Γεωμετρία των Αριθμών

Ελενη Τζανακη

Διπλωματικη Εργασια

Πανεπιστημιο Κρητης
Τμημα Μαθηματικων
Ιουνιος 2000

.

Η διπλωματική αυτή εργασία κατατέθηκε στο Τμήμα Μαθηματικών του Πανεπιστημίου Κρήτης τον Ιούνιο του 2000. Επιβλέπων ήταν ο Α. Γιαννόπουλος.

Την επιτροπή αξιολόγησης αποτέλεσαν οι: Α. Γιαννόπουλος, Μ. Παπαδημητράκης και Σ. Παπαδοπούλου.

Περιεχόμενα

Κεφάλαιο 1

Πλέγματα στον $\mathbb{R}^n$

1.1 Πλέγματα

Εργαζόμαστε στον Ευκλείδειο χώρο $\mathbb{R}^n$, τον διανυσματικό χώρο όλων των n-άδων $x = (x_1, \ldots, x_n)$ πραγματικών αριθμών. Σταθεροποιούμε το εσωτερικό γινόμενο

$$\langle x, y\rangle = x_1y_1 + \ldots + x_ny_n.$$

Αυτό το εσωτερικό γινόμενο επάγει στον $\mathbb{R}^n$ την Ευκλείδεια νόρμα $\|x\|_2 = \sqrt{\langle x, x\rangle}$. Συμβολίζουμε με D_n την Ευκλείδεια μοναδιαία μπάλα, με S^{n-1} τη μοναδιαία σφαίρα, και με ω_n τον n-διάστατο όγκο της D_n. Ορίζουμε

$$D(x, r) = \{y \in \mathbb{R}^n : \|x - y\|_2 \leq r\},$$

και $o = (0, \ldots, 0)$. Γράφουμε $L(\mathbb{R}^n)$ για το σύνολο των γραμμικών μετασχηματισμών του $\mathbb{R}^n$, και $GL(n)$ για την ομάδα των αντιστρέψιμων γραμμικών μετασχηματισμών του $\mathbb{R}^n$. Αν $T \in L(\mathbb{R}^n)$, ο συζυγής του T είναι ο $T^* \in L(\mathbb{R}^n)$ που ορίζεται από την

$$\langle Tx, y\rangle = \langle x, T^*y\rangle, \quad x, y \in \mathbb{R}^n.$$

Ορισμός Ένα υποσύνολο Λ του $\mathbb{R}^n$, $n \geq 2$, λέγεται **πλέγμα** αν υπάρχουν γραμμικώς ανεξάρτητα διανύσματα $u_1, \ldots, u_n \in \mathbb{R}^n$ για τα οποία

$$\Lambda = \{x \in \mathbb{R}^n : x = m_1u_1 + \ldots + m_nu_n, m_i \in \mathbb{Z}\}.$$

Τότε λέμε ότι το $\{u_1, \ldots, u_n\}$ είναι **βάση** του πλέγματος Λ. Ένα πλέγμα μπορεί να έχει περισσότερες από μία βάσεις (για την ακρίβεια, όπως θα δούμε παρακάτω, κάθε πλέγμα έχει άπειρες το πλήθος διαφορετικές βάσεις).

Παρατηρήσεις Ένα υποσύνολο Λ του $\mathbb{R}^n$ είναι πλέγμα αν και μόνο αν υπάρχει $T \in GL(n)$ για τον οποίο $\Lambda = T(\mathbb{Z}^n)$. Πράγματι, αν το Λ είναι πλέγμα με βάση το

$\{u_1,\dots,u_n\}$, τότε $\Lambda = T(\mathbb{Z}^n)$, όπου T ο γραμμικός μετασχηματισμός που ορίζεται από τις $T(e_i) = u_i$, $i = 1,\dots,n$. Αντίστροφα, αν $T \in GL(n)$, τότε το $T(\mathbb{Z}^n)$ είναι πλέγμα με βάση το $\{T(e_1),\dots,T(e_n)\}$.

Θεώρημα 1.1.1 *Κάθε πλέγμα Λ στον $\mathbb{R}^n$ είναι διακριτή προσθετική υποομάδα του $\mathbb{R}^n$. Λέγοντας διακριτή, εννοούμε ότι υπάρχει $r > 0$ ώστε $D(o,r) \cap (\Lambda \backslash \{o\}) = \emptyset$.*

Απόδειξη: Έστω $\Lambda = T(\mathbb{Z}^n)$, $T \in GL(n)$. Είναι φανερό ότι, αν $x, y \in \Lambda$ τότε $x - y \in \Lambda$, δηλαδή το Λ είναι προσθετική υποομάδα του $\mathbb{R}^n$.

Επίσης, αν ορίσουμε $Q = \{x \in \mathbb{R}^n : |x_i| < 1\}$, τότε $\mathbb{Z}^n \cap Q = \{o\}$. Χρησιμοποιώντας το γεγονός ότι ο T είναι ένα προς ένα, βλέπουμε ότι

$$\Lambda \cap T(Q) = T(\mathbb{Z}^n \cap Q) = \{o\}.$$

Όμως το $T(Q)$ είναι ανοικτό υποσύνολο του $\mathbb{R}^n$ και $o \in T(Q)$, άρα υπάρχει $r > 0$ ώστε $D(o,r) \subset T(Q)$. Έπεται ότι $D(o,r) \cap (\Lambda \backslash \{o\}) = \emptyset$. $\square$

Άμεσες συνέπειες του ορισμού της διακριτής προσθετικής ομάδας είναι οι εξής:

(α) Αν $D(o,r) \cap \Lambda = \{o\}$, τότε για κάθε $u \in \Lambda$ ισχύει $D(u,r) \cap \Lambda = \{u\}$.

(β) Για κάθε $R > 0$, η $D(o,R)$ περιέχει πεπερασμένα το πλήθος σημεία του Λ. Πράγματι, αν για κάποιο $R > 0$ υπήρχαν διακεκριμένα $x_n, n \in \mathbb{N}$, σημεία του Λ στην $D(o,R)$, τότε θα μπορούσαμε να βρούμε συγκλίνουσα υπακολουθία (x_{k_n}) της (x_n). Τότε, για οποιοδήποτε $r > 0$, θα μπορούσαμε να βρούμε $m, n \in \mathbb{N}$ τέτοια ώστε $o \neq x_{k_m} - x_{k_n} \in D(o,r) \cap \Lambda$. Δηλαδή, το Λ δεν θα ήταν διακριτή προσθετική υποομάδα του $\mathbb{R}^n$.

Θα χρησιμοποιήσουμε τις (α) και (β) για να δώσουμε έναν χαρακτηρισμό του πλέγματος.

Θεώρημα 1.1.2 *Ένα υποσύνολο Λ του $\mathbb{R}^n$ είναι πλέγμα αν και μόνο αν περιέχει n γραμμικώς ανεξάρτητα διανύσματα και είναι διακριτή προσθετική υποομάδα του $\mathbb{R}^n$.*

Απόδειξη: Η μία κατεύθυνση αποδείχθηκε στο Θεώρημα 1.1.1. Για την άλλη κατεύθυνση, υποθέτουμε ότι Λ είναι μία διακριτή προσθετική υποομάδα του $\mathbb{R}^n$, που περιέχει τα γραμμικώς ανεξάρτητα διανύσματα $x_1,\dots,x_n$. Θα κατασκευάσουμε μία βάση του Λ, δηλαδή ένα σύνολο $\{u_1,\dots,u_n\}$ γραμμικώς ανεξάρτητων διανυσμάτων στο Λ με την ιδιότητα: κάθε $v \in \Lambda$ γράφεται μονοσήμαντα στη μορφή $v = m_1u_1 + \ldots + m_nu_n$, όπου $m_1,\dots,m_n \in \mathbb{Z}$.

Τα $u_1,\dots,u_n$ θα οριστούν διαδοχικά. Στο πρώτο βήμα, θεωρούμε τον μονοδιάστατο υπόχωρο $F_1 = \langle x_1 \rangle$ που παράγεται από το x_1, και επιλέγουμε ως u_1 ένα μη μηδενικό διάνυσμα του $F_1 \cap \Lambda$ που έχει τη μικρότερη δυνατή απόσταση από το o. Πιό συγκεκριμένα, μπορούμε να πάρουμε $u_1 = tx_1$, όπου $t > 0$ ο μικρότερος δυνατός ώστε $tx_1 \in \Lambda$. Το Λ είναι διακριτό, άρα το ευθύγραμμο τμήμα $[o, x_1]$ θα περιέχει πεπερασμένα το πλήθος σημεία του πλέγματος. Επομένως, το u_1 είναι καλά ορισμένο.

Συνεχίζουμε επαγωγικά: θα δείξουμε ότι για κάθε $k \leq n$ μπορούμε να βρούμε $u_1, \dots, u_k \in \langle x_1, \dots, x_k\rangle$ τέτοια ώστε το $\Lambda \cap \langle x_1, \dots, x_k\rangle$ να παράγεται (με ακέραιους συντελεστές) από τα $u_1, \dots, u_k$:

$$\Lambda_k := \Lambda \cap \langle x_1, \dots, x_k\rangle = \{m_1u_1 + \dots + m_ku_k : m_i \in \mathbb{Z}\}.$$

Με μία τέτοια κατασκευή, τα u_i είναι γραμμικώς ανεξάρτητα και, για $k = n$, έχουμε

$$\Lambda = \{x \in \mathbb{R}^n : x = m_1u_1 + \dots + m_nu_n, m_i \in \mathbb{Z}\},$$

δηλαδή το Λ είναι πλέγμα.

Για την επιλογή του u_{k+1} θεωρούμε το παραλληλεπίπεδο

$$P = \{x = a_1u_1 + \dots + a_ku_k + bx_{k+1}, 0 \leq a_i < 1, 0 < b \leq 1\},$$

και επιλέγουμε σαν u_{k+1} ένα στοίχειο του $P \cap \Lambda$ για το οποίο ο συντελεστής b είναι ο ελάχιστος δυνατός. Το σύνολο $P \cap \Lambda$ είναι μη κενό γιατί $x_{k+1} \in P \cap \Lambda$, και έχει πεπερασμένα το πλήθος σημεία (γιατί το Λ είναι διακριτή ομάδα). Άρα, το u_{k+1} είναι καλά ορισμένο.

Τα $u_1, \dots, u_k$ είναι γραμμικώς ανεξάρτητα, και

$$u_{k+1} = \sum_{i=1}^{k} a_iu_i + bx_{k+1}$$

με $b \neq 0$. Αυτό σημαίνει ότι $u_{k+1} \notin \langle u_1, \dots, u_k\rangle$, άρα τα $u_1, \dots, u_{k+1}$ είναι γραμμικώς ανεξάρτητα. Θα δείξουμε ότι

$$(*) \qquad \Lambda_{k+1} := \Lambda \cap \langle x_1, \dots, x_{k+1}\rangle = \{m_1u_1 + \dots + m_{k+1}u_{k+1} : m_i \in \mathbb{Z}\}.$$

Έστω $x \in \Lambda_{k+1}$. Τα $u_1, \dots, u_{k+1}$ είναι βάση του $\langle x_1, \dots, x_{k+1}\rangle$, άρα $x = t_1u_1 + \dots + t_ku_k + t_{k+1}u_{k+1}$ για κάποιους $t_1, \dots, t_{k+1} \in \mathbb{R}$. Θέτουμε $\{z\} = z - [z]$ το κλασματικό μέρος του z, και θεωρούμε το

$$x' = \{t_1\}u_1 + \dots + \{t_k\}u_k + \{t_{k+1}\}u_{k+1} \in \Lambda.$$

Τότε,

$$\begin{aligned} x' &= \{t_1\}u_1 + \dots + \{t_k\}u_k + \{t_{k+1}\}\left(\sum_{i=1}^{k} a_iu_i + bx_{k+1}\right) \\ &= t_1'u_1 + \dots + t_k'u_k + \{t_{k+1}\}bx_{k+1} \in \Lambda, \end{aligned}$$

άρα, αν $0 < \{t_{k+1}\}$ τότε

$$x'' = \{t_1'\}u_1 + \dots + \{t_k'\}u_k + \{t_{k+1}\}bx_{k+1} \in \Lambda \cap P,$$

το οποίο είναι άτοπο αφού $\{t_{k+1}\}b < b$. Έπεται ότι $\{t_{k+1}\} = 0$, δηλαδή $t_{k+1} \in \mathbb{Z}$. Τότε όμως,

$$x' = \{t_1\}u_1 + \dots \{t_k\}u_k \in \Lambda \cap \langle x_1, \dots, x_k\rangle,$$

και, από την επαγωγική μας υπόθεση, πρέπει να έχουμε $t_1, \dots, t_k \in \mathbb{Z}$. Αυτό αποδεικνύει την $(*)$ και, επαγωγικά, το θεώρημα. $\square$

Παρατήρηση Η απόδειξη του θεωρήματος μάς δίνει ταυτόχρονα έναν τρόπο να περνάμε από ένα γραμμικώς ανεξάρτητο υποσύνολο $\{x_1, \dots, x_n\}$ ενός πλέγματος Λ σε βάση $\{u_1, \dots, u_n\}$ του Λ, με την ιδιότητα

$$\langle u_1, \dots, u_k \rangle = \langle x_1, \dots, x_k \rangle, \quad 1 \leq k \leq n.$$

1.2 Ορίζουσα ενός πλέγματος

Ορισμός Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, και $u_1, \dots, u_n$ μία βάση του. Το παραλληλεπίπεδο

$$P = \{\sum_{i=1}^{n} a_i u_i : 0 \leq a_i < 1\}$$

λέγεται **θεμελιώδες παραλληλεπίπεδο** του πλέγματος. Ο όγκος $|P|$ του P λέγεται **ορίζουσα του πλέγματος** και συμβολίζεται με $\det \Lambda$.

Η Πρόταση που ακολουθεί δείχνει ότι ο όγκος του θεμελιώδους παραλληλεπιπέδου είναι ανεξάρτητος από την επιλογή της βάσης.

Πρόταση 1.2.1 *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, και P, Q δύο θεμελιώδη παραλληλεπίπεδα του Λ. Τότε, $|P| = |Q|$.*

Απόδειξη: Έστω $\{u_1, \dots, u_n\}$ και $\{v_1, \dots, v_n\}$ οι βάσεις του Λ που ορίζουν τα θεμελιώδη παραλληλεπίπεδα P και Q. Τότε, αν U, V είναι οι πίνακες που έχουν σαν στήλες τα u_i, v_i αντίστοιχα, έχουμε

$$|P| = |\det U|, \quad |Q| = |\det V|.$$

Γράφουμε τα διανύσματα της μίας βάσης συναρτήσει των διανύσματων της άλλης, και έχουμε

$$u_i = \sum_{j=1}^{n} m_{ij} v_j, \quad v_i = \sum_{j=1}^{n} l_{ij} u_j,$$

όπου $M = (m_{ij})$ και $L = (l_{ij})$ πίνακες με ακέραιες συντεταγμένες. Τότε $U = VM^*$ και $V = UL^*$, άρα $ML = I$. Δηλαδή,

$$|\det M| \cdot |\det L| = 1,$$

και αφού $\det M, \det L \in \mathbb{Z}$, παίρνουμε $|\det M| = |\det L| = 1$. Αυτό σημαίνει ότι

$$|P| = |\det U| = |\det M| \cdot |\det V| = |\det V| = |Q|. \quad \square$$

Παρατήρηση Η απόδειξη της Πρότασης δίνει ότι: αν U και V είναι δύο βάσεις του ιδίου πλέγματος Λ, τότε συνδέονται μέσω ενός unimodular πίνακα. Υπάρχει δηλαδή πίνακας M με ακέραιες συντεταγμένες και ορίζουσα $\det M = \pm 1$, τέτοιος ώστε $U = VM^*$. Εύκολα ελέγχουμε ότι ισχύει και το αντίστροφο: αν V είναι μία βάση του πλέγματος Λ και M είναι ένας unimodular πίνακας, τότε οι στήλες του πίνακα VM^* αποτελούν βάση του Λ.

