών μορφών λογαρίθμων αλγεβρικών αριθμών. Η μέθοδός του κάνει χρήση βοηθητικής συνάρτησης πολλών μεταβλητών, η οποία έχει μηδενικές θέσεις σε κάποια προδιαγεγραμμένα σημεία και μάλιστα με κατάλληλα μεγάλη πολλαπλότητα. Έτσι υπεισέρχονται υπολογισμοί και εκτιμήσεις των παραγώγων κατάλληλα μεγάλης τάξεως της βοηθητικής συνάρτησης.

Σε αυτή την εργασία:

1. Αποδεικνύεται η ομογενής περίπτωση του θεωρήματος του A. Baker.

2. Αποδεικνύεται συγκεκριμένο κάτω φράγμα για την απόλυτη τιμή των ομογενών γραμμικών μορφών $\beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n$, με α_i, β_i αλγεβρικούς αριθμούς, όταν αυτή δεν είναι μηδέν.

3. Εφαρμόζεται το προηγούμενο φράγμα στην επίλυση της εξίσωσης Thue.

Η απόδειξη που θα παρουσιάσουμε (κεφάλαια 2 έως 6), διαφέρει σημαντικά από εκείνη του Baker. Βασίζεται στην ιδέα του M. Laurent να χρησιμοποιήσει, αντί της βοηθητικής συνάρτησης, μια ορίζουσα κατάλληλα μεγάλου μεγέθους, της οποίας τα στοιχεία είναι τιμές κάποιων συναρτήσεων σε προδιαγεγραμμένα σημεία. Συγκεκριμένα, προκύπτει ότι η απόλυτη τιμή της ορίζουσας "δεν είναι πολύ μεγάλη" (κεφάλαιο 4). Αλλά από την άλλη, η γενίκευση της κλασικής ανισότητας του Liouville (κεφάλαιο 3) συνεπάγεται ότι, η αν η ορίζουσα δεν είναι μηδέν, τότε "δεν μπορεί να είναι πολύ μικρή". Για κατάλληλες τιμές των παραμέτρων οι οποίες υπεισέρχονται στην ορίζουσα, τα προαναφερθέντα άνω και κάτω φράγματα είναι αντιφατικά, οπότε προκύπτει το συμπέρασμα ότι η ορίζουσα είναι μηδέν. Ο μηδενισμός της ορίζουσας χρησιμοποιείται κατάλληλα στο κεφάλαιο 5 για την κατασκευή πολυωνύμου n μεταβλητών, "ελεγχόμενου βαθμού", το οποίο μηδενίζεται σε προδιαγεγραμμένα σημεία. Από αυτό έπεται το συμπέρασμα ότι στον διανυσματικό χώρο K^n, όπου $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$, υπάρχει ένα διανυσματικός υπόχωρος με συγκεκριμένες ιδιότητες, αρκετά τεχνικές για να περιγραφούν εδώ. Στο κεφάλαιο 6 αποδεικνύεται ότι η ύπαρξη αυτού του διανυσματικού υποχώρου οδηγεί στο συμπέρασμα του θεωρήματος του A. Baker.
Για την μετάβαση από τον μηδενισμό της ορίζουσας στην ύπαρξη του συγκεκριμένου πολυωνύμου και από αυτό στην ύπαρξη του διανυσματικού υποχώρου απαιτούνται κάποια βασικά εργαλεία της κλασικής Αλγεβρικής Γεωμετρίας, με χαρακτηριστικότερο, μια εκδοχή του θεωρήματος του Bézout.

Στο κεφάλαιο 7 θα επαναλάμβουμε κάποια σημεία της απόδειξης του θεωρήματος του Baker πιο σχολαστικά ως προς τις υπολογιστικές "λεπτομέρειες", για να άποδείξουμε ένα *συγκεκριμένο* κάτω φράγμα γραμμικών μορφών λογαρίθμων αλγεβρικών αριθμών. Το φράγμα που θα παρουσιάσουμε δεν είναι το καλύτερο δυνατό από τα ήδη γνωστά φράγματα, αλλά είναι αρκετά χρήσιμο για την (υπολογιστική) λύση αρκετών διοφαντικών εξισώσεων. Μια εφαρμογή του συγκεκριμένου φράγματος θα παρουσιάσουμε στο τελευταίο (8ο) κεφάλαιο αυτής της εργασίας, όπου θα υπολογίσουμε ένα άνω φράγμα για της ακέραιες λύσεις της διοφαντικής εξίσωσης του Thue.

Ευχαριστώ τον καθηγητή Νικόλαο Τζανάκη για το αμέριστο ενδιαφέρον και την πολύτιμη καθοδήγηση που μου παρείχε καθ' όλη τη διάρκεια της συγγραφής αυτής της εργασίας.

Ευχαριστώ, επίσης, τους γονείς μου που με στήριξαν με κάθε τρόπο όλα αυτά τα χρόνια σε κάθε μου προσπάθεια.

Νικόλαος Δ. Κατσίπης
Ηράκλειο, Οκτώβριος 2007

Κεφάλαιο 1

Εισαγωγή

Συμβολίζουμε με $\bar{\mathbb{Q}}$ την αλγεβρική κλειστότητα του $\mathbb{Q}$ στο $\mathbb{C}$. Οπότε το $\bar{\mathbb{Q}}$ είναι το σώμα των αλγεβρικών αριθμών. Επίσης, έστω $\mathfrak{L}$ το σώμα των λογαρίθμων των μη μηδενικών αριθμών, το οποίο είναι η αντίστροφη εικόνα της εκθετικής συνάρτησης από την πολλαπλασιαστική ομάδα $\bar{\mathbb{Q}}^*$.

$$\mathfrak{L} = \{\ell \in \mathbb{C} : \mathrm{e}^{\ell} \in \bar{\mathbb{Q}}^*\}.$$

Είναι συχνά βολικότερο να γράφουμε $\ell = \log \alpha$, α αλγεβρικός αριθμός, αλλά για $\alpha \in \bar{\mathbb{Q}}^*$ το σύνολο των ℓ με $\alpha = \mathrm{e}^{\ell}$ είναι μια κλάση του $\mathbb{C}$ $modulo$ $2\pi\imath\mathbb{Z}$.
Το $\mathfrak{L}$ είναι $\mathbb{Q}-$διανυσματικός υπόχωρος του $\mathbb{C}$. Δεν είναι όμως $\bar{\mathbb{Q}}^*-$διανυσματικός υπόχωρος, αφού αν $\ell_1 \in \mathfrak{L}$ και $\alpha \in \bar{\mathbb{Q}}$ το $\alpha \cdot \ell$ δεν ανήκει εν γένει στο $\mathfrak{L}$.

> **Θεώρημα του Baker** (Ομογενής περίπτωση[1]) *Η γραμμική ανεξαρτησία των $\ell_1, \ldots, \ell_n \in \mathfrak{L}$ υπέρ το $\mathbb{Q}$ συνεπάγεται τη γραμμική τους ανεξαρτησία υπέρ το $\bar{\mathbb{Q}}$.*

Το θεώρημα αυτό αποδείχθηκε το 1966 από τον Alan Baker, [3], [4], [5], [6].

1.1 Ιστορική επισκόπηση

Ο Euler στο βιβλίο του «Introductio to analysin infinitorum» [14], όρισε την εκθετική και λογαριθμική συνάρτηση και είπε:

«*Από αυτά που ήδη γνωρίζουμε, έχουμε ότι ο λογάριθμος ενός αριθμού δεν είναι ρητός αριθμός εκτός και αν ο αριθμός αυτός είναι δύναμη της βάσης του λογαρίθμου. Οπότε, ο λογάριθμος ενός αριθμού b δεν μπορεί να εκφραστεί ως ρητός αριθμός, εκτός αν ο b είναι δύναμη της βάσης a του λογαρίθμου. Στην*

[1] Ο Baker απέδειξε και τη μη ομογενή περίπτωση· βλ. πρόλογο.

περίπτωση που ο b είναι δύναμη της βάσης a του λογαρίθμου, τότε ο λογάριθμος του b δεν μπορεί να είναι άρρητος. Αν ακόμα $\log_a b = \sqrt{n}$, τότε $a^{\sqrt{n}} = b$, το οποίο είναι αδύνατο αν οι a, b είναι ρητοί. Επιθυμούμε λοιπόν, να γνωρίζουμε λογαρίθμους ρητών αριθμών, αφού έτσι μπορούμε να βρίσκουμε λογάριθμους κλασμάτων και άρρητων. Αφού οι λογάριθμοι αριθμών, οι οποίοι δεν είναι δύναμη της βάσης του λογαρίθμου, δεν είναι ούτε ρητοί ούτε άρρητοι, είναι αυτό που ονομάζουμε υπερβατικοί αριθμοί. Γι' αυτό το λόγο οι λογάριθμοι λέγεται ότι είναι υπερβατικοί αριθμοί.»

Αργότερα, το 1900, στο διεθνές συνέδριο Μαθηματικών στο Παρίσι, ο D. Hilbert έθεσε την παρακάτω ερώτηση ως το *έβδομο πρόβλημα Hilbert*:
Η έκφραση α^β, όπου α αλγεβρικός αριθμός και β άρρητος αλγεβρικός αριθμός (για παράδειγμα $2^{\sqrt{2}}, \mathrm{e}^\pi = i^{-2i}$) πάντα παριστάνει ένα υπερβατικό αριθμό ή τουλάχιστον ένα άρρητο αριθμό.
Το πρόβλημα αυτό λύθηκε το 1934 από τους A.O. Gelfond και Th. Schneider:

Θεώρημα 1.1.1. *Αν ℓ_1, ℓ_2 είναι $\mathbb{Q}-$ γραμμικά ανεξάρτητα στοιχεία του $\mathfrak{L}$, τότε αυτά είναι και $\bar{\mathbb{Q}}-$ γραμμικά ανεξάρτητα.*

Αυτό σημαίνει ότι το πηλίκο $\frac{\ell_1}{\ell_2}$, $\ell_1, \ell_2 \in \mathfrak{L}$, $\ell_1, \ell_2 \neq 0$, είναι είτε ρητός είτε υπερβατικός αριθμός. Δεν μπορεί να είναι ένας άρρητος αλγεβρικός αριθμός, όπως για παράδειγμα ο $\sqrt{2}$. Αυτό διότι :
Αν $\frac{\ell_1}{\ell_2}$ δεν είναι ρητός αριθμός τότε προφανώς, ℓ_1, ℓ_2 είναι $\mathbb{Q}-$ γραμμικά ανεξάρτητα, άρα (Gelfond - Schneider) είναι $\bar{\mathbb{Q}}-$ γραμμικά ανεξάρτητα. Αλλά τότε αποκλείεται να είναι $\frac{\ell_1}{\ell_2} \in \bar{\mathbb{Q}}$, δηλαδή $\frac{\ell_1}{\ell_2}$ είναι υπερβατικός.

Η σύνδεση του θεωρήματος 1.1.1 με το 7ο πρόβλημα του Hilbert, μπορεί να διαπιστωθεί πιο εύκολα, αν διατυπώσουμε το παρακάτω θεώρημα το οποίο είναι ισοδύναμο με το 1.1.1.

Θεώρημα 1.1.2. *Αν ℓ και β είναι δύο μιγαδικοί αριθμοί με $\ell \neq 0$ και β όχι ρητός, τότε ένας από τους e^ℓ, β και $\mathrm{e}^{\beta\cdot\ell}$ είναι υπερβατικός.*

- Θεώρημα 1.1.1 $\Rightarrow$ Θεώρημα 1.1.2:
  Αν $\mathrm{e}^\ell \in \bar{\mathbb{Q}}$ τότε $\ell \in \mathfrak{L}$. Αν $\beta \in \bar{\mathbb{Q}}$ θα δείξουμε ότι ο $\mathrm{e}^{\beta\cdot\ell}$ είναι υπερβατικός. Πράγματι, αν δεν ήταν, τότε $\beta \cdot \ell \in \mathfrak{L}$. Αλλά τα $\beta \cdot \ell, \ell$ είναι $\bar{\mathbb{Q}}-$ γραμμικά εξαρτημένα. Άρα από θεώρημα 1.1.1 είναι και $\mathbb{Q}-$ γραμμικά εξαρτημένα. Άρα $\beta \in \mathbb{Q}$. Άτοπο.

- Θεώρημα 1.1.2 $\Rightarrow$ Θεώρημα 1.1.1:
  Έστω $\ell_1, \ell_2 \in \mathfrak{L}$ και $\alpha_1 \cdot \ell_1 + \alpha_2 \cdot \ell_2 = 0, \quad \alpha_1, \alpha_2 \in \bar{\mathbb{Q}}$. Τότε $\ell_1 = \beta \cdot \ell_2$, όπου $\beta \in \bar{\mathbb{Q}}$. Έχουμε ότι:
  $\mathrm{e}^{\ell_2} \in \bar{\mathbb{Q}}$ (αφού $\ell_2 \in \mathfrak{L}$), $\beta \in \bar{\mathbb{Q}}$ και $\mathrm{e}^{\beta\cdot\ell_2} = \mathrm{e}^{\ell_1} \in \bar{\mathbb{Q}}$ (αφού $\ell_1 \in \mathfrak{L}$). Άρα

από το θεώρημα 1.1.2 έχουμε αναγκαστικά ότι ο $\beta \in \mathbb{Q}$. Άρα οι ℓ_1, ℓ_2 είναι $\mathbb{Q}-$ γραμμικά εξαρτημένοι.

Η υπερβατικότητα του e^{π} έπεται από το θεώρημα 1.1.2 αν πάρουμε $\ell = 2\pi\imath$ και $\beta = \frac{-\imath}{2}$.

Ο Gelfond στο βιβλίο του [15], αναφέρεται στη σημασία που θα είχε μια γενίκευση του θεωρήματος 1.1.1 για περισσότερους από δύο λογαρίθμους. Αυτό το πρόβλημα, όπως αναφέραμε, λύθηκε το 1966 από τον Alan Baker. Από το θεώρημα του Baker μπορούμε να συμπεράνουμε το εξής:
Αν ένας αριθμός της μορφής:

$$\alpha_1^{\beta_1} \cdot \ldots \cdot \alpha_n^{\beta_n} = e^{(\beta_1 \cdot \log \alpha_1 + \ldots + \beta_n \cdot \log \alpha_n)},$$

($\alpha_i \neq 0, \beta_i$ *αλγεβρικοί αριθμοί), είναι αλγεβρικός, τότε είτε οι αριθμοί* $\log \alpha_1, \ldots, \log \alpha_n$ *είναι όλοι μηδέν, είτε οι αριθμοί* $1, \beta_1, \ldots, \beta_n$ *είναι γραμμικά εξαρτημένοι πάνω από το* $\mathbb{Q}$.
Η παραπάνω παρατήρηση προκύπτει χρησιμοποιώντας τα παρακάτω τρία θεωρήματα (συγκεκριμένα το θεώρημα 1.1.5).

Θεώρημα 1.1.3. *Κάθε μη μηδενικός γραμμικός συνδυασμός στοιχείων του* $\mathfrak{L}$ *με αλγεβρικούς συντελεστές είναι υπερβατικός. Με άλλα λόγια, για οποιαδήποτε* $\ell_1, \ldots, \ell_n \in \mathfrak{L}$ *και οποιουσδήποτε αλγεβρικούς αριθμούς* $\beta_0, \ldots, \beta_n$ *με* $\beta_0 \neq 0$, *έχουμε*

$$\beta_0 + \beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n \neq 0.$$

Απόδειξη. Για $n = 0$ ισχύει.
Υποθέτουμε ότι ισχύει για $n < m$, όπου $n, m \in \mathbb{N}$ και θα το αποδείξουμε για $n = m$.
Εξετάζουμε δύο περιπτώσεις:

(**i**) $\ell_1, \ldots, \ell_m$ $\mathbb{Q}-$ γραμμικά ανεξάρτητα.

(**ii**) $\ell_1, \ldots, \ell_m$ $\mathbb{Q}-$ γραμμικά εξαρτημένα.

Οπότε
(**i**) Αν $\ell_1, \ldots, \ell_m$ είναι $\mathbb{Q}-$ γραμμικά ανεξάρτητα τότε από το θεώρημα του Baker(μη ομογενής περίπτωση) είναι και $\bar{\mathbb{Q}}-$ γραμμικά ανεξάρτητα, άρα έχουμε το ζητούμενο.
(**ii**) Αν $\ell_1, \ldots, \ell_m$ είναι $\mathbb{Q}-$ γραμμικά εξαρτημένα, τότε μπορούμε να υποθέσουμε ότι υπάρχουν $\rho_1, \ldots, \rho_m \in \mathbb{Q}$, όχι όλα μηδέν, τέτοια ώστε:

$$\rho_1 \cdot \ell_1 + \ldots + \rho_m \cdot \ell_m = 0.$$

Αν, έστω, $\rho_r \neq 0 \ \ (1 \leq r \leq m)$, τότε

$$\rho_r \cdot (\beta_0 + \beta_1 \cdot \ell_1 + \ldots + \beta_m \cdot \ell_m) =$$

$$= \rho_r \cdot (\beta_0 + \beta_1 \cdot \ell_1 + \ldots + \beta_m \cdot \ell_m) - (\rho_1 \cdot \ell_1 + \ldots + \rho_m \cdot \ell_m) =$$

$$= \beta_0^{'} + \beta_1^{'} \ell_1 + \ldots + \beta_m^{'} \cdot \ell_m,$$

όπου $\beta_0^{'} = \rho_r \cdot \beta_0 \neq 0$, $\beta_j^{'} = \rho_r \cdot \beta_j - \rho_j \cdot \beta_r, \ \ (1 \leq j \leq m)$.
Αλλά στην τελευταία γραμμική μορφή λογαρίθμων το πλήθος των λογαρίθμων είναι, στην πραγματικότητα, $m-1$, διότι $\beta_r^{'} = 0$, άρα από την επαγωγική υπόθεση, η γραμμική μορφή είναι $\neq 0$. Αλλά $\rho_r \neq 0$, οπότε

$$\beta_0 + \beta_1 \cdot \ell_1 + \ldots + \beta_m \cdot \ell_m \neq 0.$$

□

Θεώρημα 1.1.4. *(Πόρισμα του θεωρήματος 1.1.3) Αν* $\beta_0, \ldots, \beta_n \in \bar{\mathbb{Q}}^*$ *και* $\ell_1, \ldots, \ell_n \in \mathfrak{L}$ *τότε*

$$\beta_0 + \beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n \notin \mathfrak{L}.$$

Απόδειξη. Σε αντίθετη περίπτωση, έστω:

$$\beta_0 + \beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n = \ell_{n+1} \in \mathfrak{L}.$$

$$\beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n - \ell_{n+1} = -\beta_0$$

Οπότε, $\beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n - \ell_{n+1} =$ μη μηδενικός αλγεβρικός αριθμός.
Αυτό όμως έρχεται σε αντίθεση με το θεώρημα 1.1.3.

□

Θεώρημα 1.1.5. *Αν* $\ell_1, \ldots, \ell_n \in \mathfrak{L}$ *και* $\beta_1, \ldots, \beta_n \in \bar{\mathbb{Q}}$ *με τους* $1, \beta_1, \ldots, \beta_n \ \ \mathbb{Q}-$ *γραμμικά ανεξάρτητους, τότε*

$$\beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n \notin \mathfrak{L}.$$

Απόδειξη. Αν $\beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n = \ell_{n+1} \in \mathfrak{L}$, τότε $\beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n + (-1)\ell_{n+1} = 0$. Άρα, αρκεί να δείξουμε ότι για κάθε $\ell_1, \ldots, \ell_k \in \mathfrak{L}$ και κάθε $\beta_1, \ldots, \beta_k \in \bar{\mathbb{Q}} \ \ \mathbb{Q}-$ γραμμικά ανεξάρτητους, έχουμε ότι

$$\beta_1 \cdot \ell_1 + \ldots + \beta_k \cdot \ell_k \neq 0.$$

Για $k = 1$ ισχύει.
Υποθέτουμε ότι ισχύει για $k < m$ και θα δείξουμε ότι ισχύει και για $k = m$.

Το αποτέλεσμα είναι συνέπεια του θεωρήματος του Baker, αν οι $\ell_1, \ldots, \ell_n$ είναι γραμμικά ανεξάρτητοι πάνω από το $\mathbb{Q}$.
Έστω ότι οι $\ell_1, \ldots, \ell_n$ είναι γραμμικά εξαρτημένοι πάνω από το $\mathbb{Q}$. Άρα υπάρχουν $\rho_1, \ldots, \rho_m \in \mathbb{Q}$ και $\beta_j^{'}$ όπως στο θεώρημα 1.1.3, αλλά τώρα $\beta_0 = \beta_0^{'} = 0$. Είναι απλό να δούμε ότι αν $\beta_1, \ldots, \beta_m$ είναι γραμμικά ανεξάρτητοι πάνω από το $\mathbb{Q}$, το ίδιο συμβαίνει και για τους $\beta_j^{'}$ με $j = 1, \ldots, r-1, r+1, \ldots, m$ και το θεώρημα προκύπτει με επαγωγή.

□

Παραδείγματα. Επειδή $\pi = -2i\mathrm{Log}i$, όπου Log είναι πρωτεύον κλάδος του λογαρίθμου, βλέπουμε αμέσως τα εξής:

- Με εφαρμογή του θεωρήματος 1.1.3 έχουμε ότι ο $\pi + \log\alpha$ είναι υπερβατικός για οποιονδήποτε αλγεβρικό αριθμό α και οποιοδήποτε λογάριθμο του α. Σημειώνουμε εσώ ότι, για την εφαρμογή του θεωρήματος 1.1.3 απαιτείται να ξέρουμε ότι $\pi + \log\alpha \neq 0$, το οποίο ισχύει διότι έχουμε ήδη δείξει ότι $\mathrm{e}^{\pi} \notin \mathfrak{L}$.
- Με εφαρμογή του θεωρήματος 1.1.4 έχουμε ότι $\mathrm{e}^{(\alpha\cdot\pi+\beta)}$ είναι υπερβατικός για οποιουσδήποτε αλγεβρικούς αριθμούς α, β με $\beta \neq 0$.

1.2 Θεώρημα του Baker. Ισοδύναμη διατύπωση

Οι μοναδικές σχέσεις γραμμικής εξάρτησης λογαρίθμων αλγεβρικών αριθμών, με αλγεβρικούς συντελαστές, είναι οι τετριμμένες, όπως για παράδειγμα

$$\log 24 = \sqrt{3}\log 9 + (1 - 2\sqrt{3})\log 3 + \sqrt{2}\log 4 + (3 - 2\sqrt{2})\log 2.$$

Αν το θεώρημα του Baker δεν ήταν αληθές, τότε από μια μη τετριμμένη μηδενική γραμμική σχέση στοιχείων ℓ του $\mathfrak{L}$, με αλγεβρικούς συντελεστές β και με το ελάχιστο μήκος, θα προέκυπτε το συμπέρασμα ότι και τα β_i και τα ℓ_i είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα.

Λήμμα 1.2.1. *Έστω $k \subset K$ δύο σώματα, $\mathfrak{E}$ ένας $K-$ διανυσματικός χώρος και $\mathfrak{M}$ είναι $k-$ υποδιανυσματικός χώρος στο $\mathfrak{E}$. Τα παρακάτω είναι ισοδύναμα:*

(**i**) *Έστω $m \geq 1$ και $\ell_1, \ldots, \ell_m$ στοιχεία του $\mathfrak{M}$ τα οποία είναι $k-$ γραμμικώς ανεξάρτητα. Τότε αυτά τα στοιχεία είναι επίσης γραμμικά ανεξάρτητα πάνω από το K στο $\mathfrak{E}$.*

(**ii**) *Έστω $m \geq 1$, $\ell_1, \ldots, \ell_m$ στοιχεία του $\mathfrak{M}$, όχι όλα μηδέν, και έστω $\beta_1, \ldots, \beta_m$ να είναι $k-$ γραμμικώς ανεξάρτητα στοιχεία του K. Τότε*

$$\beta_1 \cdot \ell_1 + \ldots + \beta_m \cdot \ell_m \neq 0.$$

(**iii**) *Έστω* $m \geq 1$, $\ell_1, \ldots, \ell_m$ $k-$ *γραμμικώς ανεξάρτητα στοιχεία του* $\mathfrak{M}$ *και* $\beta_1, \ldots, \beta_m$ $k-$ *γραμμικώς ανεξάρτητα στοιχεία του* K. *Τότε:*

$$\beta_1 \cdot \ell_1 + \ldots + \beta_m \cdot \ell_m \neq 0.$$

(**iv**) *Έστω* $m \geq 1$, $\ell_1, \ldots, \ell_m$ $k-$*γραμμικώς ανεξάρτητα στοιχεία του* $\mathfrak{M}$ *και* $\beta_1, \ldots, \beta_m$ *στο* K *τέτοια ώστε:*

$$\beta_1 \ell_1 + \ldots + \beta_m \ell_m = 0.$$

Τότε, τα $\beta_1, \ldots, \beta_m$ *είναι* $k-$*γραμμικώς εξαρτημένα.*

Απόδειξη.

- (i)$\Rightarrow$ (iii): Προφανής απόδειξη.
- (iii)$\Leftrightarrow$ (iv): Προφανής απόδειξη.
- (ii)$\Rightarrow$ (i): Υποθέτουμε ότι για $m \geq 1$ έχουμε την σχέση:

$$\beta_1 \cdot \ell_1 + \ldots + \beta_m \cdot \ell_m = 0, \text{ με } \beta_i \in K \text{ όχι όλα } 0.$$

Δήλαδή υποθέτουμε ότι τα $\ell_1, \ldots, \ell_m$ είναι γραμμικά εξαρτημάνα πάνω από το K στο $\mathfrak{E}$ και θα δείξουμε ότι τα $\ell_1, \ldots, \ell_m$ είναι $k-$ γραμμικώς εξαρτημένα (οπότε θα έχουμε το (i)).
Έστω $\beta_1^{'}, \ldots, \beta_s^{'}$, με $0 \leq s \leq m$, μια βάση του $k-$ διανυσματικού χώρου, τον οποίο παράγουν τα $\beta_1, \ldots, \beta_m$. Τότε:

$$\beta_i = \sum_{j=1}^{s} c_{ij} \cdot \beta_j^{'}, \;\; c_{ij} \in k \text{ όχι όλα μηδέν, } 1 \leq i \leq m.$$

Οπότε:

$$\sum_{j=1}^{s} \beta_j^{'} \Big(\sum_{i=1}^{m} c_{ij} \cdot \ell_i \Big) = 0 \;\; {}^{2}.$$

Αφού τα $\beta_1^{'}, \ldots, \beta_s^{'}$ είναι $k-$ γραμμικώς ανεξάρτητα (αποτελούν βάση), συμπεραίνουμε από το (ii) ότι

$$\sum_{i=1}^{m} c_{ij} \cdot \ell_i = 0 \; 1 \leq j \leq s.$$

Οπότε τα $\ell_1, \ldots, \ell_m$ είναι $k-$ γραμμικώς εξαρτημένα.

[2] $\sum_{i=1}^{m} c_{ij} \cdot \ell_i \in \mathfrak{M}$, αφού $c_{ij} \in k$ και $\mathfrak{M}$ $k-$ υποδιανυσματικός χώρος στο $\mathfrak{E}$

• (iii)⇒ (ii): Υποθέτουμε ότι $\beta_1 \cdot \ell_1 + \ldots + \beta_m \cdot \ell_m = 0$, με τα $\beta_1, \ldots, \beta_m$ γραμμικώς ανεξάρτητα πάνω από το k στο K και τα $\ell_1, \ldots, \ell_m \in \mathfrak{M}$. Θα δείξουμε ότι :

$$\ell_1 = \ell_2 = \ldots = \ell_m = 0.$$

Αν τα $\ell_1, \ldots, \ell_m$ δεν είναι όλα μηδέν, τότε θεωρώ ένα maximal υποσύνολο του $L = \{\ell_1, \ldots, \ell_m\}$ μεταξύ των υποσυνόλων του L που αποτελούνται από $k-$ γραμμικώς ανεξάρτητα στοιχεία. Χωρίς βλάβη της γενικότητας έστω $\{\ell_1, \ldots, \ell_r\}$ ένα τέτοιο υποσύνολο, οπότε $1 \leq r \leq m$. Άρα:

$$\ell_i = \sum_{j=1}^{r} c_{ij} \cdot \ell_j, \text{ όπου } c_{ij} \in k, \ r+1 \leq i \leq m$$

Συμπεραίνουμε ότι

$$\sum_{j=1}^{r} \gamma_j \cdot \ell_j = 0, \text{ με } \gamma_j = \beta_j + \sum_{i=r+1}^{m} c_{ij}\beta_i, \ 1 \leq j \leq r$$

Χρησιμοποιώντας το (iii) (αντικαθιστώντας το m με το r) συμπεραίνουμε από την γραμμική ανεξαρτησία των $\ell_1, \ldots, \ell_r$ πάνω από το k, ότι τα r στοιχεία $\gamma_1, \ldots, \gamma_r$ είναι $k-$ γραμμικώς εξαρτημένα στο K. Αλλά αφού τα $\beta_1, \ldots, \beta_m$ είναι $k-$ γραμμικώς ανεξάρτητα και λόγω της σχέσης $\gamma_j = \beta_j + \sum_{i=r+1}^{m} c_{ij}\beta_i$ έχουμε ότι και τα $\gamma_1 \ldots, \gamma_r$ είναι $k-$ γραμμικώς ανεξάρτητα. Άτοπο.
Άρα δεν γίνεται να έχουμε κανένα ℓ_i $k-$ γραμμικώς ανεξάρτητο. Άρα

$$\ell_1 = \ell_2 = \ldots = \ell_m = 0.$$

□

Όταν $k = \mathbb{Q}$, $K = \bar{\mathbb{Q}}$, $\mathfrak{M} = \mathfrak{L}$ και $\mathfrak{E} = \mathbb{C}$ η περίπτωση (i) είναι το θεώρημα του Baker.

Συνεπώς, το θεώρημα του Baker, βάση του (iv), μπορεί να επαναδιατυπωθεί ισοδύναμα ως εξής:

Θεώρημα 1.2.2. *Έστω $\ell_1, \ldots, \ell_{n+1}$ $\mathbb{Q}-$γραμμικώς ανεξάρτητα στοιχεία του $\mathfrak{L}$ και $\beta_1, \ldots, \beta_n$ αλγεβρικοί αριθμοί με*

$$\ell_{n+1} = \beta_1\ell_1 + \ldots + \beta_n\ell_n.$$

Τότε, τα $1, \beta_1, \ldots, \beta_n$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένα.

1.3 Φράγματα της απόστασης γινομένου ακεραίων από το 1

Το θεώρημα του Baker μας δείχνει ότι αριθμοί της μορφής

$$\beta_1 \log \alpha_1 + \ldots + \beta_m \log \alpha_m,$$

(με β_i, α_i αλγεβρικοί αριθμοί για $1 \leq i \leq m$) είναι μηδέν μόνο σε τετριμμένες περιπτώσεις. Μέσω της απόδειξης του θεωρήματος του Baker προκύπτουν υπολογίσιμα κάτω φράγματα για τέτοιου είδους αριθμούς. Ένα τέτοιο φράγμα θα παρουσιαστεί στο κεφάλαιο 7.

Θα παρουσιάσουμε την απλή περίπτωση, όπου $\beta_i \in \mathbb{Z}$ και $\alpha_i \in \mathbb{Z}$ με $\alpha_i \geq 2$, $1 \leq i \leq m$.
Έστω λοιπόν, $a_1, \ldots, a_m$ ρητοί ακέραιοι, οι οποίοι είναι ≥ 2 και $b_1, \ldots, b_m$ ρητοί ακέραιοι. Υποθέτουμε

$$a_1^{b_1} \cdots a_m^{b_m} \neq 1,$$

και αναζητούμε κάτω φράγμα για την απόσταση αυτών των αριθμών.

Μία τετριμμένη εκτίμηση είναι η εξής:

$$\begin{aligned} |a_1^{b_1} \cdots a_m^{b_m} - 1| &\geq \prod_{b_i<0} a_i^{b_i} \geq \mathrm{e}^{-\sum_{i=1}^m |b_i| \log a_i} \\ &\geq \mathrm{e}^{-mB \log A}, \end{aligned}$$

όπου $B = \max\{|b_1|, \ldots, |b_m|\}$ και $A = \max\{a_1, \ldots, a_m\}$. Η γενίκευση της προηγούμενης εκτίμησης, όταν τα a είναι αλγεβρικοί αριθμοί, είναι το θεώρημα 3.5.1 (Ανισότητα Liouville).

Η σχέση αυτού του είδους φραγμάτων με κάτω φράγματα γραμμικών μορφών λογαρίθμων, είναι η εξής:
Αν

$$|a_1^{b_1} \cdots a_m^{b_m} - 1| \leq \frac{1}{2}$$

τότε

$$\frac{1}{2}|b_1 \log a_1 + \ldots + b_m \log a_m| \leq |a_1^{b_1} \cdots a_m^{b_m} - 1| \leq 2|b_1 \log a_1 + \ldots + b_m \log a_m|,$$

(για z μιγαδικό αριθμό και για κάθε $0 \leq \theta < 1$, αν $|\mathrm{e}^z - 1| \leq \theta$, τότε για τον πρωταρχικό λογάριθμο, $|\log z| \leq \frac{1}{1-\theta}|z-1|$).

Άρα, η εύρεση ενός κάτω φράγματος της απόστασης του 1 και του γινομένου $a_1^{b_1} \cdots a_m^{b_m}$, είναι ισοδύναμο με την εύρεση κάτω φράγματος για μη μηδενικές γραμμικές μορφές $b_1 \log a_1 + \ldots + b_m \log a_m$.

Αποδεικνύεται, σχετικά εύκολα, το εξής

Λήμμα 1.3.1. *Έστω $m, a_1, \ldots, a_m$ ρητοί ακέραιοι οι οποίοι είναι ≥ 2. Ορίζουμε, $A = \max\{a_1, \ldots, a_m\}$. Τότε, για κάθε ακέραιο $B \geq 4 \log A$, υπάρχουν ρητοί ακέραιοι $b_1, \ldots, b_m$, με*

$$0 < \max_{1 \leq i \leq m} |b_i| < B,$$

τέτοιοι ώστε

$$|a_1^{b_1} \cdots a_m^{b_m} - 1| \leq \frac{2m \log A}{B^{m-1}}.$$

Γενικά, λέμε ότι τα $\alpha_1, \ldots, \alpha_n \in K^*$, K σώμα, είναι πολλαπλασιστικώς εξαρτημένα αν και μόνο αν υπάρχουν $b_1, \ldots, b_n \in \mathbb{Z} \setminus \{0\}$, τέτοια ώστε: $\alpha_1^{b_1} \cdots \alpha_n^{b_n} = 1$. Διαφορετικά λέμε ότι τα $\alpha_1, \ldots, \alpha_n \in K^*$ είναι πολλαπλασιαστικώς ανεξάρτητα.

Οπότε, αν τα $a_1, \ldots, a_m$ είναι πολλαπλασιαστικώς ανεξάρτητα, τότε $a_1^{b_1} \cdots a_m^{b_m} - 1 \neq 0$.

Το 1935, ο A. O. Gelfond (πρβλ. [15]), ένα χρόνο αργότερα αφού είχε λύσει το 7ο πρόβλημα του D. Hilbert, εφάρμοσε την υπερβατική μέθοδο του για να βρει ένα κάτω φράγμα για μη μηδενικές γραμμικές σχέσεις δύο λογαρίθμων αλγεβρικών αριθμών με αλγεβρικούς συντελεστές.

Ένα απλό παράδειγμα τέτοιου είδους φράγματος είναι το εξής

Λήμμα 1.3.2. *Για a_1, a_2 πολλαπλασιαστικώς ανεξάρτητα θετικούς ρητούς ακεραίους, για κάθε $\varepsilon > 0$ υπάρχει υπολογίσιμη σταθερά $C_1 = C_1(a_1, a_2, \varepsilon)$, τέτοια ώστε, για κάθε $(b_1, b_2) \in \mathbb{Z}^2$, με $(b_1, b_2) \neq (0, 0)$,*

$$|a_1^{b_1} a_2^{b_2} - 1| \geq C_1 \mathrm{e}^{-(\log B)^{5+\varepsilon}},$$

όπου $B = \max\{2, |b_1|, |b_2|\}$.

Ύστερα από αρκετές βελτιώσεις του εκθέτη $5+\varepsilon$, ο A. O. Gelfond το 1949 απέδειξε το (πρβλ. [15], Θεώρημα III)

Θεώρημα 1.3.3. *(Μη υπολογίσιμη εκτίμηση) Για κάθε $m-$αδα $(a_1, \ldots, a_m)$ πολλαπλασιαστικώς ανεξάρτητων θετικών ρητών ακεραίων, και για κάθε $\delta > 0$, υπάρχει θετική σταθερά $C_2 = C_2(a_1, \ldots, a_m, \delta)$, τέτοια ώστε, αν $b_1, \ldots, b_m$ είναι ρητοί ακέραιοι, όχι όλοι μηδέν, τότε*

$$|a_1^{b_1} a_2^{b_2} - 1| \geq C_2 \mathrm{e}^{-\delta B},$$

όπου $B = \max\{2, |b_1|, |b_2|\}$.

Ο A. O. Gelfond χρησιμοποίησε το αποτέλεσμα του θεωρήματος 1.3.3 σε πολλές διοφαντικές ερωτήσεις. Συγκεκριμένα, το εφάρμοσε για να υπολογίσει (μαζί με τον Y. V. Linnik) το πρόβλημα του Gauss για τον υπολογισμό όλων των τετραγωνικών φανταστικών σωμάτων με αριθμό κλάσεων ίσο με ένα. Επίσης, το φράγμα του το εφάρμοσε για να μελετήσει και διάφορες διοφαντικές εξισώσεις. Στο βιβλίο του [15], αναφέρεται στη μεγάλη σημασία που θα είχε για την Θεωρία Αριθμών, η εύρεση κάτω φραγμάτων για γραμμικές μορφές λογαρίθμων αλγεβρικών αριθμών με ακέραιους συντελεστές. Το πρόβλημα αυτό λύθηκε το 1966 από τον A. Baker (πρβλ. [2]), ο οποίος ανακάλυψε ένα υπολογίσιμο φράγμα για γραμμικές μορφές λογαρίθμων αλγεβρικών αριθμών με αλγεβρικούς συντελεστές.

Κεφάλαιο 2

Περιγραφή της απόδειξης

Σκοπός του κεφαλαίου αυτού είναι η περιγραφή της απόδειξης του θεωρήματος 1.2.2, το οποίο, όπως αποδείξαμε στην παράγραφο 1.2, είναι ισοδύναμο με το θεώρημα του Baker.

Οπότε, σε αυτό το κεφάλαιο τα $\ell_1, \ldots, \ell_{n+1}$ είναι $\mathbb{Q}-$ γραμμικώς ανεξάρτητα στοιχεία του $\mathfrak{L}$ (το οποίο σημαίνει ότι $\alpha_i = e^{\ell_i}$ είναι αλγεβρικοί αριθμοί) και οι $\beta_1, \ldots, \beta_n$ είναι αλγεβρικοί αριθμοί.
Υποθέτουμε ότι

$$\ell_{n+1} = \beta_1 \cdot \ell_1 + \ldots + \beta_n \cdot \ell_n \tag{2.1}$$

και θέλουμε να αποδείξουμε ότι τα $1, \beta_1, \ldots, \beta_n$ είναι $\mathbb{Q}-$ γραμμικώς εξαρτημένα.

Θα γίνει πρώτα μια περιγραφή της απόδειξης του θεωρήματος του Baker (παράγραφος 2.1). Ύστερα, στην παράγραφο 2.2, θα γίνει η απόδειξη της περίπτωσης $n = 1$ του θεωρήματος του Baker, όπου $\log \alpha_1, \beta = \beta_1$ είναι πραγματικοί αριθμοί (πραγματική περίπτωση του θεωρήματος των Gelfond-Schneider). Θα αποδείξουμε δηλαδή ότι αν $\beta \log \alpha_1 = \log \alpha_2 \in \mathfrak{L}$ (το οποίο σημαίνει ότι $\alpha_2 \in \overline{\mathbb{Q}}$), τότε ο β είναι ρητός. Για παράδειγμα, έτσι προκύπτει ότι οι $2^{\sqrt{2}}$ και $\frac{\log 2}{\log 3}$ είναι υπερβατικοί.

2.1 Η ιδέα της απόδειξης

Θα δουλέψουμε με τις εξής $n+1$ συναρτήσεις n μεταβλητών:

$$z_1, \ldots, z_n, \alpha_1^{z_1} \cdots \alpha_n^{z_n},$$

όπου φυσικά $\alpha_1^{z_1} \cdots \alpha_n^{z_n} = \mathrm{e}^{z_1\ell_1 + \ldots + z_n\ell_n}$ ($\mathrm{e}^{\ell_i} = \alpha_i$).

Παρατηρούμε ότι λόγω της σχέσης (2.1), οι συναρτήσεις αυτές παίρνουν αλγεβρικές τιμές σε όλα τα σημεία της μορφής

$$(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n),\ (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}.$$

Το σύνολο των σημείων αυτών είναι μια πεπερασμένα παραγόμενη υποομάδα του $\mathbb{C}^n$, την οποία θα γράφουμε

$$Y = \mathbb{Z}^n + \mathbb{Z}(\beta_1, \ldots, \beta_n).$$

Επίσης, παρατηρούμε ότι οι συναρτήσεις αυτές είναι αλγεβρικώς ανεξάρτητες υπέρ το $\mathbb{C}$ [1], δηλαδή για κάθε μη μηδενικό πολυώνυμο P, $n+1$ μεταβλητών με μιγαδικούς συντελεστές η συνάρτηση

$$F(z_1, \ldots, z_n) = P(z_1, \ldots, z_n, \alpha_1^{z_1} \cdots \alpha_n^{z_n})$$

δεν είναι ταυτοτικά μηδέν [2].

Επίσης, για συντομία θα γράφουμε $\underline{s}$ για $(s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}$. Όταν ο S είναι θετικός πραγματικός αριθμός, ορίζουμε $\mathbb{Z}^{n+1}(S)$ να είναι το σύνολο των $\underline{s}$ με $|s_i| < S,\ (1 \le i \le n+1)$. Το σύνολο αυτό έχει $(2[S]-1)^{n+1}$ στοιχεία. Για κάθε $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$, ορίζουμε την συνάρτηση $f_{\underline{\lambda}}$:

$$f_{\underline{\lambda}}(z_1, \ldots, z_n) = z_1^{\lambda_1} \cdot \ldots \cdot z_n^{\lambda_n} \cdot (\alpha_1^{z_1} \cdots \alpha_n^{z_n})^{\lambda_{n+1}}.$$

(Επειδή οι συναρτήσεις που ορίσαμε στην αρχή της παραγράφου είναι αλγεβρικά ανεξάρτητες, προκύπτει ότι οι f_λ δεν είναι ταυτοτικά μηδέν).

Διαλέγουμε έναν αρκετά μεγάλο ακέραιο S. Το πόσο μεγάλο θα είναι αυτό το S θα μπορούσε να υπολογιστεί ακριβώς, αλλά είναι αρκετό εδώ να πούμε ότι πρέπει να είναι μεγάλο σε σχέση με πεπερασμένες ποσότητες οι οποίες προκύπτουν από τα ℓ_i και β_i, (από τους βαθμούς και επίσης την μεγαλύτερη από τις απόλυτες τιμές των συντελεστών των ελαχίστων πολυωνύμων τους). Επίσης χρειαζόμαστε και δύο ακόμα παραμέτρους, L_0 και L_1 ($L_0, L_1 \in \mathbb{N}$), τέτοιες ώστε: $\lambda_1 + \ldots + \lambda_n \le L_0$ και $\lambda_{n+1} \le L_1$.
Θεωρούμε τον πίνακα

$$\begin{aligned}\Pi &= \Big(f_{\underline{\lambda}}(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n)\Big)_{\underline{\lambda},\underline{s}} \\ &= \Big((s_1 + s_{n+1}\beta_1)^{\lambda_1} \ldots (s_n + s_{n+1}\beta_n)^{\lambda_n} \big(\alpha_1^{s_1+s_{n+1}\beta_1} \cdots \alpha_n^{s_n+s_{n+1}\beta_n}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\underline{s}} \\ (\text{σχέση (2.1)}) &= \Big((s_1 + s_{n+1}\beta_1)^{\lambda_1} \ldots (s_n + s_{n+1}\beta_n)^{\lambda_n} \big(\alpha_1^{s_1} \cdots \alpha_n^{s_n} \alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\underline{s}},\end{aligned}$$

[1] Γενικά, οι αναλυτικές συναρτήσεις $f_1, \ldots, f_d$ n μεταβλητών είναι αλγεβρικώς ανεξάρτητες υπέρ το $\mathbb{C}$, αν και μόνο αν, για κάθε μη μηδενικό πολυώνυμο $P \in \mathbb{C}[X_1, \ldots, X_d]$, η συνάρτηση $P(f_1, \ldots, f_d)$ δεν είναι η μηδενική συνάρτηση.

[2] Η απόδειξη αυτού του ισχυρισμού είναι όμοια με εκείνη του θεωρήματος 2.2.2

όπου ο δείκτης των γραμμών είναι $\underline{\lambda}$ και των στηλών $\underline{s}$ (Παρατηρούμε ότι ο Π είναι μη μηδενικός πίνακας, αφού οι $f_{\underline{\lambda}}$ δεν είναι ταυτοτικά μηδέν). Μας ενδιαφέρει μόνο η τάξη του πίνακα Π. Επειδή το $\underline{\lambda}$ παίρνει όλες τις τιμές $(\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$ τέτοιες ώστε:

$$\lambda_1 + \ldots + \lambda_n \leq L_0 \text{ και } \lambda_{n+1} \leq L_1,$$

ο αριθμός των γραμμών είναι $\binom{L_0+n}{n} \cdot (L_1+1)$ [3]. Από την άλλη το $\underline{s}$ παίρνει όλες τις τιμές $(s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}(S)$, οπότε έχουμε $(2S-1)^{n+1}$ στήλες. Διαλέγουμε τις παραμέτρους έτσι ώστε να ικανοποιείται η εξής ανισότητα

$$(2S-1)^{n+1} \geq \binom{L_0+n}{n} \cdot (L_1+1)$$

(αριθμός γραμμών μικρότερος από αριθμό στηλών).

Η απόδειξη χωρίζεται σε δύο μέρη.

Στο πρώτο μέρος (υπερβατικό μέρος της απόδειξης), θα αποδείξουμε ότι η τάξη του παραπάνω πίνακα είναι μικρότερη του $L := \binom{L_0+n}{n} \cdot (L_1+1)$.

Στο δεύτερο μέρος (γεωμετρικό μέρος της απόδειξης), θα δείξουμε ότι ο ισχυρισμός αυτός για την τάξη του πίνακα συνεπάγεται την γραμμική εξάρτηση των $1, \beta_1, \ldots, \beta_n$.[4]

Στο πρώτο μέρος της απόδειξης, για να δείξουμε ότι η τάξη του πίνακα είναι μικρότερη από L, αυτό που κάνουμε είναι το εξής:
Εξετάζουμε μία οποιαδήποτε $L \times L$ υποορίζουσα του παραπάνω πίνακα. Αυτό σημαίνει ότι έχουμε ένα υποσύνολο των $\underline{s}$ και γράφουμε

$$\Delta = \det\Big((s_1 + s_{n+1}\beta_1)^{\lambda_1} \ldots (s_n + s_{n+1}\beta_n)^{\lambda_n} \big(\alpha_1^{s_1} \cdots \alpha_n^{s_n} \alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}} \Big)_{\underline{\lambda},\underline{s}}.$$

Αν δείξουμε ότι $\Delta = 0$, τότε η τάξη του πίνακα είναι $< L$, οπότε έχουμε επιτύχει το στόχο του πρώτου μέρους της απόδειξης. Η απόδειξη του ότι $\Delta = 0$ συνίσταται στα εξής δύο βήματα:
Πρώτα βρίσκουμε ένα άνω φράγμα για την Δ, συγκεκριμένα θα δείξουμε ότι

$$\frac{1}{L} \log|\Delta| \leq -L^{1/n} + c_1(L_0 \log S + L_1 S),$$

όπου το c_1 εξαρτάται από τα n, ℓ_i, β_i [5].
Ύστερα, με την βοήθεια της ανισότητας του Liouville, θα δείξουμε ότι αν η Δ

[3] πρβλ. παράρτημα Α΄.1

[4] Το δεύτερο μέρος της απόδειξης παρουσιάζεται στο κεφάλαιο 5

[5] Η απόδειξη αυτού του ισχυρισμού αποδεικνύεται στο κεφάλαιο 4 με εφαρμογή του λήμματος του Schwarz

δεν είναι μηδεν, τότε

$$\frac{1}{L}\log\Delta \geq -c_2(L_0\log S + L_1 S),$$

όπου το c_2 εξαρτάται από τα n, ℓ_i, β_i [6].
Ύστερα, αφού επιλέξουμε τα $L_0, L_1, S \geq 2$, να ικανοποιούν κάποιες συνθήκες συναρτήσει ενός μεγάλου αριθμού c, (ο οποίος εξαρτάται μόνο από τα n, ℓ_i, β_i), εκτιμώντας κατάλληλα αυτόν το αριθμό c από τα c_1, c_2, (να είναι αρκετά μεγάλος από τα c_1, c_2), δείχνουμε ότι οι παραπάνω δύο ανισότητες είναι αντιφατικές, οπότε καταλήγουμε στο συμπέρασμα ότι $\Delta = 0$.

Ως ένα παράδειγμα εφαρμογής των ιδεών που αναφέρθηκαν, θα παρουσιάσουμε την απόδειξη του θεωρήματος του Baker για $n = 1$ (Θεώρημα των Gelfond- Schneider) στην περίπτωση που $\ell_1, \beta_1 \in \mathbb{R}$.

2.2 Θεώρημα Gelfond - Schneider για πραγματικούς αριθμούς

Η πραγματική περίπτωση του θεωρήματος των Gelfond - Schneider διατυπώνεται ισοδύναμα ως εξής:

Θεώρημα 2.2.1. *(Η πραγματική περίπτωση των Gelfond -Schneider): Αν τα $\ell_1, \ell_2 \in \mathfrak{L} \cap \mathbb{R}$ είναι $\bar{\mathbb{Q}}-$ γραμμικώς εξαρτημένα τότε είναι και $\mathbb{Q}-$ γραμμικώς εξαρτημενα.*

Πριν την απόδειξη θα χρειαστούμε τα παρακάτω δύο θεωρήματα.

Θεώρημα 2.2.2. *Έστω $p_1(t), \ldots, p_n(t)$ πολυώυυμα στον $\mathbb{R}[t]$ με βαθμούς $d_1, \ldots, d_n$ αντίστοιχα, και έστω $w_1, \ldots, w_n$ διαφορετικοί ανά δύο πραγματικοί αριθμοί. Τότε η πραγματική συνάρτηση μιας μεταβλητής*

$$F(t) = \sum_{i=1}^{n} p_i(t)\mathrm{e}^{w_i t},$$

έχει το πολύ $d_1 + \ldots + d_n + n - 1$ πραγματικές ρίζες [7].

Απόδειξη. Θα αποδείξουμε το λήμμα κάνοντας επαγωγή στον ακέραιο $k := d_1 + \ldots + d_n + n$.

[6] Η απόδειξη αυτού του ισχυρισμού αποδεικνύεται στο κεφάλαιο 3

[7] Σε αυτό το λήμμα οι ρίζες υπολογίζονται με τις πολλαπλότητες (αυτό είναι σημαντικό για την απόδειξη η οποία θα γίνει με επαγωγή)

Για $k = 1$, έχουμε ότι $n = 1$ και $d_1 = 0$ [8].
Υποθέτουμε ότι $k \geq 2$.
Έστω ότι η υπόθεση ισχύει για $\ell = 1, \ldots, k-1$. Δηλαδή αν $n \geq 1$ και $d_1, \ldots, d_n$ είναι μη αρνητικοί ακέραιοι, τέτοιοι ώστε $d_1 + \ldots + d_n + n = \ell < k$ και $p_i(t) \in \mathbb{R}[t]$ έχει βαθμό d_i για $i = 1, \ldots, n$ τότε η συνάρτηση στην εκφώνηση του λήμματος έχει $\ell - 1$, το πολύ πραγματικές ρίζες. Θα δείξουμε ότι ισχύει αυτό και για $\ell = k$.
Πολλαπλασιάζουμε την F με $\mathrm{e}^{-w_n t}$. Αφού το πλήθος των ριζών της F και της $\mathrm{e}^{-w_n t} \cdot F$ είναι το ίδιο, μπορούμε να υποθέσουμε ότι $w_n = 0$. Έτσι, επειδή τα $w_1, \ldots, w_n$ είναι διαφορετικά ανά δύο, έχουμε ότι $w_i \neq 0$ για $1 \leq i \leq n$. Αν η F έχει τουλάχιστον N πραγματικές ρίζες τότε, από το γνωστό θεώρημα του Rolle, η F' έχει τουλάχιστον $N - 1$ πραγματικές ρίζες. Όμως, αφού $w_n = 0$, έχουμε ότι:

$$F'(t) = \sum_{i=1}^{n-1} \widetilde{p}_i(t) e^{w_i t} + \frac{d}{dt} p_n(t),$$

όπου $\widetilde{p}_i(t) = w_i p_i(t) = \frac{d}{dt} p_i(t)$ είναι πολυώνυμο βαθμού ακριβώς d_i για $i = 1, \ldots, n-1$ και βαθμού $d_n - 1$ για $i = n$ [9].
Οπότε για τους βαθμούς των πολυωνύμων $\widetilde{p}_i t$ της F' έχουμε ότι:

$$d_1 + \ldots + d_n - 1 + n = d_1 + \ldots + d_n + n - 1 = \ell' < k.$$

Άρα από την επαγωγική υπόθεση η F' έχει το πολύ:

$$d_1 + \ldots + d_n - 1 + n - 1$$

πραγματικές ρίζες.
Άρα $N - 1 \leq d_1 + \ldots + d_n + n - 2$. Οπότε:

$$N \leq d_1 + \ldots + d_n + n - 1.$$

(N = πλήθος πραγματικών ριζών της F).

□

Θεώρημα 2.2.3. [10] *Έστω r, R δύο πραγματικοί αριθμοί με $0 \leq r \leq R$, $f_1, \ldots, f_L$ συναρτήσεις μιας μεταβλητής, οι οποίες είναι αναλυτικές στον $\Delta(0, R)$ και $\zeta_1, \ldots, \zeta_L \in \Delta(0, r)$. Τότε η ορίζουσα :*

$$\Delta = \det \begin{pmatrix} f_1(\zeta_1) & \ldots & f_L(\zeta_1) \\ \vdots & \ddots & \vdots \\ f_1(\zeta_L) & \ldots & f_L(\zeta_L) \end{pmatrix}$$

[8] Διότι $d_i \in \mathbb{N}$
[9] Εδώ θεωρούμε ότι ο βαθμός του μηδενικού πολυωνύμου είναι -1
[10] πρβλ. Α΄.2 για τους ορισμούς και τους συμβολισμούς

έχει άνω φράγμα:

$$|\Delta| \leq \left(\frac{R}{r}\right)^{-L\cdot\frac{L-1}{2}} \cdot L! \cdot \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

(Το συμπέρασμα είναι τετριμμένο στην περίπτωση $R = r$).

Απόδειξη. Η ορίζουσα $\Psi(z)$ του πίνακα

$$\Big(f_\lambda(\zeta_\mu \cdot z)\Big)$$

είναι μια μιγαδική συνάρτηση μιας μεταβλητής η οποία είναι αναλυτική στον $\Delta(0,R)$. Παρακάτω θα αποδείξουμε ότι έχει στο 0 μηδενική θέση τάξεως τουλάχιστον $L\cdot\frac{L-1}{2}$. Οπότε από το λήμμα Α΄.2.1 [11], έχουμε ότι αν στο 0 έχει μηδενική θέση τάξεως N, τότε

$$|\Delta| = |\Psi(1)| \leq \left(\frac{R}{r}\right)^{-N} \cdot |\Psi|_R \leq \left(\frac{R}{r}\right)^{-L\cdot\frac{L-1}{2}} \cdot |\Psi|_R.$$

Για το $|\Psi|_R$ έχουμε ότι:

$$|\Psi|_R = {}^{12}$$

$$= \Big| \sum_{\sigma\in\, \mathbb{S}_L} \operatorname{sgn}(\sigma) \cdot f_{1\sigma(1)} \cdot f_{2\sigma(2)} \cdot \ldots \cdot f_{L\sigma(L)} \Big|_R \leq$$

$$\leq \Big|f_{1\sigma_1(1)} \cdot \ldots \cdot f_{1\sigma_1(L)}\Big| + \ldots + \Big|f_{1\sigma_{L!}(1)} \cdot \ldots \cdot f_{1\sigma_{L!}(L)}\Big| \leq$$

$$\leq L! \cdot \prod_{i=1}^{L} |f_i|_R.$$

Άρα:

$$|\Delta| \leq \left(\frac{R}{r}\right)^{-L\cdot\frac{L-1}{2}} \cdot L! \cdot \prod_{i=1}^{L} |f_i|_R.$$

Για την τάξη του 0 :
Κάθε f_λ με κέντρο το 0 έχει ανάπτυγμα Taylor:

$$f_\lambda(z) = \sum_{n_\lambda=0}^{\infty} \alpha_{n_\lambda} z^{n_\lambda}, \text{ όπου } \alpha_{n_\lambda} = \frac{f^{(n_\lambda)}(0)}{n_\lambda!}.$$

[11] Εφαρμόζουμε το λήμμα αντικαθιστώντας το r με 1 και το R με $\frac{R}{r}$.
[12] $f_{ij} = f_i(\zeta_j)$ και $\mathbb{S}_L$: η ομάδα των μεταθέσεων των L στοιχείων

Άρα,

$$\Psi(z) = \sum_{\sigma\in\mathbb{S}_L} \operatorname{sgn}(\sigma) f_{1\sigma(1)} \cdot \ldots \cdot f_{L\sigma(L)} =$$

$$= \sum_{\sigma\in\mathbb{S}_L} \Big[\operatorname{sgn}(\sigma)\Big(\sum_{n_1=0}^{\infty} \alpha_{n_1} z^{n_1} \zeta_{\sigma(1)}^{n_1}\Big) \cdot \ldots \cdot \Big(\sum_{n_L=0}^{\infty} \alpha_{n_L} z^{n_L} \zeta_{\sigma(L)}^{n_L}\Big)\Big] =$$

$$= \sum_{n_1,\ldots,n_L} \Big((\alpha_{n_1} \cdot \ldots \cdot \alpha_{n_L}) \sum_{\sigma\in\mathbb{S}_L} \operatorname{sgn}(\sigma) \cdot z^{n_1} \zeta_{\sigma(1)}^{n_1} \cdot \ldots \cdot z^{n_L} \zeta_{\sigma(L)}^{n_L}\Big) =$$

$$= \sum_{n_1,\ldots,n_L} \Big((\alpha_{n_1} \cdot \ldots \cdot \alpha_{n_L}) \cdot \det\Big(z^{n_\lambda} \cdot \zeta_\mu^{n_\lambda}\Big)_{\mu,\lambda}\Big),$$

όπου $1 \le \mu \le L$.
Αρκεί, λοιπόν να εξεταστούν οι περιπτώσεις όπου $f_\lambda(z) = z^{n_\lambda}$. Σε μία τέτοια περίπτωση

$$\Psi(z) = \det \begin{pmatrix} z^{n_1}\zeta_1^{n_1} & \ldots & z^{n_L}\zeta_1^{n_L} \\ \vdots & \ddots & \vdots \\ z^{n_1}\zeta_L^{n_1} & \ldots & z^{n_L}\zeta_L^{n_L} \end{pmatrix} =$$

$$= \det\Big[\Big(\zeta_\mu^{n_\lambda}\Big)_{\mu,\lambda} \cdot \begin{pmatrix} z^{n_1} & 0 & 0 & \ldots & 0 \\ 0 & z^{n_2} & 0 & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & & \ldots & z^{n_L} \end{pmatrix}\Big] =$$

$$= z^{n_1+\ldots+n_L} \cdot \det\Big(\zeta_\mu^{n_\lambda}\Big).$$

Η ορίζουσα $\Psi(z)$ είναι ταυτοτικά μηδέν αν τα n_j δεν είναι ανά δύο διαφορετικά. Άρα, αν η $\Psi(z)$ δεν είναι ταυτοτικά μηδέν, τότε τα n_j είναι διαφορετικά ανά δύο. Άρα

$$n_1 + n_2 + \ldots + n_L \ge 0 + 1 + \ldots + (L-1) = \frac{L(L-1)}{2}.$$

Άρα, η $\Psi(z)$ έχει στο 0 μηδενική θέση τουλάχιστον $\frac{L(L-1)}{2}$.