Αφού ο όγκος οποιουδήποτε θεμελιώδους παραλληλεπιπέδου του Λ είναι πάντα ο ίδιος, η ορίζουσα $\det \Lambda$ του Λ ορίζεται καλά. Μπορούμε μάλιστα με τη βοήθειά της να χαρακτηρίσουμε τις βάσεις του Λ:

Θεώρημα 1.2.1 *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, και $u_1, \dots, u_n \in \Lambda$. Τα $u_1, \dots, u_n$ είναι βάση του Λ αν και μόνο αν*

$$|\det(u_1, \dots, u_n)| = \det \Lambda.$$

Απόδειξη: Η μία κατεύθυνση είναι προφανής από τον ορισμό της $\det \Lambda$. Για την αντίστροφη κατεύθυνση, έστω $u_1, \dots, u_n \in \Lambda$ με $|\det(u_1, \dots, u_n)| = \det \Lambda$. Αφού $\det \Lambda > 0$, τα u_i είναι γραμμικώς ανεξάρτητα. Θα δείξουμε οτι αποτελούν βάση του Λ.

Θεωρούμε μία βάση V του Λ, και γράφουμε $U = VM^*$ και $V = UL^*$. Η V είναι βάση του πλέγματος και τα u_i ανήκουν στο Λ, άρα ο M έχει ακέραιες συντεταγμένες. Όμως,

$$|\det U| = |\det V| = \det \Lambda$$

από την υπόθεσή μας, άρα $|\det M| = 1$. Αυτό όμως μάς εξασφαλίζει ότι και ο $L = M^{-1}$ είναι ακέραιος πίνακας, διότι τα στοιχεία του είναι της μορφής

$$l_{ij} = \pm \frac{\det M_{ij}}{\det M} \in \mathbb{Z}.$$

[M_{ij} είναι ο πίνακας που προκύπτει από τον M αν «διαγράψουμε» την i-γραμμή και την j-στήλη του]. Αφού $V = UL^*$ και η V είναι βάση του Λ, τα u_i είναι βάση του Λ. $\square$

Το Θεώρημα 1.2.1 μάς δίνει ένα κριτήριο για να αποφασίζουμε αν n γραμμικώς ανεξάρτητα διανύσματα ενός πλέγματος αποτελούν βάση του. Γενικά, δεν υπάρχουν απλά γεωμετρικά κριτήρια που να απαντούν σε αυτό το ερώτημα. Η κατάσταση είναι πάντως απλή στην περίπτωση $\Lambda = \mathbb{Z}^2$:

Πρόταση 1.2.2 *Τα γραμμικώς ανεξάρτητα u_1, u_2 αποτελούν βάση του $\mathbb{Z}^2$ αν και μόνο αν στο κλειστό τρίγωνο $T = \{a_1u_1 + a_2u_2, 0 \leq a_i \leq 1, a_1 + a_2 \leq 1\}$ δεν υπάρχει άλλο σημείο του $\mathbb{Z}^2$ εκτός των o, u_1, u_2.*

Απόδειξη: Αν τα u_1, u_2 είναι βάση, τότε τα μόνα σημεία της μορφής $a_1u_1 + a_2u_2$ με $a_i \in \mathbb{Z}$ που ανήκουν στο T είναι τα o, u_1, u_2 (όταν $(a_1, a_2) = (0, 0)$ ή $(1, 0)$ ή $(0, 1)$).

Αντίστροφα: έστω ότι το $\{u_1, u_2\}$ δεν είναι βάση του $\mathbb{Z}^2$. Θα βρούμε ακέραιο σημείο στο $T^* := T \backslash \{o, u_1, u_2\}$. Υπάρχει $x \in \Lambda$ που γράφεται στη μορφή $x =$

$a_1u_1+a_2u_2$, και οι a_i δεν είναι και οι δύο ακέραιοι. Τότε, το $x' = \{a_1\}u_1+\{a_2\}u_2 \in \Lambda$ ανήκει στο παραλληλόγραμμο

$$P(u_1, u_2) := \{t_1u_1 + t_2u_2 : 0 \leq t_i \leq 1\}$$

και δεν είναι κορυφή του. Αν το x' ανήκει στο «κάτω» τρίγωνο T, τότε βρίσκεται στο T^* και έχουμε τελειώσει. Αν πάλι ανήκει στο «πάνω» τρίγωνο, τότε το $u_1 + u_2 - x'$ ανήκει στο T^* και, ταυτόχρονα, στο Λ. □

Παρατήρηση Η φυσιολογική γενίκευση της Πρότασης 1.2.2 είναι η εξής. Τα γραμμικώς ανεξάρτητα διανύσματα $u_1, \ldots, u_n$ είναι βάση του $\mathbb{Z}^n$ αν και μόνο αν το simplex με κορυφές $o, u_1, \ldots, u_n$ δεν περιέχει άλλο ακέραιο σημείο. Όμως αυτό δεν είναι σωστό: για παράδειγμα, τα $u_1 = (1, 0, 0), u_2 = (0, 1, 0), u_3 = (1, 1, 2)$ σχηματίζουν ένα simplex που δεν περιέχει άλλα ακέραια σημεία, χωρίς να αποτελούν βάση του $\mathbb{Z}^3$.

Η επόμενη πρόταση εξασφαλίζει την ύπαρξη πολλών διαφορετικών βάσεων για κάθε πλέγμα Λ στον $\mathbb{R}^n$, $n \geq 2$:

Πρόταση 1.2.3 *Αν $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ και ο μέγιστος κοινός διαιρέτης των $x_1, \ldots, x_n$ είναι 1, τότε το x επεκτείνεται σε βάση του $\mathbb{Z}^n$.*

Απόδειξη: Μπορούμε να βρούμε $y_2, \ldots, y_n \in \mathbb{Z}^n$ τέτοια ώστε τα $x, y_2, \ldots, y_n$ να είναι γραμμικώς ανεξάρτητα: αφού $x \neq o$, υπάρχει $i_0 \leq n$ τέτοιο ώστε $x_{i_0} \neq 0$, οπότε μπορούμε να πάρουμε σαν y_j τα διανύσματα e_i, $i \neq i_0$.

Κατόπιν κατασκευάζουμε βάση $\{u_1, \ldots, u_n\}$ όπως στο Θεώρημα 1.1.2, ξεκινώντας από τα $x, y_2, \ldots, y_n$. Παρατηρήστε ότι $u_1 = x$, γιατί το x είναι το πλησιέστερο προς το o ακέραιο σημείο του $\langle x \rangle$. Εδώ χρησιμοποιείται η υπόθεση ότι οι $x_1, \ldots, x_n$ έχουν μέγιστο κοινό διαιρέτη τη μονάδα. □

Πόρισμα 1.2.1 *Κάθε πλέγμα Λ στον $\mathbb{R}^n$, $n \geq 2$, έχει άπειρες το πλήθος διαφορετικές βάσεις.*

Απόδειξη: Αρκεί να εξετάσουμε την περίπτωση $\Lambda = \mathbb{Z}^n$. Υπάρχουν άπειρες το πλήθος n-άδες μη μηδενικών ακεραίων $x_1, \ldots, x_n$ που έχουν μέγιστο κοινό διαιρέτη τη μονάδα. Κάθε μία από αυτές ανήκει σε μία βάση του $\mathbb{Z}^n$, από την Πρόταση 1.2.3. Άρα, το $\mathbb{Z}^n$ έχει άπειρες διαφορετικές βάσεις. □

Το τελευταίο αποτέλεσμα αυτής της παραγράφου δίνει μία σημαντική ιδιότητα του θεμελιώδους παραλληλεπιπέδου (την οποία θα χρησιμοποιήσουμε αρκετές φορές στη συνέχεια):

Θεώρημα 1.2.2 *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, $\{u_1, \ldots, u_n\}$ μία βάση του Λ, και $P = \{a_1u_1 + \ldots + a_nu_n : 0 \leq a_i < 1\}$ το αντίστοιχο θεμελιώδες παραλληλεπίπεδο. Τότε,*

$$\mathbb{R}^n = P \oplus \Lambda.$$

Δηλαδή, οι μεταφορές του P κατά τα σημεία του Λ, καλύπτουν τον $\mathbb{R}^n$ χωρίς να επικαλύπτονται.

Απόδειξη: Έστω $x \in \mathbb{R}^n$. Τα u_i είναι βάση του $\mathbb{R}^n$, άρα μπορούμε να γράψουμε $x = \sum_{i=1}^n t_i u_i$ για κάποιους $t_i \in \mathbb{R}$. Θεωρούμε τα διανύσματα

$$y = \sum_{i=1}^n \{t_i\} u_i, \quad z = \sum_{i=1}^n [t_i] u_i.$$

Τότε, $z \in \Lambda$, $y \in P$, και

$$x = y + z \in P + \Lambda.$$

Κάθε $x \in \mathbb{R}^n$ γράφεται με μοναδικό τρόπο σε αυτήν τη μορφή: Αν για κάποιο $x \in \mathbb{R}^n$ είχαμε $x = y + z = y_1 + z_1$ με $y, y_1 \in P$, και $z, z_1 \in \Lambda$, τότε θα είχαμε $y - y_1 \in \Lambda$, δηλαδή

$$y - y_1 = \sum_{i=1}^n b_i u_i, \quad b_i \in \mathbb{Z}.$$

Όμως, $|b_i| = |a_i(y) - a_i(y_1)| < 1$. Έπεται ότι $b_i = 0$ για κάθε $i \leq n$. Οπότε $y = y_1$ και $z = z_1$, που αποδεικνύει το ζητούμενο. $\square$

Μία χρήσιμη εφαρμογή του Θεωρήματος 1.2.2 δίνεται στην επόμενη πρόταση:

Πρόταση 1.2.4 *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$. Για κάθε $R > 0$ συμβολίζουμε με $N(R)$ το πλήθος των σημείων του $\Lambda \cap D(o, R)$. Τότε,*

$$\lim_{R \to \infty} \frac{N(R)}{\omega_n R^n} = \frac{1}{\det \Lambda}.$$

Απόδειξη: Θεωρούμε το θεμελιώδες παραλληλεπίπεδο P του Λ ως προς μία βάση $\{u_1, \ldots, u_n\}$. Υπάρχει $a > 0$ τέτοιο ώστε $P \subset D(o, a)$. Για κάθε $R > 0$ ορίζουμε $U_R = \Lambda \cap D(o, R)$. Τότε,

$$\bigcup_{u \in U_R} (u + P) \subset D(o, R + a),$$

και, από το Θεώρημα 1.2.2, τα $u + P$ δεν επικαλύπτονται. Άρα,

$$N(R)(\det \Lambda) = N(R) \cdot |P| = |\bigcup_{u \in U_R} (u + P)| \leq \omega_n (R + a)^n,$$

δηλαδή,

$$(*) \qquad \frac{N(R)}{\omega_n R^n} \leq \left(\frac{R + a}{R} \right)^n \frac{1}{\det \Lambda} \to \frac{1}{\det \Lambda}.$$

Από την άλλη πλευρά, για μεγάλα $R > 0$, έχουμε

$$\bigcup_{u \in U_R} (u + P) \supset D(o, R - a).$$

Πράγματι, αν $x \in D(o, R-a)$, υπάρχουν $u \in \Lambda$ και $p \in P$ (οπότε $\|p\|_2 \leq a$) τέτοια ώστε $x = u + p$. Όμως τότε,

$$\|u\|_2 \leq \|x\|_2 + \|p\|_2 \leq R - a + a = R,$$

δηλαδή, $u \in U_R$. Όπως πρίν, καταλήγουμε στην

$$(**) \qquad \frac{N(R)}{\omega_n R^n} \geq \left(\frac{R-a}{R}\right)^n \frac{1}{\det\Lambda} \to \frac{1}{\det\Lambda}.$$

Συνδυάζοντας τις $(*)$ και $(**)$ παίρνουμε το ζητούμενο. □

1.3 Υποπλέγματα

Ορισμός: Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, και $\Lambda_0 \subseteq \Lambda$. Αν το Λ_0 είναι πλέγμα, τότε λέμε ότι το Λ_0 είναι **υποπλέγμα** του Λ. Αφού το Λ_0 είναι υποομάδα μιάς αβελιανής ομάδας, ορίζεται η ομάδα πηλίκο $\Lambda : \Lambda_0$. Ο πληθάριθμός της λέγεται **δείκτης** του Λ_0 στο Λ, και συμβολίζεται με $|\Lambda : \Lambda_0|$.

Με αυτόν το συμβολισμό, αν $|\Lambda : \Lambda_0| = s$, μπορούμε να γράψουμε το πλέγμα Λ σαν ένωση s το πλήθος ξένων συμπλόκων, δηλαδή

$$\Lambda = \bigcup_{i=1}^{s} (\Lambda_0 + a_i),$$

όπου $a_1, \ldots, a_s \in \Lambda$. Το πρώτο θεώρημα αυτής της παραγράφου υπολογίζει τον δείκτη του υποπλέγματος Λ_0 στο Λ:

Θεώρημα 1.3.1 *Έστω $V = \{v_1, \ldots, v_n\}$ μία βάση του Λ_0. Αν $P = \{\sum_{i=1}^n a_i v_i : 0 \leq a_i < 1\}$ είναι το θεμελιώδες παραλληλεπίπεδο του Λ_0 ως προς την V, τότε*

$$|\Lambda : \Lambda_0| = |P \cap \Lambda|,$$

όπου με $|A|$ συμβολίζουμε τον πληθάριθμο ενός πεπερασμένου συνόλου A.