□

Απόδειξη του Θεωρήματος 2.2.1: Έστω $\ell_1 \in \mathfrak{L} \cap \mathbb{R}$ και $\beta \in \bar{\mathbb{Q}} \cap \mathbb{R}$, τέτοια ώστε : $\ell_2 = \beta\ell_1 \in \mathfrak{L}$. Ορίζουμε $\alpha_i = \mathrm{e}^{\ell_i}$, $(i = 1, 2)$, οπότε $\alpha_i \in \bar{\mathbb{Q}}^*$ και $\alpha_1^\beta = \alpha_2$.
Θέλουμε να δείξουμε ότι τα ℓ_1, ℓ_2 ειναι $\mathbb{Q}-$ γραμμικώς εξαρτημένα, δηλαδή ότι ο β είναι ρητός.

Έστω c ένας επαρκώς μεγάλος αριθμός. Μία κατάλληλη τιμή για τον c μπορεί να υπολογιστεί μετά το τέλος της απόδειξης. Αυτή η τιμή θα εξαρτάται μόνο από τα ℓ_1 και β (και θα περιέχει επίσης και τον αλγεβρικό αριθμό α_2).
Στη συνέχεια διαλέγουμε τρεις ακέραιους αριθμούς L_0, L_1, S, οι οποίοι να ικανοποιούν τα εξής:

$$L_0 \geq 2,\ L_1 \geq 2,\ S \geq 2, \tag{2.2}$$

$$L := (L_0+1)(L_1+1), \tag{2.3}$$

$$cL_0 \log S \leq L,\ cL_1 S \leq L,\ L \leq (2S-1)^2. \tag{2.4}$$

Για παράδειγμα, θα μπορούσαμε να πάρουμε

$$L_1 = \lfloor \log S \rfloor^2 \text{ και } L_0 = \lfloor S^2 (\log S)^{-3} \rfloor,$$

με το S επαρκώς μεγάλο.
Τώρα, αν τροποποιήσουμε λίγο τον συμβολισμό και γράψουμε (λ_0, λ_1) αντί (λ_1, λ_2), για να προσαρμοστούμε στον συμβολισμό της ενότητας 2.1, βλέπουμε ότι η ορίζουσα εκείνης της ενότητας παίρνει την μορφή

$$\Pi = \Big((s_1 + s_2\beta)^{\lambda_0} \big(\alpha_1^{s_1}\alpha_2^{s_2}\big)^{\lambda_1} \Big)_{(\lambda_0,\lambda_1),(s_1,s_2)}$$

$$(\text{αφού } \alpha_2 = \alpha_1^{\beta}) = \Big((s_1 + s_2\beta)^{\lambda_0} \big(\alpha_1^{s_1+s_2\beta}\big)^{\lambda_1} \Big)_{(\lambda_0,\lambda_1),(s_1,s_2)},$$

με

$$0 \leq \lambda_0 \leq L_0,\ 0 \leq \lambda_1 \leq L_1,\ |s_1| \leq S,\ |s_2| \leq S.$$

Ο πίνακας αυτός έχει $L := (L_0+1)(L_1+1)$ γραμμές και $(2S-1)^2$ στήλες. Όπως είπαμε στην προηγούμενη ενότητα επιλέγουμε έτσι τα L_0 και L_1 ώστε:

$$L := (L_0+1)(L_1+1) \leq (2S-1)^2.$$

Όπως αναφέραμε στην προηγούμενη ενότητα, η απόδειξη του θεωρήματος του Baker χωρίζεται σε δύο μέρη. Έτσι και εδώ, στην πραγματική περίπτωση για $n = 1$, θα χωρίσουμε την απόδειξη σε δύο μέρη.

(**i**) *Πρώτο μέρος της απόδειξης:*
Θα δείξουμε ότι ο πίνακας που ορίστηκε παραπάνω έχει τάξη $< L$.
Έστω $s^{(1)}, \ldots, s^{(L)}$ οποιαδήποτε στοιχεία του $\mathbb{Z}^2(S)$. Παίρνουμε την $L \times L$ ορίζουσα

$$\Delta = \Big((s_1^{(\mu)} + s_2^{(\mu)}\beta)^{\lambda_0} \big(^{\lambda_1}\alpha_1^{s_1^{(\mu)}+s_2^{(\mu)}\beta}\big)^{\ell_1} \Big)_{\underline{\lambda},\mu},$$

με $\underline{\lambda} = (\lambda_0, \lambda_1)$, $0 \leq \lambda_0 \leq L_0$, $0 \leq \lambda_1 \leq L_1$ και $1 \leq \mu \leq L$.
Θα χρησιμοποιήσουμε το λήμμα 2.2.3 με $r = S(1+|\beta|)$ και $R = e^2 \cdot r$, για

την $f_\lambda(z) = z^{\lambda_0} \cdot e^{\lambda_1 \cdot z \cdot \ell_1}$, με $\zeta_\mu = s_1^{(\mu)} + s_2^{(\mu)}\beta$.
Έχουμε λοιπόν ότι:

$$|\Delta| \leq \left(\frac{R}{r}\right)^{-L \cdot \frac{L-1}{2}} \cdot L! \cdot \prod_{\lambda=1}^{L} |f_\lambda|_R =$$

$$= e^{-L(L-1)} \cdot L! \cdot \prod_{\lambda=1}^{L} |f_\lambda|_R,$$

όπου:

$$\begin{aligned} |f_\lambda|_R = |z^{\lambda_0 \cdot e^{\lambda_1 z \ell_1}}| \leq \\ \leq R^{\lambda_0} \cdot e^{\lambda_1 R|\ell_1|} \leq \\ \leq R^{\lambda_0} \cdot e^{L_1 R|\ell_1|}. \end{aligned}$$

Οπότε:

$$\begin{aligned} \log|\Delta| &\leq -L(L-1) + \log L! + LL_0 \log R + LL_1 R|\ell_1| \\ &\leq -L(L-1) + L\log L + LL_0 \log R + LL_1 R|\ell_1| \\ &\leq -L^2 + L + L\log L + LL_0 \log[e^2 S(1+|\beta|)] + LL_1 R|\ell_1| \\ &\leq -L^2 + L + L\log(2S-1)^2 + LL_0 \log[e^2 S(1+|\beta|)] + LL_1 R|\ell_1| \\ &\leq -L^2 + L + L\log 4S^2 + LL_0 \log[e^2 S(1+|\beta|)] + LL_1 R|\ell_1| \\ &\leq -L^2 + L + 2L\log 2S + LL_0 \log[e^2 S(1+|\beta|)] + LL_1 R|\ell_1| \\ (L_0 \geq 2) \ &\leq -L^2 + L + L_0 L \log 2S + LL_0 \log[e^2 S(1+|\beta|)] + LL_1 R|\ell_1| \\ &\leq -L^2 + LL_0 \log 2 + LL_0 \log S + 2LL_0 + LL_0 \log[S(1+|\beta|)] + LL_1 R|\ell_1| \end{aligned}$$

($L \leq LL_0 \log S$, $2LL_0 \leq 4LL_0 \log S$ και $S \geq 2$)

$$\begin{aligned} &\leq -L^2 + 7LL_0 \log S + LL_0 \log S(1+|\beta|) + LL_1 e^2 S(1+|\beta|)|\ell_1| \\ &\leq -L^2 + 7LL_0 \log S + LL_0 \log[Se^{(1+|\beta|)}] + LL_1 e^2 S(1+|\beta|)|\ell_1| \\ &\leq -L^2 + LL_0(10+|\beta|)\log S + LL_1 e^2 S(1+|\beta|)|\ell_1| \\ &\leq -L^2 + c_1 L(L_0 \log S + L_1 S), \end{aligned}$$

όπου $c_1 = \max\{10+|\beta|,\ e^2(1+|\beta|)|\ell_1|\}$.
Λόγω της επιλογής των L_0, L_1, S στην αρχή της απόδειξης καταλήγουμε στη σχέση

$$\log|\Delta| \leq \frac{-L^2}{2},$$

αν $c \geq 4c_1$ (πρβλ. σχέση 2.4) και το L είναι αρκούντως μεγάλο.
(Αυτό διότι λόγω των ανισοτήτων, $cL_0 \log S \leq L$ και $cL_1 S \leq L$, έχουμε ότι: $-L^2 + c_1 L(L_0 \log S + L_1 S) \leq -L^2 + c_1 L(\frac{L}{c} + \frac{L}{c})$, οπότε για $c \geq 4c_1$ έχουμε το ζητούμενο.)

Στο κεφάλαιο 3, μεσω της ανισότητας του Liouville, θα δείξουμε ότι, είτε η $|\Delta|$ είναι μηδέν, είτε

$$\log |\Delta| \geq -c_2 L(L_0 \log S + L_1 S),$$

όπου το c_2 εξαρτάται μόνο από τα ℓ_1, β. Για $c \geq 3c_2$ (πρβλ. σχέση 2.4) η προηγούμενη σχέση μας δίνει

$$\log |\Delta| > \frac{-L^2}{2}.$$

(Η ανισότητα προκύπτει όπως και πριν στη περίπτωση του c_1, χρησιμοποιώντας την σχέση 2.4).

Άρα συμπεραίνουμε ότι $\Delta = 0$, οπότε ο πίνακας Π έχει τάξη μικρότερη του L.

(**ii**) *Δεύτερο μέρος της απόδειξης:*
Θα δείξουμε ότι από το συμπέρασμα του πρώτου μέρους για την τάξη του πίνακα Π έπεται ότι ο β είναι ρητός.
Έχουμε ότι ο πίνακας

$$\Pi = \left((s_1 + s_2\beta)^{\lambda_0} \left(\alpha_1^{s_1+s_2\beta}\right)^{\ell_1} \right)_{(\lambda_0,\lambda_1),(s_1,s_2)},$$

με

$$0 \leq \lambda_0 \leq L_0,\ 0 \leq \lambda_1 \leq L_1,\ |s_1| \leq S,\ |s_2| \leq S,$$

έχει $L := (L_0 + 1)(L_1 + 1))$ γραμμές και $(2S-1)^2$ στήλες. Επίσης λόγω της επιλογης των παραμέτρων στην αρχή της απόδειξης έχουμε ότι : $L \leq (2S-1)^2$. Αν λοιπόν ο πίνακας έχει τάξη μικρότερη του L τότε υπάρχουν $c_i \in \mathbb{R}$ τέτοια ώστε:

$$c_1\gamma_1 + \ldots + c_L\gamma_L = \mathbf{0} \in \mathbb{R}^{(2S-1)^2},$$

όπου $\gamma_1, \ldots, \gamma_L$ οι γραμμές του παραπάνω πίνακα. Δηλαδή,

$$\sum_{i=1}^{L} c_i\gamma_i = \mathbf{0},$$

ή

$$\sum_{(\lambda_0,\lambda_1)} c_{(\lambda_0,\lambda_1)}\gamma_{(\lambda_0,\lambda_1)} = \mathbf{0}.$$

Άρα για κάθε $z = s_1 + s_2\beta$ με $(s_1, s_2) \in \mathbb{Z}^2(S)$ έχουμε ότι

$$\sum_{(\lambda_0,\lambda_1)} c_{(\lambda_0,\lambda_1)}(s_1 + s_2\beta)^{\lambda_0}\left(\alpha_1^{s_1+s_2\beta}\right)^{\ell_1} = 0.$$

Οπότε το

$$F(z) = \sum_{(\lambda_0,\lambda_1)} c_{(\lambda_0,\lambda_1)} z^{\lambda_0}\left(\alpha_1^z\right)^{\lambda_1}\ ^{13}$$

μηδενίζεται για κάθε $z = s_1 + s_2\beta$ όπου $(s_1, s_2) \in \mathbb{Z}^2(S)$.
Το πλήθος αυτών των z για τα οποία η $F(z)$ μηδενίζεται γνωρίζουμε όμως ότι είναι $(2S-1)^2$. Όμως αυτό είναι αδύνατο, διότι, λόγω του λήμματος 2.2.2, η

$$F(z) = \sum_{(\lambda_0,\lambda_1)} c_{(\lambda_0,\lambda_1)} z^{\lambda_0} e^{z\cdot\lambda_1\cdot\ell_1} =$$

$$= \sum_{\lambda_1}[\sum_{\lambda_0} c_{(\lambda_0,\lambda_1)} z^{\lambda_0}]e^{z\lambda_1\ell_1},$$

έχει το πολύ

$$(L_1+1)L_0 + L_1 + 1 - 1,$$

πραγματικές ρίζες το οποίο είναι μικρότερο του $(2S-1)^2$ [14]. Άρα υπάρχουν $z = s_1 + s_2\beta$, $z' = s_1' + s_2'\beta$ με $(s_1, s_2), (s_1', s_2') \in \mathbb{Z}^2(S)$ και $(s_1, s_2) \neq (s_1', s_2')$ τέτοια ώστε : $z = z'$. Δηλαδή:

$$s_1 + s_2\beta = s_1' + s_2'\beta,$$

δηλαδή ο β είναι ρητός.

□

[13] $F(z) = P(z, \alpha_1^z)$, όπου $P(x, y) = \sum_{(\lambda_0,\lambda_1)} x^{\lambda_0} y^{\lambda_1}$

[14] Αφού $(L_1+1)L_0 + L_1 + 1 - 1 = (L_1+1)(L_0+1) - 1 < L < (2S-1)^2$.

Κεφάλαιο 3

Ανισότητα Liouville - Κάτω φράγμα της ορίζουσας

Στο κεφάλαιο αυτό θα βρούμε ένα κάτω φράγμα της ορίζουσας Δ (παράγραφο 3.6), η οποία ορίστηκε στην παράγραφο 2.1. Για να το πετύχουμε αυτό θα χρειαστούμε την ανισότητα του Liouville η οποία μας εξασφαλίζει κάτω φράγμα για κάθε μη μηδενικό αλγεβρικό αριθμό. Πιο συγκεκριμένα, η ανισότητα του Liouville μας δίνει ένα κάτω φράγμα για τον αλγεβρικό αριθμό $P(\gamma_1, \ldots, \gamma_q)$, όπου $\gamma_1, \ldots, \gamma_q$ αλγεβρικοί αριθμοί και το πολυώνυμο $P \in \mathbb{Z}[x_1, \ldots, x_q]$ δεν μηδενίζεται στο σημείο $(\gamma_1, \ldots, \gamma_q)$. Το φράγμα αυτό εξαρτάται μόνο από το βαθμό του P, από το άνω φράγμα των απόλυτων τιμών των συντελεστών του και από τα μέτρα των γ_i.

Για να πετύχουμε τέτοια φράγματα εισάγουμε την έννοια του ύψους αλγεβρικού αριθμού. Για τον σκοπό αυτό προτάσσουμε κάποιες βασικές γνώσεις από την αλγεβρική θεωρία αριθμών (πρβλ. και Α΄.3).

3.1 $p-$αδικές απόλυτες τιμές υπέρ το $\mathbb{Q}$

Έστω p ένας πρώτος αριθμός. Για κάθε $x \in \mathbb{Z}^*$ ορίζουμε $\nu_p(x) =$ η μέγιστη δύναμη του p η οποία διαιρεί το x. Για $x = \frac{a}{b} \in \mathbb{Q}^*, a, b \in \mathbb{Z}^*$ ορίζουμε $\nu_p(x) = \nu_p(a) - \nu_p(b)$.
Επίσης για $x \in \mathbb{Q}^*$ γράφουμε την ανάλυση του x σε γινόμενο πρώτων παραγόντων ως εξής:

$$x = \pm \prod_p p^{\nu_p(x)}.$$

Για κάθε πρώτο p έχουμε λοιπόν μια απεικόνιση:

$$\nu_p : \mathbb{Q}^* \to \mathbb{Z},$$

η οποία επεκτείνεται στο 0, με $\nu_p(0) = \infty$.
Η απεικόνιση:

$$\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\},$$

ονομάζεται $p-$*αδική αποτίμηση* πάνω από το $\mathbb{Q}$ και ικανοποιεί τις παρακάτω ιδιότητες:

1. Για κάθε $x \in \mathbb{Q}$, $\nu_p(x) = \infty \Leftrightarrow x = 0$.
2. Για $x, y \in \mathbb{Q}$, $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.
3. Για $x, y \in \mathbb{Q}$, $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$.

Η ν_p σχετίζεται με την απόλυτη τιμή $|\cdot|_p$ ($p-$αδική απόλυτη τιμή) η οποία είναι μια απεικόνιση από το $\mathbb{Q}$ στο $\mathbb{Q}$ που ορίζεται ως εξής: Επιλέγουμε ϱ με $0 < \varrho < 1$ και θέτουμε

$$|x|_p = \begin{cases} \varrho^{\nu_p(x)}, & x \neq 0 \\ 0, & x = 0. \end{cases}$$

Η $p-$αδική απόλυτη τιμή ικανοποιεί τις παρακάτω ιδιότητες:

1. Για $x \in \mathbb{Q}$, $|x|_p = 0 \Leftrightarrow x = 0$.
2. Για $x, y \in \mathbb{Q}$, $|xy|_p = |x|_p |y|_p$.
3. Για $x, y \in \mathbb{Q}$, $|x + y|_p \leq \max\{|x|_p, \ |y|_p\}$ $(\leq |x|_p + |y|_p)$.

Μια τέτοια απόλυτη τιμή χαρακτηρίζεται *μη αρχιμήδεια*. Στο $\mathbb{Q}$ συνιθισμένη απόλυτη τιμή $(|\cdot|)$ χαρακτηρίζεται *αρχιμήδεια*.

Επιλέγουμε δηλαδή $\varrho = \frac{1}{p} < 1$, οπότε $|x|_p = p^{-\nu_p(x)}$.

Η $p-$αδική απόλυτη τιμή ορίζει απόσταση στο $\mathbb{Q}$, άρα τοπολογία. Η μπάλα με κέντρο $a \in \mathbb{Q}$ και ακτίνα p^{-r} με $r \in \mathbb{Z}$ είναι, συνεπώς, το σύνολο

$$\mathfrak{D}(a, r) := \{x \in \mathbb{Q}; \ |x - a|_p \leq p^{-r}\} = \{x \in \mathbb{Q}; \ \nu_p(x - a) \geq r\}.$$

Σε τυχαίο σώμα έχουμε τον εξής:

Ορισμός 3.1.1. *Έστω K ένα τυχαίο σώμα. Μία συνάρτηση $|\cdot|$ από το σώμα K στους πραγματικούς αριθμούς καλείται απόλυτη τιμή του K, αν αυτή ικανοποιεί τις παρακάτω συνθήκες:*

1. $|a| > 0$ *για κάθε* $a \neq 0$ *και* $|0| = 0$.
2. $|a + b| \leq |a| + |b|$.
3. $|ab| = |a| \cdot |b|$.

   Αν αυτί της τρίτης ιδιότητας η απόλυτη τιμή ικανοποιεί την πιο ισχυρή συνθήκη:

4. $|a + b| \leq \max\{|a|, |b|\}$,

τότε ονομάζουμε την απόλυτη τιμή μη αρχιμήδεια.

Η απόλυτη τιμή $|\cdot|$ για την οποία ισχύει: $|x| = 1$ για όλα τα $x \neq 0$ και $|0| = 0$, ονομάζεται *τετριμμένη απόλυτη τιμή*. Αποδεικνύεται ότι οι μη τετριμμένες απόλυτες τιμές είναι μη φραγμένες.

Η απόλυτη τιμή ορίζει απόσταση στο σώμα K και άρα τοπολογία στο σώμα K. Η έννοια της σύγκλισης ορίζεται ως εξής:

Η ακολουθία $\{a_n\}$ στοιχείων του K συγκλίνει στο στοιχείο $a \in K$ αν $|a_n - a| \to 0$ καθώς $n \to \infty$.
Επίσης:
Μια ακολουθία $\{a_n\}$ στοιχείων του K καλείται Cauchy αν $|a_n - a_m| \to 0$ καθώς $n, m \to \infty$. Προφανώς κάθε συγκλίνουσα ακολουθία είναι ακολουθία Cauchy.

Ένα σώμα εφοδιασμένο με μια απόλυτη τιμή καλείται *πλήρες* ως προς αυτή την απόλυτη τιμή, αν κάθε ακολουθία Cauchy είναι συγκλίνουσα, με όριο που ανήκει στο σώμα αυτό.

Γνωρίζουμε ότι η πλήρωση του $\mathbb{Q}$ ως προς την συμηθισμένη απόλυτη τιμή είναι το σώμα των πραγματικών αριθμών. Επίσης η πλήρωση του $\mathbb{Q}$ ως προς την $p-$αδική απόλυτη τιμή είναι το σώμα των $p-$αδικών αριθμών $\mathbb{Q}_p$. Κάθε $x \in \mathbb{Q}_p$ μπορεί να γραφεί:

$$x = \sum_{i=m}^{+\infty} a_i p^i,$$

όπου $a_i \in \{0, 1, \ldots, p-1\}$, $a_m \neq 0$. Το m που μπορεί να είναι και αρνητικός ακέραιος συμβολίζεται με $\nu_p(x)$ και λέγεται $p-$*αδική αποτίμηση* του $x \in \mathbb{Q}_p$. Επεκτείνοντας την $p-$αδική απόλυτη τιμή που ορίσαμε πριν για τους ρητούς, ορίζουμε

$$|x|_p = p^{-\nu_p(x)}.$$

Δύο απόλυτες τιμές $|\cdot|_1, |\cdot|_2$ ενός σώματος K λέγονται *ισοδύναμες* αν μια ακολουθία είναι Cauchy ως προς την $|\cdot|_1$ αν και μόνο αν είναι Cauchy ως προς την $|\cdot|_2$. Αυτό είναι ισοδύναμο με το να πούμε ότι οι $|\cdot|_1, |\cdot|_2$ ορίζουν

την ίδια τοπολογία στο σώμα K.

Αποδεικνύεται [10] ότι κάθε μη τετριμμένη απόλυτη τιμή του $\mathbb{Q}$ είναι ισοδύναμη είτε με την $p-$αδική απόλυτη τιμή είτε με την συνηθισμένη απόλυτη τιμή στο $\mathbb{Q}$ (Θεώρημα Ostrowski). Άρα οι μόνες πληρώσεις του $\mathbb{Q}$ είναι είτε το σώμα των πραγματικών αριθμών είτε το σώμα των $p-$αδικών αριθμών $\mathbb{Q}_p$.

Πρόταση 3.1.2. *(Τύπος Γινομένου υπέρ το $\mathbb{Q}$)*

$$|x| \cdot \prod_p |x|_p = 1,$$

για κάθε $x \in \mathbb{Q} \setminus \{0\}$, όπου $|\cdot|, |\cdot|_p$ είναι αντίστοιχα η συνηθισμένη και η απόλυτη τιμή του $\mathbb{Q}$.

Απόδειξη. Αρκεί να το δείξουμε για $x \in \mathbb{Z},\ \ x > 0$. Η περίπτωση το $x \in \mathbb{Q}\setminus\{0\}$ με $x = \frac{a}{b},\ \ a, b \in \mathbb{Z} \setminus \{0\}$ ανάγεται στην περίπτωση των ακεραίων αφού:

$$|\frac{a}{b}| \prod_p |\frac{a}{b}|_p = \frac{|a| \prod_p |a|_p}{|b| \prod_p |b|_p}.$$

Έστω λοιπόν $x \in \mathbb{Z},\ \ x > 0$, με $x = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m},\ \ p_i$ πρώτοι και $a_i \in \mathbb{Z},\ \ a_i > 0$. Τότε:

$$\begin{aligned} &|x|_q = 1, \text{ αν } q \neq p_i,\ \ i = 1, \ldots, m \\ &|x|_{p_i} = p_i^{-a_i}, \text{ για } i = 1, \ldots, m \\ &|x| = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m}. \end{aligned}$$

Άρα:

$$|x| \cdot \prod_p |x|_p = 1.$$

□

Ισοδύναμα από τον τύπο του γινομένου έχουμε ότι:

$$\sum_p \nu_p(x) \log p = \log |x|,$$

για κάθε $x \in \mathbb{Q} \setminus \{0\}$.

3.2 Απόλυτες τιμές σε αριθμητικό σώμα

Θα μελετήσουμε τις απόλυτες τιμές πάνω από αριθμητικό σώμα K. Για να το κάνουμε αυτό θα πρέπει να εξετάσουμε πώς μπορεί να επεκταθεί μια απόλυτη τιμή από το $\mathbb{Q}$ στο K. Κατ' αρχάς, παρατηρούμε ότι ο περιορισμός στο $\mathbb{Q}$ μιας μη τετριμμένης απόλυτης τιμής του σώματος K είναι μη τετριμμένη απόλυτη τιμή του $\mathbb{Q}$. Πράγματι, έστω $|\cdot|_1$ μια μη τετριμμένη απόλυτη τιμή του αριθμητικού σώματος K. Παίρνοντας τον περιορισμό της $|\cdot|_1$ στο $\mathbb{Q}$ έχουμε την απόλυτη τιμή $|\cdot|_0$ του $\mathbb{Q}$. Θα δείξουμε ότι η $|\cdot|_0$ είναι μη τετριμμένη. Έστω η βάση $\omega_1, \ldots, \omega_n$ του K υπερ το $\mathbb{Q}$. Για κάθε $x \in K$ έχουμε ότι $x = q_1\omega_1 + \ldots + q_n\omega_n$, με $q_i \in \mathbb{Q}$, οπότε

$$|x|_1 = |q_1|_0|\omega|_1 + \ldots + |q_n|_0|\omega_n|_1.$$

Αν η απόλυτη τιμή $|\cdot|_0$ είναι τετριμμένη τότε $|q_i|_0 \leq 1$ και άρα:

$$|x|_1 \leq \sum_{i=1}^{n} |\omega_i|_1,$$

για όλα τα $x \in K$. Άτοπο, αφού κάθε μη τετριμμένη απόλυτη τιμή δεν είναι φραγμένη.

Από το θεώρημα του Ostrowski συμπεραίνουμε ότι η $|\cdot|_0$ είναι ισοδύναμη είτε με την $p-$αδική απόλυτη τιμή (σε αυτή την περίπτωση η $|\cdot|_1$ είναι μη αρχιμήδεια), είτε με την συνηθισμένη απόλυτη τιμή (σε αυτή την περίπτωση η $|\cdot|_1$ είναι αρχιμήδεια).

Συμβολίζουμε με M_K το σύνολο όλων των κλάσεων απολύτων τιμών του σώματος K ως προς την ισοδυναμία απολύτων τιμών και με M_K^∞ το υποσύνολο του M_K, που αποτελείται από τις κλάσεις των αρχιμήδειων απολύτων τιμών. Για κάθε ισοδύναμη κλάση $\upsilon \in M_K$ συμβολίζουμε με K_υ την πλήρωση του K ως προς την υ. Τα στοιχεία (κλάσεις ισοδυναμίας) του M_K λέγονται και *θέσεις* του K και κάθε θέση χαρακτηρίζεται αρχιμήδεια ή μη αρχιμήδεια ανάλογα με το αν είναι κλάση ισοδυναμίας αρχιμήδειας ή μη αρχιμήδειας απόλυτης τιμής, αντιστοίχως.

Το θεώρημα του Ostrowski λέει, ουσιαστικά, ότι το $M_\mathbb{Q}$ αποτελείται από τη θέση της συνήθους απόλυτης τιμής και από τις θέσεις των p-αδικών απολύτων τιμών, καθώς ο p διατρέχει όλους τους πρώτους. Άρα, για $\upsilon_0 \in M_\mathbb{Q}$, το $\mathbb{Q}_{\upsilon_0}$ είναι το $\mathbb{R}$ είτε το $\mathbb{Q}_p$ για κάποιον πρώτο p.

Αν το K είναι επέκταση του αριθμητικού σώματος K_0 και $\upsilon_0 \in M_{K_0}$, $\upsilon \in M_K$, ο συμβολισμός $\upsilon|\upsilon_0$ σημαίνει ότι μία (άρα και κάθε) απόλυτη τιμή στη θέση υ είναι επέκταση (ως συνάρτηση ορισμένη στο K) κάποιας απόλυτης τιμής που ανήκει στη υ_0.

Αν $\upsilon \in M_K$ και $\upsilon|\upsilon_0$ με $\upsilon_0 \in M_{\mathbb{Q}}$, τότε τον βαθμό $d_\upsilon := [K_\upsilon : \mathbb{Q}_{\upsilon_0}]$ ορίζουμε ως βαθμό της υ ως προς τη συγκεκριμένη υ_0 ή, απλώς, βαθμό της υ αν είναι σαφές ποια είναι η θέση υ_0.

3.2.1 Αρχιμήδειες απόλυτες τιμές

Έστω $K = \mathbb{Q}(\alpha)$ αριθμητικό σώμα βαθμού n και f το ανάγωγο πολυώνυμο του α υπέρ το $\mathbb{Q}$, το οποίο γράφομε ως

$$f(X) = a_0X^n + \cdots a_{n-1}X + a_n \in \mathbb{Z}[X]\,, \quad (a_0, a_1, \ldots, a_n) = 1\,.$$

Έστω r_1 το πλήθος των πραγματικών ριζών και r_2 το πλήθος των ζευγών των συζυγών μιγαδικών ριζών του f, οπότε $n = r_1 + 2r_2$. Τις ρίζες αυτές συμβολίζουμε $\alpha^{(1)}, \ldots, \alpha^{(r_1)}$ (πραγματικές), $\alpha^{(r_1+1)}, \overline{\alpha^{(r_1+1)}}, \ldots, \alpha^{(r_1+r_2)}, \overline{\alpha^{(r_1+r_2)}}$ (μιγαδικές).
Υπάρχουν ακριβώς n μονομορφικές εμφυτεύσεις σωμάτων $K \hookrightarrow \mathbb{C}$, συμβολιζόμενες

$$\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \ldots \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}\,,$$

οι οποίες χαρακτηρίζονται από τις τιμές τους στο α:

$$\sigma_j(\alpha) = \alpha^{(j)}\,,\ 1 \le j \le r_1 + r_2\,, \quad \overline{\sigma}_j(\alpha) = \overline{\alpha^{(j)}}\,,\ r_1 + 1 \le j \le r_1 + r_2\,.$$

Σε κάθε εμφύτευση $\sigma :\ K \hookrightarrow \mathbb{C}$, αντιστοιχεί μια απόλυτη τιμή $|\cdot|_\sigma$ η οποία ορίζεται ως εξής: $|x|_\sigma = |\sigma(x)|$,[1] για $x \in K$. Αποδεικνύεται ότι, με αυτόν τον τρόπο παίρνουμε όλες (κατά προσέγγιση ισοδυναμίας απολύτων τιμών) τις αρχιμήδειες απόλυτες τιμές του K (όλες είναι επεκτάσεις της συνηθισμένης απόλυτης τιμής του $\mathbb{Q}$ στο K). Τη θέση της $|\cdot|_\sigma$ συμβολίζουμε $\upsilon_\sigma \in M_K$ και, σύμφωνα με τα παραπάνω, κάθε $\upsilon \in M_K^\infty$ ταυτίζεται με κάποια υ_σ.

Κάνουμε τώρα την εξής σύμβαση: Όταν για κάποια $\upsilon \in M_K^\infty$ γράφουμε $|\cdot|_\upsilon$, εννοούμε ότι αυτή η απόλυτη τιμή είναι μία από τις $r_1 + r_2$ απόλυτες τιμές $|\cdot|_{\sigma_i}$ για κάποιο $i \in \{1, \ldots, r_1 + r_2\}$.

Αν $\sigma = \sigma_j$ για κάποιο $j \in \{1, \ldots, r_1\}$, τότε $\sigma(K) \subset \mathbb{R}$, άρα $K_{\upsilon_\sigma} = \mathbb{R}$. Η εμφύτευση σ και η θέση υ_σ χαρακτηρίζονται τότε πραγματικές. Αν $\sigma = \sigma_j$ ή $\overline{\sigma}_j$ για κάποιο $j \in \{r_1 + 1, \ldots, r_1 + r_2\}$, τότε $K_{\upsilon_\sigma} = \mathbb{C}$ και η εμφύτευση σ, καθώς και η θέση υ_σ χαρακτηρίζονται μιγαδικές.
Στην περίπτωση, που μελετούμε, είναι $d_\upsilon = [K_\upsilon : \mathbb{R}]$, οπότε

$$d_\upsilon = \begin{cases} 1, & \text{αν } \upsilon = \upsilon_\sigma \text{ για κάποια πραγματική εμφύτευση } \sigma, \\ 2, & \text{αν } \upsilon = \upsilon_\sigma \text{ για κάποια μιγαδική εμφύτευση } \sigma \end{cases}$$

[1] Με $|\cdot|$ εννούμε το συνηθισμένο μέτρο μιγαδικού αριθμού στο $\mathbb{C}$ του οποίου ο περιορισμός στο $\mathbb{R}$ είναι η συνηθισμένη απόλυτη τιμή

και, συνεπώς,

$$\sum_{v\in M_K, v|v_0} d_v = [K:\mathbb{Q}] \quad \text{όταν } v_0 \text{ είναι η συνήθης απόλυτη τιμή του } \mathbb{Q}. \tag{3.1}$$

Επίσης, σύμφωνα με τα παραπάνω,

$$\prod_{v\in M_K^\infty} |\alpha|_v^{d_v} = \prod_{i=1}^{n} |\alpha^{(i)}| = \left|\frac{a_n}{a_0}\right|,$$

οπότε και

$$\prod_{v\in M_K^\infty} \max\{1, |\alpha|_v\}^{d_v} = \prod_{i=1}^{n} \max\{1, |\alpha^{(i)}|\}.$$

3.2.2 Μη αρχιμήδειες απόλυτες τιμές

Έστω $K, \alpha, n, f, M_K, M_K^\infty$ όπως στην υποενότητα 3.2.1 και p ρητός πρώτος. Χρησιμοποιούμε, επίσης, τον εξής γενικό συμβολισμό. Για κάθε πρώτο ιδεώδες $\wp$ του K και για κάθε $x \in K^*$ ορίζουμε την $\wp$-αδική αποτίμηση $\nu_\wp(x)$ του x ως τον ακέραιο με τον οποίον εμφανίζεται το $\wp$ στην κανονική ανάλυση σε πρώτα ιδεώδη του ιδεώδους $\langle x\rangle$. Επεκτείνοντας την $\wp$-αδική αποτίμηση και στο 0, ορίζουμε $\nu_\wp(0) = \infty$. Επίσης, με $e_\wp$ και $d_\wp$ συμβολίζουμε, αντιστοίχως, τον δείκτη διακλάδωσης και τον βαθμό αδρανείας του $\wp$. Η έννοια της $\wp$-αδικής αποτίμησης στο K επεκτείνει την έννοια της p-αδικής αποτίμησης στο $\mathbb{Q}$, που ορίσθηκε στην ενότητα 3.1, και σχετίζεται με αυτήν ως εξής: $\nu_\wp(x) = e_\wp \cdot \nu_p(x)$ για $x \in \mathbb{Q}$.

Το f, αν και ανάγωγο πάνω από το $\mathbb{Q}$, δεν είναι, εν γένει, ανάγωγο πάνω από το $\mathbb{Q}_p$. Έστω, λοιπόν,

$$f(X) = g_1(X)\cdots g_m(X), \quad g_i(X) \in \mathbb{Q}_p[X] \text{ ανάγωγο } (i = 1,\dots,m). \tag{3.2}$$

Τα g_i είναι διαφορετικά μεταξύ τους (μ' άλλα λόγια, το f δεν έχει πολλαπλές ρίζες πάνω από το $\mathbb{Q}_p$) και έστω ότι d_i είναι ο βαθμός του g_i $(i = 1,\dots,m)$. Θέτουμε, επίσης $K_i = \mathbb{Q}_p(\alpha_i)$, όπου $g_i(\alpha_i) = 0$. Κάθε $x = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \in \mathbb{Q}(\alpha) = K$ αντιστοιχεί στο $x_i \in K_i$, που προκύπτει όταν το α στην έκφραση του x αντικατασταθεί από το α_i. Ακόμη ακριβέστερα, η αντιστοιχία αυτή είναι μονομορφική εμφύτευση σωμάτων $K \hookrightarrow K_i$, οπότε βλέπουμε στο εξής τα K_i ως επεκτάσεις όχι μόνο του $\mathbb{Q}_p$, αλλά και του K.

Είναι πολύ σημαντικό ότι η ανάλυση του f σε ανάγωγα πολυώνυμα του $\mathbb{Q}_p[X]$ έχει στενή σχέση με την ανάλυση του ιδεώδους $\langle p\rangle$ σε πρώτα ιδεώδη του K. Συγκεκριμένα, έχουμε μια κανονική ανάλυση σε πρώτα ιδεώδη

$$\langle p\rangle = \wp_1^{e_{\wp_1}} \cdots \wp_m^{e_{\wp_m}}, \tag{3.3}$$

όπου η αρίθμηση των πρώτων ιδεωδών είναι τέτοια ώστε να ισχύει

$$\nu_p(\mathrm{N}_{K_i/\mathbb{Q}_p}(x_i)) = d_{\wp_i}\nu_{\wp_i}(x) \text{ για κάθε } x \in K, \text{ και } d_i = d_{\wp_i}e_{\wp_i} \quad (i = 1, \ldots, m). \tag{3.4}$$

Από την τελευταία σχέση, ειδικώτερα, έπεται ότι

$$n = \sum_{i=1}^{m} d_{\wp_i}e_{\wp_i} \, . \tag{3.5}$$

Για κάθε πρώτο ιδεώδες $\wp$ πάνω από τον p ορίζεται η $\wp$-αδική απόλυτη τιμή στο K:

$$|x|_{\wp} = p^{-\frac{1}{e_{\wp}}\nu_{\wp}(x)} \, , \; x \in K, \tag{3.6}$$

οπότε, ειδικώτερα, $|x|_{\wp_i} = |x|_p$ για κάθε $x \in \mathbb{Q}$. Άρα, λόγω της (3.3) βλέπουμε ότι έχουμε m $\wp$-αδικές απόλυτες τιμές $|\cdot|_{\wp_1}, \ldots, |\cdot|_{\wp_m}$, οι οποίες επεκτείνουν την $|\cdot|_p$ στο K. Οι απόλυτες τιμές αυτές είναι μη ισοδύναμες και κάθε άλλη απόλυτη τιμή, που επεκτείνει στο K την απόλυτη τιμή $|\cdot|_p$ του $\mathbb{Q}_p$, είναι ισοδύναμη με μία από αυτές τις m $\wp$-αδικές απόλυτες τιμές. Τις θέσεις (κλάσεις ισοδυναμίας) αυτών των $\wp$-αδικών απολύτων τιμών συμβολίζουμε $\upsilon_{\wp_i}$, $i = 1, \ldots, m$. Κατ' αναλογία με τη σύμβαση που κάναμε στην υποενότητα των αρχιμήδειων απολύτων τιμών, η θέση $\upsilon_{\wp}$ θα αντιπροσωπεύεται σ' αυτή την εργασία αποκλειστικά από την απόλυτη τιμή που ορίζεται από τη σχέση (3.6). Επίσης, όταν για κάποια θέση $\upsilon \in M_K$ γράφουμε $|\cdot|_{\upsilon}$ με $\upsilon|p$ εννοούμε ότι η απόλυτη τιμή $|\cdot|_{\upsilon}$ του K είναι κάποια $|\cdot|_{\wp_i}$ για κάποιο $i \in \{1, \ldots, m\}$.

Προχωρούμε τώρα να δούμε πώς επεκτείνεται η p-αδική απόλυτη τιμή $|\cdot|_p$ του $\mathbb{Q}_p$ σε μια οποιαδήποτε πεπερασμένη επέκταση, έστω L, του $\mathbb{Q}_p$ βαθμού d. Συμβολίζουμε με $\mathbb{C}_p$ την πλήρωση της αλγεβρικής κλειστότητας του $\mathbb{Q}_p$. Η $p-$αδική απόλυτη τιμή $|\cdot|_p$ του $\mathbb{Q}_p$ επεκτείνεται με μοναδικό τρόπο στην L ως εξής:

$$|x|_p = \left|\mathrm{N}_{L/\mathbb{Q}_p}(x)\right|_p^{\frac{1}{d}} \, , \;\; x \in L \tag{3.7}$$

και το L είναι πλήρες ως προς αυτή την απόλυτη τιμή. Ο παραπάνω ορισμός της απόλυτης τιμής δεν εξαρτάται από το L, οπότε αυτό επιτρέπει την επέκταση της απόλυτης τιμής $|\cdot|_p$ σε όλο το $\mathbb{C}_p$.

Εφαρμόζουμε τα παραπάνω όταν $L = K_i$, $i \in \{1, \ldots, m\}$. Η πρώτη σχέση (3.4) σε συνδυασμό με την (3.7) δίνουν

$$|x_i|_p = |x|_{\wp_i} \, , \; (i = 1, \ldots, m).$$

Ακόμη ακριβέστερα, K_i είναι η πλήρωση του K ως προς την απόλυτη τιμή $|\cdot|_{\wp_i}$. Συνεπώς, αν $\upsilon \in M_K$ και $\upsilon|p$, οπότε η υ είναι η θέση μιας $\wp$-αδικής

απόλυτης τιμής για κάποιο πρώτο $\wp = \wp_i$ που διαιρεί τον p, τότε η πλήρωση K_υ του K ως προς τη υ είναι η K_i με την απόλυτη τιμή που ορίζεται από την (3.7) για $L = K_i$ και για τον βαθμό $d_\upsilon := [K_\upsilon : \mathbb{Q}_p]$ της υ έχουμε $d_\upsilon = d_{\wp_i} e_{\wp_i}$ και η σχέση (3.5) γίνεται

$$\sum_{\upsilon \in M_K, \upsilon | \upsilon_0} d_\upsilon = [K : \mathbb{Q}] \quad \text{όταν } \upsilon_0 \text{ είναι } p\text{-αδική απόλυτη τιμή του } \mathbb{Q}. \tag{3.8}$$

Αφ' ετέρου, το $g_i(X) \in \mathbb{Q}_p[X]$ έχει d_i διαφορετικές ρίζες στο $\mathbb{C}_p$, που τις συμβολίζουμε $\alpha_i^{(j)}$, $j = 1, \ldots, d_i$ και η επέκταση $K_i/\mathbb{Q}_p$ είναι ισόμορφη με την $\mathbb{Q}_p(\alpha_i^{(j)})$ για κάθε j. Συνεπώς, αν θεωρήσουμε την p-αδική απόλυτη τιμή του $\alpha_i^{(j)} \in \mathbb{C}_p$, έχουμε $|\alpha_i^{(j)}|_p = |\alpha|_{\wp_i}$ για κάθε $j = 1, \ldots, d_i$. Άρα,

$$\prod_{i=1}^{m} \prod_{j=1}^{d_i} |\alpha_i^{(j)}|_p = \prod_{i=1}^{m} |\alpha|_{\wp_i}^{d_i}$$

και επειδή τα $\alpha_i^{(j)}$ στο παραπάνω γινόμενο είναι, ακριβώς, οι ρίζες του $f(X)$ στο $\mathbb{C}_p$ και το γινόμενό τους είναι $(-1)^n a_n/a_0$, καταλήγουμε τελικά στις σχέσεις

$$\prod_{\substack{\upsilon \in M_K \\ \upsilon | p}} |\alpha|_\upsilon^{d_\upsilon} = \prod_{\substack{\beta \in \mathbb{C}_p \\ \text{ρίζα του } f}} |\beta|_p = \Big|\frac{a_n}{a_0}\Big|_p$$

και

$$\prod_{\substack{\upsilon \in M_K \\ \upsilon | p}} \max\{1, |\alpha|_\upsilon^{d_\upsilon}\} = \prod_{\substack{\beta \in \mathbb{C}_p \\ \text{ρίζα του } f}} \max\{1, |\beta|_p\}\,.$$

3.3 Ο τύπος του γινομένου σε αριθμητικό σώμα

Ο τύπος του γινομένου στο $\mathbb{Q}$, τον οποίο αναφέραμε στην 3.1, γενικεύεται και στα αριθμητικά σώματα.

Θεώρημα 3.3.1. *(Τύπος γινομένου σε αριθμητικό σώμα) Έστω αριθμητικό σώμα K. Για κάθε μη μηδενικό $x \in K$ ισχύει*

$$\prod_{\upsilon \in M_K} |x|_\upsilon^{d_\upsilon} = 1.$$

Απόδειξη. Έστω $x \in K^*$. Έστω p ρητός πρώτος και η ανάλυση του $\langle p \rangle$ σε πρώτα ιδεώδη δίδεται από τη σχέση (3.3). Τότε, σύμφωνα με όσα αναπτύξαμε

στην υποενότητα 3.2.2, της οποίας διατηρούμε το συμβολισμό και εδώ, έχουμε

$$\prod_{\upsilon|p}|x|_{\upsilon}^{d_{\upsilon}}=\prod_{i=1}^{m}|x|_{\wp_i}^{d_i}=^{2}\prod_{i=1}^{m}p^{-d_{\wp_i}\nu_{\wp_i}(x)}=\prod_{i=1}^{m}\mathrm{N}(\wp_i)^{-\nu_{\wp_i}(x)}=\mathrm{N}(\prod_{\wp|p}\wp^{-\nu_{\wp(x)}})\,.$$

όπου N συμβολίζει τη Norm ως προς την επέκταση $K/\mathbb{Q}$. Επειδή, προφανώς, $\prod_p\prod_{\wp|p}\wp^{\nu_{\wp}(x)}=\langle x\rangle$, όπου στο πρώτο γινόμενο το p διατρέχει όλους τους πρώτους, συμπεραίνομε ότι

$$\prod_{\upsilon\in M_K\setminus M_K^{\infty}}|x|_{\upsilon}^{d_{\upsilon}}=\mathrm{N}(\langle x\rangle)^{-1}=|\mathrm{N}(x)|^{-1}\,.$$

Φυσικά, το υ στο πρώτο από τα παραπάνω γινόμενα διατρέχει όλες τις μη αρχιμήδειες απόλυτες τιμές του K.

Για να ολοκληρώσουμε την απόδειξη του θεωρήματος, μένει ν' αποδείξουμε ότι $\prod_{\upsilon\in M_K^{\infty}}|x|_{\upsilon}=|\mathrm{N}(x)|$.

Αλλά, σύμφωνα με την υποενότητα 3.2.1, της οποίας διατηρούμε και τον συμβολισμό,

$$\begin{aligned}\prod_{\upsilon\in M_K^{\infty}}|x|_{\upsilon}^{d_{\upsilon}}&=\prod_{i=1}^{r_1}|\sigma_i(x)|\prod_{i=1}^{r_2}|\sigma_{r_1+i}(x)|^2\\&=|\sigma_1(x)|\cdots|\sigma_{r_1}(x)||\sigma_{r_1+1}(x)||\overline{\sigma_{r_1+1}(x)}|\cdots|\sigma_{r_1+r_2}(x)||\overline{\sigma_{r_1+r_2}(x)}|\\&=|\mathrm{N}(x)|\,.\end{aligned}$$

□

Τέλος, επανερχόμενοι στις σχέσεις (3.1) και (3.8), βλέπουμε ότι αυτές μπορούμε να τις διατυπώσουμε υπό ενοποιημένη μορφή ως εξής:

$$\sum_{\upsilon\in M_K,\upsilon|\upsilon_0}[K_{\upsilon}:\mathbb{Q}_{\upsilon_0}]=[K:\mathbb{Q}]\quad\text{για κάθε }\upsilon_0\in M_{\mathbb{Q}}.$$

Γενικεύοντας αυτή την πρόταση έχουμε:

Θεώρημα 3.3.2. *Έστω L πεπερασμένη επέκταση του αριθμητικού σώματος K και $\upsilon\in M_K$. Τότε*

$$\sum_{w\in M_L,w|\upsilon}[L_w:K_{\upsilon}]=[L:K]\,.$$

[2] (βλέπε (3.6) και (3.4))

3.4 Απόλυτο λογαριθμικό ύψος (Weil)

Έστω α ένας αλγεβρικός αριθμός. Έστω K ένα αριθμητικό σώμα βαθμού n το οποίο περιέχει τον α. Ορίζουμε το απόλυτο λογαριθμικό ύψος του α (Weil):

$$h(\alpha) = \frac{1}{n} \sum_{v \in M_K} d_v \log \max\{1, |\alpha|_v\}.$$

Από το θεώρημα 3.3.2 έχουμε ότι το $h(\alpha)$ δεν εξαρτάται από την επιλογή του σώματος K το οποίο περιέχει το α, αλλά μόνο από το α. Αυτό διότι:

Έστω $\alpha \in K$ και έστω K' μια πεπερασμένη επέκταση του K. Έστω επίσης: $[K' : \mathbb{Q}] = n'$ και $[K : \mathbb{Q}] = n$. Αφού $\alpha \in K$, έχω ότι και $\alpha \in K'$. Οπότε αν θεωρήσουμε το $h(\alpha)$ για το K' έχουμε

$$\begin{aligned}
h(\alpha) &= \frac{1}{n'} \sum_{w \in M_{K'}} d_w \log \max\{1, |\alpha|_\omega\} \\
(|\alpha|_w = |\alpha|_v, \text{ αφού } \alpha \in K \subset K') \ &= \frac{1}{n'} \sum_{v \in M_K} \sum_{\substack{w \in M_{K'} \\ \text{η επέκταση της } v \text{ στο } K'}} d_w \log \max\{1, |\alpha|_v\} \\
&= \frac{1}{[K' : K] \cdot n} \sum_{v \in M_K} \sum_{\substack{w \in M_{K'} \\ \text{η επέκταση της } v \text{ στο } K'}} d_w \log \max\{1, |\alpha|_v\} \\
(\text{θεώρημα } 3.3.2) \ &= \frac{1}{n} \sum_{v \in M_K} d_v \log \max\{1, |\alpha|_v\}.
\end{aligned}$$

Παράδειγμα. Για δύο ρητούς ακέραιους a, b οι οποίοι είναι πρώτοι μεταξύ τους,

$$h(\frac{a}{b}) = \log \max\{|a|, |b|\}.$$

Λήμμα 3.4.1. *Έστω α_1, α_2 δύο αλγεβρικοί αριθμοί. Τότε*

1. $h(\alpha_1 \alpha_2) \leq h(\alpha_1) + h(\alpha_2)$.
2. $h(\alpha_1 + \alpha_2) \leq \log 2 + h(\alpha_1) + h(\alpha_2)$.

   Επίσης, για κάθε αλγεβρικό αριθμό $\alpha \neq 0$ και για κάθε $d \in \mathbb{Z}$,

3. $h(\alpha^d) = |d| h(\alpha)$.

Απόδειξη.

Η ανισότητα 1 ισχύει λόγω της

$$\max\{1, xy\} \leq \max\{1, x\} \cdot \{1, y\}, \text{ για κάθε } x, y \geq 0.$$

Η ανισότητα 2 ισχύει λόγω της

$$\max\{1, x+y\} \leq 2\max\{1,x\}\max\{1,y\}, \text{ για κάθε } x,y \geq 0.$$

Θα αποδείξουμε την 3:

Ισχύει το εξής:

$$\max\{1, x^n\} = \max\{1,x\}^n \text{ για κάθε } x \geq 0, n \in \mathbb{Z}.$$

Αν $d \geq 0$ τότε για κάθε αλγεβρικό αριθμό α έχουμε ότι

$$h(\alpha^d) = d \cdot h(\alpha).$$

Έστω $d < 0$. Τότε,

$$|\alpha^d|_v = \frac{1}{|\alpha|_v^{-d}} = |\frac{1}{\alpha}|_v^{-d}.$$

Οπότε για $d < 0$

$$h(\alpha^d) = -d \cdot h(\frac{1}{\alpha}).$$

Αν δείξουμε ότι $h(\frac{1}{\alpha}) = h(\alpha)$, τότε θα έχουμε δείξει ότι

$$h(\alpha^d) = |d| \cdot h(\alpha),$$

για κάθε αλγεβρικό αριθμό $\alpha \neq 0$ και $d \in \mathbb{Z}$.

Θα δείξουμε λοιπόν ότι $h(\alpha) = h(\frac{1}{\alpha})$.

Ισχύει το εξής:

$$\max\{1,x\} = x \cdot \max\{1, \frac{1}{x}\}, \;\; x > 0.$$

Άρα,

$$\begin{aligned}
h(\frac{1}{\alpha}) &= \frac{1}{n}\sum_{v\in M_K} d_v \log\max\{1, \big|\frac{1}{\alpha}\big|_v\} \\
&= \frac{1}{n}\sum_{v\in M_K} d_v \log|\alpha|_v \max\{1, \big|\alpha\big|_v\} \\
&= \frac{1}{n}\sum_{v\in M_K} d_v \log|\max\{1, \big|\alpha\big|_v\} + \frac{1}{n}\sum_{v\in M_K} d_v \log|\alpha|_v \\
&= \frac{1}{n}\sum_{v\in M_K} d_v \log|\max\{1, \big|\alpha\big|_v\} + \frac{1}{n}\sum_{v\in M_K} \log|\alpha|_v^{d_v} \\
&= \frac{1}{n}\sum_{v\in M_K} d_v \log|\max\{1, \big|\alpha\big|_v\} + \frac{1}{n}\log\big(\prod_{v\in M_K} |\alpha|_v^{d_v}\big) \\
\text{(Θεώρημα 3.3.1)} \quad &= \frac{1}{n}\sum_{v\in M_K} d_v \log|\max\{1, \big|\alpha\big|_v\} + \frac{1}{n}\log 1 \\
&= \frac{1}{n}\sum_{v\in M_K} d_v \log|\max\{1, \big|\alpha\big|_v\} = h(\alpha).
\end{aligned}$$

□

Σημείωση. Στην ανισότητα 2 ο σταθερός όρος $\log 2$ στο δεξιό μέλος δεν μπορεί να αντικατασταθεί από μικρότερη σταθερά, αφού αν πάρουμε $a_1 = a_2 = 1$, τότε,

$$\begin{aligned}
h(a_1 + a_2) = h(2) &= \sum_{v\in M_{\mathbb{Q}}} \log\max\{1, |2|_v\} \\
&= \log\{1, |2|\} + \log\max\{1, |2|_2\} + \log\max\{1, |2|_3\} + \log\max\{1, |2|_5\} + \dots \\
&= \log 2 + \log\max\{1, \frac{1}{2}\} \\
&= \log 2.
\end{aligned}$$

(Στην ανισότητα 2: $\log 2 + h(\alpha_1) + h(\alpha_2) \geq \log 2$, αφού $h(\alpha) \geq 0$).

□

Το επόμενο λήμμα μας δίνει ένα άνω φράγμα για το απόλυτο λογαριθμικό ύψος αλγεβρικού αριθμού ο οποίος δίνεται ως η τιμή ενός πολυωνύμου στους αλγεβρικούς αριθμούς $\gamma_1, \dots, \gamma_t$.

Έστω $f \in \mathbb{C}[x_1, \dots, x_t]$ ένα πολυώνυμο με t μεταβλητές και με μιγαδικούς συντελεστές. Συμβολίζουμε με $L(f)$ το άθροισμα των μέτρων των συντελεστών του f και το ονομάζουμε *μήκος* του πολυωνύμου f. Το $L(f)$ ικανοποιεί τις εξής δύο ανισότητες

- $L(f+g) \leq L(f) + L(g)$
- $L(fg) \leq L(f)L(g)$.

Η απόδειξη της πρώτης ανισότητας δεν έχει καποια δυσκολία. Για την δεύτερη ανισότητα,

Έστω $f = \sum_{\underline{i}} a_{\underline{i}} \underline{X^i}$ και $g = \sum_{\underline{j}} b_{\underline{j}} \underline{X^j}$, όπου: $\underline{i} = (i_1, \ldots, i_t) \in \mathbb{N}^t$, $\underline{X} = (x_1, \ldots, x_t)$, $\underline{X^i} = x_1^{i_1} \cdot x_2^{i_2} \cdot \ldots \cdot x_t^{i_t}$.

$$fg = \sum_{\underline{k}} \sum_{\underline{i}+\underline{j}=\underline{k}} a_{\underline{i}} b_{\underline{j}} \underline{X^k}.$$

Οπότε,

$$L(fg) = \sum_{\underline{k}} \Big| \sum_{\underline{i}+\underline{j}=\underline{k}} a_{\underline{i}} b_{\underline{j}} \Big| \leq \sum_{\underline{k}} \sum_{\underline{i}+\underline{j}=\underline{k}} |a_{\underline{i}} b_{\underline{j}}| = L(f)L(g).$$

Εφαρμογή του λήμματος 3.4.3, το οποίο θα αποδείξουμε παρακάτω, είναι το εξής

Λήμμα 3.4.2. *Έστω $f \in \mathbb{Z}[x_1, \ldots, x_t]$, είναι ένα μη μηδενικό πολυώνυμο t μεταβλητών με συντελεστές ρητούς ακεραίους. Έστω $\gamma_1, \ldots, \gamma_t$ αλγεβρικοί αριθμοί. Τότε:*

$$h\big(f(\gamma_1, \ldots, \gamma_t)\big) \leq \log L(f) + \sum_{i=1}^{t} \big(\deg_{x_i} f\big) h(\gamma_i).$$

Παρατηρήσεις.

(1) Έστω $\frac{p_1}{q_1}$ και $\frac{p_2}{q_2}$ δύο ρητοί αριθμοί με $q_i > 0$, $i = 1, 2$ και μκδ(p_1, q_1) =μκδ(p_2, q_2). Αν εφαρμόσουμε το λήμμα 3.4.2 έχουμε

$$\begin{aligned} h(\frac{p_1}{q_1} + \frac{p_2}{q_2}) &\leq \log 2 + \log \max\{|p_1|, q_1\} + \log \max\{|p_2|, q_2\} \\ &= \log 2 + h(\frac{p_1}{q_1}) + h(\frac{p_1}{q_1}), \end{aligned}$$

συμπίπτει δηλαδή με την ιδιότητα 2 του λήμματος 3.4.1 όταν a_1, a_2 είναι ρητοί.

Επίσης πιο χρήσιμο είναι το εξής:
Αν $\frac{p_1}{q_1} = \frac{a}{c}$, $\frac{p_2}{q_2} = \frac{b}{c}$ με μκδ$(a, b, c) = 1, c > 0$, τότε:

$$\begin{aligned} h(\frac{a}{c} + \frac{b}{c}) &\leq \log \max\{|a+b|, c\} \\ &\leq \log 2 + \log \max\{|a|, |b|, c\}. \end{aligned}$$

(2) Εφαρμόζοντας το λήμμα 3.4.2 με $f(x_1,\ldots,x_n) = x_1 + \ldots, x_n$, έπεται η γενίκευση της σχέσης 2 του λήμματος 3.4.1,

$$h(\alpha_1 + \ldots + \alpha_n) \leq \log n + h(\alpha_1) + \ldots + h(\alpha_n).$$

Έστω K αλγεβρικό σώμα βαθμού n. Θυμίζουμε ότι το $s-$διάστατο προβολικό επίπεδο $\mathbb{P}_s(K)$ πάνω από ένα σώμα K αποτελείται από τις κλάσεις ισοδυναμίας των $(y_0,\ldots,y_s)$, όπου y_i όχι όλα μηδέν, όταν η σχέση ισοδυναμίας είναι η εξής:

$y_0 : \ldots : y_s = y_0^{'} : \ldots : y_s^{'}$ αν και μόνο αν

$$\exists\ a \in K \text{ τέτοιο ώστε } y_i^{'} = a \cdot y_i \text{ για κάθε } i = 0,\ldots,s.$$

(Αν $K^{'} \subset K$ τότε: $\mathbb{P}_s(K^{'}) \subseteq \mathbb{P}_s(K)$).

Έστω $\vartheta_0,\ldots,\vartheta_s$ και λ στοιχεία του K με $(\vartheta_0,\ldots,\vartheta_s) \neq (0,\ldots,0)$ και $\lambda \neq 0$. Τότε:

$$\begin{aligned}
&\frac{1}{n}\sum_{v\in M_K} d_v \log\max\{|\lambda\vartheta_0|_v,\ldots,|\lambda\vartheta_s|_v\}\\
=&\frac{1}{n}\sum_{v\in M_K} d_v \log|\lambda|_v \max\{|\vartheta_0|_v,\ldots,|\vartheta_s|_v\}\\
=&\frac{1}{n}\sum_{v\in M_K} d_v \log\max\{|\vartheta_0|_v,\ldots,|\vartheta_s|_v\} + \frac{1}{n}\sum_{v\in M_K} d_v \log|\lambda|_v^{d_v}\\
=&\frac{1}{n}\sum_{v\in M_K} d_v \log\max\{|\vartheta_0|_v,\ldots,|\vartheta_s|_v\} + \frac{1}{n}\log\prod_{v\in M_K}|\lambda|_v^{d_v}\\
(\text{Θεώρημα 3.3.1})\quad =&\frac{1}{n}\sum_{v\in M_K} d_v \log\max\{|\vartheta_0|_v,\ldots,|\vartheta_s|_v\} + \frac{1}{n}\log 1\\
=&\frac{1}{n}\sum_{v\in M_K} d_v \log\max\{|\vartheta_0|_v,\ldots,|\vartheta_s|_v\}.
\end{aligned}$$

Από την παραπάνω σχέση συμπεραίνουμε ότι ο αριθμός

$$\frac{1}{n}\sum_{v\in M_K} d_v \log\max\{|\vartheta_0|_v,\ldots,|\vartheta_s|_v\},$$

εξαρτάται μόνο από την κλάση $(\vartheta_0 : \ldots : \vartheta_s)$ του $(\vartheta_0,\ldots,\vartheta_s)$ στο προβολικό επίπεδο $\mathbb{P}_s(K)$. Τον παραπάνω αριθμό θα τον συμβολίζουμε με $h(\vartheta_0 : \ldots : \vartheta_s)$, δηλαδή

$$h(\vartheta_0 : \ldots : \vartheta_s) = \frac{1}{n}\sum_{v\in M_K} d_v \log\max\{|\vartheta_0|_v,\ldots,|\vartheta_s|_v\}.$$

Επίσης: $h(\alpha) = h(1:\alpha)$.

Λήμμα 3.4.3. *Έστω K ένα αριθμητικό σώμα και $s_1, \ldots, s_t$ θετικοί ρητοί ακέραιοι. Για $1 \leq i \leq t$, έστω $\gamma_{i1}, \ldots, \gamma_{is_i}$ στοιχεία του K. Συμβολίζουμε με $\underline{\gamma}$ το σημείο $(\gamma_{ij})_{\substack{1\leq i\leq t\\ 1\leq j\leq s_i}}$ στο $K^{s_1+\ldots+s_t}$. Επίσης έστω f ένα μη μηδενικό πολυώνυμο $s_1 + \ldots + s_t$ μεταβλητών, με συντελεστές από το $\mathbb{Z}$, συνολικού βαθμού το πολύ N_i ως προς τις s_i μεταβλητές, οι οποίες αντιστοιχούν στα $\gamma_{i1}, \ldots, \gamma_{is_i}$. Τότε*

$$h\big(f(\underline{\gamma})\big) \leq \log L(f) + \sum_{i=1}^{t} N_i h(1 : \gamma_{i1} : \ldots : \gamma_{is_i}).$$

Για $s_i = 1,\ \ i = 1, \ldots, t$ έχουμε το λήμμα 3.4.2.

Απόδειξη. Γράφουμε, $f = \sum_\lambda p_\lambda \prod_{i=1}^{t}\prod_{j=1}^{s_i} X_{ij}^{\lambda_{ij}}$, όπου $p_\lambda \in \mathbb{Z}$ και το $\lambda = (\lambda_{ij})$ τρέχει σε ένα πεπερασμένο υποσύνολο του $\mathbb{N}^{s_1+\ldots+s_t}$. Λόγω της υπόθεσης έχουμε ότι

$$\lambda_{i1} + \ldots + \lambda_{is_i} \leq N_i,\ \ N_i \in \mathbb{N}.$$

(βλ. επόμενη σελλίδα)

- Αν $\upsilon \in M_K^0$, τότε

$$\begin{aligned}
\log\max\{1, |f(\underline{\gamma})|_\upsilon\} &= \log\max\Big\{1, \Big|\sum_\lambda p_\lambda \prod_{i=1}^{t}\prod_{j=1}^{s_i} \gamma_{ij}^{\lambda_{ij}}\Big|_\upsilon\Big\} \\
&\leq \log\max\Big\{1, \max_\lambda\{\big|p_\lambda \prod_{i=1}^{t}\prod_{j=1}^{s_i} \gamma_{ij}^{\lambda_{ij}}\big|_\upsilon\}\Big\} \\
&= \log\max\Big\{1, \max_\lambda\{|p_\lambda|_\upsilon \Big|\prod_{i=1}^{t}\prod_{j=1}^{s_i} \gamma_{ij}^{\lambda_{ij}}\Big|_\upsilon\}\Big\} \\
(|p_\lambda|_{\upsilon_\wp} = p^{\frac{-1}{e_\wp}\nu_\wp(p_\lambda)} \leq 1,\ \text{αφού}\ p_\lambda \in \mathbb{Z}) &\leq \log\max\Big\{1, \max_\lambda\{\prod_{i=1}^{t}\prod_{j=1}^{s_i} \big|\gamma_{ij}^{\lambda_{ij}}\big|_\upsilon\}\Big\} \\
&= \log\max\Big\{1, \max_\lambda\{1, \prod_{i=1}^{t}\prod_{j=1}^{s_i} \big|\gamma_{ij}^{\lambda_{ij}}\big|_\upsilon\}\Big\} \\
&\leq \log\max\Big\{1, \prod_{i=1}^{t} \max_\lambda\{1, \prod_{j=1}^{s_i} \big|\gamma_{ij}^{\lambda_{ij}}\big|_\upsilon\}\Big\} \\
&\leq \sum_{i=1}^{t} \log\max\{1, \max\{1, \prod_{j=1}^{s_i} |\gamma_{ij}|_\upsilon^{\lambda_{ij}}\}\}.
\end{aligned}$$

Όμως,

$$\begin{aligned}\max_{\lambda}\{1, |\gamma_{i1}|_v^{\lambda_{i1}} \cdots |\gamma_{is_i}|_v^{\lambda_{is_i}}\} &\leq \max_{\lambda}\{1, |\gamma_{i1}|_v^{\lambda_{i1}}\} \cdots \max_{\lambda}\{|\gamma_{is_i}|_v^{\lambda_{is_i}}\} \\ &\leq \max_{\lambda}\{1, |\gamma_{i1}|_v\}^{\lambda_{i1}} \cdots \max_{\lambda}\{|\gamma_{is_i}|_v\}^{\lambda_{is_i}} \\ &\leq \max\{1, |\gamma_{i1}|_v, \ldots, |\gamma_{is_i}|_v\}^{\lambda_{i1}+\ldots+\lambda_{is_i}} \\ &\leq \max\{1, |\gamma_{i1}|_v, \ldots, |\gamma_{is_i}|_v\}^{N_i}.\end{aligned}$$

Άρα, για $v \in M_K^0$

$$\log \max\{1, |f(\underline{\gamma})|_v\} \leq \sum_{i=1}^{t} N_i \log \max\{1, |\gamma_{i1}|_v, \ldots, |\gamma_{is_i}|_v\}.$$

- Αν $v \in M_K^\infty$, τότε

$$\begin{aligned}\log \max\{1, |f(\underline{\gamma})|_v\} &= \log \max\big\{1, \big|\sum_{\lambda} p_\lambda \prod_{i=1}^{t}\prod_{j=1}^{s_i} \gamma_{ij}^{\lambda_{ij}}\big|_v\big\} \\ &\leq \log \max\big\{1, \sum_{\lambda} |p_\lambda|_v \prod_{i=1}^{t}\prod_{j=1}^{s_i} |\gamma_{ij}^{\lambda_{ij}}|_v\big\} \\ &\leq \log \max\Big\{1, \sum_{\lambda} |p_\lambda|_v \cdot \max_\lambda\big\{\prod_{i=1}^{t}\prod_{j=1}^{s_i} |\gamma_{ij}^{\lambda_{ij}}|_v\big\}\Big\} \\ (\textstyle\sum_{\lambda} |p_\lambda|_v \geq 1, \text{ διότι } p_\lambda \in \mathbb{Z}) \quad &\leq \log\Big(L(f) \cdot \max\Big\{1, \max_\lambda\big\{\prod_{i=1}^{t}\prod_{j=1}^{s_i} |\gamma_{ij}^{\lambda_{ij}}|_v\big\}\Big\}\Big) \\ &= \log L(f) + \log \max\Big\{1, \max_\lambda\big\{\prod_{i=1}^{t}\prod_{j=1}^{s_i} |\gamma_{ij}^{\lambda_{ij}}|_v\big\}\Big\}\Big) \\ &\leq \log L(f) + \sum_{i=1}^{t} N_i \log \max\{1, |\gamma_{i1}|_v, \ldots, |\gamma_{is_i}|_v\}.\end{aligned}$$

Οπότε, αφού

$$h\big(f(\underline{\gamma})\big) = \frac{1}{n} \sum_{v \in M_K} d_v \log \max\big\{1, \big|f(\underline{\gamma})\big|_v\big\},$$

$$h(1 : \gamma_{i1} : \ldots : \gamma_{is_i}) = \frac{1}{n} \sum_{v \in M_K} d_v \log \max\{1, |\gamma_{i1}|_v \ldots, |\gamma_{is_i}|_v\},$$

και

$$\sum_{\upsilon\in M_K^\infty} d_\upsilon = [K:\mathbb{Q}] = \sum_{\upsilon\in M_K^0} d_\upsilon,$$

έχουμε ότι

$$h\big(f(\underline{\gamma})\big) \le \log L(f) + \sum_{i=1}^{t} N_i h(1:\gamma_{i1}:\ldots:\gamma_{is_i}).$$

□

3.5 Ανισότητες του Liouville

Η πιο απλή ανισότητα από την οποία προκύπτουν και οι υπόλοιπες είναι: $|x| \ge 1$ για κάθε $x \in \mathbb{Z}\ \ x \neq 0$. Επίσης, για ένα ρητό αριθμό $\frac{p}{q}$ με p, q πρώτοι μεταξύ τους και $q > 0$ έχουμε $|\frac{p}{q}| \ge \frac{1}{q}$.

Με όρους του λογαριθμοκού ύψους Weil του $\frac{p}{q}$ (με μκδ$(p,q) = 1$ και $q > 0$) $h(\frac{p}{q}) = \log\max\{|p|, q\}$, η προηγούμενη ανισότητα παίρνει την μορφή

$$\log|x| \ge -h(x),$$

για κάθε $x \in \mathbb{Q}^*$.

Μια πολύ χρήσιμη ανισότητα είναι επίσης η εξής:

$$\Big|\log|\alpha|_\upsilon\Big| \le [\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha), \tag{3.9}$$

για κάθε μη μηδενικό αλγεβρικό αριθμό α και κάθε τα $\upsilon \in M_{\mathbb{Q}(\alpha)}$.

Πράγματι από την σχέση

$$h(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \sum_{\upsilon\in M_{\mathbb{Q}(\alpha)}} d_\upsilon \log\max\{1, |\alpha|_\upsilon\},$$

προκύπτει ότι

$$\log|\alpha|_\upsilon \le [\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha).$$

Από την απόδειξη της 3.4.1 είδαμε ότι

$$h(\alpha) = h(\frac{1}{\alpha}),\ \text{ για } \alpha \neq 0.$$

Άρα,

$$\log|\alpha|_\upsilon \ge -[\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha),\ \text{ για } \alpha \neq 0.$$

Οπότε,

$$\left|\log|\alpha|_v\right| \leq [\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha),$$

για κάθε $v \in M_{\mathbb{Q}(\alpha)}$.

Από το λήμμα 3.4.3 και λόγω της σχέσης 3.9 έχουμε ότι αν το $f(\underline{\gamma})$ δεν είναι μηδέν τότε

$$\log\left|f(\underline{\gamma})\right|_v \geq -n\log L(f) - n\sum_{i=1}^{t} N_i h(1:\gamma_{i1}:\ldots:\gamma_{is_i}),$$

για κάθε $v \in M_K$, όπου $n=[K:\mathbb{Q}]$.

Όταν $v \in M_K^\infty$, στην παραπάνω ανισότητα το $-n\log L(f)$ μπορεί ν' αντικατασταθεί από το $-(n-1)\log L(f)$. Πράγματι, έχουμε το εξής

Λήμμα 3.5.1. *(Ανισότητα Liouville) Έστω K αριθμητικό σώμα βαθμού n, $v \in M_K^\infty$ και $s_1,\ldots,s_t$ θετικοί ακέραιοι. Για κάθε $1\leq i\leq t$, έστω τα $\gamma_{i1},\ldots,\gamma_{is_i}$ στοιχεία του K. Έστω επίσης πολυώνυμο f, $s_1+\ldots+s_t$ μεταβλητών με συντελεστές στο $\mathbb{Z}$, το οποίο δεν μηδενίζεται στο $\underline{\gamma}=(\gamma_{ij})_{\substack{1\leq i\leq t\\ 1\leq j\leq s_i}}$. Υποθέτουμε ότι ο συνολικός βαθμός του f ως προς τις μεταβλητές που αντιστοιχούν στα $\gamma_{i1},\ldots,\gamma_{is_i}$ είναι το πολύ N_i. Τότε*

$$\log\left|f(\underline{\gamma})\right|_v \geq -(n-1)\log L(f) - n\sum_{i=1}^{t} N_i h(1:\gamma_{i1}:\ldots:\gamma_{is_i}).$$

Για $t=1$, $s_1=1$, η παραπάνω πρόταση διατυπώνεται ως εξής:

Για πολυώνυμο $f\in\mathbb{Z}[x]$ βαθμού $\leq N$ και για έναν αλγεβρικό αριθμό $\alpha\in\mathbb{C}$ βαθμού n ο οποίος δεν είναι ρίζα του f, έχουμε

$$|f(\alpha)| \geq L(f)^{1-n}\cdot \mathrm{e}^{-n\cdot N\cdot h(\alpha)}.$$

(Εδώ με $|\cdot|$ συμβολίζουμε την επέκταση της αρχιμήδειας απόλυτης τιμής του $\mathbb{Q}$ στο $\mathbb{Q}(\alpha)\subseteq\mathbb{C}$).

Απόδειξη. Έστω $v\in M_K^\infty$. Από την υπόθεση έχουμε ότι: $f(\underline{\gamma})\neq 0$. Οπότε, από τον τύπο του γινομένου έχουμε ότι

$$d_v \log\left|f(\underline{\gamma})\right|_v = -\sum_{\omega\neq v} d_\omega \log\left|f(\underline{\gamma})\right|_\omega.$$

Αν $\omega\in M_K^\infty$, τότε από το λήμμα 3.4.3

$$\log\left|f(\underline{\gamma})\right|_\omega \leq \sum_{i=1}^{t} N_i \log\max\{1,|\gamma_{i1}|_\omega,\ldots,|\gamma_{is_i}|_\omega\} + \log L(f).$$

Επίσης,

$$\sum_{\substack{\omega\in M_K^\infty\\ \omega\neq v}} d_\omega = n - d_v \leq n-1$$

Αν $w \in M_K^0$, τότε επίσης από το λήμμα 3.4.3

$$\log\left|f(\underline{\gamma})\right|_w \leq \sum_{i=1}^{t} N_i \log\max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\}$$

Οπότε,

$$\begin{aligned}
d_v \log\left|f(\underline{\gamma})\right|_v &= -\sum_{w\neq v} d_w \log\left|f(\underline{\gamma})\right|_w \\
&= -\sum_{w\in M_K^0} d_w \log\left|f(\underline{w})\right|_w - \sum_{\substack{w\in M_K^\infty\\ w\neq v}} d_w \log\left|f(\underline{\gamma})\right|_w \\
&\geq -\sum_{w\in M_K^0} \Big(d_w \sum_{i=1}^{t} N_i \log\max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\}\Big) \\
&\quad -\sum_{\substack{w\in M_K^\infty\\ \omega\neq v}} \Big(d_w \sum_{i=1}^{t} N_i \log\max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\} + d_w \log L(f)\Big) \\
&= -\sum_{\substack{w\in M_K\\ w\neq v}} d_w \sum_{i=1}^{t} N_i \log\max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\} - \sum_{\substack{w\in M_K^\infty\\ w\neq v}} d_w \log L(f) \\
&\geq -\sum_{\substack{w\in M_K\\ w\neq v}} d_w \sum_{i=1}^{t} N_i \log\max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\} - (n-1)\log L(f) \\
&\geq -\sum_{w\in M_K} d_w \sum_{i=1}^{t} N_i \log\max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\} - (n-1)\log L(f) \\
&= -(n-1)\log L(f) - n\sum_{i=1}^{t} N_i \frac{1}{n} \sum_{w\in M_K} d_w \log\max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\} \\
&= -(n-1)\log L(f) - n\sum_{i=1}^{t} N_i h(1 : \gamma_{i1} : \ldots : \gamma_{is_i}).
\end{aligned}$$

Οπότε, έχουμε

$$d_v \log \left|f(\underline{\gamma})\right|_v \geq -(n-1)\log L(f) - n\sum_{i=1}^{t} N_i h(1:\gamma_{i1}:\ldots:\gamma_{is_i}).$$

Γνωρίζουμε όμως ότι αφού $v \in M_K^\infty$ τότε $d_v = 1$ ή 2.

Επειδή $-(n-1)\log L(f) - n\sum_{i=1}^{t} N_i h(1:\gamma_{i1}:\ldots:\gamma_{is_i}) < 0$ έχουμε σε κάθε περίπτωση, $(\log \left|f(\underline{\gamma})\right|_v > 0$ ή $\log \left|f(\underline{\gamma})\right|_v < 0)$, ότι

$$\log \left|f(\underline{\gamma})\right|_v \geq -(n-1)\log L(f) - n\sum_{i=1}^{t} N_i h(1:\gamma_{i1}:\ldots:\gamma_{is_i}).$$

□

Ένα επίσης πολύ σημαντικό κάτω φράγμα, το οποίο είναι συνέπεια των προηγούμενων, είναι το εξής

Θεώρημα 3.5.2. *(Θεώρημα του Liouville)*

Για κάθε $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ βαθμού $n > 1$ υπάρχει $c = c(\alpha)$ τέτοιο ώστε:

$$\left|\alpha - \frac{p}{q}\right|_v \geq \frac{c}{\max\{|p|, q\}^n},$$

να ισχύει για κάθε $\frac{p}{q} \in \mathbb{Q}$ με $q > 0$, όπου $v \in M_{\mathbb{Q}(K)}$ και K ένα αριθμητικό σώμα το οποίο περιέχει το α.

Απόδειξη. Αν $v \in M_K^\infty$ το θεώρημα προκύπτει από το λήμμα 3.5.1 με $f(x) = qx - p$. Εν τούτοις παρακάτω δίνουμε μια απόδειξη που ισχύει για κάθε $v \in M_K$.

Από την σχέση 3.9 έχουμε ότι:

$$\begin{aligned}
\log \left|\alpha - \frac{p}{q}\right|_v &\geq -[\mathbb{Q}(\alpha - \tfrac{p}{q}) : \mathbb{Q}] \cdot h(\alpha - \tfrac{p}{q}) \\
&= -[\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot h(\alpha - \tfrac{p}{q}) \\
&\geq -n\big(h(\alpha) + h\big(\tfrac{p}{q}\big) + \log 2\big).
\end{aligned}$$

Γνωρίζουμε όμως ότι: $h\big(\frac{p}{q}\big) = \log \max\{|p|, q\}$.

Άρα:

$$\begin{aligned}
\left|\alpha - \frac{p}{q}\right|_v &\geq \frac{1}{\mathrm{e}^{n\cdot h(\alpha)} \cdot \max\{|p|, q\}^n \cdot 2^n} \\
&= \frac{c(\alpha)}{\max\{|p|, q\}^n},
\end{aligned}$$

όπου $c(\alpha) = \frac{1}{\mathrm{e}^{n\cdot h(\alpha)} . 2^n}$.

□

3.6 Κάτω φράγμα για την ορίζουσα

Για $S \in \mathbb{R}^+$, $\mathbb{Z}^{n+1}(S)$ συμβολίζει (όπως έχουμε ήδη αναφέρει) το σύνολο των $\underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}$ με $|s_j| < S$ για $j = 1, \ldots, n+1$.

Έστω τώρα $S_1, \ldots, S_{n+1} \in \mathbb{R}^+$. Θέτουμε $\underline{S} = (S_1, \ldots, S_{n+1})$ και συμβολίζουμε $\mathbb{Z}^{n+1}(\underline{S})$ το σύνολο των $\underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}$ με $|s_i| < S_i$, $1 \leq i \leq n+1$.

Πρόταση 3.6.1. *Έστω $\alpha_1, \ldots, \alpha_{n+1} \in \overline{\mathbb{Q}}^*$, $\beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ και*

$D := [\mathbb{Q}(\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_n) : \mathbb{Q}]$. *Έστω επίσης, $L_0, L_1, S_1, \ldots, S_{n+1} \in \mathbb{Z}^+$. Ορίζουμε:*

$$L := \binom{L_0 + n}{n} \cdot (L_1 + 1)$$

και

$$S := \max\{S_1, \ldots, S_{n+1}\}.$$

Έστω $s^{(1)}, \ldots, s^{(L)}$, οποιαδήποτε στοιχεία του $\mathbb{Z}^{n+1}(\underline{S})$ και

$$\Delta = \det\Big((s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1)^{\lambda_1} \ldots (s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n)^{\lambda_n} (\alpha_1^{s_1^{(\mu)}} \ldots \alpha_{n+1}^{s_{n+1}^{(\mu)}})^{\lambda_{n+1}}\Big)_{\underline{\lambda},\mu},$$

με $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$, $\lambda_1 + \ldots + \lambda_n \leq L_0$, $\lambda_{n+1} \leq L_1$ και $1 \leq \mu \leq L$.

Τότε, είτε

$$\Delta = 0$$

είτε

$$\frac{1}{L}\log|\Delta| \geq -(D-1)(L_0 \log 2S + \log L) - DL_1 \sum_{i=1}^{n+1} S_i h(\alpha_i) - DL_0 h(1 : \beta_1 : \ldots : \beta_n). \tag{3.10}$$

Απόδειξη.

Ορίζουμε το πολυώνυμο $P \in \mathbb{Z}[X_1 \ldots, X_{n+1}, Y_1, \ldots, Y_{n+1}, Z_1, \ldots, Z_n]$, ως εξής:

$$P(\underline{X}, \underline{Y}, \underline{Z}) = \det\Big(P_{\underline{\lambda},\mu}(\underline{X}, \underline{Y}, \underline{Z})\Big)_{\underline{\lambda},\mu},$$

όπου

$$P_{\underline{\lambda},\mu}(\underline{X}, \underline{Y}, \underline{Z}) = \prod_{j=1}^{n}(s_j^{(\mu)} + s_{n+1}^{(\mu)} Z_j)^{\lambda_j} \prod_{i=1}^{n} \big(X_i^{\max\{s_i^{(\mu)}, 0\}} Y_i^{\max\{-s_i^{(\mu)}, 0\}}\big)^{\lambda_{n+1}}.$$

Έχουμε λοιπόν ότι:

$$\Delta = P(\alpha_1, \ldots, \alpha_{n+1}, \alpha_1^{-1}, \ldots, \alpha_{n+1}^{-1}, \beta_1, \ldots, \beta_n).$$

Για κάθε $i, \underline{\lambda}, \mu$ για το πολυώνυμο $P_{\underline{\lambda},\mu}$ ισχύουν τα εξής:

- $\deg_{X_i} \leq \lambda_{n+1} \cdot \max\{s_i^{(\mu)}, 0\}$
- $\deg_{Y_i} \leq \lambda_{n+1} \cdot \max\{-s_i^{(\mu)}, 0\}$

  και
- $\deg_{\underline{Z}}$ [3] $\leq L_0$.

Επίσης:

$$L(P_{\underline{\lambda},\mu}) \leq \prod_{j=1}^{n} \left(|s_j^{(\mu)}| + |s_{n+1}^{(\mu)}|\right)^{\lambda_j} \leq \prod_{j=1}^{n} \left(S+S\right)^{\lambda_j} \leq (2S)^{\lambda_1+\ldots+\lambda_n} \leq (2S)^{L_0}.$$

Από τον ορισμό της ορίζουσας έχουμε ότι:

$$P = \sum_{\sigma \in \mathbb{S}_L} \operatorname{sgn}(\sigma) \cdot \prod_{\mu=1}^{L} P_{\sigma(\mu),\mu}$$ [4].

Ο βαθμός της μεταβλητής X_i, (καθώς και της Y_i), του πολυωνύμου P είναι:

$$\begin{aligned}
\max\{s_i^{\mu}, 0\} \cdot \sum_{\underline{\lambda}} \lambda_{n+1} \leq S_i \sum_{\underline{\lambda}} \lambda_{n+1} &= S_i\Big(\binom{L_0+n}{n} \cdot 0 + \ldots + \binom{L_0+n}{n} \cdot L_1\Big) \\
&= S_i \binom{L_0+n}{n} \big(1+2+\ldots+L_1\big) \\
&= S_i \binom{L_0+n}{n} \frac{1+L_1}{2} L_1 = \frac{1}{2} L L_1 S_i.
\end{aligned}$$

Ο συνολικός βαθμός των μεταβλητών $Z_1, \ldots, Z_n$ του πολυωνύμου P είναι:

$$L\lambda_1 + L\lambda_2 + \ldots + L\lambda_n = L(\lambda_1 + \ldots + \lambda_n) \leq LL_0.$$

Επίσης:

$$\begin{aligned}
L(P) &\leq \Big| \prod_{\mu=1}^{L} L(P_{\sigma_1(\mu),\mu}) \Big| + \ldots + \Big| \prod_{\mu=1}^{L} L(P_{\sigma_{L!}(\mu),\mu}) \Big| \\
&\leq L! \prod_{\mu=1}^{L} (2S)^{L_0} = L!(2S)^{LL_0}.
\end{aligned}$$

Θα εφαρμόσουμε το λήμμα 3.5.1, όπου:

[3] Δηλαδή συνολικού βαθμού στα $Z_1, \ldots, Z_n$

[4] Συγκεκριμένα το σ είναι από το $\{1, \ldots, L\}$ 1-1 και επί στο σύνολο των $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$ το οποίο έχει πλήθος ίσο με $\binom{L_0+n}{n} \cdot (L_1+1)$

- $t = 2n + 3$,
- $s_1 = \ldots = s_{2n+2} = 1, \;\; s_{2n+3} = n$,
- $\gamma_{i1} = \alpha_i$ για $i = 1, \ldots, n+1$, $\gamma_{i1} = \alpha_{i-n-1}^{-1}$ για $i = n+2, \ldots, 2n+2$ και $\gamma_{2n+3,j} = \beta_j$ για $j = 1, \ldots, n$,
- $N_i = N_{n+i+1} = \frac{LL_1S_i}{2}$, $i = 1, \ldots, n+1$, $N_{2n+3} = LL_0$

και για αρχιμήδεια απόλυτη τιμή v θα πάρουμε την αρχιμήδεια απόλυτη τιμή $|\cdot|$ του $\mathbb{C}$.

Άρα:

$$\begin{aligned}
\log|\Delta| &= \log\left|P(\alpha_1, \ldots, \alpha_{n+1}, \alpha_1^{-1}, \ldots, \alpha_{n+1}^{-1}, \beta_1, \ldots, \beta_n)\right| \\
&\geq -(D-1)\log L(P) - \\
&\quad - D\sum_{i=1}^{2n+3} N_i h(1 : \alpha_1 : \ldots : \alpha_{n+1} : \alpha_1^{-1} : \ldots : \alpha_{n+1}^{-1} : \beta_1 : \ldots : \beta_n) \\
&= -(D-1)\log\left[L!(2S)^{LL_0}\right] - \\
&\quad - D\sum_{i=1}^{2n+3} N_i h(1 : \alpha_1 : \ldots : \alpha_{n+1} : \alpha_1^{-1} : \ldots : \alpha_{n+1}^{-1} : \beta_1 : \ldots : \beta_n) \\
&\geq -(D-1)(L\log L + LL_0\log 2S) - \\
&\quad - D\sum_{i=1}^{2n+3} N_i h(1 : \alpha_1 : \ldots : \alpha_{n+1} : \alpha_1^{-1} : \ldots : \alpha_{n+1}^{-1} : \beta_1 : \ldots : \beta_n).
\end{aligned}$$

Λόγω του λήμματος Α΄.5.1,

$$\begin{aligned}
& h(1 : \alpha_1 : \ldots : \alpha_{n+1} : \alpha_1^{-1} : \ldots : \alpha_{n+1}^{-1} : \beta_1 : \ldots : \beta_n) \\
& \leq h(\alpha_1) + \ldots + h(\alpha_n) + h(\alpha_1^{-1}) + \ldots + h(\alpha_n^{-n}) + h(\beta_1 : \ldots : \beta_n) \\
(h(\alpha) = h(\alpha^{-1})) \quad & = 2h(\alpha_1) + \ldots + 2h(\alpha_n) + h(\beta_1 : \ldots : \beta_n),
\end{aligned}$$

έχουμε ότι

$$\begin{aligned}
\log|\Delta| &\geq -(D-1)(L\log L + LL_0\log S) - 2D\sum_{i=1}^{n+1} N_i h(\alpha_i) - DN_{2n+3}h(1 : \beta_1 : \ldots : \beta_n) \\
&\geq -(D-1)\cdot L(\log L + L_0\log S) - 2D\frac{LL_1}{2}\sum_{i=1}^{n+1} S_i h(\alpha_i) - DLL_0 h(1 : \beta_1 : \ldots : \beta_n),
\end{aligned}$$

δηλαδή,

$$\frac{1}{L}\log|\Delta| \geq -(D-1)(L_0\log 2S+\log L)-DL_1\sum_{i=1}^{n+1}S_i h(\alpha_i)-DL_0 h(1:\beta_1:\ldots:\beta_n).$$

□

Από την πρόταση 3.6.1 έπεται το ακόλουθο

Πόρισμα 3.6.2. *Με τις ίδιες υποθέσεις της πρότασης 3.6.1, αν $\Delta \neq 0$, τότε η ανισότητα 3.10 μπορεί να πάρει την εξής μορφή*

$$\frac{1}{L}\log|\Delta| \geq -c_2(L_0\log S + L_1 S),$$

όπου $c_2 := c_2(n, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ θετική σταθερά.

Απόδειξη. Πράγματι, λόγω ορισμού του L, έχουμε ότι

$$L \leq L_0^n(n+1)(L_1+1)$$

άρα, $\log L \leq c'(L_0+L_1)$, όπου c' θετική σταθερά η οποία εξαρτάται από το n. Επίσης,

$$\begin{aligned} &S_i \leq S \\ &D \leq c'' \\ &h(\alpha_i),\, h(1:\beta_1:\ldots:\beta_n) \leq c''', \end{aligned}$$

όπου c'', c''' θετικές σταθερές οι οποίες εξαρτώνται από τα $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$. Οπότε, προκύπτει η ανισότητα

$$\frac{1}{L}\log|\Delta| \geq -c_2(L_0\log S + L_1 S),$$

όπου το c_2 είναι θετική σταθερα και εξαρτάται από τα $n, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$.

□

3.7 Κάτω φράγμα για το ύψος

Είναι γνωστό από την Αλγεβρική Θεωρία Αριθμών, (πρβλ. [26], [32]) ότι ένας αλγεβρικός ακέραιος του οποίου όλοι οι συζυγείς έχουν μέτρο ≤ 1 είναι ρίζα της μονάδας. Η γενίκευση αυτού, η οποία οφείλεται στον Kronecker, είναι η εξής:

Αν ένας μη μηδενικός αλγεβρικός αριθμός $\alpha \in K$, K αριθμητικό σώμα, ικανοποιεί $|\alpha|_v \leq 1$, για όλα τα $v \in M_K$, τότε ο α είναι ρίζα της μονάδας.

Από αυτό λοιπόν συμπεραίνουμε ότι οι μόνοι αλγεβρικοί αριθμοί α οι οποίοι ικανοποιούν την σχέση: $h(\alpha) = 0$, είναι το 0 και οι ρίζες της μονάδας [5]. Όλοι οι υπόλοιποι αλγεβρικοί αριθμοί ικανοποιούν την σχέση: $h(\alpha) > 0$. Ενδιαφέρον αλλά συγχρόνως δύσκολο πρόβλημα, είναι η εύρεση ενός *καλού* κάτω φράγματος (όταν $h(\alpha) > 0$) το οποίο θα εξαρτάται μόνο από το βαθμό του του αλγεβρικού αριθμού α.

Αν για ένα μη μηδενικό αλγεβρικό αριθμό α, ισχύει ότι $M(\alpha) < 2$ (πρβλ. παράγραφο Α΄.4) τότε ο α είναι αλγεβρικός ακέραιος (από τον ορισμό προκύπτει ότι $M(\alpha) \geq 1$). Ομοίως και ο α^{-1}. Οπότε ο α είναι μονάδα. Με άλλα λόγια, το (απόλυτο λογαριθμικό) ύψος ενός αλγεβρικού αριθμού, ο οποίος δεν είναι μονάδα είναι το λιγότερο $\log 2/d$.

Το πρόβλημα είναι λοιπόν, η εύρεση κάτω φράγματος για το ύψος αλγεβρικών αριθμών, οι οποίοι είναι μονάδες, αλλά όχι ρίζες της μονάδας.

Σημειώνουμε ότι λόγω της σχέσης, $h(\alpha) = \frac{1}{d}\log M(\alpha)$, (πρβλ. λήμμα Α΄.4.2), οι συνθήκες $h(\alpha) > 0$ και $M(\alpha) > 1$ είναι ισοδύναμες. Άρα, λόγω των παραπάνω, προκύπτει ότι για α αλγεβρικό ακέραιο, $M(\alpha) = 1$, αν και μόνο αν, ο α είναι μηδέν ή ρίζα της μονάδας [6].

Το πρόβλημα είναι λοιπόν, η εύρεση κάτω φράγματος για το ύψος αλγεβρικών αριθμών, οι οποίοι είναι μονάδες, αλλά όχι ρίζες της μονάδας.

Αποδεικνύεται ότι για κάθε θετικό ακέραιο n υπάρχει θετική σταθερά $c(n)$, τέτοια ώστε, για κάθε αλγεβρικό αριθμό α, ο οποίος δεν είναι ρίζα της μονάδας και είναι βαθμού $\leq n$, να ισχύει η ανισότητα: $h(\alpha) > c(n)$. Για παράδειγμα, αν $\alpha = 2^{1/n}$, τότε θα πρέπει $c(n) \leq \log 2/n$. Ο Lehmer διατύπωσε το εξής πρόβλημα (πρόβλημα Lehmer): *υπάρχει θετική σταθερά c_0, τέτοια ώστε $c(n) = c_0/n$;*

Το πρώτο αποτέλεσμα προς αυτή την κατεύθυνση ήρθε το 1965, όταν οι Schinzel και Zassenhauss [23], απέδειξαν το εξής:

Για κάθε μη μηδενικό αλγεβρικό αριθμό α βαθμού $n \geq 2$, ο οποίος δεν είναι ρίζα της μονάδας, ισχύει ότι: $h(\alpha) > \frac{c}{2^n}$, για κάποια θετική σταθερά c.

Το 1971, οι Blanksby και Montgomery [9], βελτίωσαν το προηγούμενο αποτέλεσμα και απέδειξαν ότι: $h(\alpha) > \frac{1}{52n^2\log(6n)}$. Το 1978, ο Stewart [25], παρουσίασε μια μέθοδο της υπερβατικής θεωρίας αριθμών και απέδειξε: $h(\alpha) > \frac{1}{10^4 n^2 \log n}$. Το αποτέλεσμα αυτό είναι προφανώς ασθενέστερο από το προηγούμενο, αλλά η μέθοδος που χρησιμοποιήθηκε είναι πολύ σημαντική. Το 1979, ο Dobrowolski [13], επεκτείνοντας την μέθοδο του Stewart απέδειξε το εξής:

---

[5] Αφού: $h(\alpha) = \frac{1}{n}\sum_{v\in M_K} d_v \log\max\{1, |\alpha|_v\}$, όπου $n = [K : \mathbb{Q}]$.

[6] Η υπόθεση εδώ για τον α, δηλαδή ότι είναι ακέραιος αλγεβρικός αριθμός, δεν μπορεί να παραληφθεί. Αντιπαράδειγμα αποτελεί ο αριθμός $\frac{3+4i}{5}$

Για κάθε $\epsilon > 0$ υπάρχει ένας ακέραιος $n_0(\epsilon)$, (ο οποίος είναι υπολογίσιμος), τέτοιος ώστε: για κάθε $n > n_0(\epsilon)$ και κάθε αλγεβρικό αριθμό α βαθμού n, ο οποίος δεν είναι ρίζα της μονάδας, ισχύει ότι

$$h(\alpha) > \frac{1-\epsilon}{n} \cdot \Big(\frac{\log\log n}{\log n}\Big)^3.$$

Ακολούθησαν ύστερα και κάποιες βελτιώσεις αυτού του αποτελέσματος, όπου το $1-\epsilon$ αντικαταστάθηκε από το $\frac{9}{4}-\epsilon$.

Σε αυτή την παράγραφο θα δώσουμε ένα φράγμα για το ύψος ακολουθώντας την υπερβατική μέθοδο του Stewart. Το απότέλεσμα αυτό θα το χρειαστούμε στο κεφάλαιο 7.

Θεώρημα 3.7.1. *Έστω α ένας μη μηδενικός αλγεβρικός αριθμός βαθμού $n \geq 2$. Υποθέτουμε ότι:*

$$h(\alpha) \leq \frac{1}{2200n^2\log n}.$$

Τότε ο α είναι ρίζα της μονάδας.

Από το θεώρημα 3.7.1 έπεται το εξής:

Αν α είναι ένας μη μηδενικός αλγεβρικός αριθμός, ο οποίος δεν είναι ρίζα της μονάδας, τότε:

$$h(\alpha) > \frac{1}{10^3 n^3}.$$

Η απόδειξη του θεωρήματος 3.7.1 χωρίζεται σε δύο μέρη, το υπερβατικό επιχείρημα και την επιλογή των παραμέτρων. Για το πρώτο μέρος χρειαζόμαστε το εξής

Λήμμα 3.7.2. *Έστω $\alpha \in \mathbb{C}$ ένας αλγεβρικός αριθμός βαθμού n με $|\alpha| \geq 1$. Αν υπάρχουν αριθμοί L, A, C, με L άρτιο θετικό ακέραιο, $A \geq 2$ ακέραιο και $C > 1$ πραγματικό, τέτοιοι ώστε:*

1. $\big(\frac{\pi}{A}\big)^2 + \big(AL\log|\alpha|\big)^2 \leq \frac{1}{C^2}$ *και*
2. $\Big(1-\frac{1}{L}\Big)\log C > 1 + \frac{2n}{L}\log L + \frac{n}{2}ALh(\alpha)$.

Τότε ο α είναι ρίζα της μονάδας.

Απόδειξη. Θα συμβολίζουμε με Log την πρωτεύουσα ή κύρια τιμή του λογαρίθμου. Δηλαδή για $z \in \mathbb{C}\setminus\{0\}$ έχουμε ότι: $\mathrm{Log}z = \log|z| + \imath\Theta$, όπου $-\pi < \Theta \leq \pi$.

Έστω οι αριθμοί L, A, C, L άρτιος θετικός ακέραιος, $A \geq 2$ ακέραιος και $C > 1$ πραγματικός, οι οποίοι ικανοποιούν τις υποθέσεις 1 και 2 του θεωρήματος.

Θεωρούμε τους AL αριθμούς, (όχι απαραίτητα διαφορετικούς),

$$\mathrm{Im}\,\mathrm{Log}\alpha^s,\ \ (0 \le s < AL),$$

οι οποίοι είναι στο διάστημα $(-\pi, \pi]$. Έστω

$$(-\pi, \pi] = \bigcup_{j=0}^{A-1} I_j,$$

όπου $I_j = (-\pi + \frac{2\pi j}{A}, -\pi + \frac{2\pi(j+1)}{A}]$, $0 \le j \le A-1$. Από την Αρχή του Περιστερώνα συμπεραίνουμε ότι κάποιο j με $0 \le j \le A-1$ τέτοιο ώστε το I_j περιέχει τουλάχιστον L από τους AL αριθμούς $\mathrm{Im}\,\mathrm{Log}\alpha^s$. Για αυτό λοιπόν το I_j έστω $\vartheta = -\pi + \frac{\pi(2j+1)}{A}$, το κέντρο του. Τότε υπάρχουν L ρητοί ακέραιοι s_λ, $1 \le \lambda \le L$, με $0 \le s_1 < s_2 < \ldots < s_L < AL$, τέτοιοι ώστε

$$\left|\mathrm{Im}\,\mathrm{Log}(\alpha^{s_\lambda}) - \vartheta\right| \le \frac{\pi}{A},\ \ 1 \le \lambda \le L.$$

Από την υπόθεση 1 και από την εκτίμηση

$$0 \le \log|\alpha^{s_\lambda}| < AL\log|\alpha|\ \ ^{7},$$

έχουμε ότι

$$\begin{aligned}\left|\mathrm{Log}(\alpha^{s_\lambda}) - i\vartheta\right| &= \left|\log|\alpha|^{s_\lambda} + i(\mathrm{Im}\,\mathrm{Log}(\alpha^{s_\lambda}) - \vartheta)\right| \\ &\le \log|\alpha^{s_\lambda}| + |\mathrm{Im}\,\mathrm{Log}(\alpha^{s_\lambda}) - \vartheta| \\ &< AL\log|\alpha| + \frac{\pi}{A} < \frac{1}{C},\ \ 1 \le \lambda \le L.\end{aligned}$$

Θεωρούμε την $L \times L$ ορίζουσα

$$\begin{aligned}\Delta &= \det\left(\alpha^{s_\lambda l}\right)_{1\le\lambda\le L,\ -\frac{L}{2}<l\le\frac{L}{2}} \\ &= \det\begin{pmatrix} \alpha^{s_1(\frac{-L}{2}+1)} & \alpha^{s_1(\frac{-L}{2}+2)} & \ldots & \alpha^{s_1\frac{L}{2}} \\ \alpha^{s_2(\frac{-L}{2}+1)} & \alpha^{s_2(\frac{-L}{2}+2)} & \ldots & \alpha^{s_2\frac{L}{2}} \\ \vdots & & \ddots & \vdots \\ \alpha^{s_L(\frac{-L}{2}+1)} & \alpha^{s_L(\frac{-L}{2}+2)} & \ldots & \alpha^{s_L\frac{L}{2}} \end{pmatrix}.\end{aligned}$$

[7] Από υπόθεση $|\alpha| \ge 1$, άρα $\log|\alpha^{s_\lambda}| = \log|\alpha|^{s_\lambda} \ge 0$

Αν πολλαπλασιάσουμε την πρώτη γραμμή με $\alpha^{s_1(\frac{L-2}{2})}$, την δεύτερη γραμμή με $\alpha^{s_2(\frac{L-2}{2})}$ και συνεχίζοντας όμοια την L γραμμή με $\alpha^{s_L(\frac{L-2}{2})}$, θα έχουμε την ορίζουσα Vandermonde

$$\det\begin{pmatrix} 1 & \alpha^{s_1} & \dots & (\alpha^{s_1})^L \\ 1 & \alpha^{s_2} & \dots & (\alpha^{s_2})^L \\ \vdots & & \ddots & \ddots \\ 1 & \alpha^{s_L} & \dots & (\alpha^{s_L})^L \end{pmatrix} = \prod_{1\le\lambda<\mu\le L}(\alpha^{s_\mu}-\alpha^{s_\lambda}).$$

Δηλαδή,

$$\Delta\cdot\prod_{\lambda=1}^{L}\alpha^{s_\lambda\frac{L-2}{2}} = \prod_{1\le\lambda<\mu\le L}(\alpha^{s_\mu}-\alpha^{s_\lambda}).$$

Αν για $s_\lambda \neq s_\mu$ έχουμε $\alpha^{s_\lambda}=\alpha^{s_\mu}$ τότε (έστω $s_\lambda > s_\mu$) $\alpha^{s_\lambda - s_\mu}=1$, δηλαδή ο α είναι ρίζα της μονάδας. Άρα αν ο α δεν είναι ρίζα της μονάδας τότε $\Delta\neq 0$.

Από την άλλη, όμως, μπορούμε να γράψουμε την Δ, ως εξής:

$$\Delta = f(\alpha,\alpha^{-1}),$$

όπου:

$f\in\mathbb{Z}[X,Y]$ με $f(X,Y)=\sum_{\sigma\in\mathbb{S}_L}\operatorname{sgn}(\sigma)\prod_{\frac{-L}{2}<l\le\frac{L}{2}}X^{\sigma(l)\max\{l,\,0\}}Y^{\sigma(l)\max\{-l,\,0\}}$ [8].

Επίσης το μήκος του f, $L(f)$, είναι το πολύ ίσο με $\sum_\sigma 1 = L!$.

Ο βαθμός του f που αντιστοιχεί:

- στην μεταβλητη X είναι το πολύ ίσος με

$$\sum_l \sigma(l)\max\{l,\,0\} < AL\sum_{l=0}^{\frac{l}{2}} l = \frac{1}{8}AL^2(L+2),$$

- στην μεταβλητη Y είναι το πολύ ίσος με

$$\sum_l \sigma(l)\max\{-l,\,0\} < AL\sum_{l=0}^{\frac{l}{2}-1} l = \frac{1}{8}AL^2(L-2).$$

[8] Συγκεκριμένα το σ είναι μια 1-1 και επί απεικόνιση από το $\{(\frac{-L}{2}+1),\dots,\frac{L}{2}\}$ στο $\{s_1,\dots,s_L\}$ και $\operatorname{sgn}(\sigma)$ είναι το πρόσιμο της μετάθεσης σ

Από το λήμμα 3.5.1 για το πολυώνυμο f όπου εδώ $\underline{\gamma} = (\alpha, \alpha^{-1})$ και $K = \mathbb{Q}(\alpha)$, έχουμε ότι όταν $\Delta = f(\alpha, \alpha^{-1}) \neq 0$, δηλαδή όταν ο α δεν είναι ρίζα της μονάδας,

$$\frac{1}{L}\log|\Delta| > -(n-1)\log L - \frac{n}{4}AL^2h(\alpha).$$

Θα προσπαθήσουμε τώρα να βρούμε ένα άνω φράγμα της ορίζουσας Δ. Θα εφαρμόσουμε το θεώρημα 2.2.3 με τις εξής υποθέσεις,

$$f_\lambda(z) = \mathrm{e}^{z(\mathrm{Log}\alpha^{s_\lambda} - i\vartheta)}, \ \ (1 \leq \lambda \leq L),$$

$$\zeta_l = l, \ \ (\frac{-L}{2} < l \leq \frac{L}{2}), \ \ r = \frac{L}{2}, \ \ R = C\frac{L}{2}.$$

Αφού $|\mathrm{e}^{li\vartheta}| = 1$, ισχύει ότι

$$|\Delta| = \Big|\det\big(f_\lambda(\zeta_\lambda)\big)_{1\leq\lambda\leq L,\ \frac{-L}{2}<l\leq\frac{L}{2}}\Big|.$$

Λόγω της σχέσης $\big|\mathrm{Log}(\alpha^{s_\lambda}) - i\vartheta\big| < \frac{1}{C}, \ \ (1 \leq \lambda \leq L)$, έχουμε ότι

$$\log|f_\lambda|_R < \frac{R}{C} = \frac{L}{2}.$$

Οπότε με εφαρμογή του θεωρήματος 2.2.3, έπεται ότι

$$|\Delta| \leq \Big(\frac{R}{r}\Big)^{-L\cdot\frac{L-1}{2}} \cdot L! \cdot \prod_{\lambda=1}^{L} |f_\lambda|_R,$$

άρα,

$$\frac{1}{L}\log|\Delta| \leq -\frac{L-1}{2}\log C + \log L + \frac{L}{2}.$$

Συγκρίνοντας τα δύο φράγματα της Δ, το άνω και το κάτω, συμπεραίνουμε εύκολα ότι

$$\frac{n}{4}AL^2h(\alpha) + n\log L + \frac{L}{2} > \frac{L-1}{2}\log C,$$

το οποίο έρχεται σε αντίθεση με την υπόθεση 2. Οπότε ο α, είναι ρίζα της μονάδας.

□

Απόδειξη του θεωρήματος 3.7.1. Το μόνο που μένει για την απόδειξη του θεωρήματος 3.7.1 είναι η κατάλληλη επιλογή των παραμέτρων A, L, C του θεωρήματος 3.7.2.

Έστω $\alpha \in \mathbb{C}$ ένας μη μηδενικός αλγεβρικός αριθμός βαθμού n ο οποίος ικανοποιεί την ανισότητα,

$$h(\alpha) \leq \frac{1}{2200n^2\log n}.$$

Θέλουμε να αποδείξουμε ότι ο α είναι ρίζα της μονάδας. Η περίπτωση $n = 2$ έπεται από το πόρισμα Α΄.4.4. Υποθέτουμε λοιπόν ότι $n \geq 3$.

Από την ανισότητα έπεται αμέσως ότι $h(\alpha) < \frac{\log 2}{n}$. Αυτό σημαίνει ότι ο α είναι αλγεβρικός ακέραιος [9]. Μπορούμε να αντικαταστήσουμε τον α από ένα συζυγή του, οπότε χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $|\alpha| \geq 1$. Από την ανισότητα,

$$\log |\alpha| \leq nh(\alpha),$$

συμπεραίνουμε ότι

$$\log |\alpha| < \frac{1}{2200n \log n}.$$

Αν για κάθε $n \geq 2$ βρούμε δύο ακέραιους $L \geq 2$ και $A \geq 2$ με L άρτιο, τέτοιους ώστε ο αριθμός $C > 0$ που ορίζεται από την σχέση

$$\frac{1}{C^2} = \Big(\frac{\pi}{A}\Big)^2 + \Big(\frac{AL}{2200n \log n}\Big)^2,$$

να ικανοποιεί την ανισότητα

$$\Big(1 - \frac{1}{L}\Big) \log C > 1 + \frac{2n}{L} \log L + \frac{AL}{2 \cdot 2200n \log n},$$

τότε το λήμμα 3.7.2 θα ικανοποιείται και άρα θα έχουμε το ζητούμενο.

Οι ζητούμενοι ακέραιοι είναι οι

$$A = 30 \text{ και } L = 2[2n \log(2n)].$$

□

Η απόδειξη του παραπάνω ισχυρισμού:

Με δεδομένη την

$$\frac{1}{C^2} = \Big(\frac{\pi}{A}\Big)^2 + \Big(\frac{AL}{2200n \log n}\Big)^2 \tag{3.11}$$

πρέπει να αποδείξουμε την

$$\Big(1 - \frac{1}{L}\Big) \log C > 1 + 2n \frac{\log L}{L} + \frac{1}{2}\sqrt{\frac{1}{C^2} - \Big(\frac{\pi}{A}\Big)^2}.$$

Αρκεί να απολδείξουμε την

$$\Big(1 - \frac{1}{L}\Big) \log C > 1 + 2n \frac{\log L}{L} + \frac{1}{2C},$$

[9] Το συμπέρασμα αυτό προκύπτει από το ύψος του Mahler και από την σχέση του με το ύψος του Weil (πρβλ παράγραφο Α΄.4).

που ισοδύναμα γράφεται

$$\frac{L-1}{\log L}\log C - \frac{L}{\log L}\cdot\Big(1+\frac{1}{2C}\Big) > 2n. \tag{3.12}$$

Για $L = 2[2n\log(2n)]$ και $A = 30$ έχω από την (3.11):

$$\frac{1}{C^2} \le \Big(\frac{\pi}{30}\Big)^2 + \Big(\frac{3}{55}\cdot\frac{\log(2n)}{\log(n)}\Big)^2,$$

$\Big(\frac{\pi}{30}\Big)^2 + \Big(\frac{3}{55}\cdot\frac{\log(2n)}{\log(n)}\Big)^2$ γνησίως φθίνουσα συνάρτηση, άρα

$$C \ge b(n_0) := \left(\Big(\frac{\pi}{30}\Big)^2 + \Big(\frac{3}{55}\cdot\frac{\log(2n_0)}{\log(n_0)}\Big)^2\right)^{-1/2} \text{ για } n \ge n_0.$$

Επίσης, $\frac{L-1}{\log L} = \frac{L}{\log L}\Big(1-\frac{1}{L}\Big)$. Εύκολα βλέπουμε ότι:

$$1 - \frac{1}{L} > 1 - \frac{1}{4n\log(2n)-2}.$$

Η $1-\frac{1}{4n\log(2n)-2}$ είναι γνησίως αύξουσα συνάρτηση. Άρα, για $n \ge n_0$,

$$\frac{L-1}{\log L} > u(n_0)\cdot\frac{L}{\log L},$$

όπου $u(n_0) := 1-\frac{1}{4n_0\log(2n_0)-2}$. Άρα, για την (3.12) αρκεί,

$$\left(u(n_0)\cdot\log(b(n_0)) - \Big(1+\frac{1}{2b(n_0)}\Big)\right)\cdot[2n\log(2n)] > n\log\big(2[2n\log(2n)]\big).$$

Για $n \ge 4 (= n_0)$ ελέγχω στο Maple ότι ισχύει αυτή η ανισότητα.

Για $n = 3$, $L = 24$ και $A = 30$ η τιμή του C που προκύπτει από τη (3.11) ικανοποιεί την (3.12).

□

Κεφάλαιο 4

Άνω φράγμα της ορίζουσας

Σκοπός του κεφαλαίου αυτού είναι η εύρεση ενός άνω φράγματος της ορίζουσας όπως αυτή ορίστηκε στην παράγραφο 2.1.

Σε αυτό το κεφάλαιο συμβολίζουμε με $f_1, \ldots, f_L$ αναλυτικές συναρτήσεις στο $\mathbb{C}^n$ και με $\zeta_1, \ldots, \zeta_L$ σημεία του $\mathbb{C}^n$. Επίσης αν f είναι μια αναλυτική συνάρτηση στο $\mathbb{C}^n$, τότα ορίζουμε: $|f|_R := \sup\{|f(z)|, z \in \Delta(0,R)\}$ ($\Delta(0,R)$ πολυδίσκος κέντρου $(0,\ldots,0) \in \mathbb{C}^n$ και ακτίνας $R = (R_1, \ldots, R_n) \in \mathbb{N}^n$). Περισσότερες λεπτομέρειες για την θεωρία που θα χρειασθούμε σε αυτό το κεφάλαιο βρίσκονται στο παράρτημα Α΄.6.

Θα προσπαθήσουμε να βρούμε ένα άνω φράγμα της ορίζουσας:

$$\Delta = \det\Big(f_\lambda(\zeta_\mu)\Big)_{1\le\lambda,\mu\le L},$$

ακολουθώντας την ιδέα του Michel Laurent [17], [18], [19]. Θα δείξουμε ότι η συνάρτηση μιας μιγαδικής μεταβλητής z,

$$\Psi(z) = \det\Big(f_\lambda(z\zeta_\mu)\Big)_{1\le\lambda,\mu\le L},$$

έχει ρίζα στο μηδέν μεγάλης πολλαπλότητας. Ύστερα το λήμμμα του Schwarz θα μας εξασφαλίσει το άνω φράγμα της ορίζουσας Δ ($\Delta = \Psi(1)$). Τέλος, το άνω φράγμα της ορίζουσας της παραγράφου 2.1, εξασφαλίζεται με κατάλληλη επιλογή των συνσρτήσεων $f_1 \ldots, f_L$ και των σημείων $\zeta_1, \ldots, \zeta_L$.

4.1 Εφαρμογή του λήμματος του Schwarz

Λήμμα 4.1.1. *Έστω $r > 0$ και $R > 0$ δύο πραγματικοί αριθμοί με $0 < r \le R$, τέτοιοι ώστε:*

$$\max_{1\le\mu\le L} |\zeta_\mu| \le r.$$

Έστω ότι η συνάρτηση

$$\Psi(z) = \det\Big(f_\lambda(z\zeta_\mu)\Big)_{1\le\lambda,\mu\le L}.$$

έχει στη θέση $z = 0$ ρίζα με πολλαπλότητα Τ. Τότε

$$|\Delta| = |\Psi(1)| \le \Big(\frac{R}{r}\Big)^{-T} L! \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

Απόδειξη. Ορίζουμε $E = \frac{R}{r} \ge 1$. Εφαρμόζουμε το λήμμα Α΄.2.1 για την συνάρτηση $\Psi(z)$ και αντικαθιστούμε όπου r το 1 και όπου R το E. Έχουμε λοιπόν για $z = 1$ (το οποίο προφανώς ανήκει στο $\Delta(0, E)$),

$$|\Psi(1)| \le \Big(\frac{R}{r}\Big)^{-T} |\Psi|_E.$$

Όμως, όπως και στην απόδειξη του λήμματος 2.2.3, έχουμε ότι

$$|\Psi|_E \le L! \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

Οπότε,

$$|\Delta| = |\Psi(1)| \le \Big(\frac{R}{r}\Big)^{-T} L! \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

□

4.2 Πολλαπλότητα της ρίζας $z = 0$ της συνάρτησης Ψ

Στη μια διάσταση, δηλαδή όταν οι $f_i, i = 1, \ldots, L$ είναι συναρτήσεις μιας μιγαδικής μεταβλητής απόδείξαμε, λήμμα 2.2.3, ότι η πολλαπλότητα της ρίζας $z = 0$ της $\Psi(z)$ είναι το λιγότερο $\frac{L(L-1)}{2}$. Σε αυτή την παράγραφο θα προσπαθήσουμε να εκτιμήσουμε την πολλαπλότητα της ρίζας $z = 0$ της συνάρτησης $\Psi(z)$ στην $n-$διάστατη περίπτωση.

Αν $k = (k_1, \ldots, k_n) \in \mathbb{N}^n$ ορίζουμε με $||k||$ τον αριθμό $k_1 + \ldots + k_n$. Επίσης για $n \ge 1$ και $L \ge 1$ ορίζουμε τον αριθμό,

$$\Theta_n(L) = \min\{||k^{(1)}||, \ldots, ||k^{(L)}||\},$$

όπου το ελάχιστο διατρέχει τις $L-$άδες $(k^{(1)}, \ldots, k^{(L)})$ στοιχείων του $\mathbb{N}^n$ τα οποία είναι διαφορετικά ανα δύο.

Στην μονοδιάστατη περίπτωση, όπως αναφέραμε στην αρχή της παραγράφου, η πολλαπλότητα της ρίζας ήταν το λιγότερο $\Theta_1(L) = \min\{||k^{(1)}||, \ldots, ||k^{(L)}||\} = {}^{1}\min\{k^{(1)}, \ldots, k^{(L)}\} = \frac{L(L-1)}{2}$, αφού η ελάχιστη τιμή του αθροίσματος L μη αρνητικών ακεραίων πετυχαίνεται αν επιλέξουμε τους $0, 1, \ldots, L-1$.

Στην $n-$διάστατη περίπτωση ισχύει το εξής

Λήμμα 4.2.1. *Η συνάρτηση μιας μιγαδικής μεταβλητης,*

$$\Psi(z) = \det\Big(f_\lambda(z\zeta_\mu)\Big)_{1\leq\lambda,\mu\leq L},$$

($f_i,\ \ i = 1, \ldots, L$ αναλυτικές στο $\mathbb{C}^n$, $\zeta_i \in \mathbb{C}^n,\ \ i = 1, \ldots, L$), έχει ρίζα στο $z = 0$ με πολλαπλότητα $\geq \Theta_n(L)$.

Απόδειξη. Κάθε $f_\lambda,\ \ \lambda = 1, \ldots, L$, είναι αναλυτική στον πολυδίσκο $\Delta(0, \rho), \rho > 0$ πραγματικός αριθμός, άρα ,για $\zeta \in \Delta(0, \rho)$, έχει ανάπτυγμα Taylor,[2]

$$f_\lambda(\zeta) = \sum_{k^{(\lambda)}\in\mathbb{N}^n} c_{k^{(\lambda)}}\zeta^{k^{(\lambda)}}.$$

Χρησιμοποιώντας το επιχείρημα της απόδειξης του λήμματος 2.2.3, αρκεί να εξετάσουμε τις περιπτώσεις, όπου

$$f_\lambda(\zeta) = \zeta^{k^{(\lambda)}},\ \ k^{(\lambda)} \in \mathbb{N}^n.$$

Σε μια τέτοια περίπτωση, $f_\lambda(z\zeta) = \zeta^{k^{(\lambda)}} z^{||k^{(\lambda)}||},\ \ z \in \mathbb{C}$.

Άρα στην ορίζουσα $\Psi(z) = \det\Big(f_\lambda(z\zeta_\mu)\Big)_{1\leq\lambda,\mu\leq L}$, στην γραμμή λ έχουμε κοινό παράγοντα το $z^{||k^{(\lambda)}||}$. Οπότε,

$$\Psi(z) = \det\Big(f_\lambda(z\zeta_\mu)\Big)_{1\leq\lambda,\mu\leq L} = \det\Big(f_\lambda(\zeta_\mu)\Big)_{1\leq\lambda,\mu\leq L} \cdot z^{||k^{(1)}||+\ldots+||k^{(L)}||}.$$

Η ορίζουσα $\Psi(z)$ είναι ταυτοτικά μηδέν αν τα $k^{(i)} \in \mathbb{N}^n$ δεν είναι διαφορετικά ανά δύο. Άρα, αν η $\Psi(z)$ δεν είναι ταυτοτικά μηδέν τότε τα $k^{(i)} \in \mathbb{N}^n$ είναι διαφορετικά ανά δύο. Άρα, όπως και στο λήμμα 2.2.3, έχουμε ότι η $\Psi(z)$ έχει ρίζα στο μηδέν με πολλαπλότητα τουλάχιστον, $\Theta_n(L)$.