Απόδειξη: Αν $y_1 \neq y_2 \in P \cap \Lambda$, τότε $y_1 + \Lambda_0 \neq y_2 + \Lambda_0$. Πράγματι, αν $y_1 + \Lambda_0 = y_2 + \Lambda_0$, τότε το $y_1 - y_2$ είναι μη μηδενικό και ανήκει στο Λ_0. Επίσης, $y_1 - y_2 \in \{\sum_{i=1}^n a_i v_i : |a_i| < 1\}$, διότι $y_1, y_2 \in P$. Όμως, το μοναδικό σημείο του Λ_0 που έχει αυτήν την ιδιότητα είναι το μηδενικό. Έπεται ότι

$$|\Lambda : \Lambda_0| \geq |P \cap \Lambda|.$$

Για την αντίστροφη ανισότητα, δείχνουμε ότι αν $x \in \Lambda$ τότε υπάρχει $y \in P \cap \Lambda$ τέτοιο ώστε $x \in y + \Lambda_0$: Πράγματι, από το Θεώρημα 1.2.2, υπάρχουν $y \in P$ και $z \in \Lambda_0$ τέτοια ώστε $x = y + z$. Αφού $x \in \Lambda$ και $z \in \Lambda_0 \subseteq \Lambda$, θα είναι $y = x - z \in \Lambda$. Άρα $y \in P \cap \Lambda$, και $x \in y + \Lambda_0$. □

Το επόμενο θεώρημα δίνει ένα «ειδικό» ζευγάρι βάσεων για τα Λ_0 και Λ (κανονική μορφή κατά Smith):

Θεώρημα 1.3.2 *Έστω Λ_0 ένα υποπλέγμα του πλέγματος Λ στον $\mathbb{R}^n$. Υπάρχουν βάσεις $U = \{u_1, \ldots, u_n\}$ του Λ και $V = \{v_1, \ldots, v_n\}$ του Λ_0, τέτοιες ώστε*

$$v_i = m_i u_i, \quad 1 = i, \ldots, n$$

και

$$m_i \mid m_{i+1}, \quad i = 1, \ldots, n-1.$$

Απόδειξη: Έστω $U = \{u_i\}$ και $V = \{v_i\}$ δύο βάσεις των Λ και Λ_0 αντίστοιχα. Κάθε $v_i \in V$ γράφεται μονοσήμαντα στη μορφή

$$v_i = m_{i1} u_1 + \ldots + m_{in} u_n, \quad m_{ij} \in \mathbb{Z}.$$

Παίρνουμε έτσι έναν ακέραιο πίνακα $M = M(U, V)$ ο οποίος εξαρτάται από την επιλογή των βάσεων U και V, για τον οποίο ισχύει η σχέση πινάκων

$$V = UM^*.$$

Θεωρούμε την κλάση $\mathcal{M} = \{M(U, V),\ U$ βάση του $\Lambda,\ V$ βάση του $\Lambda_0\}$. Η κλάση $\mathcal{M}$ μένει αναλλοίωτη ως προς τη δράση κάποιων μετασχηματισμών πινάκων:

(α) Αν μεταθέσουμε την i με την j γραμμή του πίνακα M, παίρνουμε τον πίνακα $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις U και $V_1 = V$ (με μετάθεση των v_i, v_j).

(β) Αν μεταθέσουμε την i με την j στήλη του πίνακα M, παίρνουμε τον πίνακα $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις $U_1 = U$ (με μετάθεση των u_i, u_j) και V.

(γ) Αν πολλαπλασιάσουμε την i γραμμή με -1, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις U και $V_1 = \{v_1, \ldots, -v_i, \ldots, v_n\}$.

(δ) Αν πολλαπλασιάσουμε την i στήλη με -1, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις $U_1 = \{u_1, \ldots, -u_i, \ldots, u_n\}$ και V.

(ε) Αν προσθέσουμε στην i-γραμμή την j-γραμμή πολλαπλασιασμένη επί κάποιο $s \in \mathbb{Z}$, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις U και $V_1 = \{v_1, \ldots, v_i + sv_j, \ldots, v_n\}$.

(στ) Αν προσθέσουμε στην i-στήλη την j-στήλη πολλαπλασιασμένη επί κάποιο $s \in \mathbb{Z}$, προκύπτει ο πίνακας $M_1 \in \mathcal{M}$ που αντιστοιχεί στις βάσεις $U_1 = \{u_1, \ldots, u_i - su_j, \ldots, u_n\}$ και V.

Οι παρατηρήσεις αυτές δείχνουν ότι υπάρχει $M \in \mathcal{M}$ με $m_{11} > 0$. Αυτό φαίνεται εύκολα γιατί, ξεκινώντας με τυχόντα $M_0 \in \mathcal{M}$ και εκτελώντας κατάλληλα κάποιους από τους μετασχηματισμούς που περιγράψαμε, μπορούμε να κάνουμε οποιοδήποτε μη μηδενικό στοιχείο του M θετικό και να το φέρουμε στην $(1,1)$ θέση.

Θεωρούμε όλους τους $M \in \mathcal{M}$ με $m_{11} > 0$, και κρατάμε έναν με ελάχιστο m_{11}. (αυτό το βήμα καθιστά την απόδειξη μη κατασκευαστική). Τότε, $m_{11} \mid m_{i1}, m_{1j}$ για κάθε $i, j = 1, \ldots n$. Πράγματι, αν σε κάποια περίπτωση είχαμε το αντίθετο, για παράδειγμα αν το m_{21} δεν ήταν πολλαπλάσιο του m_{11}, τότε κάνοντας την διαίρεση θα είχαμε $m_{21} = m_{11}\pi + \upsilon$ για κάποιο $0 < \upsilon < m_{11}$, $\upsilon \in \mathbb{Z}$. Τότε, πολλαπλασιάζοντας την πρώτη γραμμή με π και αφαιρώντας την από τη δεύτερη, θα παίρναμε $M_1 \in \mathcal{M}$ με $m_{21} = \upsilon$. Στη συνέχεια, αντιμεταθέτοντας την δεύτερη με την πρώτη γραμμή, θα παίρναμε έναν νέο πίνακα $M_2 \in \mathcal{M}$ ο οποίος στη θέση $(1,1)$ θα είχε το $v < m_{11}$, κάτι που είναι άτοπο από την επιλογή του πίνακα M.

Αφού λοιπόν $m_{11} | m_{i1}, m_{1j}$ για κάθε $i, j = 1, \ldots n$, μπορούμε, αφαιρώντας κατάλληλα πολλαπλάσια του m_{11} από κάθε γραμμή και στήλη του πίνακα, να μηδενίσουμε την πρώτη γραμμή και την πρώτη στήλη του πίνακα: να πάρουμε δηλαδή $M_1 \in \mathcal{M}$ με το m_{11} στην $(1,1)$-θέση και $m_{1j} = m_{i1} = 0$, $i, j = 2, \ldots, n$. Επιπλέον μπορούμε να αποδείξουμε ότι στον M_1 το m_{11} είναι διαιρέτης όλων των m_{ij} (αλλιώς, με επιτρεπτούς μετασχηματισμούς μπορούμε να βρούμε $A \in \mathcal{M}$ τέτοιον ώστε $0 < a_{11} < m_{11}$).

Θεωρούμε όλους τους πίνακες $M \in \mathcal{M}$ που έχουν τις παραπάνω ιδιότητες: το $m_{11} > 0$ είναι το ελάχιστο δυνατό στην $\mathcal{M}$, τα $m_{i1}, m_{1j} = 0$ αν $i, j \neq 1$, και κάθε m_{ij} είναι πολλαπλάσιο του m_{11}. Παίρνουμε πίνακα αυτής της μορφής με το $m_{22} > 0$ και ελάχιστο, και συνεχίζουμε όπως πρίν (αγνοώντας την πρώτη γραμμή και την πρώτη στήλη, οι οποίες έχουν οριστικοποιηθεί). Σε n βήματα, θα φτάσουμε στη ζητούμενη μορφή. $\square$

Η χρησιμότητα της κανονικής μορφής του Smith φαίνεται από το επόμενο θεώρημα.

Θεώρημα 1.3.3 *Έστω Λ_0 ένα υποπλέγμα του πλέγματος Λ στον $\mathbb{R}^n$. Αν U και V είναι βάσεις των Λ και Λ_0 αντίστοιχα, και P είναι το θεμελιώδες παραλληλεπίπεδο του Λ_0 ως προς την V, τότε*

$$|P \cap \Lambda| = |\Lambda : \Lambda_0| = |\det M(U,V)| = \frac{\det \Lambda_0}{\det \Lambda}.$$

Απόδειξη: Η πρώτη ισότητα αποδείχθηκε στο Θεώρημα 1.3.1, και για κάθε ζευγάρι βάσεων U, V των Λ, Λ_0 έχουμε

$$|\det M(U,V)| = \frac{|\det V|}{|\det U|} = \frac{\det \Lambda_0}{\det \Lambda}.$$

Αρκεί λοιπόν να δείξουμε ότι $|\det M(U,V)| = |P \cap \Lambda|$ για *κάποιο* ζευγάρι βάσεων U, V των Λ, Λ_0. Από το Θεώρημα 1.3.2, μπορούμε να επιλέξουμε βάσεις U, V τέτοιες ώστε

$$v_i = m_i u_i, \quad m_i \in \mathbb{Z}, \ i = 1, \ldots, n.$$

Τότε, είναι φανερό ότι

$$\det M(U,V) = m_1 m_2 \ldots m_n.$$

Απομένει να μετρήσουμε το πλήθος των σημείων του Λ που ανήκουν στο P. Όμως, λόγω της σχέσεως $v_i = m_i u_i$ έχουμε ότι, για κάθε $i = 1, \ldots, n$, στο ευθύγραμμο τμήμα $[o, v_i)$ υπάρχουν m_i το πλήθος σημεία του Λ. Άρα στο P θα έχουμε $m_1 m_2 \ldots m_n$ σημεία του Λ, τα $t_1 v_1 + \ldots + t_n v_n$, $t_i \in \{0, 1, \ldots, m_i - 1\}$. Αυτό αποδεικνύει το ζητούμενο. $\square$

Παρατήρηση: Το Θεώρημα 1.3.3 έχει τις εξής άμεσες, αλλά ενδιαφέρουσες, συνέπειες:

(α) Αν το Λ_0 είναι υποπλέγμα του Λ,τότε για κάθε βάση V του Λ_0, το πλήθος των σημείων του Λ που ανήκουν στο θεμελιώδες παραλληλεπίπεδο του Λ_0 ως προς την V είναι σταθερό, και ίσο με $|\Lambda : \Lambda_0|$.

(β) Μία ενδιαφέρουσα ειδική περίπτωση έχουμε αν πάρουμε σαν Λ το $\mathbb{Z}^n$. Αν $v_1, \ldots, v_n$ είναι γραμμικώς ανεξάρτητα διανύσματα του $\mathbb{R}^n$ με ακέραιες συντεταγμένες, τότε το παραλληλεπίπεδο P που ορίζουν περιέχει τόσα ακέραια σημεία όσος είναι ο όγκος του. Γιατί, αν Λ_0 είναι το υποπλέγμα του $\mathbb{Z}^n$ που παράγουν τα v_i, από το Θεώρημα 1.3.2 έχουμε

$$|P| = |\det \Lambda_0| = |\mathbb{Z}^n : \Lambda_0| = |\mathbb{Z}^n \cap P|.$$

Μία άλλη ενδιαφέρουσα εφαρμογή είναι ο **τύπος του Pick** για το πλήθος των ακεραίων σημείων που περιέχει ένα κυρτό πολύγωνο με ακέραιες κορυφές.

Θεώρημα 1.3.4 *Το πλήθος των ακεραίων σημείων μέσα σε ένα κυρτό πολύγωνο K με κορυφές ακέραια σημεία, είναι ίσο με*

$$A(K) + \frac{|\mathbb{Z}^2 \cap \mathrm{bd}(K)|}{2} + 1,$$

όπου $A(K)$ το εμβαδόν του K, και $\mathrm{bd}(K)$ το σύνορο του K.

Απόδειξη: Πρώτα αποδεικνύουμε τον τύπο για ένα τρίγωνο T. Χωρίς περιορισμό της γενικότητας, μπορούμε να υποθέσουμε ότι η μία κορυφή του T είναι το o. Αν a, b είναι οι άλλες δύο κορυφές του T, θεωρούμε το παραλληλόγραμμο $P = \{ta + sb : 0 \leq t, s < 1\}$ που παράγουν τα a, b. Από το Θεώρημα 1.3.2,

$$|\mathbb{Z}^2 \cap P| = A(P) = 2A(T).$$

Χωρίζουμε το P σε δύο τρίγωνα $T_1 = T$ και T_2 -το «πάνω» και το «κάτω»- φέρνοντας τη διαγώνιο ab. Δεν είναι δύσκολο να δούμε ότι

$$|\mathbb{Z}^2 \cap T_1^\circ| = |\mathbb{Z}^2 \cap T_2^\circ|,$$

και αν γράψουμε B για το πλήθος των ακεραίων σημείων στο εσωτερικό του T και C για το πλήθος των ακεραίων σημείων στο σύνορό του, έχουμε

$$|\mathbb{Z}^2 \cap P| = 2B + C - 2,$$

γιατί τα ακέραια σημεία της διαγωνίου βρίσκονται όλα στο P, εκτός από τα a, b. Έπεται ότι

$$B + C = \frac{1}{2}\left(|\mathbb{Z}^2 \cap P| + C + 2\right) = \frac{A(P)}{2} + \frac{C}{2} + 1 = A(T) + \frac{C}{2} + 1,$$

που είναι το ζητούμενο.

Έστω τώρα κυρτό πολύγωνο K με $n > 3$ κορυφές. Πάλι μπορούμε να υποθέσουμε ότι μία από αυτές είναι το o, και οι υπόλοιπες είναι οι $a_0, \ldots, a_{n-2}$. Χωρίζουμε το πολύγωνο σε $n-2$ τρίγωνα $T_1, \ldots T_{n-2}$ φέρνοντας τις διαγωνίους $oa_1, \ldots, oa_{n-3}$. Χρησιμοποιώντας τον τύπο που μόλις αποδείξαμε για τα τρίγωνα, έχουμε

$$|\mathbb{Z}^2 \cap T_i| = A(T_i) + \frac{C_i}{2} + 1, \quad i = 1, \ldots, n-2,$$

όπου C_i το πλήθος των ακεραίων σημείων στο σύνορο του T_i. Προσθέτοντας κατά μέλη, έχουμε

$$\sum_{i=1}^{n-2} |\mathbb{Z}^2 \cap T_i| = A(K) + \frac{1}{2}\sum_{i=1}^{n-2} C_i + (n-2).$$

Τα εσωτερικά σημεία των διαγωνίων έχουν μετρηθεί δύο φορές στο αριστερό μέλος, τα εσωτερικά σημεία των ακμών του K και οι κορυφές $a_1, \ldots, a_{n-3}$ έχουν μετρηθεί δύο φορές, οι κορυφές a_0, a_{n-2} μία φορά, και το o μετρήθηκε $(n-2)$ φορές. Άρα, αν D είναι το πλήθος των εσωτερικών σημείων των διαγωνίων, έχουμε

$$\sum_{i=1}^{n-2} |\mathbb{Z}^2 \cap T_i| = |\mathbb{Z}^2 \cap K| + D + 2(n-3).$$

Αντίστοιχα, στο δεξιό μέλος έχουμε

$$\sum_{i=1}^{n-2} C_i = 2D + E + (n-3) + (n-3),$$

όπου E το πλήθος των ακεραίων σημείων στο σύνορο του K, γιατί το o εμφανίζεται $(n-2)$ φορές, οι a_0, a_{n-1} από μία, και οι υπόλοιπες $(n-3)$ κορυφές του K από δύο. Άρα,

$$|\mathbb{Z}^2 \cap K| + D + 2(n-3) = A(K) + D + \frac{E}{2} + (n-3) + (n-2),$$

απ' όπου έπεται ότι

$$|\mathbb{Z}^2 \cap K| = A(K) + \frac{E}{2} + 1. \quad \square$$

1.4 Δυϊκό πλέγμα

Ορισμός Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$. Το σύνολο

$$\Lambda^* := \{y \in \mathbb{R}^n : \forall x \in \Lambda, \ \ \langle x, y\rangle \in \mathbb{Z}\}$$

ονομάζεται **δυϊκό πλέγμα** του Λ.

Στην επόμενη πρόταση αποδεικνύουμε ότι το Λ^* είναι όντως πλέγμα, και περιγράφουμε το Λ^* συναρτήσει του Λ:

Πρόταση 1.4.1 *Το Λ^* είναι πλέγμα στον $\mathbb{R}^n$. Αν $u_1, \ldots, u_n$ είναι μία βάση του Λ, τότε τα διανύσματα $u_1^*, \ldots, u_n^*$ που ορίζονται από τις*

$$\langle u_i, u_j^*\rangle = \delta_{ij}, \quad i, j = 1, \ldots, n$$

αποτελούν βάση του Λ^*.