□

[1] Εδώ τα $k^{(i)},\ \ i = 1 \ldots, L$ είναι στοιχεία του $\mathbb{N}$

[2] Πρβλ παράρτημα Α΄.6

4.3 Κάτω φράγμα για το $\Theta_n(L)$

Έχουμε το εξής κάτω φράγμα για το $\Theta_n(L)$:

Λήμμα 4.3.1. *Για κάθε $n \in \mathbb{N}^n$ και για κάθε $L \geq 2^n \mathrm{e}^{n+1}$, έχουμε ότι:*

$$\Theta_n(L) \geq \frac{n}{6\mathrm{e}} L^{\frac{n+1}{n}}.$$

Απόδειξη. Έστω $L \geq 2$.

Η ελάχιστη τιμή του αθροίσματος $||k^{(1)}||+\ldots+||k^{(L)}||$ πετυχαίνεται επιλέγοντας τα $k^{(\mu)}$ διαδοχικά ως εξής:

- το ένα στοιχείο, $(0,0,\ldots,0) \in \mathbb{N}^n$,
- τα n στοιχεία του $\mathbb{N}^n$ μήκους 1,
  $(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)$
- τα $\binom{n+1}{2} = \binom{n+1}{n-1}$ στοιχεία του $\mathbb{N}^n$ μήκους 2,
  $(2,0,\ldots,0),(0,2,0,\ldots,0),\ldots,(0,\ldots,0,2)$
  $(1,1,0,\ldots,0),(1,0,1,0,\ldots,0),\ldots,(0,\ldots,0,1,1)$
- και ούτω καθεξής.

Γενικά, για ένα μη αρνητικό ακέραιο a, το πλήθος των στοιχείων $k \in \mathbb{N}^n$ με μήκος $||k|| = a$ είναι ίσο με το πλήθος των διαφορετικών λύσεων $(k_1,\ldots,k_n)$ της εξίσωσης

$$k_1 + \ldots + k_n = a.$$

Το πλήθος αυτό είναι ίσο με: $\binom{n+a-1}{a} = \binom{n+a-1}{n-1}$ [3].

Για κάθε θετικό ακέραιο A έχουμε την σχέση

$$\sum_{k=0}^{A-1} \binom{n+k}{n} = \binom{n+A}{n+1}.$$

Αυτό διότι, από τον τύπο

$$\binom{n+k-1}{n+1} + \binom{n+k-1}{n} = \binom{n+k}{n+1}, \text{ έχουμε ότι}$$

[3] πρβλ παράρτημα Α΄.1

$$\begin{aligned}\binom{n+A}{n+1} &= \binom{n+A-1}{n} + \binom{n+A-1}{n+1} = \\ &= \binom{n+A-1}{n} + \binom{n+A-2}{n} + \binom{n+A-2}{n+1} = \\ &= \binom{n+A-1}{n} + \binom{n+A-2}{n} + \binom{n+A-3}{n} + \binom{n+A-3}{n+1} \\ &= \ldots = \binom{n+A-1}{n} + \ldots + \binom{n}{n} = \sum_{k=0}^{A-1}\binom{n+k}{n}.\end{aligned}$$

Έστω A θετικός ακέραιος τέτοιος ώστε:

$$\sum_{a=0}^{A}\binom{n+a-1}{n-1} = \binom{n+A}{n} \leq L < \binom{n+A+1}{n}\ ^{4}.$$

Αν ορίσω $f(x) = \frac{(x+n)\cdots(x+1)}{n!} : \mathbb{R}^+ \to \mathbb{R}^+$, τότε έχω ότι η $f(x)$ είναι συνεχής ως πολυωνυμική και $f(A) \leq L < f(A+1)$. Άρα από το Θεώρημα ενδιαμέσων τιμών έχω ότι υπάρχει $\alpha \in \mathbb{R}^+$ με $A \leq \alpha < A+1$, τέτοιο ώστε: $f(\alpha) = L$. Δηλαδή $\frac{(\alpha+n)\cdots(\alpha+1)}{n!} = L$.

Από τα παραπάνω συμπεραίνουμε ότι ο A είναι το ακέραιο μέρος του $\alpha \in \mathbb{R}^+$.

Έχουμε ότι:

$$\begin{aligned}||k^{(1)}|| + \ldots + ||k^{(L)}|| &\geq \sum_{a=0}^{A} a\binom{n+a-1}{n-1} \\ &= n\sum_{a=1}^{A}\binom{n+a-1}{n} = n\sum_{a=0}^{A-1}\binom{n+a}{n} \\ &= n\binom{n+A}{n+1}.\end{aligned}$$

Οπότε,

$$\Theta_n(L) \geq n\binom{n+A}{n+1}.$$

Έχουμε ότι $\alpha - 1 \leq A$. Άρα:

$$\begin{aligned}(n+A)(n+A-1)\cdots(1+A)A &\geq (\alpha+n-1)\cdots\alpha A \\ &= \frac{\alpha}{\alpha+n}(\alpha+n)\cdots(\alpha+1)A = \frac{\alpha}{\alpha+n}n!AL.\end{aligned}$$

[4] $\binom{n+A}{n} = \frac{(A+n)\cdots(A+1)}{n!}$

Άρα:

$$\Theta_n(L) \geq n\binom{n+A}{n+1} = \frac{A(A+1)\cdots(A+n)}{n!} \cdot \frac{n}{n+1} \geq \frac{\alpha}{\alpha+n} \cdot \frac{n}{n+1} AL.$$

Από τα προηγούμενα έχουμε ότι:

$$(\alpha+n)\cdots(\alpha+1) = n!L.$$

Άρα,

$$(\alpha+n)^n \geq n!L,$$

δηλαδή,

$$(\alpha+n) \geq (n!L)^{1/n}.$$

Διαλέγω ένα $\delta \in \mathbb{R}^+$ με:

$$(n!L)^{1/n} \leq \delta \leq (\alpha+n)$$

Άρα,

$$\delta - n \leq \alpha$$

και συνεπώς,

$$\delta - n - 1 \leq A.$$

Οπότε,

$$\begin{aligned}
\Theta_n(L) &\geq \frac{\alpha}{\alpha+n} \cdot \frac{n}{n+1} AL \\
&\geq \frac{n}{n+1} \frac{\delta-n}{\delta} (\delta - n - 1)L \\
&= \frac{n}{n+1} \delta L \Big(1 - \frac{n}{\delta}\Big)\Big(1 - \frac{n+1}{\delta}\Big), \quad \text{για κάθε } n \geq 1, \;\; L \geq 1.
\end{aligned}$$

Επίσης,

$$\delta \geq (n!L)^{1/n} \;^{5} \geq \frac{n}{\mathrm{e}} L^{1/n}.$$

Έστω $L \geq 2^n \mathrm{e}^{n+1}$.

Τότε, $\delta \geq 2(n+1)$, άρα,

$$1 - \frac{n+1}{\delta} \geq \frac{1}{2} \quad \text{και} \quad 1 - \frac{n}{\delta} \geq \frac{1}{2}.$$

Οπότε,

$$\Theta_n(L) \geq \frac{n+1}{n} \cdot \frac{n}{\mathrm{e}} L^1 L \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{n}{4\mathrm{e}(n+1)} n L^{\frac{n+1}{n}}.$$

[5] Διότι, $n! > \left(\frac{n}{\mathrm{e}}\right)^n$

Για $n \geq 2$, ισχύει ότι $\frac{n}{4\mathrm{e}(n+1)} \geq \frac{1}{6\mathrm{e}}$.

Άρα,

$$\Theta_n(L) \geq \frac{n}{6\mathrm{e}} L^{\frac{n+1}{n}}, \quad \text{για } n \geq 2 \quad \text{και} \quad L \geq 2^n \mathrm{e}^{n+1}.$$

Επίσης, για $n = 1$ έχουμε ότι:

$$\Theta_1(L) = \frac{L(L-1}{2} \geq \frac{1}{6\mathrm{e}} L^2,$$

δηλαδή η ανισότητα ισχύει και για $n = 1$.

Άρα, για κάθε $n \in \mathbb{N}$ και για κάθε $L > 2^n \mathrm{e}^{n+1}$,

$$\Theta_n(L) \geq \frac{n}{6\mathrm{e}} L^{\frac{n+1}{n}}.$$

□

4.4 Άνω φράγμα της ορίζουσας

Πρόταση 4.4.1. *Έστω $\ell_1, \ldots, \ell_n \in \mathfrak{L}$ και $\beta_1, \ldots, \beta_n$ μιγαδικοί αριθμοί. Έστω L_0, L_1, S ακέραιοι αριθμοί ≥ 2 και $L := \binom{L_0+n}{n}(L_1+1)$, με $L \leq (2S-1)^{n+1}$. Θεωρούμε την ορίζουσα, όπως ορίστηκε στην παράγραφο 2.1,*

$$\Delta = \det\Big((s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1)^{\lambda_1} \ldots (s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n)^{\lambda_n} \big(\alpha_1^{s^{(\mu)}+s_{n+1}^{(\mu)}\beta_1} \cdots \alpha_n^{s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n}\big)^{\lambda_{n+1}} \Big)_{\underline{\lambda},\mu},$$

όπου,

$$\underline{\lambda} = (\lambda_1, \ldots, \lambda_n) \in \mathbb{N}^n \ \text{ με } \lambda_1 + \ldots + \lambda_n \leq L_0, \ \ \lambda_{n+1} \leq L_1,$$
$$1 \leq \mu \leq L \ \text{ και } \ s^{(1)}, \ldots, s^{(L)} \text{ στοιχεία του } \mathbb{Z}^{n+1}(S).$$

Τότε υπάρχει σταθερά $c_1 = c_1(n, \ell_1, \ldots, \ell_n, \beta_1, \ldots, \beta_n) > 0$, τέτοια ώστε:

$$\frac{1}{L} \log|\Delta| \leq -L^{\frac{1}{n}} + c_1\big(L_0 \log S + L_1 S\big).$$

Απόδειξη. Κάνουμε την εξής επιλογή συναρτήσεων και σημείων,

$$f_\lambda(z) = z_1^{\lambda_1} \cdots z_n^{\lambda_n} \cdot \big(\alpha_1^{z_1} \cdots \alpha_n^{z_n}\big)^{\lambda_{n+1}},$$

όπου $z = (z_1, \ldots, z_n)$, και

$$\zeta_\mu = (s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1, \ldots, s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n) \in \mathbb{C}^n.$$

Για $R > 0$ πραγματικό αριθμό,

$$\begin{aligned}|f_\lambda|_R &= |z_1^{\lambda_1}\cdots z_n^{\lambda_n}\cdot\left(\alpha_1^{z_1}\cdots\alpha_n^{z_n}\right)^{\lambda_{n+1}}|_R\\ &\le R^{\lambda_1}\cdots R^{\lambda_n}\cdot \mathrm{e}^{|\lambda_{n+1}(\ell_1 z_1+\ldots+\ell_n z_n)|_R}\\ &\le R^{L_0}\cdot \mathrm{e}^{L_1\cdot R\sum_{i=1}^n|\ell_i|}.\end{aligned}$$

Οπότε,

$$\log|f_\lambda|_R \le L_0\log R + L_1 R\sum_{i=1}^n|\ell_i|.$$

Επιλέγουμε,

$$r = S(1+\max_{1\le j\le n}|\beta_j|) \quad \text{και} \quad R = r\cdot \mathrm{e}^{\frac{6\mathrm{e}}{n}}.$$

Θεωρούμε την συνάρτηση μιας μιγαδικής μεταβλητής

$$\Psi(z) = \det\Big(f_\lambda(z\zeta_\mu)\Big)_{\underline{\lambda},\mu}.$$

Από τα λήμματα 4.1.1, 4.2.1, για την συνάρτηση $\Psi(z)$, έχουμε ότι:

$$|\Delta| = |\Psi(1)| \le \Big(\frac{R}{r}\Big)^{-\Theta_n(L)} L!\prod_{i=1}^L|f_i|_R.$$

Οπότε,

$$\log|\Delta| \le -\frac{6\mathrm{e}}{n}\Theta_n(L) + \log L! + LL_0\log R + LL_1R\sum_{i=1}^n|\ell_i|. \tag{4.1}$$

- Έστω $L \ge 2^n\mathrm{e}^{n+1}$.

Λόγω του λήμματος 4.3.1 έχουμε ότι:

$$\frac{6\mathrm{e}}{n}\Theta_n(L) > L^{\frac{n+1}{n}}.$$

Άρα,

$$\begin{aligned}\log|\Delta| &\le -L^{\frac{n+1}{n}} + \log L! + LL_0\log R + LL_1R\sum_{i=1}^n|\ell_i|\\ &\le -L^{\frac{n+1}{n}} + L\log L + LL_0\log R + LL_1R\sum_{i=1}^n|\ell_i|\\ &\le -L^{\frac{n+1}{n}} + c_1\,'L(L_0\log S + L_1S),\end{aligned}$$

όπου το c_1' είναι θετικός πραγματικός και εξαρτάται αποκλειστικά από τα n, ℓ_i, β_i [6].

- Έστω $L < 2^n \mathrm{e}^{n+1}$.

Από την σχέση 4.1 έχουμε ότι:

$$\log|\Delta| \leq \log L! + LL_0 \log R + LL_1 R \sum_{i=1}^{n} |\ell_i|,$$

αν χρησιμοποιήσουμε την τετριμμένη ανισότητα, $\Theta_n(L) \geq 0$, για κάθε $L \geq 1$ και $n \in \mathbb{N}$. Για το ίδιο $c_1\,'$, έχουμε λοιπόν ότι

$$\log|\Delta| \leq c_1\,' L(L_0 \log S + L_1 S),$$

δηλαδή,

$$\frac{1}{L}\log|\Delta| \leq c_1\,'(L_0 \log S + L_1 S).$$

Όμως, αφού $L < 2^n \mathrm{e}^{n+1}$ έχουμε ότι

$$L^{1/n} < 4SL_1, \quad [7]$$

άρα,

$$\frac{1}{L}\log|\Delta| + L^{1/n} \leq c_1\,'(L_0 \log S + L_1 S) + 4SL_1,$$

δηλαδή,

$$\frac{1}{L}\log|\Delta| + L^{1/n} \leq (c_1\,' + 4)(L_0 \log S + L_1 S).$$

Άρα, για $c_1 := c_1\,' + 4$, έχουμε ότι για κάθε $L \geq 2$,

$$\frac{1}{L}\log|\Delta| \leq -L^{\frac{1}{n}} + c_1\big(L_0 \log S + L_1 S\big).$$

[6] Συγκεκριμένη τιμή για το c_1' υπολογίζεται εύκολα (πρβλ. υπολογισμό του c_1 στην απόδειξη του θεωρήματος 2.2.1)

[7] $S, L_1 \geq 2$

Κεφάλαιο 5

Γραμμική εξάρτηση των $1, \beta_1, \ldots, \beta_n$

Σε αυτό το κεφάλαιο θα αποδείξουμε ότι αν η τάξη του πίνακα Π, που ορίστηκε στην παράγραφο 2.1, είναι $< L$, τότε τα $1, \beta_1, \ldots, \beta_n$ είναι $\mathbb{Q}-$ γραμμικώς εξαρτημένα.

Συμβολίζουμε με K οποιοδήποτε σώμα χαρακτηριστικής μηδέν.

Με $K^*_{\rm tors}$ συμβολίζουμε την ομάδα των ριζών της μονάδας που ανήκουν στο K, η οποία είναι υποομάδα του K^*. Με $\sigma : K^* \to K^*/K^*_{\rm tors}$, συμβολίζουμε την κανονική απεικόνιση του K^* επί του $K^*/K^*_{\rm tors}$.

Για $x \in \mathbb{R}$ συμβολίζουμε με $\lceil x \rceil$ τον μικρότερο ακέραιο $\geq x$. Δηλαδή, $x \leq \lceil x \rceil < x + 1$.

5.1 Το κύριο αποτέλεσμα

Συγκεκριμένα, έχουμε την εξής

Πρόταση 5.1.1. *Έστω $\alpha_1, \ldots, \alpha_{n+1}$ μη μηδενικά στοιχεία του K τα οποία παράγουν μια πολλαπλασιαστική υποομάδα του K^* με* $\operatorname{rank} \geq n$ [1]. *Έστω $\beta_1, \ldots, \beta_n$ στοιχεία του K. Υποθέτουμε ότι υπάρχουν τρεις θετικοί ρητοί ακέραιοι L_0, L_1 και S οι οποίοι ικανοποιούν τις εξής ανισότητες:*

$$\Big(\frac{S}{2n}\Big)^{n+1} \geq (L_0 L_1)^n, \quad S > 2n(n+1) \quad \text{και} \quad S^n > L_1.$$

Ο δείκτης $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$ είναι τέτοιος ώστε $\lambda_1 + \ldots + \lambda_n \leq L_0$ και $\lambda_{n+1} \leq L_1$. Έχουμε δείξει, (πρβλ. Α΄.1), ότι ο δείκτης $\underline{\lambda}$ διατρέχει

[1] Δηλαδή, το πολύ ένα εξ αυτών εκφράζεται πολλαπλασιαστικά συναρτήσει των υπολοίπων

$L := \binom{L_0+n}{n}(L_1+1)$ *τιμές. Ο δείκτης* $\underline{s}$ *διατρέχει το* $\mathbb{Z}^{n+1}(S)$*, δηλαδή* $\underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1} : \ |s_i| < S, \ i = 1, \ldots, n+1$*, άρα ο* $\underline{s}$ *διατρέχει* $(2S-1)^{n+1}$ *τιμές.*

Υποθέτουμε ότι ο πίνακας $\binom{L_0+n}{n}(L_1+1) \times (2S-1)^{n+1}$*,*

$$\Pi := \Big((s_1 + s_{n+1}\beta_1)^{\lambda_1} \ldots (s_n + s_{n+1}\beta_n)^{\lambda_n} \big(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}} \Big)_{\underline{\lambda},\underline{s}},$$

διάστασης $L \times (2S-1)^{n+1}$*, έχει τάξη αυστηρά μικρότερη του πλήθους των γραμμών* Λ*.*

Τότε οι αριθμοί $1, \beta_1, \ldots, \beta_n$ *είναι* $\mathbb{Q}-$*γραμμικώς εξαρτημένοι.*

Παρατήρηση: Βάσει των υποθέσεων, προκύπτει εύκολα ότι οι γραμμές του πίνακα Π είναι λιγότερες από τις στήλες, άρα έχει νόημα η υπόθεση για την τάξη του πίνακα [2].

Απόδειξη. Θα γίνει μια περιγραφή της απόδειξης. Οι περισσότερες λεπτομέρειες θα αποδειχθούν στις επόμενες παραγράφους παρακάτω.

Χωρίζουμε την απόδειξη σε βήματα.

- *Βήμα 1ο.*

Βάσει του λήμματος 5.2.1, το οποίο θα αποδείξουμε παρακάτω στην ενότητα 5.2, αρκεί να δείξουμε ότι υπάρχει μη μηδενικό $Q \in K[X_1, \ldots, X_n]$ βαθμού $\leq 2L_0L_1$ που να μηδενίζεται στο σύνολο

$$\begin{aligned} Y(S'') &:= \mathbb{Z}^n(S'') + \mathbb{Z}(S'') \cdot (\beta_1, \ldots, \beta_n) \\ &= \{(s_1'' + s_{n+1}''\beta_1, \ldots, s_n'' + s_{n+1}''\beta_n), \ \ (s_1'', \ldots, s_{n+1}'') \in \mathbb{Z}^{n+1}(S'')\}, \end{aligned}$$

όπου $S'' = \lceil \frac{S}{2} \rceil$.

Κάποια σχόλια για το πρώτο βήμα. Για την εφαρμογή του λήμματος 5.2.1 απαιτείται να ισχύει, $\Big(\frac{2S''}{n} - 1\Big)^{n+1} > (2L_0L_1)^n$. Διαπιστώνουμε ότι η ανισότητα αυτή όντως ισχύει. Πράγματι,

Λόγω των υποθέσεων της πρότασης 5.1.1 έχουμε ότι, $(2L_0L_1)^n \leq 2^n\Big(\frac{S}{2n}\Big)^{n+1}$. Αρκεί $2^n\Big(\frac{S}{2n}\Big)^{n+1} < \Big(\frac{2S''}{n} - 1\Big)^{n+1}$. Ισοδύναμα, $\frac{1}{2}\Big(\frac{S}{n}\Big)^{n+1} < 2\Big(\frac{S}{n} - 1\Big)^{n+1}$. Ισοδύναμα, $\Big(\frac{S}{n}\Big)^{n+1} < 2\Big(\frac{2S''}{n} - 1\Big)^{n+1}$. Αλλά, $S'' > \frac{S}{2}$, άρα αρκεί, $\Big(\frac{S}{n}\Big)^{n+1} < 2\Big(\frac{S}{n} - 1\Big)^{n+1}$. Αρκεί, $\Big(\frac{S}{n}\Big)^{n+1} < \Big(2\frac{S}{n} - 2\Big)^{n+1}$. Ισοδύναμα αρκεί, $\frac{S}{n} > 2$, δηλαδή, $S > 2n$, το οποίο ισχύει αφού λόγω υπόθεσης έχουμε ότι $S >$

[2] Λόγω των ανισοτήτων $\binom{L_0+n}{n} \leq (n+1)L_0^n$ και $\big(\frac{S}{2n}\big)^{n+1} \geq (L_0L_1)^n$, προκύπτει ότι $\binom{L_0+n}{n}(L_1+1) \leq S^{n+1} < (2S-1)^{n+1}$

$2n(n+1)$.

• *Βήμα 2ο.*

Την ύπαρξη του πολυωνύμου Q του βήματος 1 μας εξασφαλίζει το λήμμα 5.3.1. Οπότε, αρκεί να δείξουμε ότι υπάρχει $P \in K[X_1, \ldots, X_n, Y]$ με $\deg_{\underline{X}} P \leq L_0$, (όπου $\underline{X} = (X_1, \ldots, X_n)$), $\deg_Y \leq L_1$, που να μηδενίζεται στο:

$$\{(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n, \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}) \in K^n \times K^*, \ \ \underline{s} \in \mathbb{Z}^{n+1}(S)\}.$$

Κάποια σχόλια για το δεύτερο βήμα.

Για την εφαρμογή του λήμματος 5.3.1, πρέπει να ισχύει η συνθήκη $\mathrm{card}\{\sigma(\alpha_1^{s'_1} \cdots \alpha_{n+1}^{s'_{n+1}}), \underline{s}' \in \mathbb{Z}^{n+1}(S')\} > L_1$, με $S' = S - \lceil \frac{S}{2} \rceil + 1$,
η οποία όμως ικανοποιείται, αφού λόγω του λήμματος Α΄.10.3 έχουμε ότι

$$\mathrm{card}\{\sigma(\alpha_1^{s'_1} \cdots \alpha_{n+1}^{s'_{n+1}}), \underline{s}' \in \mathbb{Z}^{n+1}(S')\} \geq (2S'-1)^n.$$

Όμως, λόγω της σχέσης $S+1 < 2S' < 2S+2$, προκύπτει ότι $(2S'-1)^n > S^n$, το οποίο είναι $> L_1$ λόγω των ανισοτικών σχέσεων της υπόθεσης στην πρόταση 5.1.1.

• *Βήμα 3ο.*

Η ύπαρξη του P εξασφαλίζεται από τις υποθέσεις της πρότασης 5.1.1 σχετικά με την τάξη του πίνακα.

Αυτό γίνεται ως εξής:

αφού η τάξη του πίνακα είναι $< L := \binom{L_0+n}{n}(L_1+1)$, υπάρχουν $c_i \in K$ τέτοια ώστε:

$$c_1\gamma_1 + \ldots + c_L\gamma_L = \mathbf{0} \in K^{(2S-1)^{n+1}},$$

όπου $\gamma_1, \ldots, \gamma_L$ οι γραμμές του πίνακα Π. Δηλαδή,

$$\sum_{i=1}^{L} c_i\gamma_i = \mathbf{0},$$

ή, τροποποιώντας τον συμβολισμό ως προς τον δείκτη,

$$\sum_{\underline{\lambda}} c_{\underline{\lambda}}\gamma_{\underline{\lambda}} = \mathbf{0}.$$

Στο αριστερό μέλος έχουμε ένα διάνυσμα του $K^{(2S-1)^{n+1}}$, του οποίου η τυπική συντεταγμένη είναι

$$\sum_{\underline{\lambda}} c_{\underline{\lambda}}\big((s_1 + s_{n+1}\beta_1)^{\lambda_1} \cdots (s_n + s_{n+1}\beta_n)^{\lambda_n}(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}})\big),$$

και λόγω της τελευταίας ισότητας αυτή πρέπει να είναι μηδέν.

Άρα, το πολυώνυμο

$$P(X_1, \ldots, X_n, Y) = \sum_{\underline{\lambda}} c_{\underline{\lambda}} X^{\lambda_1} \cdots X_n^{\lambda_n} Y^{\lambda_{n+1}} \in K[X_1, \ldots, X_n, Y],$$

μηδενίζεται σε κάθε σημείο

$$(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n, \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}) \in K^n \times K^*, \ \ \underline{s} \in \mathbb{Z}^{n+1}(S).$$

□

5.2 Εκτίμηση του συνόλου ριζών

Σε αυτή την ενότητα θα διατυπώσουμε και θα αποδείξουμε τον ισχυρισμό του 1ου βήματος της απόδειξης της πρότασης 5.1.1. Θα κάνουμε χρήση των παρακάτω συμβολισμών.

Αν $\mathcal{V}$ είναι ένας διανυσματικός υπόχωρος του K^n και F ένα πεπερασμένο υποσύνολο του K^n, συμβολίζουμε με $(F + \mathcal{V})/\mathcal{V}$ την εικόνα του F μέσω της κανονικής απεικόνισης ϖ του K^n επί του $K^n/\mathcal{V}$.

Αν E είναι ένα υποσύνολο του K^n το οποίο περιέχει το 0 και d ένας μη αρνητικός ακέραιος, ορίζουμε:

$$E[d] := \{x_1 + \ldots + x_d, \ \ x_i \in E, \ \ i = 1, \ldots, d\}.$$

Για παράδειγμα, $E[0] = \{0\}$, $E[1] = E$ και $E[0] \subset E[1] \subset E[2] \subset \ldots$.

Λήμμα 5.2.1. *Έστω* $\beta_1, \ldots, \beta_n \in K$. *Έστω ένα πολυώνυμο* $Q \in K[X_1, \ldots, X_n]$ *με* $\deg_{\underline{X}} Q \leq D$, *το οποίο μηδενίζεται στο*

$$Y(S'') := \{(s_1'' + s_{n+1}''\beta_1, \ldots, s_n'' + s_{n+1}''\beta_n), \ \ \underline{s} \in \mathbb{Z}^{n+1}(S'')\},$$

όπου $S'' \in \mathbb{Z}^+$.

Έστω επίσης,

$$\Big(\frac{2S''}{n} - 1\Big) > D^n.$$

Τότε τα $1, \beta_1, \ldots, \beta_n$ *είναι γραμμικώς εξαρτημένα πάνω από το* $\mathbb{Q}$.

Παρατήρηση: Από μια αλγεβρική εξάρτηση των $1, \beta_1, \ldots, \beta_n$ στο K με φράγμα στους εκθέτες οδηγούμαστε σε μια γραμμική εξάρτηση αυτών στο $\mathbb{Q}$.

Απόδειξη. Θα παρουσιάσουμε ένα σχεδιάγραμμα της απόδειξης, όπου κάποια πράγματα θα αποδειχθούν παρακάτω στις προτάσεις 5.2.4 και 5.2.5.

Ορίζουμε $S_1 = \lceil \frac{S''}{n} \rceil$. Άρα,

$$S'' \leq nS_1 \leq S'' + n - 1.$$

Αν $k_1, \ldots, k_n$ ρητοί ακέραιοι με $k_i < S_1, \;\; i = 1, \ldots, n$, τότε:

$$k_1 + \ldots + k_n < S''.$$

Οπότε για $E = Y(S_1)$, έχουμε ότι:

$$E[n] \subset Y(S'').$$

Άρα, αφού το Q μηδενίζεται στο $Y(S'')$, θα μηδενίζεται στο $E[n]$ για $E = Y(S_1)$. Ο μηδενισμός του πολυωνύμου Q σε τέτοιας μορφής σύνολο μας δίνει το δικαίωμα να συμπεράνουμε (πρόταση 5.2.4) την ύπαρξη διανυσματικού χώρου $\mathcal{V}$ του K^n, με συνδιάσταση $r \geq 1$, όπου:

$$\mathrm{Card}\Big((Y(S_1) + \mathcal{V})/\mathcal{V}\Big) \leq D^r.$$

Επειδή

$$D^n < \Big(\frac{2S''}{n} - 1\Big)^{n+1},$$

έχουμε ότι:

$$D^r < (2S_1 - 1)^{r+1}.$$

Οπότε:

$$\mathrm{Card}\Big((Y(S_1) + \mathcal{V})/\mathcal{V}\Big) < (2S_1 - 1)^{r+1}.$$

Το φράγμα αυτό για τον πληθάριθμο των διαφορετικών κλάσεων $y + \mathcal{V}$, $y \in Y(S_1)$, εξασφαλίζει (πρόταση 5.2.5) την γραμμική εξάρτηση υπερ το $\mathbb{Q}$ των $1, \beta_1, \ldots, \beta_n$.

□

Για την απόδειξη των συμπερασμάτων που χρησιμοποιήθηκαν στην απόδειξη του λήμματος 5.2.1 θα χρειαστούμε κάποια εργαλεία από την αλγεβρική γεωμετρία. Συγκεκριμένα, χρειαζόμαστε το Θεώρημα του Bézout,

Θεώρημα 5.2.2. *(Bézout)*

Υποθέτουμε ότι το K είναι αλγεβρικά κλειστό. Έστω $\{P_i\}_{i \in I}$ μια οικογένεια πολυωνύμων στο $K[X_1, \ldots, X_n]$, όπου κάθε ένα από αυτά είναι συνολικού βαθμού $\leq D$. Υποθέτουμε ότι το σύνολο F των κοινών ριζών των P_i στο K^n είναι πεπερασμένο. Τότε,

$$\mathrm{Card}F \leq D^n.$$

Μία γενίκευση του θεωρήματος του Bézout 5.2.2, είναι το παρακάτω λήμμα.

Λήμμα 5.2.3. *Έστω $\mathcal{V}$ διανυσματικός υπόχωρος του K^n διαστάσεως $n-r$, F πεπερασμένο υποσύνολο του K^n τέτοιο ώστε το $F+\mathcal{V}$ είναι αλγεβρικό σύνολο από πολυώνυμα (συνολικού) βαθμού (ως προς τις n μεταβλητές) $\leq D$. Τότε:*

$$\mathrm{Card}\Big((F+\mathcal{V})/\mathcal{V}\Big) \leq D^r.$$

Απόδειξη. Η περίπτωση $\mathcal{V}=0$, $r=n$, είναι το θεώρημα 5.2.2.

Στην γενική περίπτωση, μπορούμε να δούμε το $\mathcal{V}$, ύστερα από μια αλλαγή βάσης του K^n αν χρειαστεί, ως εξής:

$$\mathcal{V} \simeq K^{n-r} \times \{0\}^r.$$

Οπότε, μπορούμε να ταυτίσουμε το $k^n/\mathcal{V}$ με το $\{0\}^{n-r} \times K^r$. Το τυπικό στοιχείο του $\mathcal{V}$ είναι της μορφής $v=(v_1,\ldots,v_{n-r},0,\ldots,0) \in K^n$. Θεωρούμε τα πολυώνυμα,

$$P_{i,v} := P_i(v, X_{n-r+1}, \ldots, X_n), \;\; (i \in I, v \in \mathcal{V}).$$

Το $(x_{n-r+1},\ldots,x_n) \in K^n/\mathcal{V}$ είναι κοινή λύση των $P_{i,v}$ αν και μόνο αν υπάρχουν $f \in F, u \in \mathcal{V}$ τέτοια ώστε:

$$(v_1,\ldots,v_{n-r},x_{n-r+1},\ldots,x_n) = f+u.$$

Δηλαδή,αν και μόνο αν, για κάθε $v \in \mathcal{V}$,

$$(0,\ldots,0,x_{n-r+1},\ldots,x_n) = f+u-v,$$

ή

$$(0,\ldots,0,x_{n-r+1},\ldots,x_n) = f+\mathcal{V}.$$

Άρα υπάρχει μια ένα προς ένα αντιστοιχία των κοινών ριζών με τις κλάσεις του $(F+\mathcal{V})/\mathcal{V}$. Στην κοινή λύση $(x_{n-r+1},\ldots,x_n)$ αντιστοιχώ την κλάση $(0,\ldots,0,x_{n-r+1},\ldots,x_n)+\mathcal{V}$ [3]. Οπότε, λόγω του θεωρήματος 5.2.2 για τα πολυώνυμα $P_{i,v}$ έχουμε το ζητούμενο.

□

Στην αμέσως παρακάτω πρόταση θα δούμε πως ο μηδενισμός ενός πολυωνύμου σε σύνολο της μορφής $E[n],\;\; E \subseteq K^n$ το οποίο περιέχει το μηδέν, μας εξασφαλίζει την ύπαρξη υποχώρου του K^n ο οποίος ικανοποιεί κάποια συνθήκη.

[3] Η απεικόνιση είναι καλά ορισμένη. Είναι και ένα προς ένα, αφού αν $(0,\ldots,0,x_{n-r+1},\ldots,x_n)+\mathcal{V} = (0,\ldots,0,x'_{n-r+1},\ldots,x'_n)+\mathcal{V}$, τότε $(0,\ldots,0,x_{n-r+1}-x'_{n-r+1},\ldots,x_n-x'_n) \in \mathcal{V}$. Αφού $\mathcal{V} \simeq K^{n-r}\times\{0\}^r$, τότε $(x_{n-r+1},\ldots,x_n) = (x'_{n-r+1},\ldots,x'_n)$

Πρόταση 5.2.4. *Έστω n και D δύο θετικοί ακέραιοι και E ένα υποσύνολο του K^n το οποίο περιέχει το μηδέν. Υποθέτουμε ότι υπάρχει ένα μη μηδενικό πολυώνυμο $Q \in K[X_1, \ldots, X_n]$, συνολικού βαθμού $\leq D$, το οποίο μηδενίζεται στο $E[n]$. Τότε υπάρχει ένας διανυσματικός υπόχωρος $\mathcal{V}$ του K^n, με συνδιάσταση $r \geq 1$, τέτοιος ώστε:*

$$\mathrm{Card}\Big((E+\mathcal{V})/\mathcal{V}\Big) \leq D^r.$$

Απόδειξη.

- Υποθέσουμε ότι το K είναι αλγεβρικά κλειστό.

Έστω $Z = Z(Q)$ η υπερεπιφάνεια που ορίζεται από το Q στο K^n. Έχουμε τα εξής αλγεβρικά σύνολα του K^n [4]:

$$Z_0 = Z, \;\; Z_1 = \bigcap_{\gamma \in E} (Z_0 - \gamma),$$

$$Z_s = \bigcap_{\gamma \in E} (Z_{s-1} - \gamma), \;\; 1 \leq s \leq n.$$

Έπεται λοιπόν ότι:

$$Z_s = \bigcap_{\gamma \in E[s]} (Z_0 - \gamma),$$

(αφού, $x \in Z_s$, αν και μόνο αν, $x \in \bigcap_{\gamma \in E}(Z_{s-1} - \gamma)$, δηλαδή αν και μόνο αν, $\forall \gamma_1 \in E$ υπάρχει $z_{s-1} \in Z_{s-1} : \;\; x = z_{s-1} - \gamma$. Ισοδύναμα, λόγω ορισμού του Z_{s-1}, $\forall \gamma_1, \gamma_2 \in E$ υπάρχει $z_{s-2} \in Z_{s-2} : \;\; x = z_{s-2} - (\gamma_1 + \gamma_2)$. Καταλήγουμε, λοιπόν, $x \in Z_s$, αν και μόνο αν, $\forall \gamma_1, \ldots, \gamma_s \in E$ υπάρχει $z_0 \in Z_0 : \;\; x = z_0 - (\gamma_1 + \ldots + \gamma_s)$. Αυτό είναι ισοδύναμο με το ότι $x \in \bigcap_{\gamma \in E[s]}(Z_0 - \gamma)$.)

Λόγω της υπόθεσης ότι $E[n] \subseteq Z$ έχουμε ότι [5]:

$$E[n-s] \subseteq Z_s \text{ για } 1 \leq s \leq n,$$

άρα το Z_n περιέχει το $E[0] = \{0\}$.

Επίσης, εύκολα έχουμε ότι: $Z_0 \supset Z_1 \supset \ldots \supset Z_n$ [6].

Το σύνολο $T := \Big\{t \in \{1, \ldots, n\} : \;\; \dim Z_{t-1} \leq n - t\Big\}$, είναι μη κενό, αφού $1 \in T$, ($\dim Z_0 \leq n-1$). Επιλέγουμε το μεγαλύτερο $t \in T$. Επειδή, λοιπόν, $t+1 \notin T$, έχουμε ότι $\dim Z_{(t+1)-1} > n - (t+1)$, δηλαδή, $\dim Z_t > n - t - 1$. Επίσης, αφού $Z_{t-1} \subset Z_t$, έχουμε ότι $\dim Z_t \leq \dim Z_{t-1}$. Άρα,

$$n - t - 1 < \dim Z_t \leq \dim Z_{t-1} \leq n - t.$$

[4] Τομή αλγεβρικών συνόλων είναι αλγεβρικό σύνολο

[5] Προκύπτει με επαγωγή, χρησιμοποιώντας τον τύπο $Z_s = \bigcap_{\gamma \in E[s]}(Z_0 - \gamma)$. Για $s = 1$, $Z_1 = \bigcap_{\gamma \in E}(Z_0 - \gamma) \supseteq \bigcap_{\gamma \in E}(E[n] - \gamma) = E[n-1]$, αφού $E[n] \subseteq Z_0$

[6] Αφού $0 \in E$, έχουμε για παράδειγμα, ότι: $Z_1 = Z_0 \bigcap_{\gamma \in E \setminus \{0\}}(Z_0 - \gamma)$, άρα $Z_0 \supset Z_1$. Όμοια για τα υπόλοιπα.

Οπότε,

$$\dim Z_{t-1} = \dim Z_t = n - t.$$

Οπότε, τα Z_{t-1}, Z_t έχουν κοινή ανάγωγη συνιστώσα Y με $\dim Y = n - t$.

Ορίζουμε:

$$S = \{x \in K^n : \ x + Y \subset Z_{t-1}\}.$$

(Προφανώς $S \neq \emptyset$). Για κάθε $\gamma \in E$ έχουμε ότι [7]:

$$\gamma + Z_t \subset Z_{t-1}.$$

Αυτό δείχνει ότι:

$$E \subseteq S.$$

Ορίζουμε, επίσης,

$$\mathcal{V} = \{x \in K^n : \ x + Y = Y\}.$$

(Προφανώς $\mathcal{V} \neq \emptyset$).

Το Y είναι αλγεβρικό σύνολο (συγκεκριμένα ανάγωγο αλγεβρικό σύνολο). Έστω λοιπόν, $\{P_j\}_{j \in J}$ μια οικογένεια πολυωνύμων των οποίων το σύνολο των κοινών ριζών είναι το Y. Έχουμε ότι:

$$\begin{aligned} \mathcal{V} &= \{x \in K^n : \ x + y \in Y \text{ για όλα τα } y \in Y\} \\ &= \{x \in K^n : P_j(x + y) = 0 \text{ για όλα τα } j \in J \text{ και } y \in Y\}. \end{aligned}$$

(Η ισότητα $\mathcal{V} = \{x \in K^n : \ x + y \in Y \text{ για όλα τα } y \in Y\}$, ισχύει διότι:

προγανώς ισχύει ότι $\mathcal{V} \subseteq \{x \in K^n : \ x + y \in Y \text{ για όλα τα } y \in Y\}$. Επίσης, $\{x \in K^n : \ x + y \in Y \text{ για όλα τα } y \in Y\} \subseteq \mathcal{V}$, αφού αν $x \in \{x \in K^n : \ x + y \in Y \text{ για όλα τα } y \in Y\}$, τότε: $x + Y \subseteq Y$ και επειδή Y ανάγωγο αλγεβρικό σύνολο[8] τότε $x + Y = Y$).

Δηλαδή, το $\mathcal{V}$ είναι το σύνολο των κοινών ριζών στο K^n των πολυωνύμων $P_J(x+y)$ με $j \in J$ και $y \in Y$ (εδώ το x είναι μεταβλητη και $x = (x_1, \ldots, x_n) \in K^n$).

Άρα, το $\mathcal{V}$ είναι αλγεβρικό σύνολο του K^n.

Επίσης, εύκολα φαίνεται ότι το $\mathcal{V}$ είναι προσθετική ομάδα του K^n.

Άρα, λόγω του λήμματος Α΄.7.1 (πρβλ. ενότητα Α΄.7), έχουμε ότι $\mathcal{V}$ είναι διανυσματικός υπόχωρος του K^n.

Επίσης,

$$S = \bigcap_{y \in Y} (Z_{t-1} - y),$$

[7] Λόγω ορισμού του Z_t

[8] Ισχύει ότι αν Y ανάγωγο αλγεβρικό σύνολο, τότε και το $x + Y$ για $x \in K^n$ είναι ανάγωγο αλγεβρικό σύνολο

αφού,

- Αν
$$x \in \bigcap_{y \in Y} (Z_{t-1} - y),$$

τότε $\forall y \in Y : \ x \in Z_{t-1} - y$.

Οπότε, αφού $0 \in Y$, έχουμε ότι $x \in Z_{y-1} \subset S$.

Άρα,
$$\bigcap_{y \in Y} (Z_{t-1} - y) \subseteq S.$$

- Αν $x \in S$, τότε $x + Y \subset Z_{t-1}$.

Δηλαδή, για κάθε $y \in Y$, $x + y \in Z_{t-1}$. Δηλαδή,
$$x \in \bigcap_{y \in Y} (Z_{t-1} - y).$$

Άρα,
$$S \subseteq \bigcap_{y \in Y} (Z_{t-1} - y).$$

Οπότε, εύκολα συμπεραίνουμε,
$$S = \bigcap_{y \in Y} (Z_{t-1} - y) = \bigcap_{y \in Y} \bigcap_{\gamma_1 \in E} \dots \bigcap_{\gamma_{t-1} \in E} (Z - y - \gamma_1 - \ldots - \gamma_{t-1}),$$

το οποίο μας δείχνει ότι το S είναι αλγεβρικό σύνολο (τομή αλγεβρικών συνόλων με βαθμό $\leq D$, δηλαδή το σύνολο των κοινών ριζών πολυωνύμων με βαθμούς $\leq D$), με $\dim S \leq \dim Z_{t-1} = \dim Z_t$.

Επίσης, $\mathcal{V} \subseteq S$, αφού:

εύκολα βλέπουμε ότι για κάθε $x \in S$: $x + V \subset S$. Το $0 \in E \subseteq S$, άρα για $x = 0$, έχουμε το συμπέρασμα.

Για x' και x'' στοιχεία του K^n, αν $x' + Y = x'' + Y$, τότε: $x' + V = x'' + V$ [9].

Αφού το Z_{t-1} μπορεί να γραφεί ως ένωση πεπερασμένου πλήθους συνιστωσών και το $x+Y$ για $x \in S$ είναι $\subset Z_{t-1}$ (είναι και ανάγωγο αλγεβρικό σύνολο αφού το Y είναι ανάγωγο αλγεβρικό σύνολο), έχουμε ότι τα $x + Y$ για $x \in S$ είναι πεπερασμένα και άρα και οι κλάσεις $x + \mathcal{V}$, $x \in S$ είναι πεπερασμένες.

Διαλέγουμε ένα πεπερασμένο σύνολο $F = \{x_1, \ldots, x_m\}$ του K^n τέτοιο ώστε:
$$S/\mathcal{V} = (F + \mathcal{V})/\mathcal{V}.$$

[9] Έστω $x' + Y = x'' + Y$. Τότε $x' - x'' + Y = Y$, άρα, $x' - x'' \in \mathcal{V}$. Επειδή $\mathcal{V}$ προσθετική υποομάδα του K^n έχουμε ότι: $x' + \mathcal{V} = x'' + \mathcal{V}$

Τα S και $\mathcal{V}$ έχουν την ίδια διάσταση, αφού,

$$S = (x_1 + V) \cup \ldots \cup (x_m + \mathcal{V}),$$

οπότε,

$$\dim S = \dim(x_i + \mathcal{V}) = dim(\mathcal{V}) = {}^{10}n - r.$$

Το r είναι ≥ 1 αφού,

$$n - r = \dim S \leq \dim Z_t = n - t,$$

άρα, $1 \leq t \leq r$. Εφαρμόζουμε το λήμμα 5.2.3,

$$\mathrm{Card}\big((F + \mathcal{V})/\mathcal{V}\big) = \mathrm{Card}\big(S/\mathcal{V}\big) \leq D^r,$$

άρα,

$$\mathrm{Card}\big((E + \mathcal{V})/\mathcal{V}\big) \leq \mathrm{Card}\big(S/\mathcal{V}\big) \leq D^r.$$

- Έστω K τυχαίο σώμα (χαρακτηριστικής μηδέν, όχι απαραίτητα αλγεβρικά κλειστό).

Έστω λοιπόν $\overline{K}$ η αλγεβρική κλειστότητα του K^n.

Έχουμε ότι $E \subset K^n \subset \overline{K}$.

Επίσης, $P \in K[X_1, \ldots, X_n] \subset \overline{K}[X_1, \ldots, X_n]$ και $\deg P \leq D$.

Έχοντας ήδη αποδείξει, την πρόταση για αλγεβρικά κλειστό σώμα, συμπεραίνουμε ότι υπάρχει $\mathcal{V}$ διανυσματικός υπόχωρος του $\overline{K}^n$, διαστάσεως $n - r$, όπου $r \geq 1$, τέτοιος ώστε:

$$\mathrm{Card}\Big((E + \mathcal{V})/\mathcal{V}\Big) \leq D^r.$$

Θέλουμε να συμπεράνουμε την ύπαρξη ενός διανυσματικού υπόχωρου $\mathcal{V}_0$ του K^n διάστασης $n - r_0$, $r_0 \geq 1$, τέτοιου ώστε:

$$\mathrm{Card}\Big((E + \mathcal{V}_0)/\mathcal{V}_0\Big) \leq D^{r_0}.$$

Έστω $\mathcal{V}_0 = \mathcal{V} \bigcap K^n$. Εύκολα φαίνεται ότι το $\mathcal{V}_0$ είναι διανυσματικός υπόχωρος του K^n.

Ορίζουμε την απεικόνιση:

$$(E + \mathcal{V})/\mathcal{V} \ni e + \mathcal{V} \underset{\text{επί}}{\longmapsto} e + \mathcal{V}_0 \in (E + \mathcal{V}_0)/\mathcal{V}_0.$$

[10] Επειδή $\mathcal{V}$ γραμμικός χώρος η διάσταση του $\mathcal{V}$ ως αλγεβρικό σύνολο ταυτίζεται με την διάσταση του $\mathcal{V}$ ως γραμμικό χώρο

(Η απεικόνιση είναι καλά ορισμένη)

Άρα,

$$\mathrm{Card}\Big((E+\mathcal{V}_0)/\mathcal{V}_0\Big) \leq \mathrm{Card}\Big((E+\mathcal{V})/\mathcal{V}\Big) \leq D^r.$$

Αρκεί τώρα να δείξουμε ότι: $D^r \leq D^{r_0}$.

Δηλαδή αρκεί, $r_0 \geq r$, ή $n - r_0 \leq n - r$.

Αρκεί λοιπόν να δείξουμε ότι:

$$\dim_K(\mathcal{V}_0) \leq \dim_{\overline{K}}(\mathcal{V}).$$

Έστω, $v_1, \ldots, v_m$, $m \leq n$, στοιχεία του $\mathcal{V}$, $K-$γραμμικώς ανεξάρτητα.

Θα δείξουμε ότι $v_1, \ldots, v_m$, (προφανώς ανήκουν στο $\mathcal{V}$), είναι $\overline{K}-$γραμμικώς ανεξάρτητα.

Σε αντίθετη περίπτωση, υπάρχουν $\lambda_1, \ldots, \lambda_m \in \overline{K}$, όχι όλα μηδέν, τέτοια ώστε:

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = 0.$$

(Τα $v_i,\ \ i = 1, \ldots, m$, έχουν συντεταγμένες στο K).

Άρα, έχω ένα σύστημα με συντεταγμένες από το K το οποίο έχει λύση στο $\overline{K}$. Δηλαδή ο πίνακας των συντελεστών (ο οποίος έχει στοιχεία στο K) έχει τάξη $\leq m$.

Άρα το σύστημα έχει λύση στο K.

Άτοπο, αφού τα $v_1, \ldots, v_m$ έχουμε υποθέσει ότι είναι $K-$γραμμικώς ανεξάρτητα.

Άρα, τα $v_1, \ldots, v_m$ είναι $\overline{K}-$ γραμμικώς ανεξάρτητα.

□

Στην αμέσως παρακάτω πρόταση θα δούμε πως εξασφαλίζεται η γραμμική εξάρτηση των $1, \beta_1, \ldots, \beta_n$ έχοντας ως υπόθεση την σχέση

$$\mathrm{Card}\Big((Y(S_1+\mathcal{V})\Big) < (2S_1 - 1)^{r+1}.$$

Πρόταση 5.2.5. *Έστω $\beta_1, \ldots, \beta_n$ στοιχεία του K. Ορίζουμε*

$$\begin{aligned} Y :&= \mathbb{Z}^n + \mathbb{Z}(\beta_1, \ldots, \beta_n) \subset K^n \\ &= \{(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n),\ \ (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}\}. \end{aligned}$$

Τα παρακάτω είναι ισοδύναμα:

1. *Τα $1, \beta_1, \ldots, \beta_n$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα.*
2. *(α΄) Για κάθε διανυσματικό υπόχωρο $\mathcal{V}$ του K^n με συνδιάσταση $r \geq 1$, έχουμε ότι:*

$$\mathrm{rank}_{\mathbb{Z}}\Big((Y+\mathcal{V})/\mathcal{V}\Big) \geq r+1.$$

(β) Για κάθε διανυσματικό υπόχωρο $\mathcal{W}$ του K^{n+1} με συνδιάσταση $r \geq 1$, ο οποίος περιέχει το $(\beta_1, \ldots, \beta_n, -1)$, έχουμε ότι:

$$\mathrm{rank}_{\mathbb{Z}}\Big((\mathbb{Z}^{n+1} + \mathcal{W})/\mathcal{W}\Big) \geq r + 1.$$

3. *(α') Για κάθε $S \geq 1$ και για κάθε διανυσματικό υπόχωρο $\mathcal{V}$ του K^n με συνδιάσταση $r \geq 1$, έχουμε ότι:*

$$\mathrm{Card}\Big((Y(S) + \mathcal{V})/\mathcal{V}\Big) \geq (2S-1)^{r+1}.$$

(β) Για κάθε $S \geq 1$ και για κάθε διανυσματικό υπόχωρο $\mathcal{W}$ του K^{n+1} με συνδιάσταση $r \geq 1$, ο οποίος περιέχει το $(\beta_1, \ldots, \beta_n, -1)$, έχουμε ότι:

$$\mathrm{Card}\Big((\mathbb{Z}^{n+1}(S) + \mathcal{W})/\mathcal{W}\Big) \geq (2S-1)^{r+1}.$$

Απόδειξη.

Θεωρούμε την γραμμική απεικόνιση:

$$\begin{aligned} \tau:\ K^{n+1} &\underset{\text{επί}}{\longmapsto} K^n \\ (z_1, \ldots, z_n) &\longmapsto (z_1 + z_{n+1}\beta_1, \ldots, z_n + z_{n+1}\beta_n). \end{aligned}$$

(Είναι επί, αφού το γραμμικό σύστημα $x_i = z_i + z_{n+1}\beta_i,\ \ i = 1, \ldots, n$ έχει πάντα λύση στο K^{n+1}, διότι (τάξη πίνακα συντελεστών)$\leq$ (πλήθος αγνώστων).

Έχουμε επίσης ότι: $\ker(\tau) = K \cdot (\beta_1, \ldots, \beta_n, -1)$.

- 2α' $\Rightarrow$ 2β'.

Έστω $\mathcal{V}$ διανυσματικός υπόχωρος του K^n με συνδιάσταση $r \geq 1$ και $\mathrm{rank}_{\mathbb{Z}}\Big((Y + \mathcal{V})/\mathcal{V}\Big) \geq r + 1$.

Έχουμε ότι υπάρχει $\mathcal{W}$ διανυσματικός υπόχωρος του K^{n+1} με $\tau(\mathcal{W}) = \mathcal{V}$, όπου:

$$\dim \mathcal{W} = \dim \mathcal{V} + \dim \ker(\tau) = (n+1) - r.$$

Λόγω του $\mathrm{rank}_{\mathbb{Z}}\Big((Y + \mathcal{V})/\mathcal{V}\Big) \geq r + 1$, έχουμε ότι τα

$$(z^{(1)} + \lambda\beta), \ldots, (z^{(r+1)} + \lambda\beta),$$

όπου $z^{(i)} = (z_1^{(i)}, \ldots, z_n^{(i)}) \in K^n,\ \ i = 1 \ldots, r+1$, $\lambda \in \mathbb{Z}$, $\beta = (\beta_1, \ldots, \beta_n) \in K^n$, είναι $\mathbb{Z}-$γραμμικώς ανεξάρτητα στοιχεία του $(Y + \mathcal{V})/\mathcal{V}$.

Παίρνουμε τα

$$\zeta^{(1)} := (z_1^{(1)}, \ldots, z_n^{(1)}, \lambda), \ldots, \zeta^{(r+1)} := (z_1^{(r+1)}, \ldots, z_n^{(r+1)}, \lambda).$$

Θα δείξουμε ότι αυτά είναι $\mathbb{Z}-$γραμμικώς ανεξάρτητα στοιχεία του $(\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}$.

Σε αντίθετη περίπτωση υπήρχαν $a_1,\ldots,a_{r+1}\in\mathbb{Z}$ τέτοια ώστε:

$$a_1\zeta^{(1)}+\ldots+a_{r+1}\zeta^{(r+1)}\in\mathcal{W},$$

δηλαδή,

$$\tau(a_1\zeta^{(1)}+\ldots+a_{r+1}\zeta^{(r+1)})\in\tau(\mathcal{W})=\mathcal{V}.$$

Όμως,

$$\begin{aligned}\mathcal{V}\ni\tau(a_1\zeta^{(1)}+\ldots+a_{r+1}\zeta^{(r+1)})&=a_1\tau(\zeta^{(1)})+\ldots+a_{r+1}\tau(\zeta^{(r+1)})\\&=a_1(z^{(1)}+\lambda\beta)+\ldots+a_{r+1}(z^{(r+1)}+\lambda\beta).\end{aligned}$$

Άτοπο, αφού τα $(z^{(1)}+\lambda\beta),\ldots,(z^{(r+1)}+\lambda\beta)$ είναι $\mathbb{Z}-$γραμμικώς ανεξάρτητα στοιχεία του $(Y+\mathcal{V})/\mathcal{V}$.

- **2β′** $\Rightarrow$ **2α′**.

Έστω $\mathcal{W}$ διανυσματικός υπόχωρος του K^{n+1} με συνδιάσταση $r\geq 1$ και

$$\mathrm{rank}_{\mathbb{Z}}\Big((\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}\Big)\geq r+1.$$

Ορίζουμε $\mathcal{V}=\tau(\mathcal{W})$. Τότε το $\mathcal{V}$ είναι διανυσματικός υπόχωρος του K^n με συνδιάσταση $r\geq 1$ ($\dim\mathcal{V}=n-r$). Θα δείξουμε επίσης ότι

$$\mathrm{rank}_{\mathbb{Z}}\Big((Y+\mathcal{V})/\mathcal{V}\Big)\geq r+1.$$

Έστω τα στοιχεία $\eta^{(1)},\ldots,\eta^{(\rho)}\in\mathbb{Z}^{n+1}$, $\rho\geq r+1$, τα οποία $\mathrm{modulo}\mathcal{W}$ δίνουν μια βάση του $(\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}$. Αν δείξουμε ότι τα $\tau(\eta^{(1)}),\ldots,\tau(\eta^{(\rho)})$ είναι $\mathbb{Z}-$γραμμικώς ανεξάρτητα στοιχεία του $(Y+\mathcal{V})/\mathcal{V}$ τότε θα έχουμε αποδείξει το ζητούμενο.

Έστω λοιπόν ότι τα $\tau(\eta^{(1)}),\ldots,\tau(\eta^{(\rho)})$ είναι $\mathbb{Z}-$γραμμικώς εξαρτημένα στοιχεία του $(Y+\mathcal{V})/\mathcal{V}$. Τότε υπάρχουν $a_1,\ldots,a_\rho\in\mathbb{Z}$ τέτοια ώστε:

$$a_1\tau(\eta^{(1)})+\ldots+a_\rho\tau(\eta^{(\rho)})\in\mathcal{V}.$$

Δηλαδή,

$$\tau(a_1\eta^{(1)}+\ldots+a_\rho\eta^{(\rho)})=\tau(w),$$

για κάποιο $w\in\mathcal{W}$.

Οπότε,

$$(a_1\eta^{(1)}+\ldots+a_\rho\eta^{(\rho)}-w)\in\ker\tau.$$

Άρα,

$$a_1\eta^{(1)} + \ldots + a_\rho\eta^{(\rho)} + w = K \cdot (\beta_1, \ldots, \beta_n, -1) \in \mathcal{W},$$

αφού $(\beta_1, \ldots, \beta_n, -1) \in \mathcal{W}$. Άρα,

$$a_1\eta^{(1)} + \ldots + a_\rho\eta^{(\rho)} \in \mathcal{W},$$

το οποίο είναι άτοπο.

- Η απόδειξη του 3α΄$\Longleftrightarrow$3β΄ αποδεικνύεται με όμοιο τρόπο όπως το 2α΄$\Longleftrightarrow$2β΄
- 3α΄ $\Rightarrow$ 2α΄.

Έστω $e^{(1)}, \ldots, e^{(n)} \in \mathbb{Z}^n$ τα στοιχεία της κανονικής βάσης του $\mathbb{Z}^n$.

Έχουμε ότι:

$$Y = \mathbb{Z} \cdot e^{(1)} + \ldots + \mathbb{Z} \cdot e^{(n)} + \mathbb{Z} \cdot (\beta_1, \ldots, \beta_n),$$

όπου $\beta = (\beta_1, \ldots, \beta_n)$, και για $S \geq 1$

$$Y(S) = s_1e^{(1)} + \ldots + s_ne^{(n)} + s_{n+1}\beta,$$

όπου $(s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}(S)$.

Έστω $\mathcal{V}$ διανυσματικός υπόχωρος του K^n με $\mathrm{codim}(\mathcal{V}) = r \geq 1$ και για τυχαίο $S \geq 1$ υποθέτουμε ότι

$$\mathrm{Card}\Big((Y(S) + \mathcal{V})/\mathcal{V}\Big) \geq (2S-1)^{r+1}.$$

Έστω

$$\mathrm{rank}_{\mathbb{Z}}\Big((Y + \mathcal{V})/\mathcal{V}\Big) = m.$$

Υπάρχουν λοιπόν, $\underline{y}_1 + \mathcal{V}, \ldots, \underline{y}_m + \mathcal{V}$ στοιχεία του $(Y + \mathcal{V})/\mathcal{V}$, τα οποία είναι $\mathbb{Z}-$βάση του $(Y + \mathcal{V})/\mathcal{V}$ (Για $j = 1, \ldots, m$, $\underline{y}_j = s_{1,j}e^{(1)} + \ldots + s_{n,j}e^{(n)} + s_{n+1,j}\beta$).