Απόδειξη: Η απόδειξη θα βασιστεί στο γεγονός ότι

$$(\mathbb{Z}^n)^* = \mathbb{Z}^n.$$

Πράγματι, αν $x = (x_1, \ldots, x_n) \in (\mathbb{Z}^n)^*$, τότε $x_i = \langle x, e_i \rangle \in \mathbb{Z}$ για κάθε $i = 1, \ldots, n$, άρα $x \in \mathbb{Z}^n$. Αντιστρόφως, αν $x \in \mathbb{Z}^n$ τότε, προφανώς $\langle x, y \rangle \in \mathbb{Z}$ για κάθε $y \in \mathbb{Z}^n$, δηλαδή $x \in (\mathbb{Z}^n)^*$.

(α) Δείχνουμε πρώτα ότι το Λ^* είναι πλέγμα. Υπάρχει $T \in GL(n)$ τέτοιος ώστε $\Lambda = T(\mathbb{Z}^n)$. Τότε,

$$\begin{aligned} x \in \Lambda^* &\iff \forall y \in \Lambda \;\; \langle x, y \rangle \in \mathbb{Z} \\ &\iff \forall z \in \mathbb{Z}^n \;\; \langle x, Tz \rangle \in \mathbb{Z} \\ &\iff \forall z \in \mathbb{Z}^n \;\; \langle T^* x, z \rangle \in \mathbb{Z} \\ &\iff T^* x \in (\mathbb{Z}^n)^* = \mathbb{Z}^n \\ &\iff x \in T^{-*}(\mathbb{Z}^n). \end{aligned}$$

Όμως, $T^{-*} \in GL(n)$. Άρα, το $\Lambda^* = T^{-*}(\mathbb{Z}^n)$ είναι πλέγμα.

(β) Για τον δεύτερο ισχυρισμό, ας υποθέσουμε ότι $\{u_1, \ldots, u_n\}$ είναι μία βάση του Λ. Θεωρούμε τον $T \in GL(n)$ που ορίζεται από τις $T(e_i) = u_i$, $i = 1, \ldots, n$. Τότε, $\Lambda = T(\mathbb{Z}^n)$. Αν θέσουμε $u_j^* = T^{-*}(e_j)$, τότε το $\{u_1^*, \ldots, u_n^*\}$ είναι βάση του $T^{-*}(\mathbb{Z}^n) = \Lambda^*$, και

$$\langle u_i, u_j^* \rangle = \langle T e_i, T^{-*} e_j \rangle = \langle T^{-1} T e_i, e_j \rangle = \langle e_i, e_j \rangle = \delta_{ij}. \quad \square$$

Η βάση $\{u_1^*, \ldots, u_n^*\}$ του Λ^* που ορίσαμε στην Πρόταση 1.4.1 ονομάζεται **δυϊκή βάση** της $\{u_1, \ldots, u_n\}$.

1.5 Λ-υπόχωροι

Ορισμοί (α) Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$. Ένας k-διάστατος γραμμικός υπόχωρος F του $\mathbb{R}^n$ ονομάζεται **Λ-υπόχωρος** αν το $F \cap \Lambda$ είναι πλέγμα στον F. Δηλαδή αν υπάρχουν $v_1, \ldots, v_k \in F$ τέτοια ώστε

$$F \cap \Lambda = \{m_1 v_1 + \ldots + m_k v_k : m_i \in \mathbb{Z}\}.$$

(β) Έστω F ένας k-διάστατος Λ-υπόχωρος του $\mathbb{R}^n$. Ένα σύνολο σημείων $v_1, \ldots, v_k \in \Lambda$ ονομάζεται **πρωταρχικό για το** $F \cap \Lambda$ αν τα $v_1, \ldots, v_k$ αποτελούν βάση του πλέγματος $F \cap \Lambda$.

Θεώρημα 1.5.1 *Αν ο F είναι Λ-υπόχωρος και το $\{v_1, \ldots, v_k\}$ πρωταρχικό για το $F \cap \Lambda$, τότε επεκτείνεται σε βάση του Λ.*

Απόδειξη: Το Λ περιέχει n γραμμικώς ανεξάρτητα διανύσματα, επομένως μπορούμε να βρούμε $u_{k+1}, \ldots, u_n \in \Lambda$ τέτοια ώστε τα $v_1, \ldots, v_k, u_{k+1}, \ldots, u_n$ να είναι γραμμικώς ανεξάρτητα. Ξεκινώντας από αυτά τα διανύσματα, κατασκευάζουμε βάση του Λ όπως στο Θεώρημα 1.1.2. Στα πρώτα k βήματα, η κατασκευή γίνεται στον F, και αφού τα $v_1, \ldots, v_k$ είναι βάση του $F \cap \Lambda$ παραμένουν αμετάβλητα. $\square$

Ορισμός Έστω F ένας Λ-υπόχωρος. Ορίζουμε

$$F^{\perp} = \{y \in \mathbb{R}^n : \langle x, y \rangle = 0, \ \ \forall x \in F\}.$$

Θεώρημα 1.5.2 *Ο $F^{\perp}$ είναι Λ^*-υπόχωρος.*

Απόδειξη: Ο F είναι Λ-υπόχωρος, άρα υπάρχει βάση $\{v_1, \ldots, v_k\}$ του $F \cap \Lambda$. Χρησιμοποιώντας το Θεώρημα 1.5.1, την επεκτείνουμε σε βάση $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ του Λ. Θεωρούμε τη δυϊκή βάση $\{u_1, \ldots, u_n\}$ του Λ^*. Τότε, για κάθε $k+1 \leq j \leq n$ έχουμε

$$\langle v_i, u_j \rangle = 0, \quad i = 1, \ldots, k,$$

άρα $u_j \in F^{\perp}$, $j = k+1, \ldots, n$. Τα $u_{k+1}, \ldots, u_n$ είναι γραμμικώς ανεξάρτητα και ανήκουν στον $F^{\perp} \cap \Lambda^*$, επομένως ο $F^{\perp}$ είναι Λ^*-υπόχωρος. $\square$

Κεφάλαιο 2

Κυρτά σώματα στον $\mathbb{R}^n$

2.1 Κυρτά σώματα

(α) Ορισμοί

Κυρτό σώμα στον $\mathbb{R}^n$ είναι ένα μη κενό, κυρτό και συμπαγές υποσύνολο K του $\mathbb{R}^n$, που έχει μη κενό εσωτερικό. Θα λέμε ότι το κυρτό σώμα K είναι **συμμετρικό** με κέντρο συμμετρίας το o, αν για κάθε $x \in K$ έχουμε και $-x \in K$.

Πολλές φορές, θα χρειαστεί να μιλήσουμε για **ανοικτά κυρτά σώματα**. Αυτά είναι τα εσωτερικά των κυρτών σωμάτων. Ισχύει ότι: αν K είναι ένα κυρτό σώμα, τότε το K συμπίπτει με την κλειστή θήκη του εσωτερικού του.

Το **άθροισμα κατά Minkowski** δύο μη κενών υποσυνόλων A και B του $\mathbb{R}^n$ είναι το σύνολο

$$A + B := \{a + b : a \in A, b \in B\}.$$

Εύκολα ελέγχουμε ότι αν τα A και B είναι συμπαγή (αντίστοιχα, κυρτά), τότε και το άθροισμά τους $A + B$ είναι συμπαγές (αντίστοιχα, κυρτό). Ειδικότερα, το άθροισμα δύο κυρτών σωμάτων είναι κυρτό σώμα.

Με τον όρο **στοιχειώδες σύνολο** αναφερόμαστε σε μία πεπερασμένη ένωση ορθογωνίων που έχουν τις ακμές τους παράλληλες πρός τους άξονες συντεταγμένων (τις διευθύνσεις των ορθοκανονικών διανυσμάτων e_j), και έχουν ξένα εσωτερικά. Συμβολίζουμε με $\mathcal{I}$ την κλάση όλων των στοιχειωδών συνόλων.

Αν I είναι ένα τέτοιο ορθογώνιο, με μήκη ακμών $a_1, \ldots, a_n > 0$, τότε ορίζουμε τον **όγκο** του να ισούται με

$$|I| = a_1 \ldots a_n.$$

Αν $J = \cup_{k=1}^m I_k$ είναι ένα στοιχειώδες σύνολο, τότε ορίζουμε

$$|J| = \sum_{k=1}^m |I_k|.$$

Έστω τώρα A ένα μη κενό, φραγμένο υποσύνολο του $\mathbb{R}^n$. Ορίζουμε τον **εσωτερικό όγκο** του A μέσω της

$$\underline{|A|} = \sup\{|J| : J \subseteq A, J \in \mathcal{I}\},$$

και τον **εξωτερικό όγκο** του A μέσω της

$$\overline{|A|} = \inf\{|J| : A \subseteq J, J \in \mathcal{I}\}.$$

Θα λέμε ότι το A **έχει όγκο** (είναι Jordan μετρήσιμο), και θα τον συμβολίζουμε με $|A|$, αν $\underline{|A|} = \overline{|A|}$. Μπορεί κανείς να δείξει ότι

Κάθε κυρτό σώμα στον $\mathbb{R}^n$ έχει όγκο.

Οι ιδιότητες του όγκου που χρησιμοποιούμε συχνά στη συνέχεια είναι τελείως φυσιολογικές:

(α) Ο όγκος παραμένει αναλλοίωτος ως προς στροφές και μεταφορές.

(β) Αν T είναι ένας αντιστρέψιμος γραμμικός μετασχηματισμός του $\mathbb{R}^n$, τότε γιά κάθε συμπαγές υποσύνολο του $\mathbb{R}^n$ ισχύει

$$|T(K)| = |\mathrm{det}T||K|.$$

(γ) Έστω K κυρτό σώμα στον $\mathbb{R}^n$. Για κάθε $r \in \mathbb{N}$, ορίζουμε

$$N_r = \frac{1}{r}\mathbb{Z}^n \cap K.$$

Θεωρούμε το θεμελιώδες ορθογώνιο Q του $(1/r)\mathbb{Z}^n$, και την ένωση

$$\bigcup_{z \in N_r} (z + Q).$$

Ο όγκος της είναι ίσος με $|N_r|/r^n$. Είναι λογικό να υποθέσουμε (και μπορούμε να αποδείξουμε) ότι καθώς το $r \to +\infty$, παίρνουμε όλο και καλύτερη προσέγγιση του όγκου του K. Δηλαδή, ισχύει το εξής:

$$\lim_{r\to\infty} \frac{|N_r|}{|K|r^n} = 1.$$

(β) Συμμετρικά κυρτά σώματα

Θεωρούμε μία νόρμα $\|\cdot\|$ στον $\mathbb{R}^n$. Τότε, η μοναδιαία μπάλα $B_X = \{x \in \mathbb{R}^n : \|x\| \leq 1\}$ του χώρου με νόρμα $X = (\mathbb{R}^n, \|\cdot\|)$ είναι ένα συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Το γεγονός ότι η B_X είναι συμπαγές σύνολο και έχει μη κενό εσωτερικό, οφείλεται στο ότι η $\|\cdot\|$ είναι ισοδύναμη με την Ευκλείδεια νόρμα. Δηλαδή, υπάρχουν $a, b > 0$ τέτοιοι ώστε

$$a\|x\|_2 \leq \|x\| \leq b\|x\|_2, \quad x \in \mathbb{R}^n.$$

Ισοδύναμα,

$$(1/b)D_n \subseteq B_X \subseteq (1/a)D_n,$$

το οποίο δείχνει ότι η B_X είναι φραγμένο σύνολο και περιέχει μία ανοικτή μπάλα με κέντρο το o. Η B_X είναι κλειστό σύνολο, γιατί είναι κλειστή ως προς την $\|\cdot\|$, και, από την ισοδυναμία των νορμών, κάθε κλειστό σύνολο ως προς την $\|\cdot\|$ είναι κλειστό ως προς την Ευκλείδεια μετρική. Τέλος, η κυρτότητα και η συμμετρία της B_X είναι απλές συνέπειες των ιδιοτήτων της νόρμας: η $\|\cdot\|$ είναι άρτια, θετικά ομογενής συνάρτηση, και ικανοποιεί την τριγωνική ανισότητα.

Αντίστροφα, ας υποθέσουμε ότι K είναι ένα συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Ο Minkowski όρισε την συνάρτηση

$$\|x\|_K = \min\{\lambda \geq 0 : x \in \lambda K\},$$

και απέδειξε ότι είναι νόρμα, για την οποία ισχύει $\|x\|_K \leq 1$ αν και μόνο αν $x \in K$. Η ύπαρξη του λεγόμενου *συναρτησοειδούς του Minkowski* δείχνει ότι, με μία έννοια, η μελέτη των συμμετρικών κυρτών σωμάτων στον $\mathbb{R}^n$ είναι ισοδύναμη με τη μελέτη των νορμών πάνω στον $\mathbb{R}^n$:

Πρόταση 2.1.1 *Έστω $K \subseteq \mathbb{R}^n$ ένα συμμετρικό κυρτό σώμα. Τότε, το συναρτησοειδές του Minkowski*

$$\|x\|_K = \min\{\lambda \geq 0 : x \in \lambda K\}$$

είναι νόρμα, και

$$K = \{x \in \mathbb{R}^n : \|x\|_K \leq 1\}.$$

Απόδειξη: Το K περιέχει μία μπάλα με κέντρο το o. Πράγματι, αφού το K έχει μη κενό εσωτερικό, υπάρχουν $x \in K$ και $r > 0$ τέτοια ώστε $D(x,r) \subseteq K$. Λόγω συμμετρίας έχουμε $D(-x,r) \subseteq K$, και λόγω κυρτότητας, $D(o,r) = [D(x,r) + D(-x,r)]/2 \subseteq K$.

Έστω $x \in \mathbb{R}^n$. Υπάρχει $\lambda > 0$ αρκετά μεγάλο, ώστε $(1/\lambda)x \in D(o,r) \subseteq K$, άρα, $x \in \lambda K$. Αυτό δείχνει ότι, για κάθε $x \in \mathbb{R}^n$, το σύνολο $\{\lambda \geq 0 : x \in \lambda K\}$ είναι μη κενό, άρα ορίζεται το

$$\inf\{\lambda \geq 0 : x \in \lambda K\}.$$

Θεωρούμε μία γνησίως φθίνουσα ακολουθία $\lambda_s \to \lambda$. Υπάρχουν $y_s \in K$ τέτοια ώστε $x = \lambda_s y_s$, και λόγω της συμπάγειας του K μπορούμε να υποθέσουμε ότι $y_s \to y \in K$. Τότε, $x = \lambda y \in K$. Άρα το infimum είναι minimum, και η $\|x\|_K$ είναι καλά ορισμένη. Επίσης, είναι τώρα φανερό ότι $\|x\|_K \geq 0$ για κάθε $x \in \mathbb{R}^n$, και $\|x\|_K = 0$ αν και μόνο αν $x = o$.

Από τη συμμετρία του K ως προς το o, έχουμε $x \in \lambda K$ αν και μόνο αν $-x \in \lambda K$. Αυτό αποδεικνύει ότι

$$\|-x\|_K = \min\{\lambda \geq 0 : -x \in \lambda K\} = \min\{\lambda \geq 0 : x \in \lambda K\} = \|x\|_K.$$

Επίσης, αν $t > 0$, τότε

$$\begin{aligned} \|tx\|_K &= \min\{\lambda \geq 0 : tx \in \lambda K\} = \min\{\lambda \geq 0 : x \in (\lambda/t)K\} \\ &= \min\{t\mu : \mu \geq 0, x \in \mu K\} = t\min\{\mu \geq 0 : x \in \mu K\} \\ &= t\|x\|_K. \end{aligned}$$

Οι δύο προηγούμενες σχέσεις αποδεικνύουν ότι $\|tx\|_K = |t| \cdot \|x\|_K$, για κάθε $t \in \mathbb{R}$ και κάθε $x \in \mathbb{R}^n$.