Παίρνουμε τα στοιχεία

$$(\lambda_1\underline{y}_1 + \ldots + \lambda_m\underline{y}_m) + \mathcal{V}, \;\; \lambda_i \in \mathbb{Z}, 1 \leq i \leq m.$$

Θα μετρήσουμε τις $m-$άδες $(\lambda_1, \ldots, \lambda_m)$ τέτοιες ώστε το $\lambda_1\underline{y}_1 + \ldots + \lambda_m\underline{y}_m \in Y(S)$ [11]. Έτσι θα έχουμε μετρήσει το πλήθος των κλάσεων του $(Y(S) + \mathcal{V})/\mathcal{V}$

[11] Οι κλάσεις αυτές είναι διαφορετικές για διαφορετικά $(\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m$, λόγω της ιδιότητας των $y_i + \mathcal{V}$

[12]. Έχουμε ότι:

$$\lambda_1 \underline{y}_1 + \ldots + \lambda_m \underline{y}_m =$$
$$= \lambda_1(s_{1,1} + s_{n+1,1}e^{(1)} + \ldots + s_{n+1,1}\beta) + \ldots + \lambda_m(s_{1,m} + s_{n+1,m}e^{(1)} + \ldots + s_{n+1,m}\beta)$$
$$= (s_{1,1}\lambda_1 + \ldots + s_{1,m}\lambda_m)e^{(1)} + \ldots + (s_{n,1}\lambda_1 + \ldots + s_{n,m}\lambda_m)e^{(n)}$$
$$+ (s_{n+1,1}\lambda_1 + \ldots + s_{n+1,m}\lambda_m)\beta.$$

Αναζητούμε τις μη μηδενικές λύσεις του συστήματος:

$$\begin{pmatrix} s_{1,1} & \ldots & s_{1,m} \\ \vdots & \ddots & \vdots \\ s_{n+1,1} & \ldots & s_{n+1,m} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_{n+1} \end{pmatrix},$$

όπου $(z_1, \ldots, z_{n+1}) \in \mathbb{Z}^{n+1}(S)$.

Αν η τάξη του πίνακα είναι $< m$, τότε το αντίστοιχο ομογενές σύστημα έχει μη μηδενικές λύσεις $(\lambda_1, \ldots, \lambda_m)$. Οπότε,

$$\lambda_1(\underline{y}_1 + \mathcal{V}) + \ldots + \lambda_m(\underline{y}_m + \mathcal{V})$$
$$= (\lambda_1 \underline{y}_1 + \ldots + \lambda_m \underline{y}_m) + \mathcal{V} = 0 + \mathcal{V},$$

το οποίο είναι άτοπο, αφού τα $\underline{y}_1 + \mathcal{V}, \ldots, \underline{y}_m + \mathcal{V}$ είναι $\mathbb{Z}-$γραμμικώς ανεξάρτητα στοιχεία του $(Y + \mathcal{V})/\mathcal{V}$.
Άρα, η τάξη του πίνακα είναι m. Άρα, υπάρχει ένας $m \times m$ υποπίνακας

$$\begin{pmatrix} s_{i_1,1} & \ldots & s_{i_1,m} \\ \vdots & \ddots & \ddots \\ s_{i_m,1} & \ldots & s_{i_m,m} \end{pmatrix}$$

του οποίου η ορίζουσα δεν είναι μηδέν.

Το σύστημα

$$\begin{pmatrix} s_{i_1,1} & \ldots & s_{i_1,m} \\ \vdots & \ddots & \ddots \\ s_{i_m,1} & \ldots & s_{i_m,m} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix},$$

έχει μοναδική λύση, η οποία αντιστοιχεί σε μία η σε καμία λύση του αρχικού συστήματος. Το πλήθος των $(z_1, \ldots, z_m) \in \mathbb{Z}^m(S)$ είναι ίσο με $(2S-1)^m$. Άρα έχουμε $(2S-1)^m$ τουλάχιστον λύσεις. Δηλαδή, $(2S-1)^m$ τουλάχιστον, κλάσεις του $(Y(S) + \mathcal{V})/\mathcal{V}$.

[12] Αφού, τα στοιχεία του $(Y(S) + \mathcal{V})/\mathcal{V}$ είναι της μορφής $y + \mathcal{V}$ με $y \in Y(S)$ και $Y(S) \subset Y$

Αφού, λόγω υπόθεσης, $\mathrm{Card}\Big((Y(S)+\mathcal{V})/\mathcal{V}\Big) \geq (2S-1)^{r+1}$, συμπεραίνουμε ότι $m \geq r+1$.

- $2\acute{\beta} \Longleftrightarrow 1$.

Έστω $\mathcal{W}$ διανυσματικός υπόχωρος του K^{n+1} με συνδιάσταση $r \geq 1$ και $(\beta_1, \ldots, \beta_n, -1) \in \mathcal{W}$. Θα αποδείξουμε τα εξής:

(i) Γενικά:

$$\mathrm{rank}_{\mathbb{Z}}\Big((\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}\Big) \geq r.$$

(ii) Ο $\mathcal{W}$ είναι ρητός πάνω από το $\mathbb{Q}$, αν και μόνο αν,

$$\mathrm{rank}_{\mathbb{Z}}\Big((\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}\Big) = r.$$

Λόγω του ότι $(\beta_1, \ldots, \beta_n, -1) \in \mathcal{W}$, χρησιμοποιώντας τα (i), (ii), έχουμε την ισοδυναμία $2\acute{\beta} \Longleftrightarrow 1$.

Η απόδειξη του (i):

Έστω $e^{(1)}, \ldots, e^{(n)}$ η κανονική βάση του K^{n+1}.

Ορίζουμε

$$\begin{aligned} \tau_{\mathcal{W}}: \ K^{n+1} &\underset{\text{επί}}{\longmapsto} K^{n+1}/\mathcal{W} \\ \underline{x} &\longmapsto \underline{x}+\mathcal{W}. \end{aligned}$$

Έχουμε ότι

$$\dim\big(K^{n+1}/\mathcal{W}\big) = \dim K^{n+1} - \dim\mathcal{W} = r.$$

Έστω, χωρίς βλάβη της γενικότητας, ότι τα $e^{(1)}, \ldots, e^{(r)}$ είναι βάση του $K^{n+1}/\mathcal{W}$.

Τα $e^{(1)}, \ldots, e^{(r)}$ είναι επίσης $\mathbb{Z}-$γραμμικώς ανεξάρτητα στοιχεία του $(\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}$. Αυτό διότι αν

$$\lambda_1 e^{(1)} + \ldots + \lambda_r e^{(r)} \in \mathcal{W}, \ \ \lambda_i \in \mathbb{Z}, \ \ i = 1, \ldots, r,$$

τότε:

$$\lambda_1 e^{(1)} + \ldots + \lambda_r e^{(r)} = 0 + \mathcal{W} \in K^{n+1}/\mathcal{W}.$$

Άτοπο.

Άρα,

$$\mathrm{rank}_{\mathbb{Z}}\Big((\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}\Big) \geq r.$$

Η απόδειξη του (ii):

Υποθέτουμε ότι $\mathcal{W}$ είναι διανυσματικός υπόχωρος του K^{n+1} με $\mathrm{codim}(\mathcal{W}) = r \geq 1$.

Έστω $e^{(1)}, \ldots, e^{(n)}$ η κανονική βάση του K^{n+1} και $e^{(1)}, \ldots, e^{(r)}$, η βάση του

$K^{n+1}/\mathcal{W}$.

Έστω

$$\mathrm{rank}_{\mathbb{Z}}\Big((\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}\Big)=r.$$

Τότε, για κάθε $r+1\leq j\leq n$ υπάρχουν $\alpha_{1j},\ldots,\alpha_{rj}\in\mathbb{Q}$, τέτοια ώστε:

$$\alpha_{1j}e^{(1)}+\ldots+\alpha_{rj}e^{(r)}+e^{(j)}\in\mathcal{W},\ \ r+1\leq j\leq n.$$

Δηλαδή, το $\mathcal{W}$ παράγεται από τα $n+1-r$ στοιχεία:

$$(\alpha_{1j},\ldots,\alpha_{rj},0,\ldots,0,1,0,\ldots,0)\in\mathbb{Q}^{n+1},\ \ r+1\leq j\leq n.$$

Δηλαδή, ο $\mathcal{W}$ είναι ρητός πάνω από το $\mathbb{Q}$.

Αντίστροφα, έστω ότι $\mathcal{W}$ είναι ρητός πάνω από το $\mathbb{Q}$. Τότε (λόγω του λήμματος Α΄.7.2) ο $\mathcal{W}$ είναι ο χώρος λύσεων του ομογενούς συστήματος:

$$\begin{array}{ccccc} a_{11}x_1 & +\ldots+ & a_{1,n+1}x_{n+1} & = & 0\\ \vdots & & & & \vdots\\ a_{m1}x_1 & +\ldots+ & a_{m,n+1} & = & 0, \end{array}$$

όπου $a_{ij}\in\mathbb{Z}$.

Αφού $\mathrm{codim}(\mathcal{W})=r\geq 1$, έχουμε ότι $r\leq m,n+1$. Υπάρχουν λοιπόν, $\underline{\alpha}_1,\ldots,\underline{\alpha}_r$ $\mathbb{Z}-$γραμμικώς ανεξάρτητες γραμμές (του πίνακα συντελεστών του συστήματος) οι οποίες παράγουν το χώρο γραμμών Ω του συστήματος. Κάθε $\underline{x}\in\mathbb{Z}^{n+1}$ γράφεται ως εξής (γνωστό από την Γραμμική Αλγεβρα):

$$\underline{x}=\underline{w}+\underline{\omega},\ \ \text{όπου } \underline{w}\in\mathcal{W} \text{ και } \underline{\omega}\in\Omega.$$

Συμπεραίνεται λοιπόν, ότι:

$$\mathrm{rank}_{\mathbb{Z}}\Big((\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}\Big)=r.$$

- $1\Rightarrow 3\acute{6}$.

Υποθέτουμε ότι

$$\mathrm{Card}\Big((\mathbb{Z}^{n+1}(S)+\mathcal{W})/\mathcal{W}\Big)<(2S-1)^{r+1}.$$

Έστω η κανονική απεικόνιση,

$$\sigma_{\mathcal{W}}:\ \ K^{n+1}\underset{\text{επί}}{\longrightarrow}\ K^{n+1}/\mathcal{W}.$$

Έστω επίσης, $\{e^{(1)},\ldots,e^{(n+1)}\}$ η κανονική βάση του K^{n+1}. Υπάρχει ένα υποσύνολο $\{i_1,\ldots,i_r\}$ του $\{1,\ldots,n+1\}$, τέτοιο ώστε το $\{\sigma_{\mathcal{W}}(e^{(i_1)}),\ldots,\sigma_{\mathcal{W}}(e^{(i_r)})\}$

να είναι βάση του $K^{n+1}/\mathcal{W}$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $\{i_1, \ldots, i_r\} = \{1, \ldots, r\}$.

Έστω j, με $r+1 \leq j \leq n+1$. Θεωρούμε τα $\underline{s} \in \mathbb{Z}^{n+1}(S)$, όπου $s_i = 0$ για $r+1 \leq i \leq n+1$ και $i \neq j$.
Τα στοιχεία:

$$\sigma_{\mathcal{W}}(s_1 e^{(1)} + \ldots + s_r e^{(r)} + s_j e^{(j)}), \;\; (s_1, \ldots, s_r, s_j) \in \mathbb{Z}^{r+1}(S),$$

ανήκουν στο $(\mathbb{Z}^{n+1}(S) + \mathcal{W})/\mathcal{W}$.

Επειδή $\mathrm{Card}\big(\mathbb{Z}^{r+1}(S)\big) = (2S-1)^{r+1} > \mathrm{Card}\Big((\mathbb{Z}^{n+1}(S) + \mathcal{W})/\mathcal{W}\Big)$, έχουμε ότι τα στοιχεία αυτά δεν είναι διαφορετικά ανα δύο. Οπότε (Αρχή του Περιστερώνα) υπάρχει μια σχέση της μορφής:

$$\alpha_{1j} e^{(1)} + \ldots + \alpha_{rj} e^{(r)} + e^{(j)} \in \mathcal{W},$$

με $\alpha_{ij} \in \mathbb{Q}$. Αυτό σημαίνει ότι το $\mathcal{W}$ παράγεται από τα $n+1-r$ στοιχεία:

$$(\alpha_{1j}, \ldots, \alpha_{rj}, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Q}^{n+1}, \;\; r+1 \leq j \leq n+1.$$

Αφού $n+1-r = \dim \mathcal{W} < n+1$, ο $(n+1-r) \times (n+1)$ πίνακας:

$$\begin{pmatrix} \alpha_{1,r+1} & \ldots & \alpha_{r,r+1} & 1 & 0 & \ldots & 0 \\ \alpha_{1,r+2} & \ldots & \alpha_{r,r+2} & 0 & 1 & \ldots & 0 \\ \vdots & \ddots & \ldots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{1,n+1} & \ldots & \alpha_{r,n+1} & 0 & 0 & \ldots & 1 \end{pmatrix}$$

είναι τάξης $n+1-r < n+1$. Άρα, υπάρχουν $(b_1, \ldots, b_{n+1}) \neq 0$, τέτοια ώστε:

$$b_1 z_1 + \ldots + b_{n+1} z_{n+1} = 0, \text{ για όλα τα } z \in \mathcal{W}.$$

Δηλαδή ο $\mathcal{W}$ είναι διανυσματικός υπόχωρος του K^{n+1} ο οποίος παράγεται από στοιχεία του $\mathbb{Q}^{n+1}$. Άρα, ο $\mathcal{W}$ είναι ρητός πάνω από το $\mathbb{Q}$ (πρβλ. Α΄.7.2). Επειδή το $(\beta_1, \ldots, \beta_n, -1) \in \mathcal{W}$, έπεται η (μη τετριμμένη) γραμμική εξάρτηση των $1, \beta_1, \ldots, \beta_n$ υπερ το $\mathbb{Q}$. □

5.3 Απαλοιφή της μεταβλητής Y

Σε αυτή την ενότητα θα δείξουμε ότι η ύπαρξη πολυωνύμου $P \in K[X_1, \ldots, X_n, Y]$, το οποίο μηδενίζεται στο $Y(S)$, για $S = S' + S'' - 1$, [13] συνεπάγεται την ύπαρξη ενός πολυωνύμου $Q \in K[X_1, \ldots, X_n]$ (απαλοιφή της μεταβλητής Y),

[13] θα δείξουμε ακριβώς ποια είναι η σχέση των S, S', S'' και ποιες συνθήκες πρέπει να ικανοποιούν

το οποίο μηδενίζεται στο $Y(S'')$ (θα αποδείξουμε, δηλαδή, τον ισχυρισμό του 2ου βήματος).

Συγκεκριμένα έχουμε το εξής

Λήμμα 5.3.1. *Έστω $\alpha_1, \ldots, \alpha_{n+1}$ μη μηδενικά στοιχεία του K και $\beta_1, \ldots, \beta_n$ στοιχεία του K. Έστω επίσης L_0, L_1, S', S'' θετικοί ρητοί ακέραιοι. Ορίζουμε $S = S' + S'' - 1$, με $S'' = \lceil \frac{S}{2} \rceil$ (άρα $S' = S - \lceil \frac{S}{2} \rceil + 1$), και υποθέτουμε ότι*

$$\mathrm{Card}\big\{\sigma(\alpha_1^{s'_1} \cdots \alpha_{n+1}^{s'_{n+1}}),\ \ \underline{s}' \in \mathbb{Z}^{n+1}(S')\big\} > L_1.$$

Υποιθέτουμε επίσης ότι υπάρχει μη μηδενικό πολυώνυμο $P \in K[X_1, \ldots, X_n, Y]$, με $\deg_{\underline{X}}(P) \leq L_0$ και $\deg_Y(P) \leq L_1$, τέτοιο ώστε:

$$P(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n, \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}) = 0 \ \ \textit{για κάθε}\ \ \underline{s} \in \mathbb{Z}^{n+1}(S).$$

Τότε υπάρχει μη μηδενικό πολυώνυμο $Q \in K[X_1, \ldots, X_n]$ με $\deg_{\underline{X}}(Q) \leq 2L_0L_1$, τέτοιο ώστε:

$$Q(s''_1 + s''_{n+1}\beta_1, \ldots, s''_n + s''_{n+1}\beta_n) = 0, \ \ \textit{για κάθε}\ \ \underline{s''} \in \mathbb{Z}^{n+1}(S'').$$

Παρατήρηση: Το λήμμα 5.3.1 ολοκληρώνει την απόδειξη της πρότασης 5.1.1 στην περίπτωση $n = 1$ (θεώρημα Gelfond-Schneider).

Πριν την απόδειξη θα χρειαστούμε δύο λήμματα. Το λήμμα 5.3.2 αναφέρεται στην απαλείφουσα πολυωνύμων και μέσω αυτού προκύπτει το αποτέλεσμα του λήμματος 5.3.1. Το λήμμα 5.3.3 χρειάζεται για τις τεχνικές λεπτομέρειες της απόδειξης του λήμματος 5.3.1.

Λήμμα 5.3.2. *Έστω πολυώνυμα $P_1, \ldots, P_r \in K[X_1, \ldots, X_n, Y]$, με $\deg_{\underline{X}}(P_i) \leq L_0$ και $\deg_Y(P_i) \leq L_1$. Υποθέτουμε επίσης ότι τα $P_i,\ \ i = 1, \ldots, r$, δεν έχουν κοινό ανάγωγο παράγοντα στο $K[X_1, \ldots, X_n, Y]$ με βαθμό ≥ 1 στην μεταβλητή Y.*

Έστω $(\xi_j, \eta_j) \in K^n \times K,\ \ j \in J$, οι κοινές ρίζες των $P_i,\ \ i = 1, \ldots, r$.

Τότε υπάρχει ένα μη μηδενικό πολυώνυμο στο $K[X_1, \ldots, X_n]$ με $\deg_{\underline{X}} \leq 2L_0L_1$, το οποίο μηδενίζεται σε όλα τα σημεία $\xi_j \in K^n,\ \ j \in J$.

Απόδειξη. Εισάγουμε $2r$ νέες μεταβλητές

$$U_1, \ldots, U_r, V_1, \ldots, V_r.$$

Ορίζουμε δύο νέα πολυώνυμα G και H στον δακτύλιο

$$A = K[U_1, \ldots, U_r, V_1, \ldots, V_r, X_1, \ldots, X_n, Y],$$

ως εξής:

$$G = \sum_{i=1}^{r} U_i P_i(X_1, \ldots, X_n, Y), \;\; H = \sum_{i=1}^{r} V_i P_i(X_1, \ldots, X_n, Y).$$

Έστω

$$R \in K[U_1, \ldots, U_r, V_1, \ldots, V_r, X_1, \ldots, X_n],$$

η *απαλείφουσα* των πολυωνύμων G και H που αντιστοιχεί στην μεταβλητή Y.

Έχουμε τα εξής:

(1) Το $R \neq 0$.

Διαφορετικά, δηλαδή αν $R = 0$, τα G και H έχουν κοινό παράγοντα F στον δακτύλιο A με βαθμό ≥ 1 ως προς την μεταβλητή Y.
Επειδή $Q|G$, το Q δεν εξαρτάται από τα V_i [14]. Επίσης, αφού $Q|H$, το Q δεν εξαρτάται από τα U_i.
Το Q λοιπόν δεν εξαρτάται από τα V_i, U_i, άρα αφού $Q|G, H$ έπεται ότι $Q|P_i$ στο $K[X_1, \ldots, X_n, Y]$, για κάθε $i = 1, \ldots, r$.
Άτοπο, λόγω υπόθεσης.

(2) Έχουμε ότι: $\deg_{\underline{X}}(R) \leq 2L_0L_1$.

Στον δακτύλιο $K[U_1, \ldots, U_r, V_1, \ldots, V_r, X_1, \ldots, X_n][Y]$ γράφουμε τα πολυώνυμα G και H ως εξής:

$$G = g_0 + g_1 Y + \ldots + g_k Y^k, \;\; H = h_0 + h_1 Y + \ldots + g_l Y^l,$$

όπου $g_i, h_j \in K[U_1, \ldots, U_r, V_1, \ldots, V_r, X_1, \ldots, X_n]$, $i = 1, \ldots, k, j = 1, \ldots, j$ και $k, l \leq L_1$.

Γνωρίζουμε ότι:

$$R = \det \begin{pmatrix} g_0 & g_1 & \ldots & g_k & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{k-1} & g_k & \ldots & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & \ldots & g_0 & g_1 & \ldots & g_k \\ h_0 & h_1 & \ldots & h_l & 0 & \ldots & 0 \\ 0 & h_0 & \ldots & h_{l-1} & h_l & \ldots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \ldots & 0 & h_0 & \ldots & h_{l-1} & h_l \end{pmatrix} \in K[\underline{U}, \underline{V}, \underline{X}]^{(l+k)\times(l+k)},$$

$\underline{U} = (U_1, \ldots, U_r), \;\; \underline{V} = (V_1, \ldots, V_r), \;\; \underline{X} = (X_1, \ldots, X_r).$

[14] Είναι γνωστό το εξής: Αν $h \in D[X], D$ ακέραια περιοχή, και $h = fg$, $f, g \in D[X]$, με $\deg_X h = 0$, τότε και $\deg_X f = \deg_X g = 0$

Αν αναπτύξουμε την ορίζουσα R, θα έχουμε:

$$R = \sum_{\sigma \in \mathbb{S}_{k+l}} \operatorname{sgn}(\sigma) \underbrace{r_{1\sigma(1)} \cdots r_{(k+l)\sigma(k+l)}}_{\deg_{\underline{X}} \leq 2L_0L_1}{}^{15},$$

άρα και $\deg_{\underline{X}}(R) \leq 2L_0L_1$.

(3) Για κάθε $j \in J$ έχουμε ότι $R(U_1, \ldots, U_r, V_1, \ldots, V_r, \xi_j) = 0$, $(\xi_j \in K^n)$.

Είναι γνωστό ότι υπάρχουν πολυώνυμα

$$F_1, F_2 \in K[U_1, \ldots, U_r, V_1, \ldots, V_r, X_1, \ldots, X_n][Y] \text{ με } R = F_1G + F_2H.$$

Οπότε συμπεραίνουμε ότι

$$R(U_1, \ldots, U_r, V_1, \ldots, V_r, \xi_j) = 0.$$

Εκφράζουμε το R στον δακτύλιο $K[X_1, \ldots, X_n][U_1, \ldots, U_r, V_1, \ldots, V_r]$. Αν διαλέξουμε ένα από τους συντελεστές του μονωνύμου $U_1^{i_1} \cdots U_r^{i_r} \cdot V_1^{j_1} \cdots V_r^{j_r}$, έχουμε το ζητούμενο πολυώνυμο του λήμματος.

□

Λήμμα 5.3.3. *Έστω $Q \in K[X_1, \ldots, X_n, Y]$ ένα ανάγωγο πολυώνυμο με $\deg_Y(Q) \geq 1$. Έστω $u_1, \ldots, u_n, v, \lambda$ στοιχεία του K με $\lambda \neq 0$ και το v δεν είναι ρίζα της μονάδας. Υποθέτουμε ότι:*

$$Q(X_1 + u_1, \ldots, X_n + u_n, vY) = \lambda Q(X_1, \ldots, X_n, Y).$$

Τότε $Q = cY$, $c \in K, c \neq 0$.

Απόδειξη. Γράφουμε το Q στο $K[X_1, \ldots, X_n][Y]$, ως εξής:

$$Q(X_1, \ldots, X_n, Y) = \sum_{i=0}^{d} \alpha_i(X_1, \ldots, X_n) Y^i,$$

όπου $\alpha_i(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, $i = 1, \ldots, d$.

Από την υπόθεση έχουμε ότι

$$\sum_{i=0}^{d} \alpha_i(X_1 + u_1, \ldots, X_n + u_n) v^i Y^i = \lambda \sum_{i=0}^{d} \alpha_i(X_1, \ldots, X_n) Y^i.$$

Δηλαδή,

$$\alpha_i(X_1 + u_1, \ldots, X_n + u_n) v^i = \lambda \alpha_i(X_1, \ldots, X_n), \text{ για κάθε } i = 1, \ldots, d.$$

[15] αφού $k + l \leq 2L_1$ και $\deg_{\underline{X}} G$, $\deg_{\underline{X}} H \leq L_0$

Αν επικεντρωθούμε στον ομογενή όρο με τον μεγαλύτερο βαθμό, βλέπουμε ότι για κάθε $i = 1, \ldots, d$, με $\alpha_i(X_1, \ldots, X_n) \neq 0$, $v^i = \lambda$.

Επειδή όμως το v δεν είναι ρίζα της μονάδας, δεν γίνεται για $i \neq j$ (έστω $i > j$) να έχουμε ότι: $v^i = \lambda$ και $v^j = \lambda$. Αυτό διότι τότε $v^{i-j} = 1$, άτοπο.

Άρα, υπάρχει ένα και μόνο i για το οποίο $v^i = \lambda$ και $\alpha_i(X_1, \ldots, X_n) \neq 0$.

Επίσης, το i δεν είναι 0, διότι το Q είναι βαθμού≥ 1 στο Y.

Άρα,

$$Q(X_1, \ldots, X_n, Y) = \alpha_i(X_1, \ldots, X_n)Y^i,$$

όπου $\alpha_i(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$.

Επειδή όμως το Q είναι ανάγωγο έχουμε ότι

$$Q(X_1, \ldots, X_n, Y) = cY, \text{ με } c \in K, \ c \neq 0.$$

□

Απόδειξη του λήμματος 5.3.1.

Προφανώς μπορούμε να υποθέσουμε ότι το Y δεν διαιρεί το P και ότι $\deg_Y(P) \geq 1$.[16]

Για $\underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}$, ορίζουμε τον αυτομορφισμό δακτυλίων

$$T_{\underline{s}} : \ K[X_1, \ldots, X_n, Y] \longrightarrow K[X_1, \ldots, X_n, Y]$$
$$F(X_1, \ldots, X_n, Y) \longmapsto F(X_1 + s_1 + s_{n+1}\beta_1, \ldots, X_n + s_n + s_{n+1}\beta_n, \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}} Y),$$

με $T_{\underline{s}}^{-1} = T_{-\underline{s}}$.

Συνεπώς, η εικόνα, μέσω του $T_{\underline{s}}$, ενός ανάγωγου πολυωνύμου είναι ανάγωγο πολυώνυμο και οι βαθμοί των F και $T_{\underline{s}}(F)$ είναι ίδιοι.

1. Θα δείξουμε ότι τα πολυώνυμα $T_{\underline{s'}}(P)$, για $\underline{s'} \in \mathbb{Z}^{n+1}(S')$[17], δεν έχουν κοινό ανάγωγο παράγοντα με $\deg_Y \geq 1$.

Έστω

$$P = F_0 \prod_{i=1}^{k} F_i^{r_i},$$

η ανάλυση του P σε ανάγωγα στον δακτύλιο $K[X_1, \ldots, X_n][Y]$ (η ανάλυση είναι μοναδική κατά προσέγγιση σταθερών παραγόντων) , όπου $F_0 \in K[X_1, \ldots, X_n]$ (δεν εξαρτάται από το Y) και για $1 \leq i \leq k$ το F_i είναι ανάγωγο πολυώνυμο στο $K[X_1, \ldots, X_n, Y]$ με $\deg_Y \geq 1$. Επίσης, λόγω ορισμού του P, έχουμε ότι

[16] Αν $deg_Y(P) = 0$, τότε το ζητούμενο πολυώνυμο Q είναι το ίδιο το P

[17] Το S' είναι εκείνο για το οποίο ισχύει από την υπόθεση του λήμματος ότι: $\mathrm{Card}\{\sigma(\alpha_1^{s'_1} \cdots \alpha_{n+1}^{s'_{n+1}}), \ \underline{s'} \in \mathbb{Z}^{n+1}(S')\} > L_1$

$1 \leq k \leq L_1$.
Επίσης, λόγω του ομομορφισμού,

$$T_{\underline{s}'}(P) = T_{\underline{s}'}(F_0) \cdot \prod_{i=1}^{k} (T_{\underline{s}'}(F_i))^{r_i},$$

όπου $T_{\underline{s}'}(F_0) \in K[X_1, \ldots, X_n]$ (δεν εξαρτάται από το Y) και επίσης, για $1 \leq i \leq k$ το $T_{\underline{s}'}(F_i)$ είναι ανάγωγο πολυώνυμο στο $K[X_1, \ldots, X_n, Y]$ με $\deg_Y(T_{\underline{s}'}) \geq 1$.

Θα δείξουμε ότι δεν υπάρχει ανάγωγο πολυώνυμο $F \in K[X_1, \ldots, X_n, Y]$, με $\deg_{\mathrm{Y}}(\mathrm{F}) > 0$, που να διαιρεί όλα τα $T_{\underline{s}'}(P)$, με $\underline{s}' \in \mathbb{Z}^{n+1}(S')$. Πράγματι, ας υποθέσουμε το αντίθετο.

Τότε για κάθε τέτοιο $\underline{s}'$ υπάρχει δείκτης $i(\underline{s}')$ με $1 \leq i(\underline{s}') \leq k$ και ένα μη μηδενικό στοιχείο $c_{\underline{s}'}$ του K, τέτοια ώστε:

$$F = c_{\underline{s}'} \cdot T_{\underline{s}'}(F_{i(\underline{s}')}).$$

Θεωρούμε την απεικόνιση

$$\begin{aligned} \varrho : \ \mathbb{Z}^{n+1}(S') &\longrightarrow \{1, \ldots, k\} \times K^*/K^*_{\mathrm{tors}} \\ \underline{s}' &\longmapsto \big(i(\underline{s}'), \sigma(\alpha_1^{s'_1} \cdots \alpha_{n+1}^{s'_{n+1}})\big). \end{aligned}$$

Είναι γνωστό ότι το πλήθος των $\underline{s}'$ είναι $(2S'-1)^n$, το οποίο είναι μεγαλύτερο του L_1 (λόγω της υπόθεσης ότι $S^n > L_1$ και $S+1 < 2S' < 2S+2$). Το πλήθος των $i(\underline{s}')$ είναι $k \leq L_1$, ενώ ο πληθος των στοιχείων του συνόλου $\{\sigma(\alpha_1^{s'_1} \cdots \alpha_{n+1}^{s'_{n+1}}),\ \ \underline{s}' \in \mathbb{Z}^{n+1}(S')\}$ είναι, λόγω υπόθεσης, $> L_1$. Άρα, από την αρχή του περιστερώνα, έχουμε ότι υπάρχουν δύο διαφορετικά $\underline{s}' \in \mathbb{Z}^{n+1}(S')$, έστω $\underline{s}'^{(1)}, \underline{s}'^{(2)}$ για τα οποία ισχύουν τα εξής:

(α) Οι δείκτες $i(\underline{s}'^{(1)}), i(\underline{s}'^{(2)})$ είναι ίσοι, έστω i_0 η κοινή τιμή,

και

(β) Τα στοιχεία $\sigma(\alpha_1^{s'^{(1)}_1}, \ldots, \alpha_{n+1}^{s'^{(1)}_{n+1}}), \sigma(\alpha_1^{s'^{(2)}_1}, \ldots, \alpha_{n+1}^{s'^{(2)}_{n+1}})$, είνα διαφορετικά.

Η διαφορά, $\underline{s}' = \underline{s}'^{(1)} - \underline{s}'^{(2)}$, είναι ένα μη μηδενικό στοιχείο του $\mathbb{Z}^{n+1}$.

Επίσης, αφού $F = c_{\underline{s}'^{(1)}} T_{\underline{s}'^{(1)}}(F_{i_0})$ και $F = c_{\underline{s}'^{(2)}} T_{\underline{s}'^{(2)}}(F_{i_0})$, έχουμε ότι:

$$c_{\underline{s}'^{(1)}} T_{\underline{s}'^{(1)}}(F_{i_0}) = c_{\underline{s}'^{(2)}} T_{\underline{s}'^{(2)}}(F_{i_0}).$$

Άρα,

$$T_{-\underline{s}'^{(1)}}\Big(c_{\underline{s}'^{(1)}} T_{\underline{s}'^{(1)}}(F_{i_0})\Big) = T_{-\underline{s}'^{(1)}}\Big(c_{\underline{s}'^{(2)}} T_{\underline{s}'^{(2)}}(F_{i_0})\Big),$$

ή,

$$c_{\underline{s}'(1)} T_{-\underline{s}'(1)} \Big(T_{\underline{s}'(1)}(F_{i_0}) \Big) = c_{\underline{s}'(2)} T_{-\underline{s}'(1)} \Big(T_{\underline{s}'(2)}(F_{i_0}) \Big),$$

δηλαδή,

$$T_{\underline{s}'} = \frac{c_{\underline{s}'(2)}}{c_{\underline{s}'(1)}} F_{i_0},$$

όπου, $\frac{c_{\underline{s}'(2)}}{c_{\underline{s}'(1)}} = \lambda \in K^*$.

Επίσης, επειδή τα $\sigma(\alpha_1^{s_1'(1)}, \ldots, \alpha_{n+1}^{s_{n+1}'(1)}), \sigma(\alpha_1^{s_1'(2)}, \ldots, \alpha_{n+1}^{s_{n+1}'(2)})$, είναι διαφορετικά έχουμε ότι

$$\alpha_1^{s_1'(1)}, \ldots, \alpha_{n+1}^{s_{n+1}'(1)} K^*_{\text{tors}} \neq \alpha_1^{s_1'(2)}, \ldots, \alpha_{n+1}^{s_{n+1}'(2)}) K^*_{\text{tors}},$$

δηλαδή το

$$\alpha_1^{s_1'}, \ldots, \alpha_{n+1}^{s_{n+1}'}$$

δεν είναι ρίζα της μονάδας.

Εφαρμόζουμε το λήμμα 5.3.3 για το F_{i_0} με

$$u_i = s_i + s_{n+1}\beta_i, \;\; i = 1, \ldots, n$$
$$v = \alpha_1^{s_1'}, \ldots, \alpha_{n+1}^{s_{n+1}'}.$$

Έπεται λοιπόν, ότι $F_{i_0} = c \cdot Y$, $c \in K^*$.
Δηλαδή, το $P = F_0 \prod_{i=1}^{k} F_i^{r_i}$ διαιρείται με Y.
Άτοπο, λόγω υπόθεσης.
Άρα, τα πολυώνυμα $T_{\underline{s}'}(P)$, για $\underline{s}' \in \mathbb{Z}^{n+1}(S')$, δεν έχουν κοινό ανάγωγο παράγοντα με $\deg_Y \geq 1$.

2. Εδώ, θα δείξουμε την ύπαρξη του πολυωνύμου $Q \in K[X_1, \ldots, X_n]$, με $\deg_{\underline{X}} \leq 2L_0L_1$, το οποίο μηδενίζεται στο σύνολο:

$$\big\{ (s_1'' + s_{n+1}''\beta_1, \ldots, s_n'' + s_{n+1}''\beta_n, \alpha_1^{s_1''} \cdots \alpha_{n+1}^{s_{n+1}''}), \;\; \underline{s}'' \in \mathbb{Z}^{n+1}(S'') \big\}.$$

Αυτό μας το εξασφαλίζει το λήμμα 5.3.2, όπου

$$\{P_1, \ldots, P_r\} = \{T_{\underline{s}'}(P), \;\; \underline{s}' \in \mathbb{Z}^{n+1}(S')\}$$

και

$$\{(\xi_j, \eta_j), \;\; j \in J\} = \big\{ (s_1'' + s_{n+1}''\beta_1, \ldots, s_n'' + s_{n+1}''\beta_n, \alpha_1^{s_1''} \cdots \alpha_{n+1}^{s_{n+1}''}), \;\; \underline{s}'' \in \mathbb{Z}^{n+1}(S'') \big\}$$
$$\subset K^n \times K^*.$$

(Το τυχαίο P_i είναι της μορφής

$$P_i = T_{\underline{s}'}(P) = P(X_1 + s'_1 + s'_{n+1}\beta_1, \ldots, X_n + s'_n + s'_{n+1}\beta_n, \alpha_1^{s'_1} \cdots \alpha_{n+1}^{s'_{n+1}} Y).$$

Οπότε,

$$\begin{aligned} &P_i(s''_1 + s''_{n+1}\beta_1, \ldots, s''_n + s''_{n+1}\beta_n, \alpha_1^{s''_1} \cdots \alpha_{n+1}^{s''_{n+1}}) \\ &= P\big((s'_1 + s''_1) + (s'_{n+1} + s''_{n+1})\beta_1, \ldots, (s'_n + s''_n) + (s'_{n+1} + s''_{n+1})\beta_n, \alpha_1^{s'_1+s''_1} \cdots \alpha^{s'_{n+1}+s''_{n+1}}\big) \\ &= 0, \end{aligned}$$

αφού $\underline{s}' + \underline{s}'' \in \mathbb{Z}^{n+1}(S)$ για $\underline{s}' \in \mathbb{Z}^{n+1}(S')$, $\underline{s}'' \in \mathbb{Z}^{n+1}(S'')$, διότι $S = S' + S'' - 1$).

□

Κεφάλαιο 6

Η απόδειξη του θεωρήματος του Baker

Σε αυτό το κεφάλαιο θα αποδείξουμε το θεώρημα του Baker. Συγκεκριμένα θα αποδείξουμε το θεώρημα 1.2.2, το οποίο, όπως αποδείξαμε στο κεφάλαιο 1, είναι ισοδύναμο με το θεώρημα του Baker. Δηλαδή, θα αποδείξουμε το εξής:

Αν $\ell_1, \ldots, \ell_{n+1}$, $\mathbb{Q}-$*γραμμικώς ανεξάρτητα στοιχεία του* $\mathfrak{L}$ *και* $\beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ *με*

$$\ell_{n+1} = \beta_1\ell_1 + \ldots + \beta_n\ell_n, \tag{6.1}$$

τότε $1, \beta_1, \ldots, \beta_n$ *είναι* $\mathbb{Q}-$*γραμμικώς εξαρτημένα.*

- **Βήμα 1ο. Υποθέσεις.**

Έστω, $\ell_1, \ldots, \ell_{n+1}$, $\mathbb{Q}-$γραμμικώς ανεξάρτητα στοιχεία του $\mathfrak{L}$ και $\beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$. Υποθέτουμε επίσης,

$$\ell_{n+1} = \beta_1\ell_1 + \ldots + \beta_n\ell_n.$$

Για $1 \leq i \leq n+1$, ορίζουμε $\alpha_i = \mathrm{e}^{\ell_i}$.

- **Βήμα 2ο. Επιλογή των παραμέτρων.**

Θα συμβολίζουμε με c ένα αρκετά μεγάλο πραγματικό αριθμό, ο οποίος εξαρτάται μόνο από τα $n, \ell_1, \ldots, \ell_{n+1}, \beta_1, \ldots, \beta_n$ [1].

Επιλέγουμε τρεις θετικούς ρητούς ακεραίους L_0, L_1 και S, οι οποίοι ικανοποιούν τις σχέσεις

$$L_0 \geq 2, \;\; L_1 \geq 2, \;\; S \geq 2$$
$$cL_0 \log S \leq L^{1/n}, \;\; cL_1S \leq L^{1/n}, \;\; c(L_0L_1)^n \leq S^{n+1},$$

[1] Η εξάρτηση του c από τα $n, \ell_1, \ldots, \ell_{n+1}, \beta_1, \ldots, \beta_n$, θα φανεί στην απόδειξη παρακάτω όταν θα προσδιορισθεί το c σε σχέση με τα c_1, c_2

με $L := \binom{L_0+n}{n}(L_1+1)$.

(Μπορούμε να επιλέξουμε το S όσο μεγάλο θέλουμε. Για n σταθερό και c αρκετά μεγάλο μπορούμε να βρούμε L_0 και L_1 τα οποία να ικανοποιούν τις παραπάνω ανισότητες.
Για παράδειγμα, μπορούμε να πάρουμε:

$$L_0 = [S^{1+1/n}(\log S)^{-3n}] \quad \text{και} \quad L_1 = [\log S]^{2n}.$$

Οι τρεις πρώτες ανισότητες ($L_0 \geq 2,\ \ L_1 \geq 2,\ \ S \geq 2$) ικανοποιούνται για S αρκούντως μεγάλο.
Για να ικανοποιείται η ανισότητα ($cL_0 \log S \leq L$) αρκεί $c \leq \log S$, το οποίο για αρκούντως μεγάλο S ισχύει.
Για να ικανοποιείται η ανισότητα $c(L_0L_1)^n \leq S^{n+1}$ αρκεί $\frac{c}{(\log S)^2} \leq S^{n-1}$, το οποίο για αρκούντως μεγάλο S ισχύει.
Όμοια ισχύει και η άλλη ανισότητα για ακούντως μεγάλο S.)

- **Βήμα 3ο. Καθορισμός της ορίζουσας Δ.**

  Θεωρούμε τον $L \times (2S-1)^{n+1}$ πίνακα Π, (πρβλ. ενότητα 2.1),

$$\Pi = \Big((s_1 + s_{n+1}\beta_1)^{\lambda_1} \cdots (s_n + s_{n+1}\beta_n)^{\lambda_n}(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}})^{\lambda_{n+1}}\Big)_{\underline{\lambda},\underline{s}},$$

όπου ο δείκτης των γραμμών είναι $\underline{\lambda}$ και ο δείκτης των στηλών είναι $\underline{s}$. Το $\underline{\lambda}$ διατρέχει τις $(n+1)-$άδες $(\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$, όπου $\lambda_1 + \ldots + \lambda_n \leq L_0$ και $\lambda_{n+1} \leq L_1$. Το $\underline{s}$ διατρέχει όλα τα στοιχεία του $\mathbb{Z}^{n+1}(S)$.

Έστω $\underline{s}^{(1)}, \ldots, \underline{s}^{(L)}$ [2] τυχαία στοιχεία του $\mathbb{Z}^{n+1}(S)$.
Θεωρούμε την $L \times L$ υποορίζουσα του πίνακα Π:

$$\Delta = \det\Big((s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1)^{\lambda_1} \cdots (s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n)^{\lambda_n}\big(\alpha_1^{s_1^{(\mu)}} \cdots \alpha_{n+1}^{s_{n+1}^{(\mu)}}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\mu},$$

όπου $1 \leq \mu \leq L$.

- **Βήμα 4ο. Άνω φράγμα για την $|\Delta|$.**

  Από την υπόθεση (6.1) έχουμε ότι:

$$\alpha_1^{s_1+s_{n+1}\beta_1} \cdots \alpha_n^{s_n+s_{n+1}\beta_n} = \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}},$$

(εδώ είναι το μόνο σημείο της απόδειξης στο οποίο χρησιμοποιείται η υπόθεση (6.1))

οπότε,

$$\Delta = \det\Big((s_1^{(\mu)}+s_{n+1}^{(\mu)}\beta_1)^{\lambda_1} \ldots (s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n)^{\lambda_n}\big(\alpha_1^{s^{(\mu)}+s_{n+1}^{(\mu)}\beta_1} \cdots \alpha_n^{s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\mu}.$$

[2] Η ανισότητα $L \leq (2S-1)^{n+1}$ προκύπτει από την ανισότητα $c(L_0L_1)^n \leq S^{n+1}$, όπως ακριβώς προέκυψε στην πρόταση 5.1.1

και από την πρόταση 4.4.1, έχουμε ότι υπάρχει σταθερά $c_1 > 0$ [3] τέτοια ώστε:

$$\frac{1}{L}\log|\Delta| \leq -L^{1/n} + c_1(L_0 \log S + L_1 S).$$

Για $c \geq 4c_1$, έχουμε ότι:

$$\frac{1}{L}\log|\Delta| \leq -\frac{L^{1/n}}{2}. \tag{6.2}$$

(αφού, λόγω των ανισοτικών σχέσεων στο 2ο βήμα, έχουμε ότι: $-L^{1/n} + c_1(L_0 \log S + L_1 S) \leq -L^{1/n} + c_1\Big(\frac{L^{1/n}}{c} + \frac{L^{1/n}}{c}\Big)$, οπότε για $c \geq 4c_1$ έχουμε την παραπάνω ανισότητα).

• **Βήμα 5ο. Κάτω φράγμα για την $|\Delta|$.**

Η υπόθεση μας ότι οι αριθμοί $\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_n$ είναι αλγεβρικοί, μας επιτρέπει να χρησιμοποιήσουμε το πόρισμα 3.6.2 και να συμπεράνουμε ότι:

- είτε:

$$\Delta = 0$$

- είτε:

$$\frac{1}{L}\log|\Delta| \geq -c_2(L_0 \log S + L_1 S).$$

Για $c \geq 8c_2$ έχουμε ότι αν $\Delta \neq 0$ τότε:

$$\frac{1}{L}\log|\Delta| > -\frac{L^{1/n}}{2}. \tag{6.3}$$

(αφού, $c_2(L_0 \log S + L_1 S) \leq \frac{2c_2}{c} L^{1/n}$, έχουμε ότι για $c \geq 8c_2$, $c_2(L_0 \log S + L_1 S) \leq \frac{L^{1/n}}{4}$, άρα για $c \geq 8c_2$ έχουμε την (6.3)).

Οπότε, για $c \geq \max\{4c_1, 8c_2\}$, έπεται, μέσω των ανισοτήτων (6.2), (6.3), ότι $\Delta = 0$.

• **Βήμα 6ο. Το συμπέρασμα.**

Αφού $\Delta = 0$, από 5ο το βήμα συμπεραίνουμε ότι η τάξη του πίνακα Π είναι μικρότερη του L.

Από την υπόθεση ότι τα $\ell_1, \ldots, \ell_{n+1}$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα πάνω από το $\mathbb{Q}$ έπεται ότι τα $\alpha_1, \ldots, \alpha_{n+1}$, παράγουν μια πολλαπλασιαστική υποομάδα του $\mathbb{C}^*$ με $\text{rank} \geq n$ [4]. Από την επιλογή των παραμέτρων στο 2ο βήμα εύκολα

[3] Στην πρόταση 4.4.1 δείξαμε ότι το c_1 εξαρτάται μόνο από τα $n, \ell_1, \ldots, \ell_{n+1}, \beta_1, \ldots, \beta_n$

[4] Πρβλ. παράρτημα Α΄.8

συμπεραίνεται ότι οι ανισότητες τις υπόθεσης της πρότασης 5.1.1 ικανοποιούνται [5]. Άρα, εφαρμόζοντας την πρόταση 5.1.1 έχουμε ότι τα $1, \beta_1, \ldots, \beta_n$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένα, το οποίο ολοκληρώνει την απόδειξη.

[5] Λόγω της ελευθερίας που έχουμε για την επιλογή του S μπορούμε να επιλέξουμε το $S \geq 2n(n+1)$. Οι άλλες δύο ανισότητες της υπόθεσης της πρότασης 5.1.1 συμπεραίνονται εύκολα λόγω της επιλογής των παραμέτρων στο 2ο βήμα

Κεφάλαιο 7

Κάτω φράγμα για ομογενείς γραμμικές μορφές λογαρίθμων

Σε αυτό το κεφάλαιο θα παρουσιάσουμε και θα αποδείξουμε ένα κάτω φράγμα για μη μηδενικές γραμμικές μορφές λογαρίθμων,

$$\Lambda := \beta_1 \log \alpha_1 + \ldots + \beta_m \log \alpha_m,$$

με $\alpha_i, \beta_i,\ \ 1 \leq i \leq n$, αλγεβρικοί αριθμοί.

Η μέθοδος που θα χρησιμοποιήσουμε είναι ίδια με το πρώτο μέρος (υπερβατικό μέρος) της απόδειξης του θεωρήματος του Baker. Το φράγμα που θα παρουσιάσουμε δεν είναι το καλύτερο γνωστό, αλλά δεν είναι τετριμμένο. Είναι χρήσιμο σε πολλά διοφαντικά προβλήματα. Το φράγμα το οποίο θα αποδείξουμε έχει την μορφή

$$|\Lambda| > \mathrm{e}^{-c_1 (\log H)^{\kappa(m)}},$$

όπου, $\kappa(m) = 2^m (m!)^2$, το $\log H$ είναι ένα άνω φράγμα των υψών των $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m$ και c_1 θετική υπολογίσιμη σταθερά, εξαρτώμενη από το πλήθος των λογαρίθμων και το βαθμό του σώματος $\mathbb{Q}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m)$.

Τα νέα βελτιωμένα φράγματα, τα οποία είναι γνωστά σήμερα (πρβλ. [30], [20] και [8]), είναι της μορφής:

$$|\Lambda| > \mathrm{e}^{-(c_1 \log B + c_2)^{\kappa}}, \text{ με } \kappa = 1 \text{ ή } 2,$$

όπου το $\log B$ είναι άνω φράγμα των υψών των $\beta_1, \ldots, \beta_n$, $c_1 > 0$ και $c_2 \geq 0$ υπολογίσιμες σταθερές, εξαρτώμενες από τα ύψη των $\alpha_1, \ldots, \alpha_m$, το πλήθος των λογαρίθμων και το βαθμό του σώματος $\mathbb{Q}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m)$.

Εύκολα προκύπτει, ότι και το φράγμα που θα παρουσιάσουμε έρχεται στην μορφή:

$$|\Lambda| > \mathrm{e}^{-(c_1 \log B + c_2)^{\kappa}}, \text{ με } \kappa = 2^m (m!)^2,$$

όπου, το $\log B$ είναι άνω φράγμα των υψών των $\beta_1, \ldots, \beta_m$ και c_1, c_2 υπολογίσιμες σταθερές, εξαρτώμενες από τα ύψη των $\alpha_1, \ldots, \alpha_m$, το πλήθος των λογαρίθμων και το βαθμό του σώματος $\mathbb{Q}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m)$.

Κάνουμε μια παρατήρηση η οποία θα μας χρειαστεί σε αυτό το κεφάλαιο.

Παρατήρηση: Για οποιοδήποτε $m \in \mathbb{N}$ και οποιουσδήποτε $\ell_1, \ldots, \ell_m \in \mathfrak{L}$ ($\mathrm{e}^{\ell_1} = \alpha_1, \ldots, \mathrm{e}^{\ell_m} = \alpha_m \in \overline{\mathbb{Q}}$) και $\beta_1, \ldots, \beta_m \in \overline{\mathbb{Q}}$ υπάρχουν θετικοί D και H τέτοιοι ώστε

$$[\mathbb{Q}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m) : \mathbb{Q}] \leq D,$$
$$\log H \geq \max\{h(\alpha_1), \ldots, h(\alpha_m), h(\beta_1), \ldots, h(\beta_m), 1\}$$
και
$$\frac{\mathrm{e} \max\{|\ell_1|, \ldots, |\ell_m|\}}{\log H} \leq D \leq H.$$

Ένα τέτοιο ζεύγος (D, H) θα το λέμε *αποδεκτό ζεύγος φραγμάτων του* $(\ell_1, \ldots, \ell_m, \beta_1, \ldots, \beta_m) \in \mathfrak{L} \times \overline{\mathbb{Q}}^m$.

7.1 Παρουσίαση του φράγματος - Περιγραφή της απόδειξης

Το συμπέρασμα αυτού του κεφαλαίου είναι το εξής

Θεώρημα 7.1.1. *Έστω $\ell_1, \ldots, \ell_m \in \mathfrak{L}$, $m \geq 2$, ($\mathrm{e}^{\ell_1} = \alpha_1, \ldots, \mathrm{e}^{\ell_m} = \alpha_m \in \overline{\mathbb{Q}}$) και $\beta_1, \ldots, \beta_m \in \overline{\mathbb{Q}}$. Υποθέτουμε ότι ο αριθμός*

$$\Lambda = \beta_1 \ell_1 + \ldots + \beta_m \ell_m$$

δεν είναι μηδέν. Υποθέτουμε επίσης ότι το ζεύγος φυσικών αριθμών (D, H) είναι ένα αποδεκτό ζεύγος φραγμάτων του $(\ell_1, \ldots, \ell_m, \beta_1, \ldots, \beta_m) \in \mathfrak{L} \times \overline{\mathbb{Q}}^m$. Τότε

$$|\Lambda| \geq \mathrm{e}^{-(10^3 m^3 D \log H)^{k(m)}},$$

όπου $\kappa(m) = 2^m (m!)^2$.

Θα κάνουμε τώρα μια περιγραφή της απόδειξης.

Στην παράγραφο 7.2 (υπερβατικό μέρος της απόδειξης) υποθέτοντας ότι τα $\ell_1, \ldots, \ell_m$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένα και ότι τα $\beta_1, \ldots, \beta_m$ ικανοποιούν

μια συνθήκη «*ασθενούς γραμμικής ανεξαρτησίας*» θα αποδείξουμε ένα ισχυρότερο φράγμα (θεώρημα 7.2.1) για το $|\Lambda|$, με το $2m^3$ στη θέση του $\kappa(m)$. Ύστερα, στην παράγραφο 7.3 θα αποδείξουμε ότι μπορούμε πάλι να πετύχουμε ένα φράγμα για το $|\Lambda|$ (πρόταση 7.3.2) χωρίς να υποθέσουμε ότι τα $\beta_1, \ldots, \beta_m$ ικανοποιούν την συνθήκη «*ασθενούς γραμμικής ανεξαρτησίας*». Σε αυτή την περίπτωση, το φράγμα που θα εξασφαλίσουμε για το $|\Lambda|$ θα είναι εκείνο του θεωρήματος 7.1.1 (ασθενέστερο από την πρόταση 7.2.1, αφού στη θέση του $2m^3$ έχουμε το $k(m)$). Στην παράγραφο 7.4, θα αποδείξουμε το προηγούμενο φράγμα (δηλαδή της πρότασης 7.3.2) ικανοποιείται ακόμα και όταν τα $\ell_1, \ldots, \ell_m$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένα (και τότε θα έχουμε αποδείξει την γενική περίπτωση, δηλαδή το θεώρημα 7.1.1).

7.2 Υπερβατικό μέρος της απόδειξης

Θεώρημα 7.2.1. *Έστω, $\ell_1, \ldots, \ell_m \in \mathfrak{L}$ τα οποία είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα ($\mathrm{e}^{\ell_1} = \alpha_1, \ldots, \mathrm{e}^{\ell_m} = \alpha_m \in \overline{\mathbb{Q}}$), $\beta_1, \ldots, \beta_m \in \overline{\mathbb{Q}}$ και ο αριθμός*

$$\Lambda = \beta_1\ell_1 + \ldots + \beta_m\ell_m$$

δεν είναι μηδέν. Υποθέτουμε ότι το ζεύγος φυσικών αριθμών (D, H) είναι ένα αποδεκτό ζεύγος φραγμάτων του $(\ell_1, \ldots, \ell_m, \beta_1, \ldots, \beta_m) \in \mathfrak{L} \times \overline{\mathbb{Q}}^m$. Υποθέτουμε επίσης ότι τα $\beta_1, \ldots, \beta_m$ ικανοποιούν την εξής συνθήκη «ασθενούς γραμμικής ανεξαρτησίας»

> *Δεν υπάρχει γραμμική σχέση της μορφής $b_1\beta_1 + \ldots + b_m\beta_m = 0$, όπου $b_i \in \mathbb{Z}$ και*
>
> $$0 < \max_{1\le i\le m} |b_i| < 2T^{2(m-1)^2}, \quad \text{όπου } T = [10^3 m^3 D \log H].$$

Τότε

$$|\Lambda| \ge \mathrm{e}^{-(10^3 m^3 D \log H)^{2m^3}}.$$

Το θεώρημα 7.2.1 είναι άμεση συνέπεια της πρότασης 7.2.2. Με κατάλληλη επιλογή των παραμέτρων (L_0, L_1, S, A, B, και E) της πρότασης 7.2.2 πετυχαίνουμε το ζητούμενο φράγμα του θεωρήματος 7.2.1. Επίσης, θα χρειαστούμε και δύο ακόμα λήμματα (7.2.3, 7.2.4) τα οποία θα μας εξασφαλίσουν κάποιες τεχνικές λεπτομέρειες της απόδειξης του θεωρήματος 7.2.1.

Πρόταση 7.2.2. *Έστω $\ell_1, \ldots, \ell_{n+1} \in \mathfrak{L}$ ($\mathrm{e}^{\ell_i} = \alpha_i$, $1 \le i \le n+1$, αλγεβρικοί) και $\beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ με $\max\{|\beta_1|, \ldots, |\beta_n|\} \le 1$. Έστω $[\mathbb{Q}(\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_n)$:*

$\mathbb{Q}] = D$ *και έστω* A, B *και* E *πραγματικοί αριθμοί, οι οποίοι είναι* $\geq \mathrm{e}$ *και ικανοποιούν τις εξής ανισότητες:*

$$\max_{1\leq i\leq n+1} h(\alpha_i) \leq \log A, \;\; h(1:\beta_1:\ldots:\beta_n) \leq B. \tag{7.1}$$

$$E \max_{1\leq i\leq n+1} |\ell_i| \leq D\log A \tag{7.2}$$

Υποθέτουμε ότι υπάρχουν τρεις θετικοί ρητοί ακέραιοι $S, L_0, L_1 \geq 2$*, οι οποίοι ικανοποιούν την εξής συνθήκη*
(όπου $L := \binom{L_0+n}{n}(L_1+1)$ *και* $\Theta_n(L)$ *όπως ορίστηκε στην παράγραφο 4.2)*

$$\frac{1}{L}\Theta_n(L)\log E \geq D\log(2L)+DL_0\log(2BS)+L_0\log E+(3n+1)DL_1S\log A. \tag{7.3}$$

Υποθέτουμε επίσης ότι ο παρακάτω πίνακας είναι τάξης L*,*

$$\Big((s_1+s_{n+1}\beta_1)^{\lambda_1}\cdots(s_n+s_{n+1}\beta_n)^{\lambda_n}\big(\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\underline{s}},$$

όπου ο δείκτης γραμμών $\underline{\lambda} = (\lambda_1,\ldots,\lambda_{n+1}) \in \mathbb{N}^{n+1}$*, με* $\lambda_1+\ldots+\lambda_n \leq L_0$ *και* $0 \leq \lambda_{n+1} \leq L_1$ *και ο δείκτης των στηλών* $\underline{s} \in \mathbb{Z}^{n+1}(S)$*.*

Τότε ο αριθμός

$$\Lambda = \beta_1\ell_1+\ldots+\beta_n\ell_n-\ell_{n+1},$$

δεν είναι μηδέν, και αν γράψουμε $|\Lambda| = e^{-U}$*, έχουμε ότι*

$$\frac{U}{L} \leq D\log L + DL_0\log(2BS) + 2(n+1)DL_1S\log A. \tag{7.4}$$

(Από την υπόθεση για την τάξη του πίνακα συμπεραίνουμε ότι $L \leq (2S-1)^{n+1}$*).*

Απόδειξη.

Εισάγουμε δύο πίνακες, Π_1, Π_2,

$$\Pi_1 = \Big((s_1+s_{n+1}\beta_1)^{\lambda_1}\cdots(s_n+s_{n+1}\beta_n)^{\lambda_n}\big(\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\underline{s}},$$
$$\Pi_2 = \Big((s_1+s_{n+1}\beta_1)^{\lambda_1}\cdots(s_n+s_{n+1}\beta_n)^{\lambda_n}\big(\alpha_1^{s_1+s_{n+1}\beta_1}\cdots\alpha_n^{s_n+s_{n+1}\beta_n}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\underline{s}}.$$

Λόγω της υπόθεσης ότι η τάξη του πίνακα Π_1 είναι L, έχουμε ότι υπάρχουν $\underline{s}^{(1)},\ldots,\underline{s}^{(L)} \in \mathbb{Z}^{n+1}(S)$, τέτοια ώστε η ορίζουσα

$$\Delta_1 = \det\Big((s_1^{(\mu)}+s_{n+1}^{(\mu)}\beta_1)\cdots(s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n)\big(\alpha_1^{s_1^{(\mu)}}\cdots\alpha_{n+1}^{s_{n+1}^{(\mu)}{}^{\lambda_{n+1}}}\big)\Big)_{\underline{\lambda},\mu}$$

($1 \leq \mu \leq L$) δεν είναι μηδέν.

Ορίζουμε επίσης,

$$\Delta_2 = \det\Big((s_1^{(\mu)}+s_{n+1}^{(\mu)}\beta_1)^{\lambda_1}\cdots(s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n)^{\lambda_n}\big(\alpha_1^{s_1^{(\mu)}+s_{n+1}^{(\mu)}\beta_1}\cdots\alpha_n^{s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\mu}$$

μια $L\times L$ υποορίζουσα του Π_2.

Την Δ_2 την λαμβάνουμε από την Δ_1, αν αντικαταστήσουμε το α_{n+1} με το $\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$.

Επειδή $\Delta_1\neq 0$ από την ανισότητα του Liouville θα πετύχουμε ένα κάτω φράγμα για την $|\Delta_1|$. Επίσης, με βάση όσων αναφέραμε στο κεφάλαιο 4, θα πετύχουμε και ένα άνω φράγμα της $|\Delta_2|$. Ύστερα, θα δείξουμε ότι η διαφορά $|\Delta_1-\Delta_2|$ είναι άνω φραγμένη από ένα μικρό πολλαπλάσιο του $|\Lambda|$. Από αυτό θα συμπεράνουμε το κάτω φράγμα για το $|\Lambda|$ [1].

- **Βήμα 1ο.** *Κάτω φράγμα για την* $|\Delta_1|$.