Για την τριγωνική ανισότητα, παρατηρούμε ότι $x \in \|x\|_K K$ και $y \in \|y\|_K K$, οπότε η κυρτότητα του K μάς εξασφαλίζει ότι $x + y \in (\|x\|_K + \|y\|_K)K$, δηλαδή

$$\|x + y\|_K \leq \|x\|_K + \|y\|_K, \quad x, y \in \mathbb{R}^n.$$

Τέλος, $x \in K$ αν και μόνο αν $\min\{\lambda \geq 0 : x \in \lambda K\} \leq 1$, δηλαδή $\|x\|_K \leq 1$. $\square$

(γ) Το πολικό σώμα ενός συμμετρικού κυρτού σώματος

Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Το **πολικό σώμα** του K είναι το

$$K^\circ = \{y \in \mathbb{R}^n : \forall x \in K, |\langle x, y\rangle| \leq 1\}.$$

Θεωρούμε τον χώρο $X = (\mathbb{R}^n, \|\cdot\|_K)$, και τον δυϊκό του χώρο X^*. Τα γραμμικά συναρτησοειδή $f : X \to \mathbb{R}$ αναπαρίστανται από $y_f \in \mathbb{R}^n$: για κάθε $f \in X^*$ υπάρχει μοναδικό $y_f \in \mathbb{R}^n$ τέτοιο ώστε

$$f(x) = \langle y, x\rangle, \quad x \in \mathbb{R}^n,$$

και αντίστροφα κάθε $y \in \mathbb{R}^n$ ορίζει $f_y \in X^*$ με τον ίδιο τρόπο. Μπορούμε λοιπόν να ταυτίσουμε (ως γραμμικό χώρο) τον X^* με τον $\mathbb{R}^n$. Μεταφέρουμε τη νόρμα του X^* στον $\mathbb{R}^n$, ορίζοντας

$$\|y\|_* = \|f_y\|_{X^*} = \max_{x \in B_X} |f_y(x)| = \max\{|\langle y, x\rangle| : x \in K\}.$$

Τότε, η μοναδιαία μπάλα του $(\mathbb{R}^n, \|\cdot\|_*)$ είναι ακριβώς το K°. Πράγματι,

$$K^\circ = \{y \in \mathbb{R}^n : \max_{x \in K} |\langle y, x\rangle| \leq 1\} = \{y \in \mathbb{R}^n : \|y\|_* \leq 1\}.$$

Έχουμε λοιπόν αποδείξει το εξής:

Πρόταση 2.1.2 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$, και $X = (\mathbb{R}^n, \|\cdot\|_K)$. Τότε,το K° είναι η μοναδιαία μπάλα του δυϊκού χώρου του X.* $\square$

Από τον ορισμό του πολικού σώματος, και από τον χαρακτηρισμό του που μάς δίνει η προηγούμενη Πρόταση, μπορούμε εύκολα να αποδείξουμε τις παρακάτω βασικές ιδιότητές του:

Πρόταση 2.1.3 *Έστω K, K_1 συμμετρικά κυρτά σώματα στον $\mathbb{R}^n$. Τότε,*
(α) Αν $K \subseteq K_1$, τότε $K_1^\circ \subseteq K^\circ$.
(β) $(K^\circ)^\circ = K$.
(γ) Αν $T \in GL(n)$, τότε $(TK)^\circ = T^{-*}K^\circ$.
(δ) $|K||K^\circ| = |TK||(TK)^\circ|$.

Απόδειξη: (α) Αν $y \in K_1^\circ$, τότε για κάθε $x \in K_1$ έχουμε $|\langle x, y\rangle| \leq 1$, και αφού $K \subseteq K_1$ έπεται ότι για κάθε $x \in K$ θα είναι $|\langle x, y\rangle| \leq 1$, δηλαδή $y \in K^\circ$.

(β) Ο $X = (\mathbb{R}^n, \|\cdot\|_K)$ είναι αυτοπαθής, άρα το K είναι η μοναδιαία μπάλα του $X^{**} = (\mathbb{R}^n, \|\cdot\|_{K^\circ})^*$. Δηλαδή, το K είναι το πολικό σώμα του K°.

(γ) Έχουμε $y \in (TK)^\circ$ αν και μόνο αν για κάθε $x \in TK$ ισχύει $|\langle x, y\rangle| \leq 1$, δηλαδή αν, για κάθε $z \in K$ ισχύει $|\langle Tz, y\rangle| = |\langle z, T^*y\rangle| \leq 1$, δηλαδή, αν $T^*y \in K^\circ$. Άρα, $(TK)^\circ = (T^*)^{-1}(K^\circ)$.

(δ) Έχουμε $|TK| = |\det T| \cdot |K|$ και $|(TK)^\circ| = |(T^*)^{-1}(K^\circ)| = |\det T|^{-1}|K^\circ|$. Άρα,

$$|TK||(TK)^\circ| = |\det T| \cdot |K| \cdot |\det T|^{-1}|K^\circ| = |K| \cdot |K^\circ|. \quad \square$$

2.2 Η ανισότητα Brunn-Minkowski

Η ανισότητα Brunn-Minkowski συνδέει τον όγκο με την πράξη της πρόσθεσης κατά Minkowski. Θα δώσουμε μία απόδειξη που χρησιμοποιεί τα στοιχειώδη σύνολα και οφείλεται στον Lyusternik (1940):

Θεώρημα 2.2.1 ***(Ανισότητα Brunn-Minkowski).*** *Έστω A και B συμπαγή, μη κενά υποσύνολα του $\mathbb{R}^n$. Τότε,*

$$|A+B|^{1/n} \geq |A|^{1/n} + |B|^{1/n}.$$

Απόδειξη: *1η Περίπτωση:* Εξετάζουμε πρώτα την περίπτωση που τα A και B είναι ορθογώνια με τις ακμές τους παράλληλες προς τους άξονες συντεταγμένων. Υποθέτουμε ότι $a_1, \ldots, a_n > 0$ είναι τα μήκη των ακμών του A, και $b_1, \ldots, b_n > 0$ τα μήκη των ακμών του B. Τότε, το $A + B$ είναι κι αυτό ορθογώνιο με τις ακμές του παράλληλες προς τους άξονες συντεταγμένων, και αντίστοιχα μήκη $a_1 + b_1, \ldots, a_n + b_n$. Επομένως, η ανισότητα παίρνει τη μορφή

$$((a_1+b_1)\ldots(a_n+b_n))^{1/n} \geq (a_1\ldots a_n)^{1/n} + (b_1\ldots b_n)^{1/n}.$$

Ισοδύναμα, ζητάμε να δείξουμε ότι

$$\left(\frac{a_1}{a_1+b_1}\cdots\frac{a_n}{a_n+b_n}\right)^{1/n} + \left(\frac{b_1}{a_1+b_1}\cdots\frac{b_n}{a_n+b_n}\right)^{1/n} \leq 1.$$

Όμως από την ανισότητα αριθμητικού-γεωμετρικού μέσου, το αριστερό μέλος της τελευταίας ανισότητας είναι μικρότερο ή ίσο από

$$\frac{1}{n}\left(\frac{a_1}{a_1+b_1}+\ldots+\frac{a_n}{a_n+b_n}\right)+\frac{1}{n}\left(\frac{b_1}{a_1+b_1}+\ldots+\frac{b_n}{a_n+b_n}\right)=1.$$

Δηλαδή, η ανισότητα Brunn-Minkowski ισχύει σε αυτήν την απλή περίπτωση.

2η Περίπτωση: Υποθέτουμε ότι τα A, B είναι στοιχειώδη σύνολα, καθένα δηλαδή από αυτά είναι πεπερασμένη ένωση ορθογωνίων που έχουν ξένα εσωτερικά και ακμές παράλληλες προς τους άξονες συντεταγμένων.

Ορίζουμε σαν **πολυπλοκότητα** του ζευγαριού (A, B) το συνολικό πλήθος των ορθογωνίων που σχηματίζουν τα A, B. Θα αποδείξουμε την ανισότητα Brunn-Minkowski με επαγωγή ως προς την πολυπλοκότητα m του (A, B). Οταν $m = 2$, τα A και B είναι ορθογώνια και η ανισότητα έχει ήδη αποδειχθεί.

Υποθέτουμε λοιπόν ότι $m \geq 3$ και ότι το ζητούμενο ισχύει γιά ζευγάρια στοιχειωδών συνόλων με πολυπλοκότητα $\leq m-1$. Αφού $m \geq 3$, κάποιο από τα A και B (έστω το A) αποτελείται από τουλάχιστον δύο ορθογώνια. Έστω I_1, I_2 δύο από αυτά. Τα I_1 και I_2 έχουν ξένα εσωτερικά, συνεπώς μπορούμε να τα διαχωρίσουμε με ένα υπερεπίπεδο παράλληλο προς κάποιον κύριο υπόχωρο του $\mathbb{R}^n$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι αυτό το υπερεπίπεδο περιγράφεται από την $x_n = \rho$ γιά κάποιο $\rho \in \mathbb{R}$. Ορίζουμε

$$A^+ = A \cap \{x \in \mathbb{R}^n : x_n \geq \rho\} \quad , \quad A^- = A \cap \{x \in \mathbb{R}^n : x_n \leq \rho\}.$$

Τα A^+ και A^- είναι στοιχειώδη σύνολα, έχουν ξένα εσωτερικά και καθένα τους σχηματίζεται από λιγότερα ορθογώνια απ' ότι το A (Το υπερεπίπεδο $x_n = \rho$ στην χειρότερη περίπτωση χωρίζει κάθε ορθογώνιο του A σε δύο ορθογώνια, ένα στο A^+ κι ένα στο A^-. Όμως, το I_1 περιέχεται εξ ολοκλήρου στο A^+ ενώ το I_2 στο A^-). Περνώντας τώρα στο B, βρίσκουμε υπερεπίπεδο $x_n = s$ τέτοιο ώστε αν $B^+ = B \cap \{x \in \mathbb{R}^n : x_n \geq s\}$ και $B^- = B \cap \{x \in \mathbb{R}^n : x_n \leq s\}$ να ισχύει

$$(*) \qquad \frac{|A^+|}{|A|} = \frac{|B^+|}{|B|}.$$

Τα B^+ και B^- είναι στοιχειώδη σύνολα με πλήθος ορθογωνίων που δεν ξεπερνάει αυτό του B. Ονομάζουμε λ τον κοινό λόγο όγκων στην $(*)$. Προφανώς, $0 < \lambda < 1$. Είναι φανερό ότι

$$A + B = (A^+ + B^+) \cup (A^+ + B^-) \cup (A^- + B^+) \cup (A^- + B^-).$$

Από την άλλη πλευρά, αφού $A^+ + B^+ \subseteq \{x : x_n \geq \rho + s\}$ και $A^- + B^- \subseteq \{x : x_n \leq \rho + s\}$, τα $A^+ + B^+$ και $A^- + B^-$ έχουν ξένα εσωτερικά. Επομένως,

$$|A + B| \geq |A^+ + B^+| + |A^- + B^-|.$$

Με βάση την κατασκευή που κάναμε, εφαρμόζεται η επαγωγική υπόθεση στο δεξιό μέλος:

$$|A^+ + B^+|^{1/n} \geq |A^+|^{1/n} + |B^+|^{1/n} \quad , \quad |A^- + B^-|^{1/n} \geq |A^-|^{1/n} + |B^-|^{1/n},$$

οπότε κάνοντας πράξεις, και παίρνοντας υπ' όψιν την $(*)$ έχουμε

$$\begin{aligned} |A+B| &\geq \left((\lambda|A|)^{1/n}+(\lambda|B|)^{1/n}\right)^n+\left(((1-\lambda)|A|)^{1/n}+((1-\lambda)|B|)^{1/n}\right)^n \\ &= \lambda[|A|^{1/n}+|B|^{1/n}]^n+(1-\lambda)[|A|^{1/n}+|B|^{1/n}]^n=[|A|^{1/n}+|B|^{1/n}]^n, \end{aligned}$$

απ' όπου έπεται ότι

$$|A+B|^{1/n}\geq |A|^{1/n}+|B|^{1/n}.$$

Γενική Περίπτωση: Έστω A,B τυχόντα μη κενά συμπαγή υποσύνολα του $\mathbb{R}^n$. Υπάρχουν ακολουθίες $\{A_m\}$ και $\{B_m\}$ στοιχειωδών συνόλων με τις ιδιότητες

$$A_m\subseteq A \quad ,|A_m|\to|A| \quad ,B_m\subseteq B \quad , \quad |B_m|\to|B| \quad , \quad m\in\mathbb{N}.$$

Τότε $A_m+B_m\subseteq A+B$ γιά κάθε $m\in\mathbb{N}$ και

$$\begin{aligned} |A+B|^{1/n} &\geq \limsup_{m\to\infty}|A_m+B_m|^{1/n} \\ &\geq \limsup_{m\to\infty}[|A_m|^{1/n}+|B_m|^{1/n}] \\ &= |A|^{1/n}+|B|^{1/n}. \quad \square \end{aligned}$$

Η ανισότητα Brunn-Minkowski γιά κυρτά σώματα στον $\mathbb{R}^n$ συχνά διατυπώνεται ως εξής:

Πόρισμα 2.2.1 *Έστω K_1,K_2 κυρτά σώματα στον $\mathbb{R}^n$. Γιά κάθε $\lambda\in(0,1)$ ισχύει*

$$|\lambda K_1+(1-\lambda)K_2|^{1/n}\geq\lambda|K_1|^{1/n}+(1-\lambda)|K_2|^{1/n}.$$

Δηλαδή, η συνάρτηση $f:[0,1]\to\mathbb{R}$ με $f(\lambda)=|\lambda K_1+(1-\lambda)K_2|^{1/n}$ είναι κοίλη.

Απόδειξη: Αρκεί να δείξουμε ότι $f(a\lambda+(1-a)\mu)\geq af(\lambda)+(1-a)f(\mu)$ γιά κάθε $\lambda,\mu\in[0,1]$ και $a\in(0,1)$. Έχουμε

$$\begin{aligned} f(a\lambda+(1-a)\mu) &= |(a\lambda+(1-a)\mu)K_1+(1-a\lambda-(1-a)\mu)K_2|^{1/n} \\ &= |(a\lambda+(1-a)\mu)K_1+(a(1-\lambda)+(1-a)(1-\mu))K_2|^{1/n} \\ &= |a(\lambda K_1+(1-\lambda)K_2)+(1-a)(\mu K_1+(1-\mu)K_2)|^{1/n} \\ &\geq |a(\lambda K_1+(1-\lambda)K_2)|^{1/n}+|(1-a)(\mu K_1+(1-\mu)K_2)|^{1/n} \\ &= a|\lambda K_1+(1-\lambda)K_2|^{1/n}+(1-a)|\mu K_1+(1-\mu)K_2|^{1/n} \\ &= af(\lambda)+(1-a)f(\mu), \end{aligned}$$

όπου χρησιμοποιήσαμε το γεγονός ότι αν $X\subseteq\mathbb{R}^n$ κυρτό, μη κενό και $a,b>0$ τότε $aX+bX=(a+b)X$. $\square$

Μία άλλη συνέπεια της ανισότητας Brunn-Minkowski είναι η ακόλουθη ανισότητα (η οποία είναι *ανεξάρτητη της διάστασης*):

Πόρισμα 2.2.2 *Έστω A, B συμπαγή, μη κενά υποσύνολα του $\mathbb{R}^n$. Γιά κάθε $\lambda \in (0,1)$ έχουμε*

$$|\lambda A + (1-\lambda)B| \geq |A|^\lambda |B|^{1-\lambda}.$$

Απόδειξη: Η συνάρτηση log είναι κοίλη, κι αυτό έχει σαν συνέπεια την

$$x^\lambda y^{1-\lambda} \leq \lambda x + (1-\lambda)y$$

γιά κάθε $x, y > 0$ και $\lambda \in (0,1)$. Από την ανισότητα Brunn-Minkowski παίρνουμε

$$|\lambda A + (1-\lambda)B| \geq [\lambda |A|^{1/n} + (1-\lambda)|B|^{1/n}]^n \geq [|A|^{\lambda/n}|B|^{(1-\lambda)/n}]^n = |A|^\lambda |B|^{1-\lambda}. \quad \square$$

2.3 Το θεώρημα του John

Ελλειψοειδές στον $\mathbb{R}^n$ είναι ένα κυρτό σώμα της μορφής

$$(*) \qquad E = \left\{ x \in \mathbb{R}^n : \sum_{i=1}^n \frac{\langle x, v_i \rangle^2}{\alpha_i^2} \leq 1 \right\},$$

όπου $\{v_i\}_{i \leq n}$ είναι ορθοκανονική βάση του $\mathbb{R}^n$, και $\alpha_1, \ldots, \alpha_n$ είναι θετικοί πραγματικοί αριθμοί (οι διευθύνσεις και τα μήκη των ημιαξόνων του E αντίστοιχα).

Πρόταση 2.3.1 *Το $E \subseteq \mathbb{R}^n$ είναι ελλειψοειδές αν και μόνο αν υπάρχει $T \in GL(n)$ τέτοιος ώστε $E = T(D_n)$.*

Απόδειξη: Υποθέτουμε πρώτα ότι το E είναι ελλειψοειδές, ορίζεται δηλαδή από την $(*)$ για κάποια ορθοκανονική βάση $\{v_1, \ldots, v_n\}$ του $\mathbb{R}^n$, και κάποιους $\alpha_1, \ldots, \alpha_n > 0$. Έστω T ο γραμμικός μετασχηματισμός του $\mathbb{R}^n$ που ορίζεται από τις $T(v_i) = \alpha_i v_i$, $i = 1, \ldots, n$. Ο T είναι προφανώς αντιστρέψιμος, και $x \in T(D_n)$ αν και μόνο αν υπάρχει $y = \sum_{j=1}^n t_j v_j \in D_n$ με $x = Ty$. Τότε όμως, η ισότητα

$$\sum_{i=1}^n \frac{\langle x, v_i \rangle^2}{\alpha_i^2} = \sum_{i=1}^n \frac{\langle \sum_{j=1}^n t_j \alpha_j v_j, v_i \rangle^2}{\alpha_i^2} = \sum_{i=1}^n t_i^2$$

δείχνει ότι $x \in T(D_n)$ αν και μόνο αν $x \in E$, δηλαδή $E = T(D_n)$.

Αντίστροφα, έστω $T \in GL(n)$ και $E = T(D_n)$. Γράφουμε $S = T^{-1}$, και έχουμε

$$\|x\|_E^2 = \|x\|_{S^{-1}(D_n)}^2 = \|Sx\|_2^2 = \langle Sx, Sx \rangle = \langle S^*Sx, x \rangle.$$

Ο S^*S είναι συμμετρικός και θετικά ορισμένος, άρα γράφεται στη μορφή U^*DU όπου D διαγώνιος πίνακας με θετικά διαγώνια στοιχεία $\alpha_1^{-2}, \ldots, \alpha_n^{-2}$, και ο U είναι ορθογώνιος πίνακας. Θεωρούμε τον διαγώνιο πίνακα $D_1 = \sqrt{D}$ με διαγώνια στοιχεία τα $\alpha_1^{-1}, \ldots, \alpha_n^{-1}$. Αφού ο U είναι ορθογώνιος, έχουμε $S^*S = A^2$, όπου $A = U^*D_1U$. Δηλαδή,

$$\|x\|_E^2 = \langle A^2x, x\rangle = \|Ax\|_2^2 = \|D_1Ux\|_2^2 = \sum_{i=1}^{n} \frac{\langle Ux, e_i\rangle^2}{\alpha_i^2} = \sum_{i=1}^{n} \frac{\langle x, v_i\rangle^2}{\alpha_i^2},$$

όπου τα $v_i = U^*e_i$ αποτελούν ορθοκανονική βάση του $\mathbb{R}^n$. Έπεται ότι $x \in E$ αν και μόνο αν ικανοποιείται η $(*)$ για τα συγκεκριμένα v_i και α_i, δηλαδή το E είναι ελλειψοειδές. □

Παρατήρηση: Από την απόδειξη είναι φανερό ότι ο όγκος του E ισούται με

$$|E| = |D_n| \prod_{i=1}^{n} \alpha_i.$$

Θεωρούμε τώρα ένα συμμετρικό κυρτό σώμα K στον $\mathbb{R}^n$ και την οικογένεια $\mathcal{E}(K)$ όλων των ελλειψοειδών που περιέχονται στο K. Ο F. John [J] (1948) έδειξε ότι υπάρχει μοναδικό ελλειψοειδές E που περιέχεται στο K και έχει τον μέγιστο δυνατό όγκο. Θα λέμε ότι το E είναι το **ελλειψοειδές μέγιστου όγκου** του K. Για την απόδειξη, βλέπουμε ταυτόχρονα ότι υπάρχει μοναδικό ελλειψοειδές E που περιέχει το K και έχει ελάχιστο όγκο:

Πρόταση 2.3.2 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$, και $\mathcal{E}'(K)$ η οικογένεια όλων των ελλειψοειδών που περιέχουν το K. Υπάρχει μοναδικό ελλειψοειδές $E \in \mathcal{E}'(K)$ με ελάχιστο όγκο.*

Απόδειξη: Θεωρούμε τον αριθμό

$$V = \inf\{|E| : E \in \mathcal{E}'(K)\} > 0.$$

Υπάρχει ακολουθία $T_m \in GL(n)$ έτσι ώστε $E_m = T_m^{-1}(D_n) \supseteq K$ και

$$|E_m| = \frac{|D_n|}{|\det(T_m)|} \to V.$$

Αφού $\|T_m : X_K \to \ell_2^n\| \leq 1$, $m \in \mathbb{N}$, μπορούμε να βρούμε υπακολουθία $\{T_{k_m}\}$ και $S \in L(\mathbb{R}^n)$ με $T_{k_m} \to S$. Τότε,

$$|\det(S)| = |D_n|/V > 0,$$

επομένως, $S \in GL(n)$. Ορίζουμε $E = S^{-1}(D_n)$. Έχουμε

$$\|S : X_K \to \ell_2^n\| = \lim \|T_{k_m} : X_K \to \ell_2^n\| \leq 1,$$

άρα $E \supseteq K$. Αφού $|E| = V$, το E είναι ένα ελλειψοειδές που περιέχει το K, με τον ελάχιστο δυνατό όγκο.

Δείχνουμε τώρα ότι υπάρχει ένα μόνο ελλειψοειδές με αυτήν την ιδιότητα. Έστω ότι τα E_1 και E_2 περιέχουν το K και έχουν ελάχιστο όγκο. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $E_1 = D_n$ είναι η Ευκλείδεια μοναδιαία μπάλα, και

$$E_2 = \left\{ x \in \mathbb{R}^n : \sum_{i=1}^{n} \langle x, v_i \rangle^2 / \alpha_i^2 \leq 1 \right\}.$$

Θεωρούμε ένα τρίτο ελλειψοειδές, τον «μέσο όρο» τους

$$F = \left\{ x \in \mathbb{R}^n : \sum_{i=1}^{n} \frac{1}{2}(1 + \alpha_i^{-2}) \langle x, v_i \rangle^2 \leq 1 \right\}.$$

Είναι φανερό ότι $F \supseteq E_1 \cap E_2 \supseteq K$, επομένως

$$(*) \qquad |F| \geq |E_1| = |E_2|.$$

Αφού $E_1 = D_n$, η $(*)$ παίρνει τη μορφή

$$\begin{aligned} 1 = \left(\prod_{i=1}^{n} \alpha_i \right)^2 & \leq \prod_{i=1}^{n} \frac{2}{1 + \alpha_i^{-2}} \\ & = \prod_{i=1}^{n} \frac{2\alpha_i^2}{1 + \alpha_i^2} \\ & = \prod_{i=1}^{n} \frac{2\alpha_i}{1 + \alpha_i^2}, \end{aligned}$$

οπότε, $2\alpha_i = 1 + \alpha_i^2$ για κάθε $i = 1, \ldots, n$. Τότε όμως, $\alpha_i = 1$, $i = 1, \ldots, n$. Άρα, $E_1 = E_2$. $\square$

Η Πρόταση 2.3.2 μας δίνει την ύπαρξη και τη μοναδικότητα του ελλειψοειδούς μέγιστου όγκου του K:

Θεώρημα 2.3.1 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Υπάρχει μοναδικό ελλειψοειδές $E \in \mathcal{E}(K)$ με μέγιστο όγκο.*

Απόδειξη: Είδαμε ότι υπάρχει μοναδικό ελλειψοειδές F ελάχιστου όγκου που περιέχει το K°. Θεωρούμε το $E = F^\circ$. Από την Πρόταση 2.1.3(α),(β) έχουμε $E \subseteq K$, και αν E_1 είναι ένα άλλο ελλειψοειδές με $E_1 \subseteq K$, τότε $E_1^\circ \supseteq K^\circ$, άρα $|E_1^\circ| \geq |F|$. Επομένως, χρησιμοποιώντας την Πρόταση 2.1.3(δ), βλέπουμε ότι

$$|E_1| = \frac{|D_n|^2}{|E_1^\circ|} \leq \frac{|D_n|^2}{|F|} = |E|.$$

Ισότητα μπορεί να ισχύει μόνο αν $E_1^\circ = F$, δηλαδή $E_1 = E$. Άρα, το E είναι το μοναδικό ελλειψοειδές μέγιστου όγκου του K. $\square$

Ο F. John [J] έδειξε ότι αν η D_n είναι το ελλειψοειδές μέγιστου όγκου που περιέχεται στο συμμετρικό κυρτό σώμα K, τότε $K \subseteq \sqrt{n} D_n$ (*Θεώρημα του John*):

Θεώρημα 2.3.2 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Υποθέτουμε ότι η Ευκλείδεια μοναδιαία μπάλα D_n είναι το ελλειψοειδές μέγιστου όγκου που περιέχεται στο K. Τότε,*

$$K \subseteq \sqrt{n} D_n.$$

Απόδειξη: Υποθέτουμε ότι το συμπέρασμα δεν ισχύει. Τότε, υπάρχει x στο σύνορο του K το οποίο βρίσκεται έξω από την $\sqrt{n}D_n$. Αλλάζοντας συντεταγμένες αν χρειαστεί, μπορούμε να υποθέσουμε ότι $x = ae_1$, όπου $a > \sqrt{n}$. Από τη συμμετρία του K έπεται ότι,

$$K \supset W = \mathrm{co}\{D_n, \pm ae_1\}.$$

Για κάθε $\gamma, \delta > 0$ ορίζουμε το ελλειψοειδές

$$E_{\gamma,\delta} = \big\{x \in \mathbb{R}^n : \frac{x_1^2}{\gamma^2} + \sum_{i=2}^{n} \frac{x_i^2}{\delta^2} \leq 1\big\}.$$

Ισχυρισμός. Αν $\gamma > 1$ και $\gamma^2 \leq a^2 - a^2\delta^2 + \delta^2$, τότε $E_{\gamma,\delta} \subseteq W \subseteq K$.

[Πράγματι: λόγω της σφαιρικής συμμετρίας του $E_{\gamma,\delta}$ και του W ως προς τις $(n-1)$ τελευταίες μεταβλητές, μπορούμε να υποθέσουμε ότι $n = 2$. Τότε, το W ορίζεται από τις εφαπτόμενες από τα $(\pm a, 0)$ στον δίσκο D_2, και τον D_2. Τα σημεία επαφής των τεσσάρων εφαπτομένων με τον δίσκο είναι τα

$$\left(\pm\frac{1}{a}, \pm\frac{\sqrt{a^2-1}}{a}\right),$$

και οι εξισώσεις των τεσσάρων εφαπτομένων είναι οι

$$y = \frac{\pm a \pm x}{\sqrt{a^2-1}}.$$

Αν $\gamma > 1$, τότε η έλλειψη $E_{\gamma,\delta}$ θα περιέχεται στο W αν δεν τέμνει τις τέσσερις ευθείες, και, εξετάζοντας τη δευτεροβάθμια εξίσωση που προκύπτει, καταλήγουμε στη συνθήκη του ισχυρισμού.]

Από την άλλη πλευρά, ο όγκος του $E_{\gamma,\delta}$ ισούται με $|E_{\gamma,\delta}| = |D_n|\gamma\delta^{n-1}$. Αν λοιπόν $\gamma\delta^{n-1} > 1$, τότε $|E_{\gamma,\delta}| > |D_n|$. Με την υπόθεση ότι $a > \sqrt{n}$, θα δείξουμε ότι υπάρχουν $\gamma > 1$ και $\delta > 0$ που ικανοποιούν ταυτόχρονα τις

$$\gamma\delta^{n-1} > 1 \quad , \quad \gamma^2 = a^2 - a^2\delta^2 + \delta^2.$$

Αυτό είναι άτοπο, γιατί θα έχουμε βρεί ελλειψοειδές που περιέχεται στο K και έχει όγκο γνήσια μεγαλύτερο από τον όγκο της D_n.

Λύνοντας ως προς δ, έχουμε $\delta = \sqrt{\frac{a^2-\gamma^2}{a^2-1}}$, και μελετάμε τη συνάρτηση

$$f(\gamma) = \gamma\left(\frac{a^2-\gamma^2}{a^2-1}\right)^{\frac{n-1}{2}}, \quad 1 < \gamma < a.$$

Η f έχει μέγιστο στο $\gamma_0 = a/\sqrt{n}$, το οποίο ισούται με

$$f(\gamma_0) = \frac{a}{\sqrt{n}} \left(\frac{a\sqrt{n-1}}{\sqrt{n}\sqrt{a^2-1}} \right)^{n-1} > 1,$$

κάτι που μπορούμε να δείξουμε παρατηρώντας ότι η $g(x) = x^n/(x^2-1)^{(n-1)/2}$ είναι αύξουσα στο $(\sqrt{n}, +\infty)$. $\square$

Κεφάλαιο 3

Το πρώτο θεώρημα του Minkowski

3.1 Το θεώρημα του Minkowski

Η Γεωμετρία των Αριθμών ασχολείται κυρίως με προβλήματα της εξής μορφής: Δίνονται μία συνάρτηση $F : \mathbb{R}^n \to \mathbb{R}$ με $F(0, \dots, 0) = 0$, και ένας θετικός πραγματικός αριθμός λ. Το ζητούμενο είναι να βρεθούν ακέραιοι $a_1, \dots, a_n$, όχι όλοι μηδέν, για τους οποίους

$$(1) \qquad |F(a_1, \dots, a_n)| \leq \lambda.$$

Θεωρούμε την τυχούσα n-άδα $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ σαν σημείο του Ευκλείδειου χώρου $\mathbb{R}^n$, και συμβολίζουμε με K το σύνολο όλων των $x \in \mathbb{R}^n$ που ικανοποιούν την

$$(2) \qquad |F(x)| = |F(x_1, \dots, x_n)| \leq \lambda.$$

Τότε, το αρχικό μας πρόβλημα διατυπώνεται ισοδύναμα ως εξής: Κάτω από ποιές προϋποθέσεις το σύνολο K περιέχει σημείο $u \in \mathbb{Z}^n \backslash \{o\}$; Υπάρχουν δύο σημαντικές ιδέες πίσω από αυτήν τη μετάφραση του προβλήματος. Πρώτον, παίρνουμε υπ' όψιν μας τις τιμές της F σε κάθε $x \in \mathbb{R}^n$, και όχι μόνο τις τιμές της στα $u \in \mathbb{Z}^n$. Κατ' αυτόν τον τρόπο, είναι δυνατό να χρησιμοποιήσουμε αναλυτικές μεθόδους για την αντιμετώπιση του προβλήματος. Δεύτερον, η ερμηνεία που δίνουμε στο πρόβλημα είναι γεωμετρική, κάτι που ευνοεί την εισαγωγή νέων εννοιών και μεθόδων οι οποίες βασίζονται στη γεωμετρική μας διαίσθηση.