Αφού $\Delta_1\neq 0$, από την πρόταση 3.6.1, έχουμε ότι:

$$\frac{1}{L}\log|\Delta_1|\geq -U_1,$$

όπου $U_1=(D-1)(L_0\log(2S)+\log L)+DL_0\log B+(n+1)DL_1S\log A$.

(Το U_1 δεν προκύπτει με αυτή την μορφή άμεσα από την πρόταση 3.6.1. Χρειάζεται να χρησιμοποιήσουμε και τις ανισότητες της (7.1)).

- **Βήμα 2ο.** *Άνω φράγμα για την* $|\Delta_2|$.

Θα εφαρμόσουμε τα αποτελέσματα του κεφαλαίου 4 στις συναρτήσεις

$$f_{\underline{\lambda}}(z_1,\ldots,z_n)=z_1^{\lambda_1}\cdots z_n^{\lambda_n}\big(\alpha_1^{z_1}\cdots\alpha_n^{z_n}\big)^{\lambda_{n+1}}$$

και στα σημεία

$$\zeta_\mu=\big(s_1^{(\mu)}+s_{n+1}^{(\mu)}\beta_1,\ldots,s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n\big)\in\mathbb{C}^n,\ \ (1\leq\mu\leq L)$$

με $r=2S$ και $R=Er$ ($\max_{1\leq\mu\leq L}|\zeta_\mu|\leq r$, αφού έχουμε υποθέσει ότι $|\beta_j|\leq 1$). Επαναλαμβάνοντας την απόδειξη της πρότασης 4.4.1 και χρησιμοποιώντας τις ανισότητες (7.1) και (7.2), συμπεραίνουμε το εξής:

$$\frac{1}{L}\log|\Delta_2|\leq -U_2,$$

όπου $U_2=\frac{1}{L}\Theta_n(L)\log E-\log L-L_0\log(2ES)-2nDL_1S\log A$.

- **Βήμα 3ο.** *Άνω φράγμα για την διαφορά* $|\Delta_1-\Delta_2|$.

[1] Η διαφορά στην απόδειξη του του θεωρήματος του Baker ήταν ότι $\Lambda=0$ και τότε οι πίνακες ήταν ίδιοι (παρακάτω στην απόδειξη θα δείξουμε ότι εδώ $\Lambda\neq 0$)

Όπως και στην απόδειξη της πρότασης 3.6.1, μπορούμε να γράψουμε την ορίζουσα Δ_1 ως την τιμή ενός πολυωνύμου στα $\alpha_1, \ldots, \alpha_{n+1}$ και $\alpha_1^{-1}, \ldots, \alpha_{n+1}^{-1}$ με συντελεστές από το σώμα $\mathbb{Q}(\beta_1, \ldots, \beta_n)$:

$$\Delta_1 = \sum_{\underline{t}} q_{\underline{t}} \alpha_1^{t_1} \cdots \alpha_{n+1}^{t_{n+1}}, \quad (q_{\underline{t}} \in \mathbb{Q}(\beta_1, \ldots, \beta_n))$$

όπου $\underline{t} = (t_1, \ldots, t_{n+1})$ με $|t_i| \leq LL_1S$.

Χρησιμοποιώντας την υπόθεση ότι $|\beta_i| \leq 1$, συμπεραίνουμε εύκολα ότι:

$$\sum_{\underline{t}} |q_{\underline{t}}| \leq L!(2S)^{LL_0}.$$

Θέτουμε $x = \alpha_{n+1}$ και $y = \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$. Τότε:

$$\Delta_1 - \Delta_2 = \sum_{\underline{t}} q_{\underline{t}} \alpha_1^{t_1} \cdots \alpha_n^{t_n} (x^{t_{n+1}} - y^{t_{n+1}}).$$

Αφού $|\ell_i| \leq \frac{D \log A}{E}$ (χρησιμοποιούμε επίσης και την ανισότητα $L! \leq L^L$), έχουμε ότι:

$$\log|\Delta_1 - \Delta_2| \leq L \log L + LL_0 \log(2S) + \frac{nD}{E} LL_1 S \log A + \log \max_{|t| \leq LL_1S} |x^t - y^t|.$$

Για κάθε ακέραιο t με $-LL_1 \leq t \leq LL_1S$, έχουμε:

$$|x^t - y^t| \leq |\alpha_{n+1}^t||1 - \mathrm{e}^{t\Lambda}| \leq {}^{2} \ \mathrm{e}^{|t\ell_{n+1}|} |t\Lambda| \mathrm{e}^{|t\Lambda|}.$$

Μπορούμε επίσης, (χωρίς βλάβη της γενικότητας), να υποθέσουμε ότι $|\Lambda| LL_1S \leq 1$ [3].

Οπότε,

$$|x^t - y^t| \leq \mathrm{e}^{LL_1S|\ell_{n+1}|} LL_1S|\Lambda|\mathrm{e}$$

και, συνεπώς,

$$\begin{aligned} \log|x^t - y^t| &\leq \log(\mathrm{e}^{LL_1S|\ell_{n+1}|} LL_1S|\Lambda|\mathrm{e}) \\ &= LL_1S|\ell_{n+1}| + \log(LL_1S) - U + 1 \\ &\leq \frac{D}{E} LL_1S \log A + \log(LL_1S) + 1 - U. \end{aligned}$$

---

[2] Έστω $z \in \mathbb{C}$. Για κάθε $\delta > 0$, με $\mathrm{Re}(z) \leq \delta$, έχουμε ότι $|\mathrm{e}^z - 1| \leq \frac{\mathrm{e}^\delta - 1}{\delta}|z|$, οπότε $|\mathrm{e}^z - 1| \leq |z|\mathrm{e}^\delta$ (Η απόδειξη προκύπτει από την σχέση: για $x = \mathrm{Re}(z)$, $\left|\int_0^1 \mathrm{e}^{tz} dt\right| \leq \int_0^1 |\mathrm{e}^{tz}| dt = \int_0^1 \mathrm{e}^{tx} dt$).

[3] Αφού, αν $|\Lambda| LL_1S \geq 1$, τότε $\mathrm{e}^{-U} LL_1S \geq 1$, δηλαδή $U \leq \log(LL_1S)$. Έτσι, θα είχαμε το συμπέρασμα της πρότασης, σχετικά με το άνω φράγμα του U

Επίσης ισχύει ότι

$$1 + \log(2LL_1S) + \frac{D}{E}(n+1)LL_1S\log A \leq (n+1)DLL_1S\log A.$$

(1+log(2LL1S)+$\frac{D}{E}$(n+1)LL1S log A = log(2eLL1S)+$\frac{D}{E}$(n+1)LL1S log A. Χρησιμοποιούμε τις υποθέσεις, $A \geq \mathrm{e}$, $E \geq \mathrm{e}$, $D \geq 1$, $n \geq 1$, $S \geq 2$, $L_1 \geq 2$. Επίσης,
$L := \binom{L_0+n}{n}(L_1+1) = \frac{(L_0+n)!}{L_0!n!}(L_1+1) = \frac{(L_0+1)\cdots(L_0+1)}{n!}(L_1+1) \geq \frac{(n+2)\cdots(1+2)}{n!}\cdot 3 \geq 9$, άρα $x = 2\mathrm{e}LL_1S \geq 72\mathrm{e}$ και $\log x \leq \frac{1}{\mathrm{e}^2}(\mathrm{e}-1)x$).

Άρα, τελικά,

$$|\Delta_1 - \Delta_2| \leq \mathrm{e}^{-LU_3},$$

όπου

$$U_3 = \frac{U}{L} - L_0\log(2S) - (n+1)DL_1S\log A - \log L + \frac{\log 2}{L}.$$

- **Βήμα 4ο.** *Συμπεράσματα.*

(1) Ο αριθμός Λ δεν είναι μηδέν.

Διαφορετικά, αν $\Lambda = 0$, τότε $\ell_{n+1} = \beta_1\ell_1 + \ldots + \beta_n\ell_n$, δηλαδή $x = \alpha_{n+1} = \mathrm{e}^{\ell_1}$ είναι ίσο με το $y = \alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n} = \mathrm{e}^{\beta_1\ell_1+\ldots+\beta_n\ell_n}$.

Όμως τότε, από το 3ο βήμα,

$$\Delta_1 = \Delta_2 =: \Delta.$$

Τότε, από το 1ο βήμα και από το 2ο βήμα, έπεται

$$-U_1 \leq \frac{1}{L}\log|\Delta| \leq -U_2.$$

Συγκρίνοντας τα φράγματα U_1 και U_2, καταλήγουμε σε άτοπο, λόγω της ανισότητας (7.3).

(2)
$$\frac{U}{L} \leq D\log L + DL_0\log(2BS) + 2(n+1)DL_1S\log A.$$

Πράγματι, χρησιμοποιώντας την τριγωνική ανισότητα, συμπεραίνουμε ότι

$$|\Delta_1| \leq |\Delta_2| + |\Delta_1 - \Delta_2|,$$

άρα, από τα βήματα 1, 2 και 3,

$$\mathrm{e}^{-LU_1} \leq \mathrm{e}^{-LU_2} + \mathrm{e}^{-LU_3}.$$

Από την ανισότητα (7.3), έπεται εύκολα ότι

$$U_1 + \frac{1}{L}\log 2 \leq U_2,$$

άρα,

$$U_3 \leq U_1 + \frac{1}{L}\log 2.$$

Από αυτή την ανισότητα (χρησιμοποιώντας το αποτέλεσμα του βήματος 3), έπεται το ζητούμενο άνω φράγμα για το U.

□

Το επόμενο λήμμα 7.2.3 είναι η πιο αναλυτική έκφραση της συνεπαγωγής $1 \Rightarrow 3\acute{\alpha}$ του λήμματος 5.2.5. Έχουμε λοιπόν,

Λήμμα 7.2.3. *Έστω K ένα σώμα χαρακτηριστικής μηδέν, S_1 ένας θετικός ρητός ακέραιος και $\mathcal{V}$ ένας διανυσματικός υπόχωρος του K^m με $\mathrm{codim}\mathcal{V} = r \geq 1$, τέτοια ώστε:*

$$\mathrm{Card}\Big((\mathbb{Z}^m(S_1) + \mathcal{V})/\mathcal{V}\Big) < (2S_1 - 1)^{r+1}.$$

Τότε:

1. *υπάρχει μια βάση $\{v_1, \ldots, v_{m-r}\}$ του $\mathcal{V}$ με $v_j \in \mathbb{Z}^m(2S_1 - 1)$, για κάθε $1 \leq j \leq m - r$.*

2. *ο διανυσματικός υπόχωρος $\mathcal{V}$ του K^n είναι τομή r αλγεβρικών συνόλων, τα οποία ορίζονται από τις εξισώσεις:*

$$b_{i1}z_1 + \ldots + b_{im}z_m = 0, \;\; 1 \leq i \leq r,$$

όπου, για $1 \leq i \leq r$, $b_i = (b_{i1}, \ldots, b_{ir}) \in \mathbb{Z}^m(2S_1 - 1)$.

Απόδειξη.

1. Έστω η κανονική απεικόνιση

$$\sigma_{\mathcal{V}} : \;\; K^m \underset{\text{επί}}{\longrightarrow} \;\; K^m/\mathcal{V}$$

και $\{e^{(1)}, \ldots, e^{(m)}\}$ η κανονική βάση του K^m. Αφού $\dim(\mathcal{V}) = m - r$, υπάρχει ένα υποσύνολο $\{i_1, \ldots, i_r\}$ του $\{1, \ldots, r\}$ τέτοιο ώστε το σύνολο

$$\{\sigma_{\mathcal{V}}(e^{(i_1)}), \ldots, \sigma_{\mathcal{V}}(e^{(i_r)})\}$$

είναι βάση του $K^m/\mathcal{V}$.

Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $\{i_1, \ldots, i_r\} = \{1, \ldots, m\}$.

Για j με $r+1 \leq j \leq m$, θεωρούμε $\underline{s} = (s_1, \ldots, s_m) \in \mathbb{Z}^m(S_1)$ με $s_i = 0$ για $r+1 \leq i \leq m$ και $i \neq j$. Έστω το σύνολο των στοιχείων:

$$\Sigma_{\mathcal{V}} = \{\sigma_{\mathcal{V}}(s_1 e^{(1)} + \ldots + s_r e^{(r)} + s_j e^{(j)}), \ \ (s_1, \ldots, s_r, s_j) \in \mathbb{Z}^{r+1}(S_1)\},$$

(είναι στοιχεία του $(\mathbb{Z}^m(S_1) + \mathcal{V})/\mathcal{V}$).
Όμως,

$$\mathrm{Card}\big(\mathbb{Z}^{r+1}(S_1)\big) = (2S_1 - 1)^{r+1} > \mathrm{Card}\Big(\mathbb{Z}^m(S_1 + \mathcal{V})/\mathcal{V}\Big)^4,$$

άρα δύο τουλάχιστον στοιχεία του συνόλου $\Sigma_{\mathcal{V}}$ συμπίπτουν του $(\mathbb{Z}^m(S_1) + \mathcal{V})/\mathcal{V}$.

Οπότε, για κάθε j με $r+1 \leq j \leq m$, υπάρχουν $\underline{s}^{(j)}, \underline{s}'^{(j)} \in \mathbb{Z}^{r+1}(S_1)$, τέτοια ώστε:

$$\begin{aligned} &s_1^{(j)} e^{(1)} + \ldots + s_r^{(j)} e^{(r)} + s_j^{(j)} e^{(j)} + \mathcal{V} \\ &= s_1^{'(j)} e^{(1)} + \ldots + s_r^{'(j)} e^{(r)} + s_j^{'(j)} e^{(j)} + \mathcal{V}, \end{aligned}$$

δηλαδή,

$$(s_1^{(j)} - s_1^{'(j)}) e^{(1)} + \ldots + (s_r^{(j)} - s_r^{'(j)}) e^{(r)} + (s_j^{(j)} - s_j^{'(j)}) e^{(j)} \in \mathcal{V}.$$

Άρα, τα $m - r$ στοιχεία

$$(s_1^{(j)} - s_1^{'(j)}, \ldots, s_r^{(j)} - s_r^{'(j)}, 0, \ldots, 0, s_j^{(j)} - s_j^{'(j)}, 0, \ldots, 0),$$

(είναι $K-$γραμμικώς ανεξάρτητα), αποτελούν βάση του $\mathcal{V}$.

Επίσης, για κάθε $i = 1, \ldots, m$,

$$\big|s_i^{(j)} - s_i^{'(j)}\big| \leq |s_i^{(j)}| + |s_i^{'(j)}| \leq (S_1 - 1) + (S_1 - 1) = 2S_1 - 2.$$

2. Από το 1 και από το λήμμα Α΄.7.2 συμπεραίνουμε ότι υπάρχει γραμμική απεικόνιση $f : K^m \to K^r (\cong K^m/\mathcal{V})$, με $\ker f = \mathcal{V}$, της οποίας ο πίνακας ως προς τις κανονικές βάσεις έχει συντελεστές στο $\mathbb{Q}$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι αυτοί οι συντελεστές είναι ακέραιοι.

(α) Υποθέτουμε ότι $r = 1$.

Σε αυτή την περίπτωση ο $\mathcal{V}$ είναι ο πυρήνας της γραμμικής απεικόνισης:

$$f : K^m \underset{\text{επί}}{\longrightarrow} K^m/\mathcal{V} \cong K$$

[4] Από την υπόθεση ότι $\mathrm{Card}\Big(\mathbb{Z}^m(S_1 + \mathcal{V})/\mathcal{V}\Big) < (2S_1 - 1)^{r+1}$, έπεται επίσης ότι $V \neq 0$ και άρα $m > r$

με $f(x_1,\ldots,x_n)=a_1x_1+\ldots+a_mx_m$, $a_1,\ldots,a_m\in\mathbb{Z}$ (πρβλ. λήμμα Α΄.7.2), και μπορούμε να υποθέσουμε ότι $a_1,\ldots,a_m$ είναι πρώτοι μεταξύ τους. Ύστερα από μετάθεση των συντεταγμένων και αντικατάσταση του f από το $-f$ αν χρειαστεί, μπορούμε να υποθέσουμε ότι $a_1=\max\{|a_1|,\ldots,|a_m|\}$.

Έχουμε ότι $\mathrm{Card}(f(\mathbb{Z}^m(S_1)))\leq\mathrm{Card}(\sigma_{\mathcal{V}}(\mathbb{Z}^m(S_1)))$, αφού ισχύει ότι αν $f(\underline{s}')\neq f(\underline{s}'')$, για $\underline{s}',\underline{s}''\in\mathbb{Z}^m(S_1)$, τότε και $\sigma_{\mathcal{V}}(\underline{s}')\neq\sigma_{\mathcal{V}}(\underline{s}'')$.

Πράγματι, σε αντίθετη περίπτωση θα είχαμε ότι $\underline{s}'-\underline{s}''\in\ker(\sigma_{\mathcal{V}})=\mathcal{V}$. Όμως και $\ker f=\mathcal{V}$, άρα $\underline{s}'-\underline{s}''\in\ker(f)$. Οπότε, $f(\underline{s}')=f(\underline{s}'')$, το οποίο είναι αδύνατο.

Άρα, $\mathrm{Card}(f(\mathbb{Z}^m(S_1)))<(2S_1-1)^2$. Με την βοήθεια της προηγούμενης ανισότητας θα αποδείξουμε, αμέσως παρακάτω, ότι $a_1<(2S_1-1)$.

Ορίζουμε,

$$d_i=\text{μκδ}(a_1,\ldots,a_i),\ \ 1\leq i\leq m,$$

(ειδικώτερα, $d_1=b_1$ και $d_m=1$), και θεωρούμε το σύνολο

$$E=\{(x_1,\ldots,x_m)\in\mathbb{Z}^m,\ \ -S_1<x_i\leq -S_1+\frac{d_{i-1}}{d_i},\ \ 2\leq i\leq m\}.$$

Αν περιορίσουμε την f στο E, τότε αυτή είναι ένα προς ένα, διότι, αν δύο διαφορετικά στοιχεία του E έχουν την ίδια εικόνα μέσω της f, τότε η διαφορά τους $(y_1,\ldots,y_m)$ ανήκει στον πυρήνα της f και ικανοποιεί

$$|y_i|<\frac{d_{i-1}}{d_i},\ \ 2\leq i\leq m.$$

Έστω $i\geq 2$ ο μεγαλύτερος φυσικός τέτοιος ώστε $y_i\neq 0$. Τότε λόγω της σχέσης

$$a_iy_i=-a_1y_1-\ldots-a_{i-1}y_{i-1},$$

συμπεραίνουμε ότι το d_{i-1} διαιρεί το μκδ$(a_i,d_{i-1})=d_i$. Άρα, το d_{i-1}/d_iδιαιρεί το $|y_i|$. Άτοπο, λόγω της σχέσης $|y_i|<d_{i-1}/d_i$. Άρα, η f είναι 1-1 στο $E\bigcap\mathbb{Z}^m(S_1)$.

Οπότε, (το αριστερό μέλος στην παρακάτω ανισότητα είναι ο πληθάριθμος του $E\cap\mathbb{Z}^m(S_1)$)

$$(2S_1-1)\prod_{i=2}^{m}\min\{2S_1-1,d_{i-1}/d_i\}<(2S_1-1)^2.$$

Άρα, αναγκαστικά για κάθε $i=2\leq i\leq m$, είναι $\min\{2S_1-1,\frac{d_{i-1}}{d_i}\}=\frac{d_{i-1}}{d_i}$.

Οπότε,

$$2S_1-1>\prod_{i=2}^{m}d_{i-1}/d_i=d_1/d_m=a_1.$$

(β) Υποθέτουμε τώρα ότι $r \geq 1$.
Έστω

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{r1} & \dots & a_{rm} \end{pmatrix}, \ a_{ij} \in \mathbb{Z}$$

ο πίνακας της f. Έχουμε ότι $\mathcal{V} = \mathcal{N}(A)$ (=ο χώρος λύσεων του ομογενούς $AX = \mathbf{0}$).

Από την βασική Γραμμική Άλγεβρα,

$\mathcal{N}(A)^{\perp}$ (ορθογώνιο συμπλήρωμα του $\mathcal{N}(A)$) = χώρος γραμμών του A,

άρα, $r = \operatorname{codim}(\mathcal{V}) = \dim(\mathcal{V}^{\perp}) = \dim(\mathcal{N}(A)^{\perp})$ =διάσταση του χώρου γραμμών του A. Με άλλα λόγια, η τάξη του A είναι r. Χωρίς βλάβη της γενικότητας θεωρώ ότι οι r τελευταίες γραμμές του πίνακα A είναι γραμμικώς ανεξάρτητες.

Έστω $i \in \{m-r+1, \dots, m\}$, αυθαίρετο, αλλά σταθερό παρακάτω.

$$\pi_i : K^m \to K^{m-r+1},$$

όπου $\pi_i(x_1, \dots, x_m) = (x_1, \dots, x_{m-r}, x_i)$.

• $\mathcal{V} \cap \ker \pi_i = \{0\}$. Διότι, αν $x \in \mathcal{V} \cap \ker \pi_i$, τότε $x_1 = \dots = x_{m-r} = x_i = 0$ και, επιπλέον, $AX = \mathbf{0}$. Αλλά τότε,

$$\begin{pmatrix} a_{1,m-r+1} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{r,m-r+1} & \dots & a_{rm} \end{pmatrix} \cdot \begin{pmatrix} x_{m-r+1} \\ \vdots \\ x_{i-1} \\ 0 \\ x_{i+1} \\ \vdots \\ x_m \end{pmatrix} = \mathbf{0}.$$

Η ορίζουσα του πίνακα είναι $\neq 0$ (είναι οι τελευταίες r στήλες του A), άρα όλα τα x_j είναι 0.

• Εφαρμόζουμε το λήμμα Α΄.10.2, με $C = \Big(\mathbb{Z}^m(S_1 + \mathcal{V})\Big)/\mathcal{V}$, $C' = \Big(\mathbb{Z}^{m-r+1}(S_1 + \pi_i(\mathcal{V}))\Big)/\pi_i(\mathcal{V})$ και $f : C \to C'$, (προσωρινά χρησιμοποιούμε το σύμβολο f με άλλη σημασία), οριζόμενη: $f(x + \mathcal{V}) = \pi_i(x) + \pi_i(\mathcal{V})$. Η f είναι καλά ορισμένη (συμπεραίνεται εύκολα). Η f είναι επί, άρα $\operatorname{Card}\big(f(C)\big) = \operatorname{Card}(C')$. Επίσης, για να εκτιμήσουμε (κάτω φράγμα) το $\min f^{-1}(c')$, $c' \in C'$, θεωρώ το τυπικό στοιχείο του C', που είναι της

μορφής $\pi_i(x) + \pi_i(V)$, για κάποιο $x \in \mathbb{Z}^m(S_1)$. Παρατηρώ ότι, για κάθε $y \in \mathbb{Z}^m(S_1) \cap \ker \pi_i$, είναι $f(x + y + \mathcal{V}) = \pi_i(x) + \pi_i(\mathcal{V})$, άρα

$$\begin{aligned}\mathrm{Card}\Big(f^{-1}\big(\pi_i(x) + \pi_i(\mathcal{V})\big)\Big) &\geq \mathrm{Card}\Big(x + y + \mathcal{V} : y \in \mathbb{Z}^m(S_1) \cap \ker \pi_i\Big) \\ &= \mathrm{Card}\Big(\mathbb{Z}^m(S_1) \cap \ker \pi_i\Big).\end{aligned}$$

Η τελευταία ισότητα ισχύει διότι, διαφορετικά $y \in \ker \pi_i$, αντιστοιχούν σε διαφορετικές κλάσεις $x + y + \mathcal{V}$. Αλλά εύκολα, ο τελευταίος πληθάριθμος είναι $(2S_1 - 1)^{r-1}$. Οπότε, συμπεραίνουμε ότι $\mathrm{Card}\Big(f^{-1}(c')\Big) \geq (2S_1 - 1)^{r-1}$, $\forall c' \in C'$. Τώρα, από το λήμμα Α΄.10.2 συμπεραίνουμε ότι:

$$\mathrm{Card}\Big(\mathbb{Z}^{m-r+1}(S_1 + \pi_i(\mathcal{V})\Big)/\pi_i(\mathcal{V}) < (2S_1 - 1)^2.$$

• Ισχύει $\mathrm{codim}\Big(\pi_i(\mathcal{V})\Big)$. Πράγματι, η γραμμική απεικόνιση $\pi_i : \mathcal{V} \to K^{m-r+1}$, είναι $1-1$, λόγω της $\mathcal{V} \cap \ker \pi_i = \{0\}$. Άρα, $\dim\Big(\pi_i(\mathcal{V})\Big) = \dim(\mathcal{V}) = m - r$, οπότε, $\mathrm{codim}\Big(\pi_i(\mathcal{V})\Big) = (m - r + 1) - (m - r) = 1$.

• Εφαρμόζοντας το (2α'), συμπεραίνουμε ότι υπάρχουν $b_{ij} \in \mathbb{Z}(2S_1 - 1), j = 1, \ldots, m - r, i$, έτσι ώστε:

$$\pi_i(\mathcal{V}) = \{(y_1, \ldots, y_{m-r+1}) : b_{i1}y_1 + \ldots + b_{i,m-r}y_{m-r} + b_{ii}y_{m-r+1} = 0\}.$$

• Αν εφαρμόσουμε το παραπάνω συμπέρασμα για $i = m - r + 1, \ldots, m$ βλέπουμε ότι κάθε $x = (x_1, \ldots, x_m) \in \mathcal{V}$ ικανοποιεί το ομογενές γραμμικό σύστημα με πίνακα:

$$B = \begin{pmatrix} b_{m-r+1,1} & \ldots & b_{m-r+1,m-r} & b_{m-r+1,m-r+1} & 0 & \ldots & 0 \\ b_{m-r+2,1} & \ldots & b_{m-r+2,m-r} & 0 & b_{m-r+2,m-r+2} & \ldots & 0 \\ \vdots & & \vdots & & & & \\ b_{m1} & \ldots & b_{m,m-r} & 0 & 0 & \ldots & b_{mm} \end{pmatrix}.$$

Δηλαδή, $\mathcal{V} \subseteq \mathcal{N}(B)$. Βέβαια, στην περίπτωση μας χρειάζεται μία μόνο γραμμή του πίνακα B, αλλά εδώ το αναφέρουμε ακριβέστερα, χωρίς περισσότερο κόπο. □

Το λήμμα 7.2.4 είναι η πρόταση 5.1.1 σε πιο αναλυτική έκφραση.

Λήμμα 7.2.4. *Αν ισχύουν οι υποθέσεις της πρότασης 5.1.1, τότε υπάρχει μια γραμμική σχέση της μορφής*

$$b_1\beta_1 + \ldots + b_n\beta_n = b_{n+1},$$

με $(b_1, \ldots, b_{n+1}) \in \mathbb{Z}^{n+1}$ *και*

$$0 < \max_{1 \le i \le n+1} |b_i| < \frac{S}{n}.$$

Απόδειξη.

(Η απόδειξη είναι σχεδόν ίδια με την απόδειξη της πρότασης 5.1.1. Η διαφορά είναι στην εφαρμογή του λήμματος 5.2.5. Εδώ εφαρμόζουμε το λήμμα 7.2.3 το οποίο είναι η αναλυτικότερη έκφραση της συνεπαγωγής $1 \Rightarrow 3\acute{\alpha}$ του λήμματος 5.2.5.)

Λόγω της υπόθεσης έχουμε ότι $S \ge 2n(n+1)$, άρα,

$$\Big(\frac{S}{n}\Big)^{n+1} < 2\Big(\frac{S}{n} - 1\Big)^{n+1},$$

αφού $\Big(1 + \frac{1}{2n+1}\Big) < 2$, για $n \ge 1$.

Θέτουμε

$$S'' = \lceil \frac{S}{2} \rceil \ \text{ και } \ S' = S - S'' + 1.$$

Έχουμε λοιπόν ότι:

$$S' = S'' = \frac{S+1}{2}, \quad \text{αν } S = \text{περιττός},$$
$$S' = \frac{S}{2} + 1, \ \ S'' = \frac{S}{2}, \quad \text{αν } S = \text{άρτιος}$$

Από την υπόθεση ότι $S^n > L_1$, συμπεραίνουμε επίσης ότι

$$(2S' - 1)^n > L_1 \quad \text{και} \quad \Big(\frac{2S''}{n} - 1\Big) > (2L_0L_1)^n.$$

Αφού η τάξη του πίνακα της υπόθεσης είναι $< L$, συμπεραίνουμε (όπως και στην απόδειξη της πρότασης 5.1.1) ότι υπάρχει πολυώνυμο $P \in K[X_1, \ldots, X_n, Y]$,

$$P(X_1, \ldots, X_n, Y) = \sum_{\underline{\lambda}} c_{\underline{\lambda}} X_1^{\lambda_1} \cdots X_n^{\lambda_n} Y^{\lambda_{n+1}},$$

το οποίο μηδενίζεται σε κάθε σημείο

$$(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n, \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}) \in K^n \times K^*,$$
$$\underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}(S).$$

Λόγω της υπόθεσης ότι τα $\alpha_1, \ldots, \alpha_{n+1}$ παράγουν μια πολλαπλασιαστική υποομάδα του $\mathbb{C}^*$, μπορούμε να συμπεράνουμε (όπως και στην απόδειξη της πρότασης 5.1.1) ότι

$$\mathrm{Card}\Big\{\sigma(\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}),\ \ \underline{s}'=(s'_1,\ldots,s'_{n+1})\in\mathbb{Z}^{n+1}(S')\Big\}>L_1.^{5}$$

Εφαρμόζοντας λοιπόν το λήμμα 5.3.1, συμπεραίνουμε ότι υπάρχει $Q\in K[\underline{X}], \underline{X}=(X_1,\ldots,X_n)$ με $\deg_{\underline{X}}\leq 2L_0L_1$, τέτοιο ώστε το Q να μηδενίζεται σε κάθε σημείο του

$$Y(S'')=(s''_1+s''_{n+1}\beta_1,\ldots,s''_n+s''_{n+1}\beta_n),$$

όπου $\underline{s}=(s''_1,\ldots,s''_{n+1})\in\mathbb{Z}^{n+1}(S'')$.

Ορίζουμε, $S_1=\lceil\frac{S''}{n}\rceil$. Τότε, για $E=Y(S_1)$, έχουμε ότι $E[n]\subset Y(S'')$ [6].

Εφαρμόζοντας την πρόταση 5.2.4, για το πολυώνυμο Q και για $E=Y(S_1)$, συμπεραίνουμε ότι υπάρχει διανυσματικός υπόχωρος $\mathcal{V}$ του K^n, με $\mathrm{codim}(\mathcal{V})=r\geq 1$, τέτοιος ώστε:

$$\mathrm{Card}\Big(E+\mathcal{V}/\mathcal{V}\Big)\leq(2L_0L_1)^r<(2S_1-1)^{r+1}.$$

Από το λήμμα 5.2.5 έπεται ότι υπάρχει διανυσματικός χώρος $\mathcal{W}$ του K^{n+1} με $\mathrm{codim}(\mathcal{W})=r\geq 1$, ο οποίος περιέχει το $(\beta_1,\ldots,\beta_n,-1)$ και

$$\mathrm{Card}\Big((\mathbb{Z}^{n+1}(S_1)+\mathcal{W})/\mathcal{W}\Big)<(2S_1-1)^{r+1}.$$

Οπότε, από το λήμμα 7.2.3, συμπεραίνουμε ότι ο $\mathcal{W}$ περιέχεται σε ένα αλγεβρικό υποσύνολο του K^n το οποίο δίνεται από την

$$b_1z_1+\ldots+b_{n+1}z_{n+1}=0,$$

όπου $|b_i|<2S_1-2$, για κάθε $i=1,\ldots,n+1$. Αφού το $(\beta_1,\ldots,\beta_n,-1)$ ανήκει στο $\mathcal{W}$, έχουμε οτι

$$b_1\beta_1+\ldots+b_n\beta_n=b_{n+1}.$$

□

Απόδειξη του θεωρήματος 7.2.1.

- *Διαιρούμε με το μεγαλύτερο* $|\beta_i|$.

[5] $\sigma:\ K^*\underset{\text{επί}}{\longrightarrow}K^*/K^*_{\mathrm{tors}}$, η κανονική απεικόνιση

[6] $E[n]$, όπως ορίστηκε στην παράγραφο 5.2

Έστω $|\beta_m| = \max\{|\beta_1|, \ldots, |\beta_m|\}$. Διαιρώντας με το β_m έχουμε ότι (μπορούμε να υποθέσουμε ότι $\frac{\beta_m}{\beta_m} = -1$):

$$\begin{aligned}\Lambda' = \frac{\Lambda}{\beta_m} &= \frac{\beta_1}{\beta_m}\ell_1 + \ldots + \frac{\beta_{m-1}}{\beta_m}\ell_{m-1} - \ell_m \\ &= \beta'_1\ell_1 + \ldots + \beta'_{m-1}\ell_{m-1} - \ell_m,\end{aligned}$$

όπου $|\beta_i| \leq 1$, για κάθε $1 \leq i \leq m-1$.

Θα αποδείξουμε ότι

$$|\Lambda'| \geq \mathrm{e}^{-(10m^3 D\log H)^{2m^3-1}}.$$

Η γενική περίπτωση, δηλαδή ότι

$$|\Lambda| \geq \mathrm{e}^{-(10^3 m^3 D\log H)^{2m^3}},$$

έπεται από την ανισότητα [7]

$$|\beta_m| \geq \mathrm{e}^{-D\log H}$$

και από την ανισότητα

$$(10^3 m^3 D\log H)^{2m^3-1} + D\log H \leq (10^3 m^3 D\log H)^{2m^3},$$

(έχουμε ότι:

$$\begin{aligned}|\Lambda| = |\beta_m|\cdot|\Lambda'| &\geq \mathrm{e}^{-D\log H}\cdot \mathrm{e}^{-(10m^3 D\log H)^{2m^3-1}} \\ &= \mathrm{e}^{-\left((10^3 m^3 D\log H)^{2m^3-1} + D\log H \leq (10^3 m^3 D\log H)^{2m^3}\right)} \\ &\geq \mathrm{e}^{-(10^3 m^3 D\log H)^{2m^3}}).\end{aligned}$$

Θα εφαρμόσουμε την πρόταση 7.2.2 με

$$n = m-1,\ \ E = \mathrm{e},\ \ A = H,\ \ B = H^m.$$

(Το H επιλέγεται έτσι ώστε να ικνοποιούνται οι εξής ανισότητες της πρότασης 7.2.2

$$\max_{1\leq i\leq n} h(\alpha_i) \leq \log H \text{ και } e\max_{1\leq i\leq n+1}|\ell_i| \leq D\log H.$$

[7] Από την ανισότητα του Liouville 3.9, για v την αρχιμήδεια απόλυτη τιμή του $\mathbb{C}$, $\log|\beta_m| \geq -Dh(\beta_m)$, άρα, $|\beta_m| \geq \mathrm{e}^{-Dh(\beta_m)} \geq \mathrm{e}^{-D\log H}$.

Ύστερα, για $B = H^m$ η ανισότητα $h(1 : \beta_1 : \ldots : \beta_n) \leq \log B$ θα ικανοποιείται λόγω του λήμματος Α΄.5.2)

- *Σχόλια για την επιλογή των παραμέτρων L_0, L_1 και S.*

Θα εξηγήσουμε την διαδικασία επιλογής κατάλληλων τιμών για τις παραμέτρους L_0, L_1 και S.

Για την εφαρμογή της πρότασης 7.2.2 πρέπει να επιλέξουμε κατάλληλες τιμές (θετικές ακέραιες τιμές) για τα L_0, L_1 και S, έτσι ώστε να ικανοποιούνται η εξής συνθήκες:

1. να ισχύει η ανισότητα (7.3),
2. Ο πίνακας της πρότασης 7.2.2 να έχει την μέγιστη τάξη, δηλαδή να έχει τάξη L

Η δεύτερη συνθήκη θα επιτευχθεί με την βοήθεια του λήμματος 7.2.4 σε συνδυασμό με την «*ασθενή γραμμική ανεξαρτησία*» των $\beta_1, \ldots, \beta_m$ (θεώρημα 7.2.1). Άρα, για την εφαρμογή του λήμματος 7.2.4, απαιτείται επιπλέον:

$$(2n)^{n+1}(L_0L_1)^n \leq S^{n+1}, \tag{7.5}$$

$$S \geq 2n(n+1) \quad \text{και} \quad S^n > L_1. \tag{7.6}$$

Η επιλογή των παραμέτρων L_0, L_1 και S γίνεται ευκολότερα, (για λόγους που θα φανούν παρακάτω), αν απαιτήσουμε να ικανοποιούνται επιπλέον των παραπάνω συνθηκών και οι εξής:

- $L := \binom{L_0+n}{n}(L_1+1) > 2^n \mathrm{e}^{n+1}$, (οπότε από το λήμμα 4.3.1, $\Theta_n(L) \geq \frac{n}{6\mathrm{e}} L^{\frac{n+1}{n}}$)
-

$$D\log(2L) + DL_0\log(2H^{n+1}S) + L_0 < 25n^3DL_0\log H. \tag{7.7}$$

Οπότε, με βάση τις προηγούμενες σχέσεις, για να ικανοποιείται η ανισότητα (7.3),

$$\frac{1}{L}\Theta_n(L)\log E \geq D\log(2L) + DL_0\log(2BS) + L_0\log E + (3n+1)DL_1S\log A,$$

αρκεί να ικανοποιείται η

$$L^{1/n} \geq 150\mathrm{e}n^2DL_0\log H + \frac{6\mathrm{e}}{n}(3n+1)DL_1S\log H.$$

- *Επιλογή των παραμέτρων L_0, L_1 και S.*

Θυμίζουμε ότι $n = m-1$. Άρα, ο αριθμός T στην υπόθεσης της πρότασης 7.2.1 γίνεται

$$T = [10^3(n+1)^3 D \log H].$$

Θέτουμε

$$S = 2nT^{2n^2}, \;\; L_0 = T^{2n^2+n} \;\; \text{και} \;\; L_1 = T^n.$$

Έχουμε ότι

$$L \geq \frac{L_0^n L_1}{n^n} = n^{-n} T^{2n^3+n^2+n} \;\; [8]. \tag{7.8}$$

Επίσης,

$$L = \binom{L_0+n}{n}(L_1+1) \leq 2T^{2n^3+n^2+n} \;\; [9]. \tag{7.9}$$

- *Επαλήθευση της συνθήκης 1.*

Θα εξετάσουμε αν ικανοποιείται η ανισότητα (7.3) της πρότασης 7.2.2, για τις τιμές των L_0, L_1 και S που επιλέξαμε παραπάνω.

Λόγω της (7.8) έπεται ότι

$$L > 2^n \mathrm{e}^{n+1}.$$

Επίσης, ισχύουν και οι παρακάτω ανισότητες,

$$\log(2L) < L_0 \log \frac{3}{2} \;\; \text{και} \;\; \log(3S) \leq \log(6n) + 2n^2 \log T < (25n^3 - n - 2)\log H.$$

(Εδώ χρησιμοποιούμε την υπόθεση ότι $H \geq D$).

Οπότε,

$$\begin{aligned} D\log(2L) + DL_0 \log(2H^{n+1}S) + L_0 &< (n+2)DL_0 \log H + DL_0 \log(3S) \\ &< 25n^3 DL_0 \log H < \frac{1}{12\mathrm{e}} T^{2n^2+n+1}, \end{aligned}$$

και αφού $T > 10^3 n^3 D \log H$ και $L_0 = T^{2n^2+n}$, έπεται ότι

$$D\log(2L) + DL_0 \log(2H^{n+1}S) + L_0 < \frac{1}{12\mathrm{e}} T^{2n^2+n+1}. \tag{7.10}$$

Αποδείξαμε λοιπόν την (7.7).

[8] Η ανισότητα αυτή έχει αποδειχθεί στο κεφάλαιο 5

[9] Η σχέση αυτή είναι ισοδύναμη με την σχέση $L < 2L_0^n L_1$, η οποία αποδεικνύεται επαγωγικά

Επίσης,

$$(3n+1)DL_1S\log H \le 4nDL_1S\log H < \frac{8}{10^3 n}T^{2n^2+n+1} < \frac{1}{12\mathrm{e}}T^{2n^2+n+1}. \tag{7.11}$$

Από την (7.8) και από το λήμμα 4.3.1, συμπεραίνουμε ότι $(E = \mathrm{e})$

$$\begin{aligned}\frac{1}{L}\Theta_n(L)\log E = \frac{1}{L}\Theta_n(L) &\ge \frac{1}{L}\frac{6n}{\mathrm{e}}L^{1+1/n}\\ &= \frac{L^{1/n}n}{6\mathrm{e}} > \frac{1}{6\mathrm{e}}T^{2n^2+n+1}.\end{aligned}$$

Από τα παραπάνω έπεται ότι η ανισότητα (7.3) είναι αληθής.

• *Επαλήθευση της συνθήκης 2.*

Θα δείξουμε ότι ο πίνακας στην υπόθεση της πρότασης 7.2.2 έχει τάξη L. Αυτό θα το πετύχουμε μέσω του λήμματος 7.2.4. Θα δείξουμε λοιπόν ότι οι υποθέσεις του λήμματος 7.2.4 ικανοποιούνται, δηλαδή ότι αληθεύουν οι ανισότητες (7.5), (7.6).

Έχουμε ότι:

$$L_0L_1 = T^{2n(n+1)},$$

οπότε,

$$S^{n+1} = (2n)^{n+1}T^{2n^2(n+1)} = (2n)^{n+1}(L_0L_1)^n.$$

Οι δύο ανισότητες της (7.6), είναι άμεση συνέπεια του ορισμού των L_1, S.

Η υπόθεση ότι τα $\alpha_1,\dots,\alpha_{n+1}$ παράγουν μια πολλαπλασιαστική υποομάδα του $\mathbb{C}^*$ τάξης τουλάχιστον n, έπεται από την γραμμική ανεξαρτησία των $\ell_1,\dots,\ell_{n+1}$ υπέρ το $\mathbb{Q}$ (πρβλ. Α΄.8.1) [10].

Λόγω της υπόθεσης ότι τα $\beta_1,\dots,\beta_n,-1$ δεν ικανοποιούν την συνθήκη της «*ασθενούς γραμμικής ανεξαρτησίας*» (υπόθεση θεωρήματος 7.2.1) με συντελεστές $< 2T^{2n^2}(=\frac{S}{n})$, το συμπέρασμα του λήμματος 7.2.4 δεν είναι αληθές. Άρα, ο πίνακας της πρότασης 7.2.2 έχει τάξη L.

• *Συμπέρασμα.*

Τώρα από την (7.4) μπορούμε να πετύχουμε ένα άνω φράγμα για το U. Έχουμε λοιπόν,

$$\begin{aligned}\frac{1}{L}U &\le D\log L + DL_0\log(2BS) + 2(n+1)DL_1S\log A\\ &\le D\log L + DL_0\log(2H^{n+1}S) + 2(n+1)DL_1S\log H\\ (\text{λόγω των } (7.10),(7.11)\ ) &\le \frac{1}{12\mathrm{e}}T^{2n^2+n+1} + \frac{1}{12\mathrm{e}}T^{2n^2+n+1} = \frac{1}{6\mathrm{e}}T^{2n^2+n+1}.\end{aligned}$$

[10] Η υπόθεση ότι τα $\ell_1,\dots,\ell_{n+1}$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα χρειάζεται σε αυτό μόνο το σημείο της απόδειξης

Οπότε, λόγω της (7.9),

$$U < \frac{L}{6\mathrm{e}} T^{2n^2+n+1} < T^{(n+1)^3+n^3-n}$$

Ισχύει ότι $(n+1)^3 + n^3 - n < 2(n+1)^3 - 1$. Άρα,

$$U < T^{2(n+1)^3-1}.$$

Οπότε,

$$|\Lambda'| \geq \mathrm{e}^{-(10m^3 D \log H)^{2m^3-1}}.$$

$(n = m - 1)$

□

7.3 Γραμμική ανεξαρτησία των συντελεστών

Σε αυτή την ενότητα θα αποδείξουμε ότι μπορούμε να πετύχουμε ένα φράγμα για το $|\Lambda|$, χωρίς την υπόθεση της «ασθενούς γραμμικής ανεξαρτησίας» των $\beta_1, \ldots, \beta_m$. Για την επίτευξη αυτού του στόχου θα χρειαστούμε το επόμενο λήμμα.

Λήμμα 7.3.1. *Έστω m_0 ακέραιος ≥ 1 και συναρτήσεις U, T_0, με πεδίο ορισμού το $\mathbb{N}\times\mathbb{R}_{\geq 1}$ και τιμές στο $\mathbb{R}_{>0}$, οι οποίες στην περίπτωση που $m_0 \geq 2$, ικανοποιούν την εξής συνθήκη:*

$$U(x-1, 2yT_0(x,y)) + \log T_0(x,y) \leq U(x,y), \ \ \forall (x,y) \in \{2,\ldots,m_0\} \times \mathbb{R}_{\geq 1}. \tag{7.12}$$

Για κάθε $m \in \{1,\ldots,m_0\}$, έστω η εξής πρόταση Π_m:

> *Αν $(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m) \in (\mathfrak{L}^m\times\overline{\mathbb{Q}}^m)_* := \{(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m) \in \mathfrak{L}^m \times \overline{\mathbb{Q}}^m : \beta_1\ell_1 + \ldots + \beta_m\ell_m \neq 0\}$*
>
> *και (D,H) αποδεκτό ζεύγος φραγμάτων για το $(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m)$,*
>
> *τότε*
>
> $$|\Lambda := \beta_1\ell_1 + \ldots + \beta_m\ell_m| > \mathrm{e}^{-U(m, D\log H)}.$$

Για κάθε $m \in \{1,\ldots,m_0\}$ έστω επίσης, η εξής πρόταση Π'_m:

> *Αν $(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m) \in (\mathfrak{L}^m\times\overline{\mathbb{Q}}^m)_* := \{(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m) \in \mathfrak{L}^m \times \overline{\mathbb{Q}}^m : \beta_1\ell_1 + \ldots + \beta_m\ell_m \neq 0\}$*
>
> *και (D,H) αποδεκτό ζεύγος φραγμάτων για το $(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m)$,*

και $b_1\beta_1 + \ldots + b_m\beta_m \neq 0$, *για κάθε* $(b_1, \ldots, b_m) \in \mathbb{Z}^m$ *με* $0 < \max_{1\leq j\leq m} |b_j| < T_0(m, \log H)$,

τότε

$$|\Lambda := \beta_1\ell_1 + \ldots + \beta_m\ell_m| > \mathrm{e}^{-U(m, D\log H)}.$$

Τότε, η αλήθεια της πρότασης Π'_m *για κάθε* $m \in \{1, \ldots, m_0\}$ *συνεπάγεται την αλήθεια της* Π_m *για κάθε* $m \in \{1, \ldots, m_0\}$.

Απόδειξη.

Θα δείξουμε ότι για κάθε $1 \leq m \leq m_0$, η (Π_m) ισχύει ανεξάρτητα από το αν τα $\beta_1, \ldots, \beta_m$ ικανοποιούν, ή όχι, την συνθήκη γραμμικής ανεξαρτησίας (προφανώς, λόγω της υπόθεσης, αν τα $\beta_1, \ldots, \beta_m$ ικανοποιούν την συνθήκη γραμμικής ανεξαρτησίας, τότε η (Π_m) ισχύει).

Η απόδειξη θα γίνει με επαγωγή στο m_0.

Για $m_0 = 1$ το αποτέλεσμα είναι προφανές.

Παίρνουμε τυχαίο m με $2 \leq m \leq m_0$ και υποθέτουμε ότι η πρόταση (Π_{m-1}) ισχύει ακόμα και όταν τα $\beta_1, \ldots, \beta_{m-1}$ δεν ικανοποιούν την συνθήκη γραμμικής ανεξαρτησίας. Θα δείξουμε ότι αυτό ισχύει και για την (Π_m).

Έστω ότι υπάρχουν $(b_1, \ldots, b_m) \in \mathbb{Z}^m$ με $0 < \max\{|b_1, \ldots, |b_m|\} < T_0(m, D\log H)$, τέτοια ώστε:

$$b_1\beta_1 + \ldots + b_m\beta_m = 0.$$

Ένα τουλάχιστον από τα b_i δεν είναι μηδέν, έστω το b_m. Θα απαλείψουμε το β_m,

$$\begin{aligned} 0 \neq b_m\Lambda &= b_m(\beta_1\ell_1 + \ldots + \beta_m\ell_m) - b_m \underbrace{(b_1\beta_1 + \ldots + b_m\beta_m)}_{=0} \\ &= \sum_{i=1}^{m-1} \beta_i\widetilde{\ell}_i, \end{aligned}$$

όπου, $\widetilde{\ell}_i = b_m\ell_i - b_i\ell_m$, για $1 \leq i \leq m-1$ [11].

Αν θέσουμε $\alpha_i = \mathrm{e}^{\ell_i}$ και $\widetilde{\alpha}_i = \mathrm{e}^{\widetilde{\ell}_i}$, $(\alpha_i, \widetilde{\alpha}_i$ αλγεβρικοί αριθμοί), έχουμε ότι $\widetilde{\alpha}_i = \frac{\alpha_i^{b_m}}{\alpha_i^{b_i}}$. Οπότε,

$$h(\widetilde{\alpha}_i) \leq |b_m|h(\alpha_i) + |b_i|h(\alpha_m) \leq \log H',$$

όπου $\log H' = 2(\log H)T_0(m, D\log H)$.

[11] Σημειώνουμε ότι αν τα $\ell_1, \ldots, \ell_m$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα, τότε και τα $\widetilde{\ell}_1, \ldots, \widetilde{\ell}_{m-1}$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα.

Αν τα $\beta_1, \ldots, \beta_{m-1}$ δεν ικανοποιούν την συνθήκη γραμμικής ανεξαρτησίας, τότε λόγω της επαγωγικής υπόθεσης έχουμε ότι:

$$|b_m\Lambda| \geq \mathrm{e}^{-U(m-1, D\log H')}.$$

Αν τα $\beta_1, \ldots, \beta_{m-1}$ ικανοποιούν την συνθήκη γραμμικής ανεξαρτησίας, τότε λόγω του ότι ισχύει η Π_{m-1}, έχουμε πάλι ότι:

$$|b_m\Lambda| \geq \mathrm{e}^{-U(m-1, D\log H')}.$$

Άρα, σε κάθε περίπτωση,

$$\begin{aligned} |\Lambda| &\geq \frac{\mathrm{e}^{-U(m-1, D\log H')}}{|b_m|} \\ &\geq \mathrm{e}^{-U(m-1, D\log H') - \log T_0(m, D\log H)} \\ \text{(λόγω της 7.12)} \quad &\geq \mathrm{e}^{-U(m, D\log H)}. \end{aligned}$$

□

Εφαρμόζουμε το λήμμα 7.3.1, για τις συναρτήσεις:

$$U(x,y) = (10^3x^3y)^{\kappa(x)}, \;\; T_0(x,y) = 2[10^3x^3y]^{2(x-1)^2}, \;\; x \in \mathbb{N}, y \in \mathbb{R}_{\geq 1}.$$

στο $(x,y) = (m, D\log H)$, $m \geq 2$.

Λόγω των ανισοτήτων: (όπου $T_0 = T_0(m, D\log H)$)

$$U(m-1, 2D(\log H)T_0) \leq \Big(4(10^3m^3D\log H)^{2(m-1)^2+1}\Big)^{\kappa(m-1)}$$

και

$$\big(2(m-1)^2+1\big)\kappa(m-1) \leq (2m^2-m)\kappa(m-1) \leq \kappa(m) - m\kappa(m-1),$$

συμπεραίνουμε την αλήθεια της ανισότητας (7.12).

Άρα, μέσω του λήμματος 7.3.1, συμπεραίνουμε από το θεώρημα 7.2.1, την εξής [12]

Πρόταση 7.3.2. *Έστω, $\ell_1, \ldots, \ell_m \in \mathfrak{L}$ τα οποία είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα ($\mathrm{e}^{\ell_1} = \alpha_1, \ldots, \mathrm{e}^{\ell_m} = \alpha_m \in \overline{\mathbb{Q}}$), $\beta_1, \ldots, \beta_m \in \overline{\mathbb{Q}}$ και ο αριθμός*

$$\Lambda = \beta_1\ell_1 + \ldots + \beta_m\ell_m$$

[12] Στο θεώρημα 7.2.1 έχουμε $|\Lambda| \geq \mathrm{e}^{-(10^3m^3D\log H)^{2m^3}} \geq \mathrm{e}^{-(10^3m^3D\log H)^{k(m)}}$, για κάθε $m \in \mathbb{N}$

δεν είναι μηδέν. Υποθέτουμε ότι το ζεύγος φυσικών αριθμών (D, H) *είναι ένα αποδεκτό ζεύγος φραγμάτων του* $(\ell_1, \ldots, \ell_m, \beta_1, \ldots, \beta_m) \in \mathfrak{L} \times \overline{\mathbb{Q}}^m$.

Τότε

$$|\Lambda| \geq \mathrm{e}^{-(10^3 m^3 D \log H)^{\kappa(m)}},$$

όπου $\kappa(m) = 2^m (m!)^2$.

□

Παρατήρηση:

Στην πρόταση 7.3.2 το φράγμα που πετυχαίνουμε για το $|\Lambda|$ είναι ασθενέστερο από αυτό του θεωρήματος 7.2.1. Θα πετυχαίναμε το ίδιο φράγμα αν η ανισότητα (7.12) ήταν αληθής για τις συναρτήσεις:

$$U(x, y) = (10^3 x^3 y)^{2x^3}, \;\; T_0(x, y) = 2[10^3 x^3 y]^{2(x-1)^2}, \;\; x \in \mathbb{N}, y \in \mathbb{R}_{\geq 1}.$$

για $(x, y) = (m, D \log H)$.

Όμως για $(x, y) = (3, 1 \log \mathrm{e})$, με απλούς υπολογισμούς συμπεραίνουμε ότι η ανισότητα 7.12 δεν είναι αληθής για τις

$$U(x, y) = (10^3 x^3 y)^{2x^3}, \;\; T_0(x, y) = 2[10^3 x^3 y]^{2(x-1)^2}.$$

7.4 Γραμμική εξάρτηση των λογαρίθμων

Σε αυτή την ενότητα θα δείξουμε ότι το συμπέρασμα της πρότασης 7.3.2 ισχύει και στην περίπτωση που τα $\ell_1, \ldots, \ell_m \in \mathfrak{L}$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένα (θα αποδείξουμε δηλαδή την γενική περίπτωση, δηλαδή το θεώρημα 7.1.1). Θα χρειαστούμε το επόμενο λήμμα,

Λήμμα 7.4.1. *Έστω* $\ell_1, \ldots, \ell_m \in \mathfrak{L}$ $\mathbb{Q}-$*γραμμικώς εξαρτημένα. Για* $j = 1, \ldots, m$, *θέτουμε* $\mathrm{e}^{\ell_j} = \alpha_j \in \overline{\mathbb{Q}}$ *και* $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_m) : \mathbb{Q}]$. *Έστω,* $\log H \geq 1$, *τέτοιο ώστε:*

$$\max_{1 \leq j \leq m} h(\alpha_j) \leq \log H \text{ και } \max_{1 \leq j \leq m} |\ell_j|/D \leq \log H.$$

Τότε υπάρχουν $(t_1, \ldots, t_m) \in \mathbb{Z}^m \setminus (0, \ldots, 0)$, *τέτοια ώστε:*

$$t_1 \ell_1 + \ldots + t_m \ell_m = 0,$$

με $\max\{|t_1|, \ldots, |t_m|\} \leq (10^3 m D^3 \log H)^{m-1}$.

Απόδειξη.

(Ένα σχόλιο που θα μας χρειαστεί στην απόδειξη:

Για κάθε $n \in \mathbb{Z}^+$ με $\varphi(n)$ συμβολίζουμε την συνάρτηση του Euler, οπότε $\varphi(n) = n\prod_{p|n}(1-\frac{1}{p})$. Έχουμε ότι:

$$\varphi(n)^2 = n^2 \prod_{p|n}(1-\frac{1}{p})^2 = n \cdot \left(\frac{n}{\prod_{p|n}\left(\frac{p}{p-1}\right)^2} \right).$$

Όμως,

$$\prod_{p|n}\left(\frac{p}{p-1}\right)^2 \leq \prod_{p|n} p \prod_{p|n} \frac{p}{(p-1)^2} \leq 2n.$$

Οπότε, $\varphi(n)^2 \geq \frac{n}{2}$.

Άρα, αν $\varphi(n) = D$, τότε $n \leq 2D^2$.)

Για $m = 1$ το λήμμα είναι τετριμμένο, οπότε υποθέτουμε ότι $m \geq 2$.

Μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι οποιοιδήποτε $m-1$ από τους $\ell_1, \ldots, \ell_m$ είναι γραμμικώς ανεξάρτητοι. Οπότε, υπάρχει μοναδικό (κατά προσέγγιση προσήμου) σύνολο πρώτων μεταξύ τους ακεραίων $t_1, \ldots, t_m$, με

$$t_1\ell_1 + \ldots + t_m\ell_m = 0.$$

Οπότε,

$$\alpha_1^{t_1} \cdots \alpha_m^{t_m} = 1.$$

Έστω k ακέραιος με $1 \leq k \leq m$. Ορίζουμε:

$$c_j = c = (10^3 m D^3 \log H)^{-1}, \;\; 1 \leq j \leq m, j \neq k,$$

και

$$c_k = \frac{1}{c^{m-1}},$$

(Παρατηρούμε ότι $c_1 \cdots c_m = 1$).

Με κατάλληλη εφαρμογή του θεωρήματος των γραμμικών μορφών του Minkowski Α΄.11.2,

(Εδώ, $1 \leq i \leq m, \;\; 1 \leq j \leq m$,

$$B = (\beta_{ij}) = \begin{pmatrix} 1 & 0 & \ldots & 0 & -\frac{t_1}{t_k} & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & -\frac{t_2}{t_k} & 0 & \ldots & 0 \\ \vdots & & & \ddots & & & & \\ 0 & 0 & \ldots & 0 & -\frac{t_k}{t_k} & 0 & \ldots & 0 \\ \vdots & & & & & & \ddots & \\ 0 & 0 & \ldots & 0 & -\frac{t_m}{t_k} & 0 & \ldots & 1 \end{pmatrix},$$

ο οποίος έχει ορίζουσα -1.)

συμπεραίνουμε ότι υπάρχουν $s_1, \ldots, s_m \in \mathbb{Z}$, όχι όλοι μηδέν, τέτοιοι ώστε:

$$\left| s_j - s_k \frac{t_j}{t_k} \right| < c_j, \;\; 1 \leq j \leq m, j \neq m,$$

και

$$|s_k| \leq \frac{1}{c^{m-1}}.$$

Θα δείξουμε ότι $s_1\ell_1 + \ldots + s_m\ell_m = 0$.
(Τότε, αφού $t_1, \ldots, t_m$ είναι πρώτοι μεταξύ τους, έχουμε ότι $(s_1, \ldots, s_m) = \lambda(t_1, \ldots, t_m)$, όπου $\lambda \in \mathbb{Z}$. Άρα, για το τυχαίο k με $1 \leq k \leq m$, έχουμε ότι $|t_k| \leq |s_k| \leq c^{1-m} = (10^3 m D^3 \log H)^{m-1}$).

Θα δείξουμε πρώτα ότι $\alpha = \alpha_1^{s_1} \cdots \alpha_m^{s_m}$ είναι ρίζα της μονάδας.

Έχουμε λοιπόν,

$$\alpha^{t_k} = \prod_{j=1}^{m} \alpha_j^{s_j t_k} = \frac{\prod_{j=1}^{m} \alpha_j^{s_j t_k}}{1^{s_k}}$$

$$= \frac{\prod_{j=1}^{m} \alpha_j^{s_j t_k}}{\alpha_1^{t_1 s_k} \cdots \alpha_m^{t_m s_k}} = \prod_{1 \leq j \leq m} \alpha_j^{s_j t_k - s_k t_j}.$$

Οπότε,

$$h(\alpha^{t_k}) = h\Big(\prod_{1 \leq j \leq m} \alpha_j^{s_j t_k - s_k t_j} \Big).$$

Λόγω του λήμματος 3.4.1, έχουμε ότι:

$$|t_k| \cdot h(\alpha) \leq \sum_{\substack{1 \leq j \leq m \\ j \neq k}} |s_j t_k - s_k t_j| \cdot h(\alpha_j).$$

Άρα,

$$h(\alpha) \leq cm \log H \leq (10D)^{-3}.$$

Οπότε, από το θεώρημα 3.7.1 έπεται ότι το α είναι ρίζα της μονάδας.