Γεωμετρικές μέθοδοι αυτού του τύπου είχαν ήδη χρησιμοποιηθεί από τον Gauss [Ga] και τον Dirichlet [Di], οι οποίοι εργάζονταν σε προβλήματα σχετικά με τις θετικά ορισμένες τετραγωνικές μορφές. Πρώτος όμως ο Minkowski [Mi1] ανέπτυξε μία συστηματική θεωρία, απέδειξε ένα γενικό θεώρημα για n-διάστατα κυρτά σώματα K, και το εφάρμοσε σε μεγάλο πλήθος σημαντικών προβλημάτων. Η νέα θεωρία ονομάστηκε «γεωμετρία των αριθμών» από τον ίδιο το Minkowski.

Το 1850, ο Hermite [Her] απέδειξε ότι, αν F είναι μία θετικά ορισμένη τετραγωνική μορφή n μεταβλητών, τότε η (1) έχει μη τετριμμένη ακέραια λύση αν το λ ξεπερνάει μία τιμή που εξαρτάται μόνο από το n και τη διακρίνουσα της F. Η απόδειξή του ήταν αριθμητικής φύσεως. Ο Minkowski μετέφρασε το αποτέλεσμα του Hermite σαν ένα θεώρημα για ελλειψοειδή, και έδωσε μία νέα γεωμετρική απόδειξή του. Στη συνέχεια παρατήρησε ότι, οι μόνες ιδιότητες του ελλειψοειδούς που απαιτούνταν για την απόδειξη, ήταν η κυρτότητα και η συμμετρία του ως προς το o. Κατέληξε έτσι στο εξής θεώρημα (*πρώτο θεώρημα του Minkowski*):

Θεώρημα 3.1.1 *Έστω K ανοικτό, συμμετρικό ως προς το o, κυρτό σώμα στον $\mathbb{R}^n$. Αν $|K| > 2^n$, τότε το K περιέχει τουλάχιστον ένα $u \in \mathbb{Z}^n\setminus\{o\}$.*

Το αποτέλεσμα αυτό δεν επιδέχεται βελτίωση. Αν θεωρήσουμε τον κύβο $Q = \{x : |x_i| < 1, i = 1, \ldots, n\}$, τότε $|Q| = 2^n$, αλλά $Q \cap \mathbb{Z}^n = \{o\}$.

Το Θεώρημα 3.1.1 γενικεύεται αμέσως για τυχόν πλέγμα Λ στον $\mathbb{R}^n$. Αρκεί να παρατηρήσουμε ότι $\Lambda = T(\mathbb{Z}^n)$ για κάποιον $T \in GL(n)$ με $|\det T| = \det\Lambda$, και να χρησιμοποιήσουμε το Θεώρημα 3.1.1 για το συμμετρικό κυρτό σώμα $T^{-1}(K)$:

Θεώρημα 3.1.2 *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, και K ένα ανοικτό, συμμετρικό ως προς το o, κυρτό σώμα στον $\mathbb{R}^n$. Αν $|K| > 2^n \det\Lambda$, τότε το K περιέχει τουλάχιστον ένα $u \in \Lambda\setminus\{o\}$.* □

Περιγράφουμε πρώτα την αρχική **απόδειξη του Minkowski:** Θεωρούμε ένα κλειστό, συμμετρικό ως προς το o, κυρτό σώμα K. Για κάθε $\lambda > 0$, θεωρούμε το σώμα λK. Αφού το K είναι φραγμένο, για μικρά λ έχουμε $\lambda K \cap \mathbb{Z}^n = \{o\}$, και αφού το K περιέχει μία μπάλα με κέντρο το o, για μεγάλα λ θα έχουμε $\lambda K \cap (\mathbb{Z}^n\setminus\{o\}) \neq \emptyset$.

Αφού $o \in \lambda K$, από την κυρτότητα του K έπεται ότι: αν $0 < \lambda < \lambda'$, τότε $\lambda K \subset \lambda' K$. Παίρνοντας υπ' όψιν και το γεγονός ότι το K είναι κλειστό, συμπεραίνουμε ότι, για κάθε $\lambda > 0$,

$$\lambda K = \bigcap\{\lambda' K : \lambda' > \lambda\}.$$

Ειδικότερα, αν **ορίσουμε**

$$\lambda_1 = \inf\{\lambda > 0 : \lambda K \cap (\mathbb{Z}^n\setminus\{o\} \neq \emptyset\},$$

τότε

$$(*) \qquad \lambda_1 K \cap (\mathbb{Z}^n\setminus\{o\}) \neq \emptyset,$$

υπάρχει δηλαδή ένας ελάχιστος $\lambda_1 > 0$ για τον οποίο το $\lambda_1 K$ περιέχει μη μηδενικό ακέραιο σημείο (το οποίο, βέβαια, θα βρίσκεται στο σύνορό του). Για την απόδειξη της $(*)$, σταθεροποιούμε $\lambda_* > \lambda_1$ και θεωρούμε φθίνουσα ακολουθία $\lambda_* > \mu_n \to \lambda_1$. Το $\lambda_* K$ περιέχει πεπερασμένα το πλήθος μη μηδενικά ακέραια σημεία, και, για κάθε n, κάποιο από αυτά ανήκει στο $\mu_n K$. Υπάρχουν λοιπόν $u \neq o$, $u \in \mathbb{Z}^n$, και υπακολουθία μ_{k_n} τέτοια ώστε $u \in \mu_{k_n} K$ για κάθε n. Τότε,

$$u \in \bigcap_n \mu_{k_n} K = \lambda_1 K.$$

Στη συνέχεια, για κάθε $\lambda > 0$, θεωρούμε τα σύνολα $\lambda K + u$, $u \in \mathbb{Z}^n$. Για μικρά λ, τα σύνολα $\lambda K + u$ είναι ξένα ανά δύο. Με ένα επιχείρημα ανάλογο προς το προηγούμενο, δείχνουμε ότι υπάρχει ελάχιστος $\lambda_0 > 0$ για τον οποίο υπάρχει $u \in \mathbb{Z}^n \setminus \{o\}$ τέτοιο ώστε $\lambda_0 K \cap (\lambda_0 K + u) \neq \emptyset$.

Λήμμα 3.1.1 *Για κάθε κλειστό σώμα K ισχύει η ισότητα $\lambda_1 = 2\lambda_0$.*

Απόδειξη: Έστω $x \in \lambda_0 K \cap (\lambda_0 K + u)$, $u \in \mathbb{Z}^n \setminus \{0\}$. Τότε, λόγω της συμμετρίας του K, έχουμε $u - x \in \lambda_0 K$ και $x \in \lambda_0 K$, άρα $u \in 2\lambda_0 K$. Επομένως,

$$\lambda_1 \leq 2\lambda_0.$$

Από την άλλη πλευρά, αν $u \in \lambda_1 K \cap (\mathbb{Z}^n \setminus \{o\})$, τότε, παρατηρώντας ότι $-u/2 \in (\lambda_1/2)K$ από τη συμμετρία του K, γράφουμε

$$\frac{u}{2} = -\frac{u}{2} + u \in \frac{\lambda_1}{2} K \cap \left(\frac{\lambda_1}{2} K + u \right),$$

επομένως, $\lambda_0 \leq (\lambda_1/2)$. □

Ο Minkowski ολοκλήρωνε το επιχείρημά του ως εξής: Τα $\lambda_0 K + u$, $u \in \mathbb{Z}^n$, έχουν ξένα εσωτερικά. Αυτό έχει σαν συνέπεια την ανισότητα $|\lambda_0 K| \leq 1$ (Λήμμα του Blichfeldt, βλέπε παρακάτω). Σύμφωνα με το Λήμμα, αυτό σημαίνει ότι

$$\lambda_1^n |K| \leq 2^n.$$

Αν υποθέσουμε ότι το K δεν περιέχει μη μηδενικό ακέραιο σημείο, τότε $\lambda_1 > 1$, δηλαδή $|K| < 2^n$. Επομένως, κάθε κλειστό, συμμετρικό ως προς το o κυρτό σώμα K με όγκο $|K| \geq 2^n$, περιέχει μη μηδενικό $u \in \mathbb{Z}^n$.

Για την περίπτωση του ανοικτού K, υποθέτοντας ότι $|K| > 2^n$, βρίσκουμε $\lambda < 1$ τέτοιο ώστε $\lambda^n |K| > 2^n$, οπότε $|\lambda \overline{K}| = \lambda^n |K| > 2^n$. Εφαρμόζοντας το προηγούμενο αποτέλεσμα, βρίσκουμε μη μηδενικό ακέραιο σημείο $u \in \lambda \overline{K} \subset K$. □

Παρατηρήσεις: Το επιχείρημα του Minkowski (ειδικότερα η εισαγωγή των παραμέτρων λ_0, λ_1 και το Λήμμα 3.1.1), είναι σημαντικό για ιστορικούς λόγους. Τον οδήγησε στον ορισμό της **νόρμας που επάγεται από το** K (τον οποίο συναντήσαμε στο Κεφάλαιο 2), και στον ορισμό των **διαδοχικών ελαχίστων** του K (τα οποία θα συναντήσουμε στο Κεφάλαιο 4).

Η απόδειξη δίνει ότι, αν το K υποτεθεί κλειστό, τότε η ανισότητα $|K| \geq 2^n$ είναι αρκετή για να εξασφαλίσουμε μη μηδενικό ακέραιο σημείο στο K.

Δίνουμε τώρα την απόδειξη του Λήμματος του Blichfeldt [Bl1], το οποίο χρησιμοποιήθηκε στο επιχείρημα του Minkowski, και κατόπιν αποδεικνύουμε το πρώτο θεώρημα του Minkowski χωρίς να κάνουμε χρήση των παραμέτρων λ_0 και λ_1:

Θεώρημα 3.1.3 *Έστω M ένα Jordan μετρήσιμο υποσύνολο του $\mathbb{R}^n$, με $|M| > 1$. Υπάρχουν $x \neq y$ στο M τέτοια ώστε $x - y \in \mathbb{Z}^n \setminus \{o\}$.*

Απόδειξη: Η απλή απόδειξη που θα δώσουμε, οφείλεται στον Hajos [Ha]. Υποθέτουμε ότι $|M| > 1$. Αν το M δεν είναι φραγμένο, παρατηρούμε ότι η τομή του M με μπάλα κατάλληλα μεγάλης ακτίνας θα έχει όγκο μεγαλύτερο από 1. Υποθέτουμε λοιπόν, χωρίς περιορισμό της γενικότητας, ότι το M είναι φραγμένο. Θεωρούμε το θεμελιώδες παραλληλεπίπεδο του $\mathbb{Z}^n$

$$P = \{x \in \mathbb{R}^n : 0 \leq x_i < 1, i = 1, \dots, n\}.$$

Το σύνολο των $u \in \mathbb{Z}^n$ για τα οποία $(u + P) \cap M \neq \emptyset$, είναι πεπερασμένο, ας υποθέσουμε ότι είναι το $\{u^1, \dots, u^{r_0}\}$. Για κάθε $r = 1, \dots, r_0$, ορίζουμε $M_r = (u^r + P) \cap M$, και παίρνουμε τη μεταφορά $M'_r = M_r - u^r \subseteq P$. Παρατηρούμε ότι, από το Θεώρημα 1.2.2,

$$\sum_{r=1}^{r_0} |M'_r| = \sum_{r=1}^{r_0} |M_r| = \sum_{r=1}^{r_0} |(u^r + P) \cap M| = \sum_{u \in \mathbb{Z}^n} |(u + P) \cap M| = |M| > 1,$$

άρα τα M'_r πρέπει να επικαλύπτονται. Υπάρχουν δηλαδή $r \neq s \in \{1, \dots, r_0\}$ και $z \in M'_r \cap M'_s$. Τότε, τα $x = z + u^r$ και $y = z + u^s$ ανήκουν στο M, και $x - y = u^r - u^s \in \mathbb{Z}^n \setminus \{o\}$. □

Παρατήρηση Το ίδιο ισχύει αν υποθέσουμε ότι το M είναι φραγμένο, κλειστό, και $|M| \geq 1$. Γιατί αν πάρουμε μία φθίνουσα ακολουθία $\lambda_r \to 1$, έχουμε $|\lambda_r M| > 1$, άρα υπάρχουν $x_r, y_r \in \lambda_r M$ τέτοια ώστε $o \neq x_r - y_r \in \mathbb{Z}^n$. Τότε, οι (x_r), (y_r) έχουν υπακολουθίες $x_{k_r} \to x \in M$, $y_{k_r} \to y \in M$, και εύκολα ελέγχουμε ότι $x - y \in \mathbb{Z}^n \setminus \{o\}$.