Έστω n η τάξη του α. Τότε το ελάχιστο πολυώνυμο του α υπέρ το $\mathbb{Q}$ είναι το $n-$οστό κυκλοτομικό πολυώνυμο, άρα $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \varphi(n)$. Όμως $\alpha \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, άρα $\varphi(n) \leq D$. Οπότε, $n \leq 2D^2 \leq \frac{2\pi}{cm|\ell_j|}$, για κάθε $j = 1, \ldots, m$. Από την άλλη, λόγω της $1 = \alpha^n = \alpha_1^{ns_1} \cdot \alpha_m^{ns_m}$, έχουμε

$$n \sum_{j=1}^{m} s_j \ell_j \in 2\pi i \mathbb{Z}.$$

Επίσης,

$$\Big|n\sum_{j=1}^{m} s_j\ell_j\Big| = \Big|n\sum_{j=1}^{m}\Big(s_j - \frac{s_k t_j}{t_k}\Big)\ell_j\Big|$$
$$< n\sum_{\substack{1\le j\le m\\ j\neq k}} c|\ell_j| \le (m-1)\cdot\frac{2\pi}{m} < 2\pi.$$

Άρα,

$$s_1\ell_1 + \ldots + s_m\ell_m = 0.$$

□

Από το λήμμα 7.4.1 συμπεραίνουμε το κύριο συμπέρασμα της παραγράφου:

Λήμμα 7.4.2. *Έστω m_0 ακέραιος ≥ 1 και $U : \mathbb{N}\times\mathbb{R}_{\geq 1}\to\mathbb{R}_{>0}$, η οποία, στην περίπτωση που $m_0 \geq 2$, ικανοποιεί την εξής συνθήκη για κάθε $m \in \{2,\ldots,m_0\}$:*

$$U\big(m-1, D\log(2TH^2)\big)+\log T \le U(m, D\log H), \quad \text{όπου } T = (10^3 mD^3\log H)^{m-1} \tag{7.13}$$

για κάθε $D\geq 1$ και κάθε $H\geq 1$.
Για κάθε $m\in\{1,\ldots,m_0\}$ έστω $(\mathfrak{L}^m\times\overline{\mathbb{Q}}^m)_* := \{(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m)\in\mathfrak{L}^m\times\overline{\mathbb{Q}}^m : \beta_1\ell_1+\ldots+\beta_m\ell_m\neq 0\}$.
Έστω ότι, για κάθε $m\in\{1,\ldots,m_0\}$, για κάθε $(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m)\in\mathfrak{L}^m\times\overline{\mathbb{Q}}^m$, με τα $\ell_1,\ldots,\ell_m$ $\mathbb{Q}-$γραμμικώς ανεξάρτητα, και κάθε ζεύγος φραγμάτων (D,H), αποδεκτό για το $(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m)$ ισχύει η ανισότητα:

$$|\Lambda := \beta_1\ell_1+\ldots+\beta_m\ell_m| > \mathrm{e}^{-U(m,D\log H)} \tag{7.14}$$

Τότε, για κάθε $m\in\{1,\ldots,m_0\}$, κάθε $(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m)\in\mathfrak{L}^m\times\overline{\mathbb{Q}}^m$ και κάθε ζεύγος φραγμάτων (D,H) αποδεκτό για το $(\ell_1,\ldots,\ell_m,\beta_1,\ldots,\beta_m)$, ισχύει η (7.14).

Απόδειξη.

Θα δείξουμε ότι για κάθε $1\leq m\leq m_0$, η (Π_m) ισχύει ανεξάρτητα από το αν τα $\ell_1,\ldots,\ell_m$ είναι γραμμικώς ανεξάρτητα, ή όχι, υπέρ το $\mathbb{Q}$ (προφανώς, λόγω της υπόθεσης, αν τα $\ell_1,\ldots,\ell_m$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα, τότε η (Π_m) ισχύει).

Η απόδειξη θα γίνει με επαγωγή στο m_0.

Για $m_0 = 1$ έχουμε το ζητούμενο. Αφού ο $\Lambda = \beta_1\ell_1$ δεν είναι μηδέν, συμπεραίνουμε ότι ο ℓ_1 είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητος. Οπότε, η Π_1 ισχύει λόγω της υπόθεσης.

Έστω $m_0 \geq 2$. Επιλέγουμε τυχαίο $m \in \{2, \ldots, m_0\}$. Υποθέτουμε ότι η πρόταση (Π_{m-1}) ισχύει ακόμα και όταν οι $\ell_1, \ldots, \ell_{m-1}$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένοι. Θα δείξουμε ότι το ίδιο συμβαίνει και για την (Π_m).

Έστω,

$$0 \neq \Lambda = \beta_1\ell_1 + \ldots + \beta_m\ell_m,$$

και έστω ότι οι $\ell_1, \ldots, \ell_m$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένοι.

Από το λήμμα 7.4.1, συμπεραίνουμε ότι υπάρχουν $t_1, \ldots, t_m \in \mathbb{Z}$, όχι όλοι μηδέν, τέτοιοι ώστε:

$$t_1\ell_1 + \ldots + t_m\ell_m = 0,$$

και $0 < \max\{|t_1|, \ldots, |t_m|\} \leq T$, όπου $T = (10^3 m D^3 \log H)^{m-1}$.

Τουλάχιστον ένα από τα t_i δεν είναι μηδέν, έστω το t_m.

Θα απαλείψουμε το ℓ_m ως εξής:

$$\begin{aligned} 0 \neq t_m\Lambda &= t_m(\beta_1\ell_1 + \ldots + \beta_m\ell_m) - \beta_m \underbrace{(t_1\ell_1 + \ldots + t_m\ell_m)}_{=0} \\ &= \widetilde{\beta}_1\ell_1 + \ldots + \widetilde{\beta}_{m-1}\ell_{m-1}, \end{aligned}$$

όπου $\widetilde{\beta}_j = t_m\beta_j - \beta_m t_j,\ \ 1 \leq j \leq m-1$.

Από το λήμμα 3.4.2, για $f_j(x_1, x_2) = t_m x_1 - t_j x_2,\ \ 1 \leq j \leq m-1$, έχουμε ότι:

$$\begin{aligned} h(\widetilde{\beta}_j) &\leq \log(2T) + h(\beta_j) + h(\beta_m) \\ &\leq \log(2T) + \log H + \log H \leq \log H, \end{aligned}$$

όπου $H = 2TH^2$.

Αν τα $\ell_1, \ldots, \ell_{m-1}$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένα, τότε από επαγωγική υπόθεση,

$$|t_m\Lambda| \geq \mathrm{e}^{-U(m-1, \log H')}.$$

Αν τα $\ell_1, \ldots, \ell_{m-1}$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα τότε από την αλήθεια της Π_{m-1} έπεται ότι:

$$|t_m\Lambda| \geq \mathrm{e}^{-U(m-1, \log H')}.$$

Άρα, σε κάθε περίπτωση,

$$\begin{aligned} |\Lambda| &\geq \frac{\mathrm{e}^{-U(m-1, \log H')}}{|t_m|} \\ &\geq \mathrm{e}^{-U(m-1, \log H') - \log T} \\ \text{(λόγω της 7.13)} \quad &\geq \mathrm{e}^{-U(m, D\log H)}. \end{aligned}$$

□

Εφαρμόζουμε το λήμμα 7.4.2 για την συνάρτηση

$$U(x,y) = (10^3 x^3 y)^{\kappa(x)}, \;\; x \in \mathbb{N}, y \in \mathbb{R}_{\geq 1}\,, \quad \kappa(x) = 2^x (x!)^2\,,$$

στο $(x,y) = (m, D\log H)$, $m \geq 2$.

Η ανισότητα 7.13 του λήμματος 7.4.2 είναι αληθής.

(Θέλουμε να αποδείξουμε ότι:

$$U\big(m-1, D\log(2TH^2)\big) + \log T \leq U(m, D\log H).$$

Αρκεί να αποδείξουμε ότι:

$$2\Big(10^3 m^3 D\log(2TH^2)\Big)^{\kappa(m-1)} \leq \Big(10^3 m^3 D\log H\Big)^{\kappa(m)}.$$

Αρκεί δηλαδή,

$$2\Big(3\cdot 10^3 m^3 D\log H + 10^3 m^3 D\log T\Big)^{\kappa(m-1)} \leq \Big(10^3 m^3 D\log H\Big)^{\kappa(m)}.$$

Για $c = 12m^2$, (όχι το βέλτιστο c) έχουμε ότι:

$$\log T \leq \log H^c.$$

Άρα, αρκεί

$$2\Big((3+12m^2)\cdot 10^3 m^3 D\log H\Big)^{\kappa(m-1)} \leq \Big(10^3 m^3 D\log H\Big)^{\kappa(m)}.$$

Σημειώνουμε επίσης ότι $\kappa(m) = 2m^2\kappa(m-1)$.

Το συμπέρασμα έπεται τώρα εύκολα.)

Άρα, μέσω του λήμματος 7.4.2, συμπεραίνουμε από την πρόταση 7.3.2 το θεώρημα 7.1.1.

Κεφάλαιο 8

Η εξίσωση του Thue

8.1 Ιστορικά σχόλια

Το 1909 ο A. Thue [27], βελτίωσε το αποτέλεσμα του Liouville (πρβλ. θεώρημα 3.5.2, όπου $|\cdot|_v$ αρχιμήδεια απόλυτη τιμή, συγκεκριμένα η συνηθισμένη απόλυτη τιμή του $\mathbb{C}$):

Αν α είναι αλγεβρικός αριθμός βαθμού n, τότε υπάρχει σταθερά $c(\alpha)$, τέτοια ώστε:

$$\text{για κάθε } \frac{p}{q} \in \mathbb{Q} \ , \left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^{\frac{n}{2}+1}}.$$

Στο ίδιο άρθρο, χρησιμοποιώντας το παραπάνω αποτέλεσμα, απέδειξε το εξής :

Αν $F(X,Y) \in \mathbb{Z}[X,Y]$ είναι ένα ανάγωγο ομογενές πολυώνυμο βαθμού τουλάχιστον 3 και m ένας μη μηδενικός ρητός ακέραιος, τότε η εξίσωση

$$F(X,Y) = m, \tag{8.1}$$

έχει πεπερασμένου πλήθους ακέραιες λύσεις (x,y).

Πράγματι, έστω ότι η $F(X,Y) = m$ έχει άπειρες ακέραιες λύσεις και έστω (x,y) μια τέτοια ακέραια λύση. Τότε,

$$F(X,Y) = \prod_{i=1}^{n}(x - \xi^{(i)}y) = m,$$

όπου $\xi^{(i)}$ (αλγεβρικοί αριθμοί με βαθμό ≥ 3) οι ρίζες του $g(X) = F(X,1) = 0$, $i = 1, \ldots, n$.

Υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι:

$$\left|\frac{x}{y}-\xi^{(1)}\right| \leq \left|\frac{x}{y}-\xi^{(i)}\right|, \;\; i=2,\ldots,n.$$

Από την τριγωνική ανισότητα προκύπτει ότι:

$$\begin{aligned}\left|\frac{x}{y}-\xi^{(i)}\right| &\geq \frac{1}{2}\left(\left|\frac{x}{y}-\xi^{(i)}\right|+\left|\frac{x}{y}-\xi^{(1)}\right|\right)\\ &\geq \frac{1}{2}|\xi^{(i)}-\xi^{(1)}|, \;\; \text{για κάθε } i=2,\ldots,n.\end{aligned}$$

Οπότε,

$$|F(x,y)| = |y^n|\left|\frac{x}{y}-\xi^{(1)}\right|\cdots\left|\frac{x}{y}-\xi^{(n)}\right|,$$

ή

$$|m| \geq k\cdot|y^n|\cdot\left|\frac{x}{y}-\xi^{(1)}\right|,$$

όπου $k=\frac{1}{2^{n-1}}\prod_{i=2}^{n}|\xi^{(i)}-\xi^{(1)}|$.

Από αυτό έχουμε ότι:

$$\frac{m}{k|y|^n} \geq \left|\frac{x}{y}-\xi^{(1)}\right|.$$

Οπότε, από το θεώρημα του Thue,

$$\frac{c}{y^{\frac{n}{2}+1}} \leq \frac{m}{ky^n},$$

δηλαδή,

$$\frac{1}{y^{\frac{n}{2}+1}} \leq \frac{m(ck)^{-1}}{y^n}.$$

Όμως, για $n \geq 3$, η παραπάνω ανισότητα ισχύει για πεπερασμένο πλήθος ζευγάρια (x,y), το οποίο έρχεται σε αντίφαση με την υπόθεση. Άρα, η $F(X,Y)=m$ έχει πεπερασμένο πλήθος ακέραιες λύσεις.

Παρατηρούμε ότι η απόδειξη του Thue είναι μη κατασκευαστική.

Η πρώτη κατασκευαστική απόδειξη του θεωρήματος του Thue δόθηκε το 1968 από τον Alan Baker [7], ως συνέπεια της μελέτης που έκανε στις γραμμικές μορφές λογαρίθμων αλγεβρικών αριθμών. Το αποτέλεσμα του Baker εξασφαλίζει ένα φράγμα, το οποίο υπολογίζεται, για το $\max\{|x|,|y|\}$ των ακέραιων λύσεων (x,y) της (8.1).

8.2 Η κατασκευαστική απόδειξη

Έστω

$$F(X,Y)=\sum_{i=0}^{n} f_i X^{n-i}Y^i \in \mathbb{Z}[X,Y],$$

με $\deg(F)\geq 3$ και έστω m ένας μη αρνητικός ακέραιος. Θεωρούμε την εξίσωση του Thue

$$F(X,Y)=m, \tag{8.2}$$

με αγνώστους $X,Y\in\mathbb{Z}$. Αν το F δεν είναι ανάγωγο πάνω από το $\mathbb{Q}$, τότε η (8.2) ανάγεται σε ένα σύστημα πεπερασμένου πλήθους εξισώσεων της ίδιας μορφής με ομογενή ανάγωγα πολυώνυμα [1]. Για τις εξισώσεις βαθμού 1 και 2 (εξισώσεις του Pell) γνωρίζουμε την διαδικασία επίλυσης τους. Οπότε, μπορούμε να υποθέσουμε από τώρα ότι το F είναι ανάγωγο ομογενές πολυώνυμο πάνω από το $\mathbb{Q}$ βαθμού $n\geq 3$.

Θεώρημα 8.2.1. *Έστω $F(X,Y)$ ένα ανάγωγο ομογενές πολυώνυμο με ακέραιους συντελεστές και βαθμό ≥ 3. Έστω m ένας μη μηδενικός ακέραιος. Υπάρχει μια θετική σταθερά c, η οποία είναι υπολογίσιμη (σε όρους του F), τέτοια ώστε για όλες τις ακέραιες λύσεις (x,y) της διοφαντικής εξίσωσης $F(X,Y)=m$ να ισχύει το εξής:*

$$\max\{|x|,|y|\}<c.$$

Απόδειξη. Αρχικά θα κάνουμε μια περιγραφή της απόδειξης και ύστερα θα παρουσιάσουμε σε βήματα τις λεπτομέρειες.

Έστω $F(X,Y)=f_0X^n+\ldots+f_{n-1}XY^{n-1}+f_nU^n$, με $n\geq 3$ και $F(X,Y)=m$. Στόχος μας είναι η απόδειξη ύπαρξης υπολογίσιμης σταθεράς c, τέτοια ώστε για κάθε ακέραια λύση (x,y) της εξίσωσης $F(X,Y)=m$, να ισχύει $\max\{|x|,|y|\}<c$. Θεωρώντας το $f_0^{n-1}F(X,Y)=f_0^{n-1}m$ και $f_0^{n-1}F(X,Y)=F'(X,Y)$ με $x=f_0X$, παρατηρούμε ότι μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι $f_0=1$.

Έστω

$$g(X)=F(X,1).$$

Από τις n ρίζες, έχει s πραγματικές και $2t$ συζυγείς μιγαδικές. Αν $s=0$ τότε η επίλυση της εξίσωσης Thue είναι τετριμμένη (πρβλ. πρόταση 8.2.2). Υποθέτουμε λοιπόν, ότι έχει τουλάχιστον μια πραγματική ρίζα. Αριθμούμε τις ρίζες της $g(X)=0$, ως εξής:

$$\xi^{(1)},\ldots,\xi^{(s)},\ \ (s\geq 1),\ \text{οι πραγματικές ρίζες}$$

[1] Αν ένα πολυώνυμο διαιρεί ένα ομογενές πολυώνυμο είναι και αυτό ομογενές πολυώνυμο

και

$$\xi^{(s+1)}, \overline{\xi^{(s+1)}}, \ldots, \xi^{(s+t)}, \overline{\xi^{(s+t)}}, \text{ οι μιγαδικές ρίζες },$$

οπότε, έχουμε $t \geq 0$ ζευγάρια συζυγών μιγαδικών ριζών, και $s + 2t = n$.

Δουλεύουμε στο σώμα $K = \mathbb{Q}(\xi)$, όπου $g(\xi) = 0$. Το σύνολο των αλγεβρικών ακεραίων του σώματος K είναι δακτύλιος, του οποίου τα αντιστρέψιμα στοιχεία (μονάδες) είναι πεπερασμένα παραγόμενα και μάλιστα, οι γεννήτορες άπειρης τάξης είναι r το πλήθος, όπου $r = s+t-1$ (Θεώρημα Α΄.3.2, Dirichlet).

Έστω (x, y) μια ακέραια λύση της εξίσωσης Thue. Τότε

$$m = F(x, y) = \left(x - \xi^{(1)}y\right) \cdots \left(x - \xi^{(n)}y\right) = \beta^{(1)} \cdots \beta^{(n)},$$

όπου $\beta^{(i)} := x - \xi^{(i)}y$, $i = 1, \ldots, m$.

Η σχέση $\prod_{i=1}^{n} \beta^{(i)} = m$, είναι ισοδύναμη με την σχέση $\mathrm{Norm}(\beta) = m$, ($\beta = x - \xi y$). Από την Αλγεβρική θεωρία Αριθμών, είναι γνωστό ότι υπάρχει πεπερασμένο πλήθος αλγεβρικών ακεραίων $\mu \in K$, όπου για κάθε αλγεβρικό ακέραιο α του K με $\mathrm{Norm}(\alpha) = m$, να είναι $\alpha =$(κάποιο μ)$\cdot$(κάποια μονάδα). Άρα,

$$x - \xi y = \beta = \mu \cdot \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r},$$

και μεταφέραμε το πρόβλημα σε άγνωστους εκθέτες.

Στο ξ μπορώ να δώσω n διαφορετικές τιμές (μέσω των n εμφυτεύσεων του K στο $\mathbb{C}$. Οι εκθέτες παραμένουν ίδιοι λόγω ισομορφισμού). Έστω λοιπόν,

$$x - \xi^{(i)}y = \mu^{(i)}(\varepsilon_1^{(i)})^{a_1} \cdots (\varepsilon_r^{(i)})^{a_r}. \tag{8.3}$$

Επανερχόμαστε στην σχέση $\prod_{i=1}^{n} \beta^{(i)} = m$. Από αυτή την σχέση προκύπτει (πρβλ. 1ο βήμα) ότι αν η λύση (x, y) δεν είναι πολύ «μικρή», τότε αναγκαστικά, ένα ακριβώς από αυτά τα $\beta^{(i)}$ είναι πολύ μικρό σε σχέση με το y και όλα τα άλλα $\beta^{(i)}$ είναι «μεγάλα».

Συγκεκριμένα, υπάρχει i_0 τέτοιο ώστε:

$$|\beta^{(i_0)}| < c_2|y|^{-(n-1)}$$

και για κάθε $i \neq i_0$,

$$|\beta^{(i)}| > c_1|y|,$$

με c_1, c_2 θετικές σταθερές. Επίσης, αποδεικνύεται ότι $\xi^{(i_0)} \in \mathbb{R}$.

Για τρία διαφορετικά i, έστω i_0, j, k, θεωρούμε τις σχέσεις [2]

$$\beta^{(i)} = x - \xi^{(i)}y$$
$$\beta^{(j)} = x - \xi^{(j)}y$$
$$\beta^{(k)} = x - \xi^{(k)}y,$$

[2] μόνο σε αυτό το σημείο γίνεται χρήση του $n \geq 3$

και από τις τρεις σχέσεις απαλείφουμε τα x, y και οδηγούμαστε (πρβλ. 2ο βήμα) στην σχέση

$$\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\beta^{(k)}}{\beta^{(j)}}-1=\frac{\xi^{(k)}-\xi^{(j)}}{\xi^{(k)}-\xi^{(i_0)}}\cdot\frac{\beta^{(i_0)}}{\beta^{(j)}}.$$

Στην παραπάνω σχέση, παρατηρούμε ότι το δεξιό μέλος είναι αρκετά μικρό. Άρα, το αριστερό μέλος μπορεί να προσεγγιστεί πολύ ικανοποιητικά από το

$$\Lambda:=\log\Big|\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\beta^{(k)}}{\beta^{(j)}}\Big|.$$

Άρα, λόγω της σχέσης (8.3), καταλήγουμε στην σχέση

$$\Lambda=\log\Big|\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\mu^{(k)}}{\mu^{(j)}}\Big|+\sum_{i=1}^{r}a_i\log\Big|\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(k)}}\Big|.$$

Από αυτή την σχέση, αποδεικνύται σχετικά εύκολα (3ο βήμα) ότι το $|\Lambda|$ είναι πολύ «μικρό» σε σχέση με το $|y|$. Συγκεκριμένα,

$$|\Lambda|<(\text{σταθερά})\cdot|y|^{-n}.$$

Με διάφορους τεχνικούς χειρισμούς (5ο βήμα), εισάγουμε στο παραπάνω φράγμα το $A=\max\{|a_1|,\dots,|a_r|\}$,

$$|\Lambda|<K_1\mathrm{e}^{-K_2A}, \tag{8.4}$$

όπου K_1, K_2, υπολογίσιμες θετικές σταθερές.

Αφού $\Lambda\neq 0$, από το φράγμα για τις γραμμικές μορφές λογαρίθμων (πρβλ. κεφάλαιο 7), προκύπτει (7ο βήμα) η εξής ανίσωση

$$|\Lambda|>\mathrm{e}^{-K_3(\log A+K_4)^{\kappa}}, \tag{8.5}$$

όπου K_3, K_4, κ, υπολογίσιμες θετικές σταθερές.

Από τις (8.4) και (8.5) προκύπτει (8ο βήμα) ότι

$$A<C_1+C_2(\log A+K_4)^{\kappa},$$

όπου C_1, C_2 υπολογίσιμες θετικές σταθερές. Οπότε, προκύπτει ένα άνω φράγμα για το A.

Από το άνω φράγμα για το A, προκύπτει ένα άνω φράγμα για τα $\beta^{(i)}$ (9ο βήμα).

Από τις σχέσεις, (οι οποίες προκύπτουν από την διαδικασία της απαλοιφής)

$$y = \frac{\beta^{(j)} - \beta^{(i)}}{\xi^{(i)} - \xi^{(j)}}$$

και

$$x = \xi^{(i)} \frac{\beta^{(j)} - \beta^{(i)}}{\xi^{(i)} - \xi^{(j)}} + \beta^{(i)},$$

βρίσκουμε φράγμα για τα x και y (10ο βήμα).

Θα παρουσιάσουμε τώρα τις λεπτομέρειες τις απόδειξης στα παρακάτω βήματα.

Με $c, c_1, c_2, \ldots, c_{16}$ συμβολίζουμε θετικές σταθερές οι οποίες μπορούν να υπολογιστούν με ακριβή υπολογισμό (στις περισσότερες από αυτές ο ακριβής υπολογισμός παραλείπεται).

- Βήμα 1ο. *Φράγματα των* β_i.

Έστω $i_0 \in \{1, \ldots, n\}$, τέτοιο ώστε:

$$|\beta^{(i_0)}| = \min_{1 \le i \le n} |\beta^{(i)}|.$$

Έχουμε ότι:

$$\prod_{i=1}^{n} |\beta^{(i)}| = |m|.$$

Από την ελαχιστότητα του $|\beta^{(i_0)}|$, έχουμε ότι για κάθε $i \neq i_0$:

$$\begin{aligned} |y||\xi^{(i)} - \xi^{(i_0)}| &= |\beta^{(i)} - \beta^{(i_0)}| \\ &\le |\beta^{(i)}| + |\beta^{(i_0)}| \le 2|\beta^{(i)}|. \end{aligned}$$

Άρα,

$$|\beta^{(i)}| \ge c_1|y|, \quad \text{για κάθε } i \neq i_0. \tag{8.6}$$

Επίσης,

$$\begin{aligned}|\beta^{(i_0)}| &= |m| \prod_{i\neq i_0} |\beta^{(i)}|^{-1} \\ &\leq |m| \prod_{i\neq i_0} \big(\frac{1}{2}|y||\xi^{(i)} - \xi^{(i_0)}|^{-1}\big) \\ &= \frac{2^{n-1}|m|}{\Big|\prod_{i\neq i_0}\big(\xi^{(i)} - \xi^{(i_0)}\big)\Big||y|^{n-1}} \\ &= \frac{2^{n-1}|m|}{|g'(\xi^{(i_0)})||y|^{n-1}} \\ &= c_2|y|^{-(n-1)}.\end{aligned}$$

(Γενικά: Αν $f(t) \in \mathbb{Q}(x)$ ένα μονικό πολυώνυμο με ρίζες τα $t_1, \ldots, t_n \in \mathbb{C}$, τότε $|f(t)| = |(t-t_1)\cdots(t-t_n)|$. Οπότε, για κάθε $t \neq t_i$, $\big(\log f(t)\big)' = \frac{1}{f(t)}f'(t)$. Άρα, $\big(\log(|t-t_1|+\ldots+\log|t-t_n|)\big)' = \frac{1}{f(t)}f'(t)$, δηλαδή $\sum_{i=1}^{n}\frac{f(t)}{t-t_i} = f'(t)$.)

Αν $i_0 > s$, ($t \geq 1$), τότε

$$\begin{aligned}\Big|\frac{x}{y} - \xi^{(i_0)}\Big| &= \frac{\beta^{(i_0)}}{|y|} \\ &\leq \frac{2^{n-1}|m|}{|g'(\xi^{(i_0)})|}\cdot|y|^n,\end{aligned}$$

το οποίο είναι αδύνατο για αρκετά μεγάλο $|y|$. Άρα, $i_0 \in \{1,\ldots,s\}$.

Για

$$|y| > y_1 = \lceil (4c_2)^{1/(n-2)} \rceil \tag{8.7}$$

προκύπτει ότι

$$\begin{aligned}\Big|\frac{x}{y} - \xi^{(i_0)}\Big| = |\beta^{(i_0)}||y|^{-1} \leq c_2|y|^{-n} &\leq \frac{1}{4}y_1^{n-2}|y|^{-n} \\ &\leq \frac{1}{2}|y|^{-2}\end{aligned}$$

και άρα $\Big|\frac{x}{y} - \xi^{(i_0)}\Big| < \frac{1}{2}|y|^{-2}$, αφού το $\xi^{(i_0)}$ είναι άρρητος.

Οπότε, για κάθε $i = 1, \ldots, n$ και για $y > y_1$,

$$\begin{aligned}|\beta^{(i)}| = |x - \xi^{(i)}y| &= |x - \xi^{(i)}y + y\xi^{(i_0)} - y\xi^{(i_0)}| \\ &\leq |x - y\xi^{(i_0)}| + |y||\xi^{(i)} - \xi^{\xi^{(i_0)}}| \\ &\leq \frac{1}{2|y|} + |y||\xi^{(i_0)} - \xi^{(i)}| \\ &< \Big(\frac{1}{2} + \max_{1\leq i_1<i_2\leq n} |\xi^{i_1} - \xi^{i_2}|\Big)|y|.\end{aligned}$$

Αν η (8.7) δεν ικανοποιείται, τότε έχουμε ένα άνω φράγμα για το $|y|$ και οπότε και για το $|x|$.

- Βήμα 2ο. *Ορισμός του* Λ.

Έστω $y > y_1$ και $i_0 \in \{1, \ldots, s\}$ όπως ορίστηκε στο (8.2). Επιλέγουμε, $j, k \in \{1, \ldots, n\}$ τέτοια ώστε τα i_0, j, k να είναι διαφορετικά (μόνο σε αυτό το σημείο γίνεται χρήση του $n \geq 3$) και είτε $j, k \in \{1, \ldots, s\}$, είτε $j + t = k$ (άρα, $\xi^{(k)} = \overline{\xi^{(j)}}$). Αφού $\beta^{(i)} = x - y\xi^{(i)}$ για $i = i_0, j, k$, απαλοίφοντας τα x και y (αυτό γίνεται αφού έχουμε δύο μεταβλητές), προκύπτει

$$\beta^{(i_0)}(\xi^{(j)} - \xi^{(k)}) + \beta^{(j)}(\xi^{(k)} - \xi^{(i_0)}) + \beta^{(k)}(\xi^{(i_0)} - \xi^{(j)}) = 0$$

και ισοδύναμα,

$$\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}} - 1 = \frac{\xi^{(k)} - \xi^{(j)}}{\xi^{(k)} - \xi^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}}. \tag{8.8}$$

Λόγω της (8.2), το δεξί μέλος είναι αρκετά μικρό.

Αν τα $j, k \in \{1, \ldots, s\}$, θέτουμε

$$\Lambda = \log\Big|\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}}\Big|,$$

(και την ονομάζουμε *πραγματική περίπτωση*)

και αν $j, k \in \{s + 1, \ldots, s + 2t\}$, θέτουμε

$$\Lambda = \frac{1}{i}\mathrm{Log}\Big(\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}}\Big),$$

(και την ονομάζουμε *μιγαδική περίπτωση*),

όπου γενικά για $z \in \mathbb{C}$, με $\mathrm{Log}(z)$ συμβολίζουμε την πρωταρχική τιμή του λογαρίθμου του z (οπότε $-\pi < \mathrm{ImLog}(z) \leq \pi$). Αφού $\xi^{(k)} = \overline{\xi^{(j)}}$, προκύπτει ότι $\Lambda \in \mathbb{R}$ και $|\Lambda| \leq \pi$.

- Βήμα 3ο. *Άνω φράγμα (ως προς το $|y|$) για το $|\Lambda|$.*

Έστω

$$c_3 = \max_{i_1 \neq i_2 \neq i_3 \neq i_1} \Big| \frac{\xi^{(i_1)} - \xi^{(i_2)}}{\xi^{(i_1)} - \xi^{(i_3)}} \Big|.$$

Πραγματική περίπτωση:

Για αρκετά μεγάλο y (έστω $|y| > y_2$, ο ακριβής υπλολογισμός του y_2 παραλείπεται)[3], προκύπτει μέσω του (8.2) ότι:

$$\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}} > 0.$$

Το δεξί μέλος της (8.8) ισούται με:

$$\mathrm{e}^{\Lambda} - 1.$$

Μέσω του (8.2) και του ορισμού της σταθεράς c_3, από την σχέση (8.8) προκύπτει ότι:

$$|\mathrm{e}^{\Lambda} - 1| < c_3 \frac{c_2 |y|^{-(n-1)}}{c_1 |y|} = c_4 |y|^{-n}.$$

Επίσης, από το $|\mathrm{e}^{\Lambda} - 1| < \frac{1}{2}$, έπεται ότι:

$$|\Lambda| \leq 2 \log 2 |\mathrm{e}^{\Lambda} - 1| \leq c_5 |\mathrm{e}^{\Lambda} - 1| < c_5 c_4 |y|^{-n}.$$

Μιγαδική περίπτωση:

Το δεξί μέλος της (8.8) ισούται με:

$$\mathrm{e}^{i\Lambda} - 1.$$

Συμπεραίνουμε ότι για αρκετά μεγάλο $|y|$, (έστω $|y| > y_2^*$, ο ακριβής υπολογισμός του y_2^* παραλείπεται) [4]:

$$|\mathrm{e}^{i\Lambda} - 1| < c_4 |y|^{-n} < \frac{1}{2}.$$

Όμως,

$$|\mathrm{e}^{i\Lambda} - 1| = 2 |\sin \frac{\Lambda}{2}|,$$

οπότε, $|\sin \frac{\Lambda}{2}| < \frac{1}{4}$ και άρα:

$$|\Lambda| < 2 \frac{1/4}{\sin \frac{1}{4}} |\sin \frac{\Lambda}{2}| \leq c_6 |\mathrm{e}^{i\Lambda} - 1|,$$

[3] Αν $|y| < y_2$, τότε έχουμε ένα άνω φράγμα για το $|y|$ και οπότε και για το $|x|$.
[4] Αν $|y| < y_2$, τότε έχουμε ένα άνω φράγμα για το $|y|$ και οπότε και για το $|y|$.

(η συνάρτηση $\frac{2\sin(\frac{1}{2}t)}{t}$ είναι θετική, άρτια και γνησίως φθίνουσα συνάρτηση στο διάστημα $0 \leq t \leq \pi$. Επίσης, γνωρίζουμε ότι $\Lambda \leq \pi$).

Οπότε,

$$|\Lambda| \leq c_6 c_4 |y|^{-n}.$$

Άρα, σε κάθε περίπτωση,

$$|\Lambda| < c_7 |y|^{-n}. \tag{8.9}$$

- Βήμα 4ο. *Η αναγωγή στις γραμμικές μορφές λογαρίθμων.*

Στο δακτύλιο των ακεραίων του σώματος K, υπάρχει ένα σύστημα θεμελιωδών μονάδων $\varepsilon_1, \ldots, \varepsilon_r$, όπου $r = s + t - 1$ (Θεώρημα Dirichlet Α΄.3.2). Αφού F είναι ανάγωγο και $s > 0$, είναι γνωστό (Αλγεβρική Θεωρία Αριθμών) ότι οι μόνες ρίζες της μονάδας που ανήκουν στο K είναι οι ± 1. Σήμερα, ο πρακτικός αυπολογισμός θεμελιωδών μονάδων, είναι εν-γέννει πολύ εύκολα εφικτός με τα υπολογιστικά πακέτα, όπως τα PARI, KASH, MAGMA, τα οποία έχουν στηριχθεί στις σημαντικές εργασίες των Buchmann, Pohst και Zassenhauss (πρβλ. [11], [12] και [22]).

Υποθέτουμε λοιπόν ότι είναι γνωστό ένα τέτοιο σύστημα θεμελιωδών μονάδων. Από την άλλη, υπάρχουν πεπερασμένου πλήθους μη συνεταιρικά $\mu_1, \ldots, \mu_r$ του K, τέτοια ώστε:

$$\mathrm{N}(\mu_i) = m, \;\; i = 1, \ldots, r.$$

Υποθέτουμε λοιπόν ότι είναι γνωστό ένα τέτοιο σύστημα από μ_i. Έστω M το σύνολο των $\pm\mu_i$ (στην περίπτωση που $|m| = 1$, έπεται ότι $M = \{-1, +1\}$).

Για κάθε ακέραια λύση (x, y) της $F(X, Y) = m$ υπάρχει κάποιο $\mu \in M$ και $a_1, \ldots, a_r$, τέτοια ώστε:

$$\beta = \mu \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}.$$

Η 8.8 λοιπόν γίνεται,

$$\begin{aligned} &\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{i_0} - \xi^{(k)}} \cdot \frac{\mu^{(k)}}{\mu^{(j)}} \cdot \prod_{i=1}^{r} \Big(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}} \Big)^{a_i} - 1 \\ &= - \frac{\xi^{(k)} - \xi^{(j)}}{\xi^{(k)} - \xi^{(i_0)}} \cdot \frac{\mu^{(i_0)}}{\mu^{(j)}} \cdot \prod_{i=1}^{r} \Big(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}} \Big)^{a_i}. \end{aligned}$$

Οπότε, στην πραγματική περίπτωση, προκύπτει ότι:

$$\Lambda = \log \Big| \frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\mu^{(k)}}{\mu^{(j)}} \Big| + \sum_{i=1}^{r} a_i \log \Big| \frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(k)}} \Big|, \tag{8.10}$$

και στην μιγαδική περίπτωση,

$$\Lambda = \mathrm{Arg}\Big(\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\mu^{(k)}}{\mu^{(j)}}\Big)+\sum_{i=1}^{r}a_i\mathrm{Arg}\Big(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\Big)+a_0\cdot 2\pi, \tag{8.11}$$

όπου $a_0\in\mathbb{Z}$ και $-\pi<\mathrm{Arg}(z)\leq\pi$ για κάθε $z\in\mathbb{C}$.

Παρατηρούμε ότι το $i\Lambda$ στην μιγαδική περίπτωση, είναι γραμμική μορφή (πρωταρχικών) λογαρίθμων αλγεβρικών αριθμών, με ακέραιους συντελεστές.

- Βήμα 5ο. *Άνω φράγμα για τα $|a_i|$ ως προς το $|y|$.*

Έστω $A=\max_{1\leq i\leq r}|a_i|$. Έστω επίσης, $I=\{h_1,\ldots,h_r\}\subset\{1,\ldots,n\}$.

Έχουμε ότι:

$$\underbrace{\begin{pmatrix}\log|\varepsilon_1^{(h_1)}| & \ldots & \log|\varepsilon_r^{(h_1)}|\\ \log|\varepsilon_1^{(h_2)}| & \ldots & \log|\varepsilon_r^{(h_2)}|\\ \vdots & & \vdots\\ \log|\varepsilon_1^{(h_r)}| & \ldots & \log|\varepsilon_r^{(h_r)}|\end{pmatrix}}_{=:U_I}\cdot\begin{pmatrix}a_1\\ \vdots\\ a_r\end{pmatrix}=\begin{pmatrix}\log\left|\frac{\beta^{(h_1)}}{\mu^{(h_1)}}\right|\\ \vdots\\ \log\left|\frac{\beta^{(h_r)}}{\mu^{(h_r)}}\right|\end{pmatrix}. \tag{8.12}$$

Για κάθε $h\in\{1,\ldots,n\}$ έχουμε από την (8.2) ότι:

$$|\beta^{(h)}|<\Big(\frac{1}{2}+\max_{1\leq i_1<i_2\leq n}|\xi^{(i_1)}-\xi^{(i_2)}|\Big)|y|,$$

άρα,

$$\Big|\frac{\beta^{(h)}}{\mu^{(h)}}\Big|<c_8|y|,\ \text{ για } h=1,\ldots,n.$$

Προκύπτει ότι $c_8|y|>1$, για αρκετά μεγάλο $|y|$ (παραλείπεται ο υπολογισμός) έστω $|y|>y_3$ [5] (y_3 μεγαλύτερο από y_1, y_2 και y_2^*).

Οπότε,

$$\log\Big|\frac{\beta^{(h)}}{\mu^{(h)}}\Big|<\log(c_8|y|),\ \ h=1,\ldots,n\ \ (\log(c_8|y|)>0,\ \text{αφού } c_8|y|>1). \tag{8.13}$$

Θα δείξουμε ότι

$$\Big|\log\Big|\frac{\beta^{(i)}}{\mu^{(i)}}\Big|\Big|<(n-1)\log(c_8|y|),\ \text{για } i=1,\ldots,n. \tag{8.14}$$

[5] Αν $|y|<y_3$, τότε έχουμε ένα άνω φράγμα για το $|y|$ και οπότε και για το $|x|$.

Αν $\left|\frac{\beta^{(i)}}{\mu^{(i)}}\right| \geq 1$, τότε από την (8.13) έχουμε το ζητούμενο.

Αν $\left|\frac{\beta^{(i)}}{\mu^{(i)}}\right| < 1$, τότε από την σχέση

$$\prod_{h=1}^{n} \left|\frac{\beta^{(h)}}{\mu^{(h)}}\right| = 1,$$

προκύπτει ότι

$$\begin{aligned}\left|\log\left|\frac{\beta^{(i)}}{\mu^{(i)}}\right|\right| &= -\log\left|\frac{\beta^{(i)}}{\mu^{(i)}}\right| \\ &= \sum_{\substack{h=1 \\ h\neq i}}^{n} \log\left|\frac{\beta^{(h)}}{\mu^{(h)}}\right| < (n-1)\log(c_8|y|),\end{aligned}$$

λόγω της (8.13).

Από τις (8.12), (8.14), προκύπτει ότι:

$$|A| < c_9 \log(c_8|y|). \tag{8.15}$$

(Συγκεκριμένα από τις (8.12), (8.14) προκύπτει ότι:

$$A < (n-1)\cdot \min_{I}\{\max_{1\leq i\leq r} \sum_{i=1}^{r} |u_{il}|\},$$

όπου τα u_{il} είναι τα στοιχεία του πίνακα U_I^{-1}).

- Βήμα 6ο. *Άνω φράγμα (ως προς το A) για το $|\Lambda|$.*

Από την (8.15), έπεται ότι:

$$|y| > \frac{\mathrm{e}^{A/c_9}}{c_8}.$$

Οπότε, από την (8.9) προκύπτει ότι:

$$|\Lambda| < \frac{c_7}{c_8}\mathrm{e}^{-nA/c_9}. \tag{8.16}$$

- Βήμα 7ο. *Κάτω φράγμα για το $|\Lambda|$ (Γραμμικές μορφές λογαρίθμων).*

Αφού $\Lambda \neq 0$ (λόγω ορισμού του Λ και ότι $\frac{\xi^{(k)}-\xi^{(j)}}{\xi^{(k)}-\xi^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}} \neq 0$), τότε από το θεώρημα 7.1.1, προκύπτει ότι,

$$|\Lambda| > \mathrm{e}^{-c_{10}(\log A + c_{11})^{\kappa}}, \tag{8.17}$$

(κ θετική σταθερά, εξαρτώμενη μόνο από το πλήθος των λογαρίθμων).

- Βήμα 8ο. *Άνω φράγμα για το A (ανεξάρτητο από το $|y|$).*

Από τις (8.16) και (8.17) συμπεραίνουμε το εξής:

$$|A| < c_{12}(\log|A| + c_{11})^{\kappa} + c_{13}.$$

Οπότε,[6]

$$|A| < c_{14}.$$

- Βήμα 9ο. *Άνω φράγμα για τα β_i.*

Θα δείξουμε ότι τα $\beta^{(i)},\ \ i = 1, \ldots, n$ είναι άνω φραγμένα από μια σταθερά η οποία δεν εξαρτάται από τα $|y|$ και το $|x|$. Για τυχαίο $i \in \{1, \ldots, n\}$, έχουμε:

$$\beta^{(i)} = \mu \cdot (\varepsilon_1^{(i)})^{a_1} \cdots (\varepsilon_r^{(i)})^{a_r}$$

οπότε λόγω του άνω φράγματος των a_i, έχουμε ότι:

$$\max_{1 \le i \le n} |\beta^{(i)}| \le c_{15}. \tag{8.18}$$

- Βήμα 10ο. *Άνω φράγμα για τις ακέραιες λύσεις.*

Έχουμε ότι:

$$y = \frac{\beta^{(j)} - \beta^{(i)}}{\xi^{(i)} - \xi^{(j)}}$$

και

$$x = \xi^{(i)} \frac{\beta^{(j)} - \beta^{(i)}}{\xi^{(i)} - \xi^{(j)}} + \beta^{(i)}.$$

Οπότε,

$$|y| \le \frac{1}{2c_1}\Big(|\beta^{(j)}| + |\beta^{(i)}|\Big) \le {}^{7}\frac{c_{15}}{c_1},$$

και

$$|x| \le |\xi^{(i)}||y| + |\beta^{(i)}| \le c_{16}$$

Άρα,

$$\max\{|x|, |y|\} < c.$$

□

Επίσης, αναφέρουμε την απόδειξη της (τετριμμένης) περίπτωσης για την εξίσωση Thue, όπου οι ρίζες της $g(X) = F(X, 1) = 0$ είναι όλες μιγαδικές.

[6] Γενικά είναι γνωστό ότι αν $0 < x < d_1 + d_2 \log x$, d_1, d_2 θετικές σταθερές, τότε έπεται άνω φράγμα για το x

[7] Λόγω της 8.18

Πρόταση 8.2.2. *Αν όλες οι ρίζες της $g(x) = F(X,1) = 0$ είναι μιγαδικές τότε το πλήθος των (ακέραιων) λύσεων (x,y) της $F(X,Y) = m$ είναι πεπερασμένο.*

Απόδειξη.

Έστω $\deg(g(X)) = n \geq 3$ και η $g(X) = 0$ δεν έχει πραγματικές ρίζες. Έστω οι ρίζες της $g(X) = 0$,

$$\xi^{(k)} = \alpha_k + i\gamma_k, \;\; \alpha_k, \gamma_k \in \mathbb{R}, \;\; \gamma_k \neq 0 \;\; \text{για κάθε } k = 1, \ldots, n.$$

Αν (x,y) ακέραια λύση της $F(X,Y) = m$, τότε

$$|x - \xi^{(k)}y| = \sqrt{(x - y\alpha_k)^2 + y^2\gamma_k^2} \geq |\gamma_k|.$$

οπότε,

$$|m| = \prod_{k=1}^{n} |x - \xi^{(k)}y| \geq |x - \xi^{(1)}y| \cdot |\gamma_2| \cdots |\gamma_n|$$

και

$$|m| = \prod_{k=1}^{n} |x - \xi^{(k)}y| \geq |x - \xi^{(2)}y| \cdot |\gamma_1||\gamma_3| \cdots |\gamma_n|.$$

Οπότε, υπάρχουν θετικές σταθερές c_1, c_2, τέτοιες ώστε:

$$-c_1 \leq |x| - |\xi^{(1)}||y| \leq c_1$$

και

$$-c_2 \leq -|x| + |\xi^{(2)}||y| \leq c_2.$$

Άρα,

$$|y| \leq \frac{c_1 + c_2}{\big||\xi^{(2)}| - |\xi^{(1)}|\big|}.$$

Παίρνουμε όλους τους δυνατούς συνδιασμούς των $\big||\xi^{(j)}| - |\xi^{(i)}|\big|$ και διαλέγουμε αυτό με την μικρότερη τιμή. Οπότε έχουμε ένα άνω φράγμα για το $|y|$. Από τις παραπάνω ανισότητες προκύπτει και ένα άνω φράγμα για το $|x|$.

□

Παράρτημα Α΄

Παράρτημα

Α΄.1 Συνδυαστικό επιχείρημα

Έστω ο πίνακας Π της ενότητας 2.1,

$$\Pi = \Big((s_1 + s_{n+1}\beta_1)^{\lambda_1} \dots (s_n + s_{n+1}\beta_n)^{\lambda_n} (\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}})^{\lambda_{n+1}}\Big)_{\underline{\lambda},\underline{s}},$$

με $\underline{s} \in \mathbb{Z}^{n+1}(S)$ και το $\underline{\lambda} \in \mathbb{N}^{n+1}$ τρέχει πάνω απο τα $(\lambda_1, \dots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$ όπου $\lambda_1 + \ldots + \lambda_n \leq L_0$ και $\lambda_{n+1} \leq L_1$. Ο αριθμός των γραμμών του παραπάνω πίνακα είναι $\binom{L_0+n}{n}(L_1+1)$, διότι:

(1) Το πλήθος των $(\lambda_1, \dots, \lambda_n)$ με $\lambda_1 + \ldots + \lambda_n \leq L_0$ είναι ίσο με το άθροισμα του πλήθους των λύσεων των:

$$\lambda_1 + \ldots + \lambda_n = k,$$

για όλα τα k με $0 \leq k \leq L_0$. Το πλήθος των λύσεων της $\lambda_1 + \ldots + \lambda_n = k$ είναι: $\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$. Η απόδειξη του ισχυρισμού αυτού είναι:
Θεωρούμε τον αριθμό n σαν n μπάλες στην σειρά και την τυχούσα διαμέριση του n, δηλαδή τον τυχόντα τρόπο να γράψουμε $n = x_1 + \ldots + x_k$ σαν ένα χωρισμό της σειράς από μπάλες με $k-1$ τοιχώματα. Για παράδειγμα :

$$\text{ooo}||\text{oo}|\text{o}|\text{oo}\dots,$$

έχουμε $x_1 = 3, x_2 = 0, x_3 = 2, x_4 = 1, x_5 = 2, \dots$ Άρα για να βρούμε το πλήθος των λύσεων της $n = x_1 + \ldots + x_k$ αρκεί να μετρήσουμε πόσα διαφορετικά σχήματα, σαν αυτό παραπάνω, υπάρχουν, αφού είναι φανερό ότι σε κάθε τέτοιο σχήμα αντιστοιχεί και μία λύση της $n = x_1 + \ldots + x_k$ και αντίστροφα. Ένα τέτοιο σχήμα κατασκευάζεται μονοσήμαντα ως εξής :

Βάζουμε στη σειρά $n+k-1$ αντικείμενα και κατόπιν ονομάζουμε τα n από αυτά μπάλες και τα υπόλοιπα $k-1$ τοιχωματα. Αυτό μπορεί να γίνει με $\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$ τρόπους.
Οπότε το πλήθος των $(\lambda_1, \ldots, \lambda_n)$ με $\lambda_1 + \ldots + \lambda_n \leq L_0$ είναι:

$$\sum_{k=0}^{L_0} \binom{k+n-1}{k} =$$

$$= \sum_{k=0}^{L_0} \binom{k+n-1}{n-1} = \binom{L_0+n}{n},$$

αφού από τον γνωστό τύπο $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$ έχω ότι:

$$\binom{L_0+n}{n} = \binom{L_0+n-1}{n-1} + \binom{L_0+n-1}{n} =$$

$$= \binom{L_0+n-1}{n-1} + \binom{L_0+n-2}{n-1} + \binom{L_0+n-2}{n} =$$

$$= \binom{L_0+n-1}{n-1} + \ldots + \binom{n-1}{n-1}.$$

(2) Για το λ_{n+1} έχουμε L_1+1 επιλογές.
Οπότε έχουμε ότι το πλήθος των γραμμών είναι $\binom{L_0+n}{n} \cdot (L_1+1)$.

Α΄.2 Μιγαδικές συναρτήσεις μιας μεταβλητής

Γενικός συμβολισμός, $\Delta(0,R)$, όπου $z_0 \in \mathbb{C}, R \in \mathbb{R}^+$: κλειστός δίσκος ακτίνας R και κέντρου z_0.
Επίσης, λέμε ότι μια μιγαδική συνάρτηση f μιας μιγαδικής μεταβλητής είναι αναλυτική στο $\Delta(0,R)$ αν είναι συνεχής στον $\Delta(0,R)$ και αναλυτική στον ανοικτό δίσκο $|z| < R$.
Συμβολίζουμε με $|f|_R$ τον αριθμό $sup\{|f(z)|,\, z \in \Delta(0,\mathrm{R})\}$.
Από την Αρχή του Μεγίστου έχουμε ότι $|f|_R = sup\{|f(z)|,\, |z| = R\}$.

Λήμμα Α΄.2.1. *(Εφαρμογή του Λήμματος του Schwarz): Έστω f αναλυτική στο $\Delta(0,R)$ η οποία έχει στο 0 μηδενική θέση τάξεως N. Αν $0 < r < R$ και $\alpha \in \Delta(0,\mathrm{R})$, τότε*

$$|f(\alpha)|_r < \left(\frac{R}{r}\right)^{-N} \cdot |f|_R$$

.

Απόδειξη. Θέτω $f(z) = z^N g(z)$, όπου g αναλυτική στο $\Delta(0, R)$. Αφού $r \leq R$ έχουμε ότι

$$|g(\alpha)| \leq |g|_R.$$

Από την Αρχή του Μεγίστου για την g έχουμε ότι:

$$|g|_r = r^{-N}|f|_r$$

και

$$|g|_R = R^{-N}|f|_R.$$

Οπότε,

$$|f(\alpha)|_r = r^N|g|_r \leq r^N|g|_R = r^N R^{-N}|f|_R = \left(\frac{R}{r}\right)^{-N} \cdot |f|_R.$$

□

Α΄.3 Σχόλια στα Αριθμητικά Σώματα

Έστω $\alpha \in \mathbb{C}$ ένας αλγεβρικός αριθμός. Η εικόνα του ομομορφισμού $\mathbb{Q}[X] \to \mathbb{C}$, η οποία απεικονίζει το $f \in \mathbb{Q}[X]$ στο $f(\alpha)$, είναι το αριθμητικό σώμα $\mathbb{Q}(\alpha)$, το οποίο παράγεται από το α υπέρ το $\mathbb{Q}$. Ο πυρήνας του προηγούμενου ομομορφισμού είναι πρώτο (άρα και maximal) ιδεώδες του $\mathbb{Q}[X]$, το οποίο έχει ένα μοναδικό μονικό γεννήτορα. Αυτός ο γεννήτορας f καλείται το *ανάγωγο πολυώνυμο του α υπέρ το $\mathbb{Q}$*. Ο βαθμός του f ονομάζεται *βαθμός* του αλγεβρικού αριθμού α. Δύο αλγεβρικοί αριθμοί ονομάζονται συζυγείς αν αυτοί έχουν το ίδιο ανάγωγο πολυώνυμο υπέρ το $\mathbb{Q}$.

Έστω a_0 ο μικρότερος θετικός ακέραιος τέτοιος ώστε το $g = a_0 f$, να έχει ακέραιους συντελεστές. Το $g = a_0 f$,

$$g(X) = a_0 X^n + \ldots + a_n \in \mathbb{Z}[X],$$

ονομάζεται το *ελάχιστο πολυώνυμο του α υπέρ το $\mathbb{Z}$*. Το πολυώνυμο g είναι ανάγωγο στο δακτύλιο πολυωνύμων $\mathbb{Z}[X]$, το οποίο σημαίνει ότι το g είναι ανάγωγο στο $\mathbb{Q}[X]$ και οι $a_0, \ldots, a_n$ είναι πρώτοι μεταξύ τους. Ο αριθμός α ονομάζεται *αλγεβρικός ακέραιος* αν $a_0 = 1$ και ονομάζεται *μονάδα* αν $a_0 = 1$ και $a_n = \pm 1$. Το σύνολο των αλγεβρικών ακεραίων στο σώμα $\overline{\mathbb{Q}}$ των αλγεβρικών αριθμών είναι δακτύλιος και συμβολίζεται με $\mathbb{A}$.

Ένα αριθμητικό σώμα είναι ένα υπόσωμα K του $\mathbb{C}$, το οποίο αν θεωρηθεί ως διανυσματικός χώρος πάνω απο το $\mathbb{Q}$, είναι πεπερασμένης διάστασης. Συμβολίζουμε την διάσταση του K υπέρ το $\mathbb{Q}$ με $[K : \mathbb{Q}]$ και ονομάζουμε *βαθμό*

του K υπέρ το $\mathbb{Q}$. Ο βαθμός του αλγεβρικού αριθμού α είναι ίσος με $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ και ο α ονομάζεται γεννήτορας του σώματος $\mathbb{Q}(\alpha)$.

Αν $K_1,\ K_2,\ K_3$ αριθμητικά σώματα με $K_1 \subset K_2 \subset K_3$ τότε ισχύει ότι: (πολλαπλασιαστικότητα βαθμών)

$$[K_3 : K_2] \cdot [K_2 : K_1] = [K_3 : K_1].$$

Από την πολλαπλασιαστικότητα των βαθμών συμπεραίνουμε ότι για κάθε αριθμητικό σώμα K ισχύει ότι: $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, όπου $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. Αποδεικνύεται όμως ότι:

Θεώρημα Α΄.3.1. *(Θεώρημα πρωταρχικού στοιχείου)*
Σε κάθε αριθμητικό σώμα K υπάρχει $\gamma \in K$ τέτοιο ώστε:

$$K = \mathbb{Q}(\gamma).$$

Έστω $K = \mathbb{Q}(\alpha)$ ένα αριθμητικό σώμα βαθμού n. Έστω επίσης f το ελάχιστο πολυώνυμο του α υπέρ το $\mathbb{Q}$ και $\alpha_1, \ldots, \alpha_n$, οι ρίζες του f (οι συζυγείς του α). Γνωρίζουμε ότι υπάρχουν ακριβώς n εμφυτεύσεις του K στο $\mathbb{C}$ και αυτές δίνονται από:

$$\begin{aligned} \sigma_i :\ K &\longrightarrow \mathbb{C} \\ \alpha &\longmapsto \alpha_i, \end{aligned}$$

$1 \leq i \leq n$. Αν $\sigma_i(\alpha) \in \mathbb{R}$ τότε $\sigma_i(K) \subset \mathbb{R}$ και η εμφύτευση σ_i ονομάζεται πραγματική. Αν $\sigma_i(\alpha) \in \mathbb{C}$ τότε $\sigma_i(K) \subset \mathbb{C}$ και η εμφύτευση σ_i ονομάζεται μιγαδική.

Επίσης θυμίζουμε ότι η norm του σώματος K συμβολίζεται με $N = N_{K/\mathbb{Q}} :\ K \to \mathbb{Q}$. Για $\alpha \in K$ έχουμε ότι $N(\alpha) :=$ η ορίζουσα του ενδομορφισμού $x \to \alpha x$ του $\mathbb{Q}-$ διανυσματικού χώρου K.

Αν $[K : \mathbb{Q}] = n$, τότε:

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

Για τις μονάδες ενός αριθμητικού σώματος σημειώνουμε επίσης τα εξής:
Ένας ακέραιος αριθμός ε λέγεται *μονάδα* αν ο αντίστροφος αυτού αριθμός ε^{-1} είναι επίσης ακέραιος αλγεβρικός αριθμός.

Επίσης, ισχύει ότι ο αλγεβρικός αριθμός ε του αριθμητικού σώματος αριθμών K είναι μονάδα αν είναι ακέραιος αλγεβρικός αριθμός και αν $N_{K/\mathbb{Q}}(\varepsilon) = \pm 1$.

Έχει αποδειχθεί το εξής θεώρημα για τις μονάδες ενός αριθμητικού σώματος αριθμών K,

Θεώρημα Α΄.3.2. *(Dirichlet)*

Έστω K ένα αριθμητικό σώμα αριθμών. Υπάρχει αλγεβρικός αριθμός α τέτοιος ώστε $K = \mathbb{Q}(\alpha)$. Υποθέτουμε ότι το ελάχιστο πολυώνυμο το α υπερ το $\mathbb{Q}$ έχει s πραγματικές ρίζες και $2t$ μιγαδικές ρίζες. Θέτουμε $r = s + t - 1$. Τότε υπάρχουν r μονάδες $\varepsilon_1, \ldots, \varepsilon_r$ του K, οι λεγόμενες θεμελιώδεις μονάδες του K, και μια ρίζα της μονάδας ζ του K μέγιστης τάξης m έτσι ώστε κάθε μονάδα ε του K να έχει μονοσήμαντη παράσταση της μορφής:

$$\varepsilon = \zeta^{n_0} \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r},$$

όπου $1 \leq n_0 \leq m$ και n_i ακέραιοι.

Αν συμβολίσουμε με E_K το σύνολο των μονάδων του αριθμητικού σώματος K, τότε αυτό αποτελει πολλαπλασιαστική ομάδα και ισχύει:

$$E_K = < \zeta > \otimes < \varepsilon_1 > \otimes \ldots \otimes < \varepsilon_r >,$$

όπου $< \zeta >$ κυκλική ομάδα τάξης m και $< \varepsilon_i >,\ i = 1, \ldots, r$, κυκλικές ομάδες άπειρης τάξης.

Ένα ιδεώδες $\mathcal{I}$ του K λέγεται *κλασματικό* ιδεώδες αν υπάρχει $d \in \mathbb{A} \setminus \{0\}$, τέτοιο ώστε το $d \cdot \mathcal{I}$ είναι ιδεώδες του δακτυλίου $\mathbb{A}$ με την συνήθη έννοια.

Τα *ακέραια* ιδεώδη είναι τα ιδεώδη του δακτυλίου $\mathbb{A}$.

Αν $\mathcal{I}$ είναι ένα κλασματικό ιδεώδες του αριθμητικού σώματος K, τότε υπάρχει ένας ακέραιος αλγεβρικός αριθμός d, τέτοιος ώστε: $d\mathcal{I} = \mathcal{J} \subset \mathbb{A}$. Το $\mathcal{J}$ είναι ακέραιο ιδεώδες και ισχύει $\mathcal{I} = d^{-1}\mathcal{J}$. Αντίστροφα, αν $\mathcal{J}$ είναι ένα ακέραιο ιδεώδες του αριθμητικού σώματος αριθμών K και $d \neq 0$ ένας ακέραιος αλγεβρικός αριθμός του K, τότε το σύνολο $\mathcal{I} = d^{-1}\mathcal{J}$, είναι ένα κλασματικό ιδεώδες του K.

Αν $\alpha \in K$ με $\alpha \neq 0$, τότε το σύνολο:

$$< \alpha > = \alpha \cdot \mathbb{A} = \{a\alpha,\ \ a \in \mathbb{A}\},$$

λέγεται *κύριο* ιδεώδες του K που παράγεται από το α.

Έστω $\mathcal{I}, \mathcal{J}$ δύο ιδεώδη του K. Το ιδεώδες $\mathcal{I}$ διαιρεί το ιδεώδες $\mathcal{J}$ αν $\mathcal{J} \subset \mathcal{I}$. Επίσης το ιδεώδες $\mathcal{I}$ διαιρεί τον $\alpha \in K$ αν $\mathcal{I} | < \alpha >$.

Ορίζουμε *norm* του ιδεώδους $\mathcal{I}$, να είναι το πλήθος των στοιχείων του δακτυλίου $\mathbb{A}/\mathcal{I}$ και συμβολίζεται $N_K(\mathcal{I})$.

Ένα ιδεώδες $\wp$ του αριθμητικού σώματος αριθμών K, λέγεται *πρώτο* αν είναι ακέραιο ιδεώδες διάφορο του $\mathbb{A}$ και ισχύει:

$$\wp | \alpha\beta,\ \ \alpha, \beta \in \mathbb{A} \Longrightarrow \wp | \alpha \text{ ή } \wp | \beta.$$

Αν $\wp$ είναι πρώτο ιδεώδες του K τότε το $\wp \cap \mathbb{Z}$ είναι μη μηδενικό ιδεώδες του $\mathbb{Z}$ και ισχύει ότι $\wp \cap \mathbb{Z} = p\mathbb{Z}$, για κάποιο πρώτο $p \in \mathbb{Z}$.

Ισχύει ότι κάθε πρώτο ιδεώδες $\wp$ του K είναι και maximal. Άρα το $\mathbb{A}/\wp$ είναι σώμα. Αποδεικνύεται ότι:

$$\left|\mathbb{A}/\wp\right| = N_K(\wp) = p^f,$$

όπου $p \in \mathbb{Z}$ πρώτος με $P\mathbb{Z} = \wp \cap \mathbb{Z}$ και $f \geq 1$ φυσικός (ο f ονομάζεται βαθμός του $\wp$ και είναι $f = [\mathbb{A}/\wp : \mathbb{F}_p]$).

Ισχύει το εξής:

Κάθε ιδεώδες $\mathcal{I}$ του αριθμητικού σώματος K, αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών του K,

$$\mathcal{I} = \wp_1^{e_1} \cdots \wp_n^{e_r},$$

όπου $e_i \in \mathbb{Z}, i = 1, \ldots, r$.

Ισχύει το εξής θεμελιώδες

Θεώρημα Α΄.3.3. *Αν $p \in \mathbb{Z}$ πρώτος με*

$$< p >= \wp_1^{e_1} \cdots \wp_r^{e_r},$$

είναι η ανάλυση του ιδεώδους $< p >= p\mathbb{A}$ σε γινόμενο πρώτων ιδεωδών του K και $f_1, \ldots, f_r$ οι βαθμοί των $\wp_1, \ldots, \wp_r$ αντίστοιχα, τότε:

$$e_1 f_1 + \ldots + e_r f_r = n.$$

όπου $n = [K : \mathbb{Q}]$.

(Βιβλιογραφία: [1], [32])

Α΄.4 Μέτρο του Mahler

Έστω $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \in \mathbb{C}[x]$ ένα μη μηδενικό πολυώνυμο βαθμού n με $a_0 > 0$ και:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = a_0 \prod_{i=1}^{n} (x - \alpha_i),$$

(α_i οι ρίζες του f στο $\mathbb{C}$).

Το *μέτρο Mahler του* f είναι ο αριθμός:

$$M(f) = a_0 \prod_{i=1}^{n} \max\{1, |\alpha_i|\}.$$

Ισχύει ότι:

$$M(f_1 f_2) = M(f_1) M(f_2),$$

για $f_1, f_2 \in \mathbb{C}[x]$.

Επίσης, αποδεικνύεται ότι:

$$M(f) = M(f^*),$$

όπου $f \in \mathbb{C}[x]$ και $f^* = x^{\deg(f)} f(\frac{1}{x})$ (*αντίστροφο πολυώνυμο του* f).

Όταν α είναι ένας αλγεβρικός αριθμός με ελάχιστο πολυώνυμο $f \in \mathbb{Z}[x]$, ορίζουμε:

$$M(\alpha) = M(f),$$

να είναι το μέτρο Mahler του α.

Από τον ορισμό, προκύπτει ότι $M(\alpha) \geq 1$, για κάθε αλγεβρικό αριθμό α.

Μία ακόμα ιδιότητα του μέτρου Mahler είναι το:

Λήμμα Α΄.4.1. *Έστω* $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \in \mathbb{Z}[x]$. *Τότε, για κάθε* $0 < j \leq n$,

$$|a_j| \leq \binom{n}{j} M(f).$$

Απόδειξη. Είναι άμεση συνέπεια του ορισμού του $M(f)$ και των τύπων του Vietta (για το πολυώνυμο f):

$$a_j = (-1)^{n-j} a_0 \sum_{s_1, \ldots, s_i} \alpha_{s_1, \ldots, \alpha_{s_n}},$$

όπου α_{s_i} για $i = 1, \ldots, n$, είναι οι ρίζες του f στο $\mathbb{C}$.

□

Στο παρακάτω λήμμα, δίνεται η σχέση του μέτρου Mahler και του λογαριθμικού ύψους (Weil),

Λήμμα Α΄.4.2. *Έστω* α *ένας αλγεβρικός μιγαδικός αριθμός βαθμού* n. *Τότε:*

$$h(\alpha) = \frac{1}{n} \log M(\alpha).$$

Απόδειξη. Συμβολίζουμε με $a_0 > 0$ τον συντελεστή του μεγιστοβάθμιου όρου του ελαχίστου πολυωνύμου του α. Επίσης, έστω $K = \mathbb{Q}(\alpha)$.
Γνωρίζουμε ότι:

$$\begin{aligned} M(\alpha) &= a_0 \prod_{i=1}^{n} \max\{1, |\alpha_i|\} \\ &= a_0 \prod_{v \in M_K^\infty} \max 1, |\alpha|_v^{d_v} \\ &= a_0 \prod_{v \in M_K^\infty} \max\{1, |\alpha|_v\}^{d_v}. \end{aligned}$$

Επίσης,

$$h(\alpha) = \frac{1}{n} \sum_{v \in M_K} d_v \log \max\{1, |\alpha|_v\}.$$

Άρα, αρκεί να δείξουμε ότι:

$$a_0 = \prod_{v \in M_K^0} \max\{1, |\alpha|_v\}^{d_v}.$$

Από τον τύπο του γινομένου στο $\mathbb{Q}$:

$$|a_0| \prod_p |a_0|_p = 1,$$

έχουμε ότι:

$$a_0 = \prod_p |a_0|_p^{-1}.$$

Άρα, αρκεί να δείξουμε ότι αν $(p) = \wp_1^{e_1} \cdots \wp_m^{e_m}$, η ανάλυση του (p) στο K, τότε:

$$|a_0|_p^{-1} = \prod_{v_{\wp_i}} \max\{1, |\alpha|_{v_{\wp_i}}\}^{d_{v_{\wp_i}}}.$$

Αυτό αποδεικνύεται μέσω του επόμενου λήμματος:

Λήμμα Α΄.4.3. *Έστω p πρώτος αριθμός. Έστω $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ πολυώνυμο βαθμού n και μκδ$(a_0, \ldots, a_n) = 1$.*
Έστω $\alpha_1, \ldots, \alpha_n$ οι ρίζες του στο $\mathbb{C}_p$:

$$f(x) = a_0 \prod_{i=1}^{n} (x - \alpha_i).$$

Τότε:

$$|a_0|_p = \prod_{i=1}^{n} \max\{1, |\alpha_i|_p\} = 1.$$

Απόδειξη. Μπορούμε να υποθέσουμε ότι:

$$|a_1|_p \leq \ldots \leq |a_n|_p.$$

Αφού τα a_i είναι πρώτα μεταξύ τους, ισχύει ότι:[1]

$$\max\{|a_0|_p, \ldots, |a_n|_p\} = 1.$$

Από τους τύπους του Vieta έχουμε ότι:

$$\frac{a_i}{a_0} = (-1)^i \sum_{s_1,\ldots,s_i} \alpha_{s_1} \cdots \alpha_{s_i}, \;\; 1 \leq i \leq n.$$

- Αν $|\alpha_i|_p \leq 1$ [2] για κάθε $1 \leq i \leq n$, τότε:

$$\begin{aligned} \left|\frac{a_i}{a_0}\right|_p &= \left|(-1)^i \sum_{s_1,\ldots,s_i} \alpha_{s_1} \cdots \; \alpha_{s_i}\right|_p \\ &\leq \max\{|\alpha_{s_1}|_p, \ldots, |\alpha_{s_i}|_p\} \leq 1, \end{aligned}$$

δηλαδή,

$$|a_i|_p \leq |a_0|_p, \;\; \forall i = 1, \ldots, n,$$

οπότε,

$$\max |a_0|_p, \ldots, |a_n|_p = |a_0|_p = 1,$$

από το οποίο προκύπτει το ζητούμενο.

- Αν υπάρχει j, $1 \leq j \leq n$, τέτοιο ώστε:

$$|\alpha_1|_p \leq \ldots \leq |\alpha_{j-1}|_p \leq 1 \leq |\alpha_j|_p \leq |\alpha_n|_p,$$

τότε:

$$\begin{aligned} \max\{\left|\frac{a_i}{a_0}\right|_p, \;\; 1 \leq i \leq n\} &= \max\{\left|(-1)^i \sum_{s_1,\ldots,s_i} \alpha_{s_1} \cdots \; \alpha_{s_i}\right|_p\} = |\alpha_j \cdots \alpha_n|_p \\ &= \prod_{i=1}^{n} \max\{1, |\alpha_i|_p\}. \end{aligned}$$

[1] κάποιο από αυτά δεν έχει το p στην ανάλυση του σε πρώτους, άρα $|\cdot|_p = 1$

[2] εδώ με $|\cdot|_p$ συμβολίζουμε την επέκταση της $p-$αδικής απόλυτης τιμής από το $\mathbb{Q}_p$ στο $\mathbb{C}_p$ (πρβλ. παράγραφο 3.2.2). Για $a \in \mathbb{Q}$ αυτή συμπίπτει με την $p-$αδική απόλυτη τιμή του $\mathbb{Q}_p$

Άρα,

$$\max\{|a_1|_p,\ldots,|a_n|_p\} = |a_0|_p \prod_{i=1}^{n} \max\{1,|\alpha_i|_p\}.$$

Αφού, $|a_0|_p \leq \max\{|a_1|_p,\ldots,|a_n|_p\}$, έχουμε ότι:

$$\max\{|a_0|_p,|a_1|_p,\ldots,|a_n|_p\} = |a_0|_p \prod_{i=1}^{n} \max\{1,|\alpha_i|_p\}.$$

□

Όπως αναφέραμε στην παράγραφο 3.7, έχουμε ότι:

Για α αλγεβρικό ακέραιο, $M(\alpha)=1$, αν και μόνο αν, ο α είναι 0 ή ρίζα της μονάδας.

Έστω α αλγεβρικός ακέραιος βαθμού n και $f \in \mathbb{Z}[x]$ το ελάχιστο πολυώνυμο του. Παρουσιάζουν λοιπόν ενδιαφέρον, οι εξής αριθμοί:

$$M_n = \inf\{M(f) : f \in \mathbb{Z}[x], \deg(f)=n, \text{ με } M(f)>1\},$$

($M(f)=M(\alpha)$).

Για δοσμένο φυσικό n είναι εύκολο να υπολογιστούν όλα αυτά τα ελάχιστα πολυώνυμα. Συγκεκριμένα, μας ενδιαφέρουν τα πολυώνυμα $f \in \mathbb{Z}[x]$, $\deg(f)=n$, με $M(f)\leq 2$. Τα πολυώνυμα αυτά, υπολογίζονται με την βοήθεια του λήμματος Α΄.4.1. Δηλαδή, οι συντελεστές των πολυωνύμων αυτών, για $0<j\leq n$ ικανοποιούν την ανισότητα:

$$|a_j| \leq 2\binom{n}{j}.$$

Έχοντας λοιπόν, την συγκεκριμένη λίστα με τα πολυώνυμα (με δοσμένο βαθμό n), υπολογίζουμε (με τη βοήθεια της Maple) τις ρίζες τους και ύστερα τα μέτρα Mahler των πολυωνύμων, (λόγω των σχέσεων $\pm M(f(\pm x)) = M(f)$ και $M(f^*)=M(f)$, δεν χρειάζεται να υπολογίσουμε τις ρίζες όλων των πολυωνύμων της λίστας).

Έτσι, βρίσκεται ο αριθμός M_n, για δοσμένο n. Έχουμε λοιπόν, για παράδειγμα, ότι:

για $n=1$, $M_1=2$ και το πολυώνυμο είναι το $f=x-2$, (με ρίζα $\alpha=2$)

για $n=2$, $M_2=1.618...$ και το πολυώνυμο είναι το $f=x^2-x-1$, (με ρίζα $\alpha=\dfrac{1+\sqrt{5}}{2}$)

για $n=3$, $M_3=1.324...$ και το πολυώνυμο είναι το $f=x^3-x+1$.(με ρίζα $\alpha=1.324717957...$

Λόγω των παραπάνω και μέσω της σχέσης $h(\alpha)=\frac{1}{n}\log M(\alpha)$ του λήμματος Α΄.4.2, προκύπτουν, άμεσα, κάτω φράγματα για το λογαριθμικό ύψος. Συμπεραίνεται λοιπόν, το

Πόρισμα Α΄.4.4. *Έστω α αλγεβρικός αριθμός βαθμού n. Τότε:*

$$\begin{aligned}
&\textit{Για } n=1, \quad h(a) \geq \log 2 = 0.6931...,\\
&\textit{Για } n=2, \quad 2h(a) \geq \log\Big(\frac{1+\sqrt{5}}{2}\Big) = 0.4812...,\\
&\textit{Για } n=3, \quad 3h(a) \geq \log(1.324717957...) = 0.2811....
\end{aligned}$$

Α΄.5 Μια σχέση μεταξύ υψών

Λήμμα Α΄.5.1. *Έστω K ένα αριθμητικό σώμα. Αν $x_1,\ldots,x_n,y_1,\ldots,y_n \in K$, (όχι όλα μηδέν), τότε:*

$$h(1:x_1:\ldots:x_n:y_1:\ldots:y_n) \leq h(x_1)+\ldots+h(x_n)+h(1:y_1:\ldots:y_n).$$

Απόδειξη. Από τον ορισμό του ύψους h αρκεί να δείξουμε ότι:

$$\begin{aligned}
&\frac{1}{n}\sum_{v\in M_K} d_v \log\max\{1,|x_1|_v,\ldots,|x_n|_v,|y_1|_v,\ldots,|y_n|_v\}\\
\leq&\frac{1}{n}\sum_{v\in M_K} d_v\big(\log\max\{1,|x_1|_v\}+\ldots+\log\max\{1,|x_n|_v\}+\log\max\{1,|y_1|_v,\ldots,|y_n|_v\}\big).
\end{aligned}$$

Δηλαδή, αρκεί

$$\begin{aligned}
&\log\max\{1,|x_1|_v,\ldots,|x_n|_v,|y_1|_v,\ldots,|y_n|_v\}\\
\leq&\big(\log\max\{1,|x_1|_v\}+\ldots+\log\max\{1,|x_n|_v\}+\log\max\{1,|y_1|_v,\ldots,|y_n|_v\}\big),
\end{aligned}$$

ή

$$\begin{aligned}
&\max\{1,|x_1|_v,\ldots,|x_n|_v,|y_1|_v,\ldots,|y_n|_v\}\\
\leq&\max\{1,|x_1|_v\}\cdots\max\{1,|x_n|_v\}\cdot\max\{1,|y_1|_v,\ldots,|y_n|_v\}.
\end{aligned}$$

Αρκεί λοιπόν για οποιουσδήποτε $a_1,\ldots,a_n\in\mathbb{R}_{>0}$, να ισχύει

$$\max\{1,a_1,\ldots,a_n\}\leq\max\{1,a_1\}\cdots\max\{1,a_k\}\cdot\max\{1,a_{k+1},\ldots,a_n\},$$

για κάθε k με $1\leq k\leq n$.

Αυτό ισχύει διότι

- Αν όλα τα $a_1,\ldots,a_n$ είναι <1, τότε έχουμε ότι $1\leq 1$, το οποίο ισχύει.
- Αν $a_j=\max\{1,a_1,\ldots,a_n\}$, $(1\leq j\leq n)$, με $a_j>1$, τότε: $a_j\leq a_j\cdot A$, όπου $A\geq 1$, το οποίο ισχύει.

□

Άμεση συνέπεια του προηγούμενου λήμματος είναι το

Λήμμα Α΄.5.2. *Έστω K ένα αριθμητικό σώμα. Αν $x_1, \ldots, x_n \in K$ (όχι όλα μηδέν), τότε*

$$h(x_1 : \ldots : x_n) \leq \sum_{i=1}^{n} h(x_i).$$

Α΄.6 Συναρτήσεις πολλών μιγαδικών μεταβλητών

Για $z = (z_1, \ldots, z_n) \in \mathbb{C}^n$, συμβολίζουμε με

$$|z| := \max\{|z_1|, \ldots, z_n\}.$$

Γενικά, αν $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$, τότε συμβολίζουμε

$$||a|| := a_1 + \ldots + a_n$$
$$a! := a_1! a_2! \ldots a_n!.$$

Επίσης, για $z \in \mathbb{C}^n$ και $a \in \mathbb{N}^n$,

$$z^a := z_1^{a_1} \cdots z^{a_n}.$$

Για $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ και $\rho = (\rho_1, \ldots, \rho_n) \in \mathbb{R}^n$, τότε ο πολυδίσκος με κέντρο α και με (πολυ) ακτίνα ρ είναι το σύνολο

$$\Delta(\alpha, \rho) = \{z \in \mathbb{C}^n \ |z_1 - \alpha_1| < \rho_1, \ldots, |z_n - \alpha_n| < \rho_n\}.$$

Με $\overline{D}(\alpha, \rho)$ συμβολίζουμε την κλειστότητα του $\Delta(\alpha, \rho)$ στο $\mathbb{C}^n$.

Επίσης, αν $z \in \mathbb{C}^n$, τότε γράφουμε $z = x + iy$, όπου $x, y \in \mathbb{R}^n$.

Για μια συνεχή και παραγωγίσιμη μιγαδική συνάρτηση g σε ένα ανοικτό σύνολο $\Omega \subset \mathbb{C}^n$, θέτουμε

$$\frac{\partial g}{\partial z_j} = \frac{1}{2}\left(\frac{\partial g}{\partial x_j} - i\frac{\partial g}{\partial y_j}\right)$$
$$(D^a g)(z) = \frac{\partial^{|a|}}{\partial z_1^{a_1} \ldots \partial z_n^{a_n}} g(z).$$

Ορισμός Α΄.6.1. *Έστω Ω ένα ανοικτό σύνολο του $\mathbb{C}^n$ και f μια μιγαδική συνάρτηση η οποία ορίζεται στο Ω. Λέμε ότι η f είναι αναλυτική στο Ω αν σε κάθε σημείο $\alpha \in \Omega$ αντιστοιχεί μια γειτονιά U και μια δυναμοσειρά*

$$\sum_{a \in \mathbb{N}^n} c_a (z - \alpha)^a = \sum_{a_1, \ldots, a_n \geq 0} c_{a_1 \ldots a_n} (z - \alpha_1)^{a_1} \ldots (z - \alpha_n)^{a_n},$$

η οποία συγκλίνει στην $f(z)$ για κάθε $z \in U$.

Θεώρημα Α΄.6.2. *Έστω f αναλυτική στον πολυδίσκο $\Delta(\alpha, \rho)$. Τότε για κάθε $z \in \Delta(\alpha, \rho)$, έχουμε ότι:*

$$f(z) = \sum_{a \in N^n} c_a (z - \alpha)^a,$$

όπου, $c_a = \frac{1}{a!}(D^a f)(\alpha)$.

(Βιβλιογραφία: [21])

Α΄.7 Σχόλια στην Αλγεβρική Γεωμετρία

Έστω K ένα αλγεβρικά κλειστό σώμα χαρακτηριστικής μηδέν και $n \in \mathbb{N}$.

Ένα *αλγεβρικό υποσύνολο* (ή *αλγεβρικό σύνολο*) του K^n είναι ένα υποσύνολο του K^n το οποίο είναι το σύνολο ριζών μιας οικογένειας πολυωνύμων του $K[X_1, \ldots, X_n]$. Δηλαδή, αν $\mathcal{V}$ είναι αλγεβρικό υποσύνολο του K^n, τότε:

$$\mathcal{V} = \{\underline{x} \in K^n, f(\underline{x}) = 0 \text{ καθώς } f \in T \subseteq K[X_1, \ldots, X_n]\},$$

όπου T μια οικογένεια πολυωνύμων του $K[X_1, \ldots, X_n]$.
Έχει αποδειχθεί ότι για κάθε αλγεβρικό υποσύνολο $\mathcal{V}$ του K^n υπάρχει $\mathcal{J}$ ιδεώδες του $K[X_1, \ldots, X_n]$ τέτοιο ώστε:

$$\mathcal{V} = \{\underline{x} \in K^n, f(\underline{x}) = 0 \text{ για κάθε } f \in \mathcal{J}\}.$$

Από τον ορισμό προκύπτει ότι τομή μιας οικογένειας αλγεβρικών υποσυνόλων του K^n είναι αλγεβρικό υποσύνολο του K^n και επίσης, η πεπερασμένη ένωση αλγεβρικών υποσυνόλων του K^n είναι αλγεβρικό υποσύνολο του K^n.

Αν X είναι ένα υποσύνολο του K^n, συμβολίζουμε με $\mathcal{I}(X)$:

$$\mathcal{I}(X) = \{f \in K[X_1, \ldots, X_n], \;\; f(\underline{x}) = 0 \text{ για κάθε } x \in X\},$$

το *ιδεώδες του X*.

Ένα αλγεβρικό υποσύνολο του K^n λέγεται *ανάγωγο* αν είναι μη κενό και δεν μπορεί να γραφεί ως ένωση δύο αλγεβρικών υποσυνόλων του K^n τα οποία να περιέχονται γνησίως σε αυτό. Ένα ανάγωγο αλγεβρικό σύνολο λέγεται *αλγεβρική πολλαπλότητα* του K^n ή πιο απλά *πολλαπλότητα* του K^n. Οπότε, αν μια αλγεβρική πολλαπλότητα του K^n περιέχεται σε μια πεπερασμένη ένωση αλγεβρικών συνόλων, τότε περιέχεται σε ένα από αυτά.

Αποδεικνύεται ότι κάθε αλγεβρικό υποσύνολο $\mathcal{V}$ του K^n είναι πεπερασμένη ένωση αλγεβρικών πολλαπλοτήτων $\mathcal{U}_1, \ldots, \mathcal{U}_s$ του K^n του $\mathcal{V}$) (τις οποίες ονομάζουμε *συνιστώσες* του $\mathcal{V}$):

$$\mathcal{V} = \mathcal{U}_1 \cup \ldots \cup \mathcal{U}_s.$$

Ισχύει επίσης το εξής:

$\mathcal{I}(\mathcal{U}_i)$ είναι πρώτο ιδεώδες του $K[X_1, \ldots, X_n]$, αν και μόνο αν το $\mathcal{U}_i$ είναι αλγεβρική πολλαπλότητα.

Αν, λοιπόν, $\mathcal{U}$ είναι αλγεβρική πολλαπλότητα, τότε το $\mathcal{I}(\mathcal{U})$ είναι πρώτο ιδεώδες. Άρα,

$$K[X_1, \ldots, X_n]/\mathcal{I}(\mathcal{U}),$$

είναι ακέραια περιοχή και συμβολίζεται με $K[\mathcal{U}]$.
Άρα, ορίζεται το σώμα πηλίκων της, το οποίο συμβολίζεται με $K(\mathcal{U})$, (σώμα συναρτήσεων του $\mathcal{U}$).

Η *διάσταση* αλγεβρικής πολλαπλότητας $\mathcal{U}$ ορίζεται να είναι ο βαθμός υπερβατικότητας της επέκτασης $K(\mathcal{U})/K$, δηλαδή ίση με το μέγιστο πλήθος αλγεβρικά ανεξάρτητων στοιχείων [3] του $K(\mathcal{U})$ υπέρ το K.

Αν μια αλγεβρική πολλαπλότητα $\mathcal{U}$ του K^n, δίνεται από γραμμικά πολυώνυμα (σε αυτή την περίπτωση το $\mathcal{U}$ είναι μεταφορά ενός διανυσματικού χώρου $\mathcal{W}$ του K^n), η έννοια της διάστασης της πολλαπλότητας $\mathcal{U}$ ταυτίζεται με την έννοια της διάστασης του γραμμικού χώρου $\mathcal{W}$.

Η *διάσταση* ενός αλγεβρικού υποσυνόλου του K^n είναι η μέγιστη διάσταση των συνιστωσών του αλγεβρικού υποσυνόλου (κάθε ένα από αυτά είναι αλγεβρική πολλαπλότητα).

Αν $\mathcal{V}, \mathcal{V}'$ είναι δύο μη κενά αλγεβρικά υποσύνολα του K^n με $\mathcal{V}' \subseteq \mathcal{V}$, τότε $\dim(\mathcal{V}') \leq \dim(\mathcal{V})$, με την ισότητα να ισχύει αν και μόνο αν τα $\mathcal{V}$ και $\mathcal{V}'$ έχουν κοινή συνιστώσα (αλγεβρική πολλαπλότητα) με διάσταση $\dim(\mathcal{V})$. Αυτό προκύπτει από το γεγονός ότι κάθε συνιστώσα του $\mathcal{V}'$ περιέχεται σε μία συνιστώσα του $\mathcal{V}$. Συγκεκριμένα, ένα αλγεβρικό υποσύνολο $\mathcal{V}$ του K^n διάστασης d περιέχει πεπερασμένου πλήθους αλγεβρικές πολλαπλότητες διάστασης d.

(Βιβλιογραφία: [16])

Παρακάτω αναφέρουμε κάποια χρήσιμα συμπεράσματα.

Λήμμα Α΄.7.1. *Ένα υποσύνολο $\mathcal{V}$ το οποίο είναι συγχρόνως προσθετική ομάδα του K^n και αλγεβρικό σύνολο του K^n, είναι διανυσματικός υπόχωρος του K^n.*

[3] Έστω ένας (μεταθετικός) δακτύλιος A και ένας υποδακτύλιος k του A ο οποίος είναι σώμα. Τα στοιχεία $a_1, \ldots, a_n \in A$ είναι αλγεβρικώς ανεξάρτητα υπέρ το k αν δεν υπάρχει μη μηδενικό πολυώνυμο $P \in k[X_1, \ldots, X_n]$, τέτοιο ώστε $P(a_1, \ldots, a_n) = 0$

Απόδειξη. Αφού το $\mathcal{V}$ είναι προσθετική υποομάδα του K^n έχουμε ότι το $\mathcal{V}$ είναι προσθετικά κλειστο στο K^n. Οπότε, για να αποδείξουμε ότι είναι διαωυσματικός υπόχωρος του K^n αρκεί να δείξουμε ότι για τυχαίο $\alpha \in K$ το $\alpha(x_1, \ldots, x_n) \in \mathcal{V}$, για κάθε $(x_1, \ldots, x_n) \in \mathcal{V}$.

Έστω $(x_1, \ldots, x_n)$ στοιχείο του $\mathcal{V}$ και έστω $P \in K[X_1, \ldots, X_n]$ με $P \in I(\mathcal{V})$ ($I(\mathcal{V})$ είναι το ιδεώδες του αλγεβρικού συνόλου $\mathcal{V}$).

Έστω, $f: \ K \to K$, με $f(k) = P(kX_1, \ldots, kX_n)$.

Έχουμε ότι για αν $\underline{x} = (x_1, \ldots, x_n) \in \mathcal{V}$ και $n \in \mathbb{Z}$, τότε και το $n\underline{x} \in \mathcal{V}$, αφού $\mathcal{V}$ προσθετική υποομάδα του K^n. Άρα, αν $P(\underline{x}) = 0$, τότε και $P(n\underline{x}) = 0$, για κάθε $n \in \mathbb{Z}$. Οπότε, το πολυώνυμο $f(k)$ έχει ρίζες όλα τα $k \in \mathbb{Z}$. Άρα, το f είναι ταυτοτικά μηδέν. Δηλαδή, για κάθε $\underline{x} \in \mathcal{V}$ το $k\underline{x} \in \mathcal{V}$, για κάθε $k \in K$.

□

Λήμμα Α΄.7.2. *Έστω $k \subset K$ δύο σώματα. Έστω $\mathcal{V}$ ένας διανυσματικός υπόχωρος του K^n, με $\dim = n - r, \ 1 \leq r \leq n$.*

Οι παρακάτω προτάσεις είναι ισοδύναμες:

1. *Το $\mathcal{V}$ είναι τομή αλγεβρικών συνόλων τα οποία ορίζονται από γραμμικές μορφές με συντελεστές από το k.*
2. *Το $\mathcal{V}$ έχει βάση της οποίας τα στοιχεία ανήκουν στο k^n.*
3. *Υπάρχει μια επί γραμμική απεικόνιση από το K^n στο K^r με πυρήνα τον $\mathcal{V}$, της οποίας ο πίνακας (ως προς τις κανονικές βάσεις) έχει συντελεστές στο k.*

Ένας τέτοιος διανυσματικός υπόχωρος του K^n λέγεται ρητός πάνω από το k.

Απόδειξη.

- $1 \Longrightarrow 2$.

Έστω $\mathcal{V}$ διανυσματικός υπόχωρος του K^n, με $\dim\mathcal{V} = n - r, \ 1 \leq r \leq n$, ($\mathcal{V} \neq \emptyset$), ο οποίος είναι τομή αλγεβρικών συνόλων τα οποία ορίζονται από γραμμικές μορφές με συντελεστές από το k. Δηλαδή ο $\mathcal{V}$ είναι ο χώρος λύσεων του συστήματος:

$$\begin{array}{ccc} a_{11}x_1 + & \ldots & +a_{1n}x_n \quad = 0 \\ \vdots & & \vdots \\ a_{m1}x_1 + & \ldots & +a_{mn}x_n \quad = 0, \end{array}$$

όπου $a_{ij} \in k \ \ i = 1, \ldots m, j = 1, \ldots n$.

Αφού $\mathcal{V} \neq \emptyset$, το σύστημα έχει λύση. Επειδή $a_{ij} \in k$, έχουμε ότι $V \subseteq k^n$. Άρα ο $\mathcal{V}$ έχει βάση της οποίας τα στοιχεία ανήκουν στο k^n.

- $2 \Longrightarrow 3$.

Έστω $\mathcal{V} =< v^{(1)}, \ldots, v^{(n-r)} >$, με $v^{(i)} \in k^n$, $i = 1, \ldots, n-r$.

Έστω επίσης η βάση του k^n : $v^{(1)}, \ldots, v^{(n-r)}, w^{(1)}, \ldots, w^{(r)}$.

Αυτά είναι και βάση του K^n, διότι διαφορετικά θα υπήρχαν $x_1, \ldots, x_n \in K$, τέτοια ώστε:

$$x_1 v^{(1)} + \ldots + x_{n-r} v^{(n-r)} + x_{n-r+1} w^{(1)} + \ldots + x_n w^{(r)} = 0.$$

Δηλαδή, σύστημα:

$$(v^{(1)}, \ldots, v^{(n-r)}, w^{(1)}, \ldots, w^{(r)}) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0,$$

έχει μη τετριμμένη λύση. Όμως, $v^{(1)}, \ldots, v^{(n-r)}, w^{(1)}, \ldots, w^{(r)} \in k^n$. Άρα, το σύστημα έχει μη τετριμμένη λύση στο k^n. Άτοπο.

Έστω η γραμμική απεικόνιση:

$$f : K^n \underset{\text{επί}}{\longmapsto} < w^{(1)}, \ldots, w^{(r)} >$$
$$\lambda_1 v^{(1)} + \ldots + \lambda_{n-r} v^{(n-r)} + \mu_1 w^{(1)} + \ldots + \mu_r w^{(r)} \longmapsto \mu_1 w^{(1)} + \ldots + \mu_r w^{(r)},$$

$\lambda_i, \mu_j \in K$, $i = 1, \ldots, n-r, j = 1, \ldots, r$.

Επίσης, ισχύει ότι:

$$< w^{(1)}, \ldots, w^{(r)} > \cong K^r,$$

μέσω της γραμμικής απεικόνισης:

$$g : < w^{(1)}, \ldots, w^{(r)} > \overset{1-1}{\underset{\text{επί}}{\longmapsto}} K^r$$
$$(i = 1, \ldots, r) \quad w^{(i)} \longmapsto e^{(i)},$$

(μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι τα $e^{(1)}, \ldots, e^{(r)}$ είναι αυτά τα οποία παράγουν το K^r).

Έστω η γραμμική απεικόνιση $h = g \circ f : K^n \longrightarrow K^r$.

Έχουμε ότι $\ker h = \mathcal{V}$.

Έστω $e^{(1)}, \ldots, e^{(n)}$ η κανονική βάση του K^n. Όμως, $e^{(1)}, \ldots, e^{(n)} \in k^n$, άρα υπάρχουν $\lambda_{li}, \mu_{lj} \in k$, τέτοια ώστε:

$$\lambda_{l1} v^{(1)} + \ldots + \mu_{lr} w^{(r)} = e^{(l)}, \text{ για κάθε } l = 1, \ldots, n.$$

Άρα, για κάθε $l = 1, \ldots, n$

$$f(e^{(l)}) = \mu_{lj} w^{(1)} + \ldots + \mu_{lr} w^{(r)}, \ \mu_{lj} \in k.$$

Οπότε, για κάθε $l = 1, \ldots, n$,

$$g(f(e^{(l)})) = \mu_{lj}^{(1)} + \ldots + \mu_{lr} e^{(r)}, \;\; \mu_{lj} \in k.$$

Άρα, ο πίνακας της γραμμικής απεικόνισης (ως προς τις κανονικές βάσεις) έχει στοιχεία στο k.

- $3 \Longrightarrow 1$.

Έστω μια γραμμική απεικόνιση,

$$f : \; K^n \underset{\text{επί}}{\longmapsto} K^r,$$

με πυρήνα $\mathcal{V}$, με πίνακα, (ως προς τις κανονικές βάσεις), $A \in k^{n \times n}$.

Γνωρίζουμε ότι ο $\mathcal{V} = \ker f$, είναι ο χώρος λύσεων του συστήματος,

$$AX = 0.$$

Δηλαδή, ο $\mathcal{V}$ είναι τομή αλγεβρικών συνόλων που ορίζονται απο γραμμικές μορφές με συντελεστές στοιχεία του $A \in k^{n \times n}$.

□

Α΄.8 Ένα σχόλιο για την γραμμική ανεξαρτησία των $\ell_1, \ldots, \ell_{n+1} \in \mathfrak{L}$

Λήμμα Α΄.8.1. *Αν τα $\ell_1, \ldots, \ell_{n+1} \in \mathfrak{L}$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα, τότε τα $\alpha_1 = \mathrm{e}^{\ell_1}, \ldots, \alpha_{n+1} = e^{\ell_{n+1}}$ ($\alpha_i \in \overline{\mathbb{Q}}$) παράγουν μια υποομάδα του $\mathbb{C}^*$ με $\mathrm{rank} = n+1$ ή n.*

Απόδειξη.

Διακρίνουμε τις εξής δύο περιπτώσεις:

είτε τα $\ell_1, \ldots, \ell_{n+1}, 2\pi i$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα, είτε τα $\ell_1, \ldots, \ell_{n+1}, 2\pi i$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένα.

Εξετάζουμε χωριστά την κάθε περίπτωση.

- Έστω ότι τα $\ell_1, \ldots, \ell_{n+1}, 2\pi i$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα.

Από αυτή την υπόθεση εύκολα έπεται ότι (ικάνη και αναγκαία συνθήκη) τα $\alpha_1, \ldots, \alpha_{n+1}$ είναι πολλαπλασιαστικώς ανεξάρτητα. Άρα, παράγουν μια πολλαπλασιαστική ομάδα του $\mathbb{C}^*$ με $\mathrm{rank} = n+1$.

- Έστω ότι τα $\ell_1, \ldots, \ell_{n+1}, 2\pi i$ είναι $\mathbb{Q}-$γραμμικώς εξαρτημένα.

Υπάρχουν δηλαδή $b_1, \ldots, b_{n+1} \in \mathbb{Z}$, όχι όλα μηδέν, τέτοια ώστε:

$$b_1 \ell_1 + \ldots + b_{n+1} \ell_{n+1} = k 2\pi i, \;\; k \in \mathbb{Z}.$$

Επειδή τα $\ell_1, \ldots, \ell_{n+1}$ είναι $\mathbb{Q}-$γραμμικώς ανεξάρτητα, έπεται ότι $|k| \geq 1$. Μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι $k \geq 1$.

Έστω $k \geq 1$, το ελάχιστο τέτοιο k, για το οποίο υπάρχουν $b_1, \ldots, b_{n+1} \in \mathbb{Z}$, όχι όλα μηδέν, έστω $b_{n+1} \neq 0$, τέτοια ώστε:

$$b_1\ell_1 + \ldots + b_{n+1}\ell_{n+1} = k2\pi i.$$

Αν υπάρχουν $c_1, \ldots, c_{n+1} \in \mathbb{Z}$, με

$$c_1\ell_1 + \ldots + c_{n+1}\ell_{n+1} = r2\pi i \text{ και } r \neq 0,$$

τότε εύκολα συμπεραίνεται ότι $(c_1, \ldots, c_{n+1}) = s(b_1, \ldots, b_{n+1})$, για κάποιο $s \in \mathbb{Z}$ (διαιρούμε το r με το k, έστω $r = sk+v$, $0 \leq v < k$, και χρησιμοποιούμε την ιδιότητα που έχει το k).

Συμπεραίνουμε ότι τα $\alpha_1, \ldots, \alpha_n$ είναι πολλαπλασιαστικώς ανεξάρτητα, αφού αν

$$\alpha_1^{x_1} \cdots \alpha_n^{x_n} = 1,$$

τότε

$$x_1\ell_1 + \ldots + x_n\ell_n + 0\ell_{n+1} = \mu 2\pi i, \;\; \mu \in \mathbb{Z}, \;\; \mu \neq 0$$

και λόγω των όσο είπαμε παραπάνω έχουμε ότι

$$(x_1, \ldots, x_n, 0) = \rho(b_1, \ldots, b_n, b_{n+1}), \;\; \rho \in \mathbb{Z}.$$

Επειδή όμως έχουμε υποθέσει ότι $b_{n+1} \neq 0$ έπεται ότι $\rho = 0$. Άρα $(x_1, \ldots, x_n, 0) = (0, \ldots, 0)$.

Άρα τα $\alpha_1, \ldots, \alpha_{n+1}$ παράγουν μια υποομάδα του $\mathbb{C}^*$ με $\text{rank} = n$.

□

Α΄.9 Απαλείφουσα δύο πολυωνύμων

Έστω A ένας δακτύλιος με μοναδική παραγοντοποίηση και

$$f = a_0 + a_1X + \ldots + a_pX^p, \;\; g = b_0 + b_1X + \ldots + b_qX^q$$

δύο πολυώνυμα του $A[X]$, θετικού βαθμού.

Πρόταση Α΄.9.1. *Τα πολυώνυμα f και g ένα κοινό παράγοντα θετικού βαθμού, αν και μόνο αν υπάρχουν πολυώνυμα $\alpha, \beta \in A[X]$ με $\deg(\alpha) < p$ και $\deg(\beta) < q$, έτσι ώστε:*

$$f\beta = g\alpha$$

Απόδειξη. Ας υποθέσουμε ότι $f = \phi\alpha$ και $g = \phi\beta$ όπου α, β και ϕ είναι πολυώνυμα του $A[X]$ με $\deg(\phi) \geq 1$. Τότε

$$f\beta = \phi\alpha\beta = g\alpha,$$

όπου $\deg(\alpha) < p$ και $\deg(\beta) < q$.

Αντιστρόφως, υποθέτουμε ότι υπάρχουν πολυώνυμα $\alpha, \beta \in A[Q]$ με $\deg(\alpha) < p$ και $\deg(\beta) < q$, έτσι ώστε:

$$f\beta = g\alpha.$$

Τότε, κάθε παράγοντας του f θετικού βαθμού είναι και παράγοντας του $g\alpha$. Καθώς όμως $\deg(\alpha) < p$, ένας τουλάχιστον τέτοιος παράγοντας του f είναι και παράγοντας του g. Έτσι, τα f και g έχουν ένα κοινό παράγοντα θετικού βαθμού.

□

Θεωρούμε τον τετραγωνικό πίνακα

$$M(f,g) = \begin{pmatrix} a_0 & a_1 & \dots & a_p & 0 & \dots & 0 \\ 0 & a_0 & \dots & a_{p-1} & a_p & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & \dots & a_0 & a_1 & \dots & a_p \\ b_0 & b_1 & \dots & b_q & 0 & \dots & 0 \\ 0 & b_0 & \dots & b_{q-1} & b_q & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & b_0 & \dots & b_{q-1} & b_q \end{pmatrix}.$$

Ο $M(f,g)$ έχει τα a_i στις πρώτες q γραμμές και τα b_i στις υπόλοιπες p γραμμές. Καλούμε *απαλείφουσα* των πολυωνύμων f και g την ορίζουσα του πίνακα $M(f,g)$ και την συμβολίζουμε με $R(f,g)$.

Αποδεικνύεται ότι η απαλείφουσα $R(f,g)$ είναι ομογενές πολυώνυμο βαθμού q ως προς τους συντελεστές $a_0, \dots, a_p$ και ομογενές πολυώνυμο βαθμού q ως προς τους συντελεστές $b_0, \dots, b_q$.

Πρόταση Α΄.9.2. *Τα πολυώνυμα f και g έχουν ένα κοινό παράγοντα θετικού βαθμού, αν και μόνο αν $R(f,g) = 0$.*

Απόδειξη. Έστω τα πολυώνυμα,

$$\alpha(X) = \alpha_0 + \alpha_1 X + \dots \alpha_{p-1} X^{p-1}, \;\; \beta(X) = \beta_0 + \beta_1 X + \dots \beta_{q-1} X^{q-1} \in A[X]$$

Τότε

$$f\alpha = g\beta,$$

αν και μόνο αν

$$\begin{aligned} a_0\beta_0 &= b_0\alpha_0 \\ a_1\beta_0 + a_0\beta_1 &= b_1\alpha_0 + b_0\alpha_1 \\ &\vdots \\ a_p\beta_{q-1} &= b_q\alpha_{p-1}. \end{aligned}$$

Το παραπάνω σύστημα με αγνώστους τα $\alpha_0, \ldots, \alpha_{p-1}, \beta_0, \ldots, \beta_{q-1}$, έχει μη μηδενική λύση, αν και μόνο αν η ορίζουσα των συντελεστών των αγνώστων είναι μηδέν. Όμως, η ορίζουσα αυτή ισούται με την $R(f, g)$, κατά προσέγγιση προσήμου. Άρα, υπάρχουν πολυώνυμα $\alpha, \beta \in A[X]$, με $\deg(\alpha) < p$ και $\deg(\beta) < q$, τέτοια ώστε $f\alpha = g\beta$, αν και μόνο αν $R(f, g) = 0$. Σύμφωνα με την πρόταση Α΄.9.1, τα f και g έχουν ένα κοινό παράγοντα θετικού βαθμού, αν και μόνο αν $R(f, g) = 0$.

□

Πρόταση Α΄.9.3. *Υπάρχουν πολυώνυμα α και β βαθμού $\leq q-1$ και $p-1$ αντίστοιχα, τέτοια ώστε:*

$$R(f, g) = \alpha f + \beta g.$$

Απόδειξη. Έστω, $A_1, \ldots, A_{p+q}$ οι συμπαράγοντες των στοιχείων της πρώτης στήλης του πίνακα $M(f, g)$. Τότε

$$\begin{aligned} a_0A_1 + b_0A_{q+1} &= R(f, g), \\ a_1A_1 + a_0A_2 + b_1A_{q+1} + b_0A_{q+2} &= 0, \\ &\vdots \\ a_pA_q + b_qA_{p+q} &= 0. \end{aligned}$$

Από την άλλη πλευρά έχουμε

$$\begin{aligned} f &= a_0 + a_1X + \ldots + a_pX^p, \\ Xf &= a_0X + a_1X^2 + \ldots + a_pX^{p+1}, \\ &\vdots \\ X^{q-1}f &= a_0X^{q-1} + a_1X^q + \ldots + a_pX^{p+q-1}, \\ g &= b_0 + b_1X + \ldots + b_qX^q, \\ Xg &= b_0X + b_1X^2 + \ldots + b_qX^{q+1}, \\ &\vdots \\ X^{p-1}g &= b_0X^{p-1} + b_1X^p + \ldots + b_qX^{p+q-1}. \end{aligned}$$

Στη συνέχεια πολλαπλασιάζουμε την $i-$οστή εξίσωση με το A_i και προσθέτουμε τους αντίστοιχους όρους για $i = 1, \ldots, p+q$. Έτσι, παίρνουμε

$$(A_1 + \ldots + A_q X^{q-1})f + (A_{q+1} + \ldots + A_{p+q}X^{p-1})g = R(f,g).$$

□

(Βιβλιογραφία: [33])

Α΄.10 Υπολογιστικά επιχειρήματα

Λήμμα Α΄.10.1. *Έστω C ένα πεπερασμένο σύνολο και $f : C \longrightarrow C'$ μια απεικόνιση. Τότε:*

$$\mathrm{Card}(C) = \sum_{c' \in f(C)} \mathrm{Card}(f^{-1}(c')).$$

Απόδειξη.

Η απεικόνιση f ορίζει μια σχέση ισοδυναμίας " $\sim$ " στα στοιχεία του C:

$$c_1, c_2 \in C, \;\; c_1 \sim c_2 \text{ αν και μόνο αν } f(c_1) = f(c_2).$$

Το πλήθος των κλάσεων είναι $\mathrm{Card}(f(C))$. Οι κλάσεις είναι της μορφής:

$$\{f^{-1}(c'), \;\; c' \in \; f(C)\}.$$

Οπότε,

$$\mathrm{Card}(C) = \sum_{c' \in \; f(C)} \mathrm{Card}(f^{-1}(c')).$$

□

Άμεση συνέπεια του λήμματος Α΄.10.1 είναι το

Πόρισμα Α΄.10.2. *Έστω C ένα πεπερασμένο σύνολο και $f : C \longrightarrow C'$ μια απεικόνιση. Τότε:*

$$\mathrm{Card}(f(C)) \cdot \min_{c' \in f(C)} \mathrm{Card}(f^{-1}(c')) \leq \mathrm{Card}(C) \leq \mathrm{Card}(f(C)) \cdot \max_{c' \in f(C)} \mathrm{Card}(f^{-1}(c')).$$

□

Μια εφαρμογή των παραπάνω είναι το

Λήμμα Α΄.10.3. *Έστω K ένα σώμα χαρακτηριστικής μηδέν.*

Υποθέτουμε ότι τα $\alpha_1, \ldots, \alpha_{n+1} \in K^*$ παράγουν μια υποομάδα του $\mathbb{C}^*$ με $\mathrm{rank} \geq n$. *Έστω επίσης, η κανονική απεικόνιση,*

$$\sigma : \;\; K^* \underset{\text{επί}}{\longrightarrow} \;\; K^*/K^*_{\mathrm{tors}}.$$

Τότε, για κάθε $S \geq 1$,

$$\mathrm{Card}\{\sigma(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}), \;\; \underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}(S)\} \geq (2S-1)^n.$$

Απόδειξη.

Αν τα $\alpha_1, \ldots, \alpha_{n+1}$ είναι πολλαπλασιαστικώς ανεξάρτητα, τότε:

$$\mathrm{Card}\{\sigma(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}) = (2S-1)^{n+1} \geq (2S-1)^n.$$

Διαφορετικά, η απεικόνιση,

$$\begin{aligned} h: \quad \mathbb{Z}^{n+1} &\longrightarrow K^*/K^*_{\mathrm{tors}} \\ (s_1, \ldots, s_{n+1}) &\longmapsto \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}, \end{aligned}$$

έχει πυρήνα της μορφής $\underline{a}\mathbb{Z}$, όπου $\underline{a} = (a_1, \ldots, a_{n+1}) \in \mathbb{Z}^{n+1}$.

Εφαρμόζουμε το πόρισμα Α΄.10.2 του λήμματος Α΄.10.1 για $C = \mathbb{Z}^{n+1}(S)$, $C' = K^*/K^*_{\mathrm{tors}}$ και f τον περιορισμό της h στο $C = \mathbb{Z}^{n+1}(S)$. Έστω $c' = f(\underline{s}^{(0)}) \in f(C)$, τέτοιο ώστε το $\mathrm{Card}(f^{-1}(c'))$ να είναι το μέγιστο. Οπότε,

$$\mathrm{Card}(C) \leq \mathrm{Card}(f(C)) \cdot \mathrm{Card}(f^{-1}(c')).$$

Για κάθε $\underline{s} \in f^{-1}(c')$, υπάρχει $\lambda_{\underline{s}} \in \mathbb{Z}$ με

$$\underline{s} - \underline{s}^{(0)} = \lambda_{\underline{s}} \underline{a}.$$

Έστω $i \in \{1, \ldots, n+1\}$ τέτοιο ώστε $a_i \neq 0$. Άρα, όλα τα $\lambda_{\underline{s}} = \frac{s_i - s_i^{(0)}}{a_i}$ και ισχύει ότι

$$|\lambda_{\underline{s}}| = \Big|\frac{s_i - s_i^{(0)}}{a_i}\Big| \leq \frac{2S-2}{|a_i|} \leq 2S-2.$$

Οπότε, $\mathrm{Card}(f^{-1}(c')) \leq 2S-2$ και άρα

$$\mathrm{Card}(f(C)) \geq \frac{(2S-1)^{n+1}}{2S-2} \geq \frac{(2S-1)^{n+1}}{2S-1} = (2S-1)^n.$$

□

Α΄.11 Θεώρημα Γραμμικών μορφών Minkowski

Θεώρημα Α΄.11.1. *Έστω A ένα σύνολο του $\mathbb{R}^n$ το οποίο είναι κυρτό, φραγμένο και συμμετρικό ως προς την αρχή των αξόνων, με όγκο $v(A)$* [4].

Αν $v(A) > 2^n$ τότε το A περιέχει ένα ακέραιο σημείο διαφορετικό από το μηδέν.

[4] Ο όγκος ενός συνόλου του R^n είναι το ολοκλήρωμα Riemann της χαρακτηριστικής συνάρτησης του συνόλου

Απόδειξη.

Συμβολίζουμε με A_m το σύνολο των ρητών σημείων του A των οποίων οι συντεταγμένες έχουν παρανομαστή m. Οπότε,

$$A_m = \{(\frac{t_1}{m}, \ldots, \frac{t_n}{m}) \in A,\ \ t_i \in \mathbb{Z},\ \ i = 1, \ldots, n\}.$$

Έστω $|A_m|$ ο πληθάριθμος του συνόλου A_m. Τότε, καθώς $m \to \infty$ ο αριθμός των σημείων του A_m είναι ασυμπτωτικά ίσος με $v(A)m^n$. Οπότε, για αρκτά μεγάλο m, έχουμε ότι:

$$|A_m| > (2m)^n.$$

Οπότε, υπάρχουν δύο διαφορετικά σημεία, $\underline{a} = (\frac{a_1}{m}, \ldots, \frac{a_n}{m}), \underline{b} = (\frac{b_1}{m}, \ldots, \frac{b_n}{m}) \in A_m$, τέτοια ώστε:

$$a_i \equiv b_i \pmod{2m},\ \text{ για κάθε } i = 1, \ldots, n.$$

Άρα, το $\frac{1}{2}(\underline{a} - \underline{b})$ είναι ακέραιο σημείο, διαφορετικό του $(0, \ldots, 0)$.

Τα $\underline{a}, \underline{b} \in A_m$, άρα ανήκουν στο A. Επίσης, $-\underline{b} \in A$, αφού το A είναι συμμετρικό ως προς το $(0, \ldots, 0)$. Το $\frac{1}{2}\underline{a} + \frac{1}{2}(-\underline{b}) = \frac{1}{2}(\underline{a} - \underline{b}) \in A$, αφού A είναι κυρτό.

□

Σχόλιο: Η προϋπόθεση $v(A) > 2^n$ είναι αυστηρή, διότι για $A = \{(x_1, \ldots, x_n) \in \mathbb{R}^n,\ |x_i| < 1\}$ έχουμε ότι $v(A) = 2^n$, αλλά δεν περιέχει κανένα ακέραιο σημείο διαφορετικό του $(0, \ldots, 0)$.

Θεώρημα Α΄.11.2. *(Θεώρημα γραμμικών μορφών του Minkowski)*

Έστω $B = (\beta_{ij})$, ένας $n \times n$ πίνακας πραγματικών αριθμών με ορίζουσα ± 1. Υποθέτουμε ότι $c_1, \ldots, c_n$ είναι θετικοί πραγματικοί αριθμοί με $c_1 \cdots c_n = 1$. Τότε υπάρχει ένα μη μηδενικό ακέραιο σημείο $(x_1, \ldots, x_n)$, τέτοιο ώστε:

$$|\beta_{i1}x_1 + \ldots + \beta_{in}x_n| < c_i,\ \ i = 1, \ldots, n-1,$$

και

$$|\beta_{n1}x_1 + \ldots + \beta_{nn}x_n| \leq c_n.$$

Απόδειξη.

Γράφουμε

$$L_i(\underline{x}) = \beta_{i1}x_1 + \ldots + \beta_{in}x_n,\ \ 1 \leq i \leq n.$$

Θέτουμε

$$L'_i(\underline{x}) = \frac{1}{c_i}L_i(\underline{x}),\ \ 1 \leq i \leq n.$$

Άρα, αρκεί να αποδείξουμε ότι

$$|L_i'(\underline{x})| < 1, \;\; 1 \leq i \leq n-1,$$

και

$$L_n'(\underline{x}) \leq 1.$$

Η ορίζουσα των $L_1', \ldots, L_n'$ είναι ίση με την $\det(B) = \pm 1$. Οπότε, μπορούμε να υποθέσουμε ότι $c_1 = \ldots = c_n = 1$.

Για κάθε $\varepsilon > 0$, ορίζουμε A_ε να είναι το σύνολο των $\underline{x} \in \mathbb{R}^n$ για τα οποία $L_i(\underline{x}) < 1, \;\; i = 1, \ldots, n-1$ και $L_n(\underline{x}) < 1 + \varepsilon$.

Το A_ε είναι συμμετρικό και φραγμένο. Επίσης είναι και κυρτό, αφού αν $\underline{x}, \underline{y} \in A_\varepsilon$ και $\lambda \in \mathbb{R}$ με $0 \leq \lambda \leq 1$, τότε

$$\begin{aligned} \big|L_i\big(\lambda\underline{x} + (1-\lambda)y\big)\big| &\leq \lambda\big|L_i(\underline{x})\big| + (1-\lambda)\big|L_i(\underline{y})\big| \\ &< \begin{cases} \lambda + 1 - \lambda = 1, & \text{για } i = 1, \ldots, n-1, \\ \lambda(1+\varepsilon) + (1-\lambda)(1+\varepsilon) = 1 + \varepsilon, & \text{για } i = n. \end{cases} \end{aligned}$$

Αφού, $\upsilon(A) = (1+\varepsilon)2^n > 2^n$, συμπεραίνουμε από το θεώρημα Α΄.11.1, ότι υπάρχει μη μηδενικό ακέραιο σημείο $\underline{x}_\varepsilon$ στο A_ε.

Θεωρούμε τα $A_{1/k}$, για $k \in \mathbb{N}$. Ισχύει ότι $A_1 \supseteq A_{1/2} \supseteq \cdots$. Έτσι παίρνουμε μια ακολουθία ακέραιων σημείων $\underline{x}_{1/k}$ των $A_{1/k}$, για $k \in \mathbb{N}$. Αφού το A_1 είναι φραγμένο και περιέχει πεπερασμένο το πλήθος ακέραια σημεία, υπάρχει ένα ακέραιο σημείο $\underline{y}$ της μορφής $\underline{x}_{1/k}$ για άπειρα το πλήθος k. Τότε,

$$L_i(\underline{y}) < 1, \;\; i = 1, \ldots, n-1,$$

και

$$L_n(\underline{y}) \leq 1.$$

□

(Βιβλιογραφία: [24])

Βιβλιογραφία

[1] E. Artin *Algebraic Numbers and Algebraic functions*, Lectures Notes by I. Adamson. Princenton and New York University, 1951

[2] A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge 1975.

[3] A. Baker, *Linear forms in the logarithms of algebraic numbers I*, Mathematika 13, 204-216, 1966.

[4] A. Baker, *Linear forms in the logarithms of algebraic numbers II*, Mathematika 14, 102-107, 1967.

[5] A. Baker, *Linear forms in the logarithms of algebraic numbers III*, Mathematika 14, 220-228, 1967.

[6] A. Baker, *Linear forms in the logarithms of algebraic numbers IV*, Mathematika 15, 204-216, 1968.

[7] A. Baker, *Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms*, Philos. Trans. Roy. Soc. London Ser. A 263, 173-191, 1968.

[8] A. Baker, G. Wüstholz, *Logarithmic forms and group varieties*, J. reine angew. Math. 442, 19-62, 1993.

[9] P.E Blanksby, H.L Montgomery, *Algebraic Integers near the Unit Circle*, Acta Arith. 18, 355-369, 1971.

[10] Z.I Borevich, I.R Shafarevich, *Number Theory*, Academic Press, London New York 1966.

[11] J. Buchmann, *A generalization of Voronoi's unit Algorithm* I & II, J. Number Theory 20, 177-191, 192-209, 1986.

[12] J. Buchmann, *The generalized Voronoi algorithm in totally real algebraic numbers fields*, Lecture Notes In Computer Science, 204, 479-486, 1985.

[13] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34, no 4, 391-401, 1979.

[14] L. Euler, *Introduction to Analysis of the infinite*, BOOK I. μεταφρασμένο από τα Λατινικά (Introductio to analysin infinitorum). Springer-Verlag, New York-Berlin, 1988.

[15] A.O Gelfond, *Transcendental Number Theory*, Moscow 1952, μεταφρ. στα Αγγλικά Dover publications, New York 1960.

[16] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, No 52, Springer-Verlag, New York-Heidelberg, 1977.

[17] M. Laurent, *Sur quelques résultats récents de transcendance*, Journées arithmétiques Luminy 1989, Astérisque, 198-200, 209-230, 1991.

[18] M. Laurent, *Hauters de matrices d'interpolation; in Approximations Diophantienennes et Nombres Transcendants*, Lumine 1990, éd. P. Phillipon, de Gruyter, 215-238, 1992.

[19] M. Laurent, *Linear forms in two logarithms and interpolation determinants*, Acta Atith. 66, no 2, 181-199, 1994.

[20] M. Laurent,M. Mignotte, Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d' interpolation*, J. Number Theory, 55 285-321, 1995.

[21] R. Narasimhan *Several Complex Variables*, Chicago Lectures in Math. New York, 1971.

[22] M. Pohst, H. Zassenhauss, *On effective computation of fundamental units* I & II, Math. Comp. 38, 275-291, 293-329, 1982.

[23] A. Schinzel, H. Zassenhauss, *A refinement of two theorems of Kronecker*, Michigan Math. J. 12, 81-85, 1965.

[24] W. Schmidt, *Diophantine Approximation* , Lect. Notes. 785, Springer, Berlin Heidelberg New York, 1980.

[25] C.L Stewart, *Algebraic Integers whose Conjugates lie near the Unit Circle*, Bull. Soc. Math. France 106, no 2, 169-176, 1978.

[26] K.B. Stolarsky, *Algebraic Numbers and Diophantine Approximation*, M. Decker, New York, 1974.

[27] A. Thue, *Uber Annaherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135, 284-305, 1909.

[28] N. Tzanakis, B.M.M de Weger, *On the Practical Solution of the Thue Equation*, J. Number Theory 31, 99-132, 1989.

[29] M. Waldschmidt, *Linear Independence of Logarithms of Algebraic Numbers*, Matscience Lecture Notes, Madras 1992.

[30] M. Waldschmidt, *A lower bound for linear forms in logarithms*, Acta Arith. 37, 257-283, 1980.

[31] M. Waldschmidt, *Un demi-sècle de Transcendence*,(μισός αιώνας υπερβατικότητας) στον τόμο Development of Mathematics 1950-2000, J.-P. Pier (ed), Birkhäuser, 1121-1186, 2000.

[32] Κ. Λάκκης, *Θεωρία Αριθμών*, Ζήτη, Θεσσαλονίκη, 1984.

[33] Δ. Μ. Πουλάκης, *Εισαγωγή στην Γεωμετρία των Αλγεβρικών Καμπυλών*, Ζήτη, Θεσσαλονίκη, 2006.

Ευρετήριο