Απόδειξη του θεωρήματος 3.1.1: Θεωρούμε το $M = K/2$. Το M είναι Jordan μετρήσιμο και, από την υπόθεσή μας, $|M| > 1$. Από το Λήμμα του Blichfeldt, υπάρχουν $x, y \in M$ τέτοια ώστε $o \neq x - y \in \mathbb{Z}^n$. Όμως, από τον ορισμό του M, υπάρχουν $w_1, w_2 \in K$ με $x = w_1/2$ και $y = w_2/2$. Το K είναι συμμετρικό ως προς το o, άρα $-w_2 \in K$, και κυρτό, άρα

$$x - y = \frac{w_1 + (-w_2)}{2} \in K.$$

Δηλαδή, $o \neq x - y \in K \cap \mathbb{Z}^n$. □

3.2 Άλλες αποδείξεις και γενικεύσεις του θεωρήματος

Δίνουμε τώρα δύο ακόμα αποδείξεις του πρώτου θεωρήματος του Minkowski. Η πρώτη βασίζεται σε μία επέκταση του Λήμματος του Blichfeldt, την οποία απέδειξε ο Mordell [Mor]. Η απόδειξή της χρησιμοποιεί την αρχή του Dirichlet, είναι δηλαδή αριθμητικής φύσεως:

Λήμμα 3.2.1 *Έστω $k \in \mathbb{N}$, και M Jordan μετρήσιμο υποσύνολο του $\mathbb{R}^n$ με $|M| > k$. Τότε, υπάρχει $z \in \mathbb{R}^n$ τέτοιο ώστε το $M + z$ να περιέχει τουλάχιστον $k+1$ διακεκριμένα ακέραια σημεία.*

Απόδειξη: Για κάθε $r \in \mathbb{N}$, θεωρούμε το πλέγμα $(1/r)\mathbb{Z}^n$. Συμβολίζουμε με N_r τον πληθάριθμο του συνόλου $M \cap (1/r)\mathbb{Z}^n$. Από τον ορισμό του Jordan μετρήσιμου συνόλου και τις παρατηρήσεις στην Παράγραφο 2.1(α), έχουμε

$$\lim_{r\to\infty} \frac{|M|}{N_r(1/r)^n} = 1,$$

δηλαδή, για μεγάλα r ισχύει η ανισότητα

$$N_r > r^n k.$$

Παίρνουμε ένα τέτοιο $r \in \mathbb{N}$, και θεωρούμε το σύνολο

$$A_r = \{u \in \mathbb{Z}^n : (1/r)u \in M\}.$$

Το A_r έχει πληθάριθμο $N_r > r^n k$, και τα σημεία του ανήκουν σε r^n το πολύ κλάσεις υπολοίπων mod$r$. Επομένως, μπορούμε να βρούμε $u^1, \ldots, u^{k+1} \in A_r$ τα οποία ανήκουν στην ίδια κλάση mod$r$. Τότε, τα σημεία $\frac{u^1}{r}, \ldots, \frac{u^{k+1}}{r}$ ανήκουν στο M, και τα

$$x_i = \frac{u^i - u^1}{r} \in \mathbb{Z}^n, \quad i = 1, \ldots, k+1.$$

Άρα, αν θέσουμε $z = (1/r)u^1$, το $M + z$ περιέχει $k+1$ ακέραια σημεία. □

Χρησιμοποιώντας το Λήμμα του Mordell, ο van der Corput [vdC] γενίκευσε το πρώτο θεώρημα του Minkowski ως εξής:

Θεώρημα 3.2.1 *Έστω $k \in \mathbb{N}$, και K ένα ανοικτό, συμμετρικό ως προς το o, κυρτό σώμα στον $\mathbb{R}^n$, με όγκο $|K| > 2^n k$. Τότε, το K περιέχει τουλάχιστον k ζευγάρια ακεραίων σημείων $\pm u^i \neq o$.*

Απόδειξη: Το $K/2$ έχει όγκο μεγαλύτερο από k. Από το Λήμμα του Mordell, υπάρχουν $z \in \mathbb{R}^n$ και $v^1, \ldots, v^{k+1}$ διακεκριμένα ακέραια σημεία, τέτοια ώστε

$$z + v^i \in \frac{1}{2}K, \quad i = 1, \ldots, k+1.$$

Μπορούμε να υποθέσουμε ότι τα v^i είναι **διατεταγμένα λεξικογραφικά**. Δηλαδή, αν $i < i'$ τότε $v^i_s < v^{i'}_s$, όπου s είναι ο πρώτος δείκτης για τον οποίο $v^i_s \neq v^{i'}_s$. Τότε, για κάθε $i = 1, \ldots, k$ έχουμε

$$u^i := v^{i+1} - v^1 = (z + v^{i+1}) - (z + v^1) \in \left(\frac{1}{2}K - \frac{1}{2}K\right) \cap (\mathbb{Z}^n \backslash \{o\}) = K \cap (\mathbb{Z}^n \backslash \{o\}),$$

και, τα ζευγάρια $\pm u^i$, $i=1,\ldots,k$, είναι διακεκριμένα, γιατί κάθε u^i έχει θετική την πρώτη μη μηδενική συντεταγμένη του (οπότε, δεν μπορεί να συμβεί $u^i = -u^j$ αν $i \neq j$). □

Ο Siegel [Si] απέδειξε έναν γενικό τύπο από τον οποίο προκύπτει ως πόρισμα το πρώτο θεώρημα του Minkowski. Η απόδειξη αυτού του τύπου χρησιμοποιεί την ταυτότητα του Parseval. Η ιδέα είναι η εξής:

Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$, χ η χαρακτηριστική συνάρτηση του $K/2$, και

$$\phi(x) = \sum_{u\in\mathbb{Z}^n} \chi(u+x).$$

Τότε, η $\phi(x_1,\ldots,x_n)$ είναι περιοδική ως προς κάθε μεταβλητή, με περίοδο 1. Αν $P=\{x : 0\leq x_i < 1, i=1,\ldots,n\}$ είναι το σύνηθες θεμελιώδες παραλληλεπίπεδο του $\mathbb{Z}^n$, ο τύπος του Parseval μάς δίνει

$$\int_P \phi^2(x)dx = \sum_{u\in\mathbb{Z}^n} |\alpha(u)|^2,$$

όπου

$$\begin{aligned}\alpha(u) &= \int_P \phi(x)e^{-2\pi i\langle u,x\rangle}dx\\ &= \sum_{u\in\mathbb{Z}^n}\int_P \chi(u+x)e^{-2\pi i\langle u,x\rangle}dx\\ &= \int_{\mathbb{R}^n}\chi(x)e^{-2\pi i\langle u,x\rangle}dx,\end{aligned}$$

είναι οι συντελεστές Fourier της ϕ.

Θεώρημα 3.2.2 *Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$ που δεν περιέχει μη μηδενικό ακέραιο σημείο, και ϕ, α όπως παραπάνω. Τότε,*

$$2^n = |K| + \frac{4^n}{|K|}\sum_{u\in\mathbb{Z}^n\setminus\{o\}} |\alpha(u)|^2.$$

Απόδειξη: Αφού $K\cap\mathbb{Z}^n=\{o\}$, τα σύνολα $u+\frac{1}{2}K$, $u\in\mathbb{Z}^n$, είναι ξένα, επομένως

$$u\neq u' \Longrightarrow \chi(x+u)\chi(x+u') = 0.$$

Αυτό έχει σαν συνέπεια την $\phi^2=\phi$ στον $\mathbb{R}^n$, άρα

$$\alpha(o) = \int_P \phi(x)dx = \int_P \phi^2(x)dx = |\alpha(o)|^2 + \sum_{u\in\mathbb{Z}^n\setminus\{o\}} |\alpha(u)|^2.$$

Όμως,

$$\alpha(o) = \int_{\mathbb{R}^n}\chi(x)dx = \frac{|K|}{2^n},$$

άρα
$$\frac{|K|}{2^n}=\frac{|K|^2}{4^n}+\sum_{u\in\mathbb{Z}^n\setminus\{o\}}|\alpha(u)|^2,$$
και η απόδειξη ολοκληρώνεται αν πολλαπλασιάσουμε τα δύο μέλη της τελευταίας ισότητας με $4^n/|K|$. $\square$

Πόρισμα 3.2.1 *Έστω K ανοικτό συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Αν $K\cap\mathbb{Z}^n=\{o\}$, τότε $|K|\leq 2^n$.* $\square$

Έστω K κλειστό κυρτό σώμα στον $\mathbb{R}^n$, το οποίο περιέχει το o στο εσωτερικό του. Ο **συντελεστής ασυμμετρίας** του K ως προς το o, είναι ο μικρότερος $\sigma=\sigma(K)>0$ για τον οποίο
$$x\in K\Longrightarrow -x\in\sigma K.$$
Παρατηρήστε ότι, $\sigma(K)\geq 1$ για κάθε K, με ισότητα αν και μόνο αν το K είναι συμμετρικό ως προς το o. Ο Mahler [Mah1] παρατήρησε ότι η απόδειξη του θεωρήματος του Minkowski για τη συμμετρική περίπτωση, ουσιαστικά χρησιμοποιεί το γεγονός ότι $\sigma=1$, και απέδειξε την εξής γενίκευσή του:

Θεώρημα 3.2.3 *Έστω K κυρτό σώμα στον $\mathbb{R}^n$, που περιέχει το o στο εσωτερικό του. Αν $|K|>(1+\sigma(K))^n$, τότε $K\cap(\mathbb{Z}^n\setminus\{o\})\neq\emptyset$.*

Απόδειξη: Θεωρούμε το σώμα $K_1=(1+\sigma)^{-1}K$. Τότε, $|K_1|>1$, άρα υπάρχουν $x,y\in K_1$ τέτοια ώστε $y-x\in\mathbb{Z}^n\setminus\{o\}$. Τα K και K_1 είναι ομοιοθετικά, άρα έχουν τον ίδιο συντελεστή ασυμμετρίας, και αφού $x\in K_1$ συμπεραίνουμε ότι $-\sigma^{-1}x\in K_1$. Τότε, χρησιμοποιώντας την κυρτότητα του K_1, βλέπουμε ότι
$$y-x=(1+\sigma)\left(\frac{1}{1+\sigma}y+\frac{\sigma}{1+\sigma}(-\sigma^{-1}x)\right)\in(1+\sigma)K_1=K.$$
Δηλαδή, $y-x\in K\cap(\mathbb{Z}^n\setminus\{o\})$. $\square$

3.3 Εφαρμογές στη θεωρία των αριθμών

(α) Ομογενείς γραμμικές μορφές

Η πιό γνωστή εφαρμογή του Θεωρήματος του Minkowski αφορά συστήματα ομογενών γραμμικών μορφών:

Θεώρημα 3.3.1 *Έστω $\xi_i(x_1,\ldots,x_n)=a_{i1}x_1+\ldots+a_{in}x_n$, $i=1,\ldots,n$, ομογενείς γραμμικές μορφές, με πραγματικούς συντελεστές a_{ij}, και μη μηδενική ορίζουσα Δ. Αν $t_1,\ldots,t_n>0$ και $t_1t_2\ldots t_n=|\Delta|$, τότε υπάρχει $(x_1,\ldots,x_n)\in\mathbb{Z}^n\setminus\{o\}$ τέτοιο ώστε*
$$|\xi_i(x_1,\ldots,x_n)|\leq t_i,\quad i=1,\ldots,n.$$

Απόδειξη: Θεωρούμε το παραλληλεπίπεδο

$$P = \{x : |\xi_i(x_1, \ldots, x_n)| \leq t_i, i = 1, \ldots, n\}.$$

Αν T είναι ο γραμμικός μετασχηματισμός που ορίζεται από τον πίνακα (a_{ij}), τότε $P = T^{-1}(P_1)$, όπου

$$P_1 = \{x : |x_i| \leq t_i, i = 1, \ldots, n\}.$$

Άρα,

$$|P| = |T^{-1}(P_1)| = \frac{|P_1|}{|\Delta|} = 2^n \frac{t_1 t_2 \ldots t_n}{|\Delta|} = 2^n.$$

Από το Θεώρημα του Minkowski, υπάρχει $x \in P \cap (\mathbb{Z}^n \backslash \{o\})$. □

Εφαρμογή *Έστω $a_1, \ldots, a_n \in \mathbb{R}$. Υπάρχουν ακέραιοι $u_1, \ldots, u_{n+1}$ τέτοιοι ώστε*

$$|u_{n+1} a_i - u_i| \leq \frac{1}{u_{n+1}^{1/n}}, \quad i = 1, \ldots, n.$$

Απόδειξη: Θέτουμε $\xi_{n+1}(x_1, \ldots, x_{n+1}) = x_{n+1}$, και

$$\xi_i(x_1, \ldots, x_{n+1}) = x_{n+1} a_i - x_i, \quad i = 1, \ldots, n.$$

Τότε $|\Delta| = 1$, άρα για κάθε $t > 1$ υπάρχει $(u_1, \ldots, u_{n+1}) \in \mathbb{Z}^n \backslash \{o\}$ με την ιδιότητα

$$|u_{n+1}| \leq t, \quad |u_{n+1} a_i - u_i| \leq t^{-1/n}.$$

Το u_{n+1} δεν μπορεί να είναι ίσο με μηδέν, γιατί τότε όλοι οι u_i, $i \leq n$ θα ήταν απολύτως μικρότεροι του 1, δηλαδή ίσοι με μηδέν. Επίσης, αντικαθιστώντας, αν χρειαστεί, όλους τους u_i με τους αντίθετούς τους, μπορούμε να υποθέσουμε ότι $u_{n+1} > 0$. Έπεται ότι

$$|u_{n+1} a_i - u_i| \leq \frac{1}{t^{1/n}} \leq \frac{1}{u_{n+1}^{1/n}}, \quad i = 1, \ldots, n. \quad \square$$

(β) Τετραγωνικές μορφές

Στη συνέχεια, εφαρμόζουμε το Θεώρημα του Minkowski σε μία θετικά ορισμένη τετραγωνική μορφή:

Θεώρημα 3.3.2 *Έστω $A = (a_{ij})$ συμμετρικός, θετικά ορισμένος $n \times n$ πίνακας. Θεωρούμε την τετραγωνική μορφή*

$$T(x_1, \ldots, x_n) = T(x) = \langle Ax, x \rangle.$$

Αν $D = \det(a_{ij})$ είναι η διακρίνουσα της T, μπορούμε να βρούμε $(u_1, \ldots, u_n) \in \mathbb{Z}^n \backslash \{o\}$ τέτοιο ώστε

$$T(u_1, \ldots, u_n) \leq \frac{4}{\pi} \left(\Gamma(\frac{n}{2} + 1)^2 D \right)^{1/n}.$$

Απόδειξη: Υπάρχει συμμετρικός, θετικά ορισμένος B τέτοιος ώστε $B^2 = A$. Ορίζουμε

$$K_r = \{x \in \mathbb{R}^n : T(x) \leq r\},$$

όπου $r > 0$. Έχουμε $T(x) \leq r$ αν και μόνο αν $\|Bx\|_2^2 \leq r$. Δηλαδή, $K_r = \sqrt{r}B^{-1}(D_n)$. Επομένως,

$$|K_r| = \frac{r^{n/2}}{\det(B)}\omega_n = \frac{r^{n/2}}{\sqrt{D}} \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}.$$

Επιλέγουμε $r_0 > 0$ έτσι ώστε να έχουμε $|K_{r_0}| = 2^n$. Τότε, από το Θεώρημα του Minkowski, μπορούμε να βρούμε $(u_1, \ldots, u_n) \in K_{r_0} \cap (\mathbb{Z}^n \backslash \{o\})$, δηλαδή,

$$T(u_1, \ldots, u_n) \leq r_0 = \frac{4}{\pi}\left(\Gamma(\frac{n}{2}+1)^2 D\right)^{1/n}. \quad \square$$

(γ) Γινόμενο γραμμικών μορφών

Έστω $\xi_i(x_1, \ldots, x_n) = a_{i1}x_1 + \ldots + a_{in}x_n$, $i = 1, \ldots, n$, ομογενείς γραμμικές μορφές, με πραγματικούς συντελεστές a_{ij}, και μη μηδενική ορίζουσα Δ. Παίρνοντας $t_1 = \ldots = t_n = |\Delta|^{1/n}$ στο Θεώρημα 3.3.1, βλέπουμε ότι υπάρχει $(x_1, \ldots, x_n) \in \mathbb{Z}^n \backslash \{o\}$ τέτοιο ώστε

$$\prod_{i=1}^{n} |\xi_i(x_1, \ldots, x_n)| \leq |\Delta|.$$

Μπορούμε να δώσουμε ένα καλύτερο άνω φράγμα για το γινόμενο των ξ_i:

Θεώρημα 3.3.3 *Αν ξ_i και Δ όπως παραπάνω, υπάρχει $(x_1, \ldots, x_n) \in \mathbb{Z}^n \backslash \{o\}$ τέτοιο ώστε*

$$\prod_{i=1}^{n} |\xi_i(x_1, \ldots, x_n)| \leq \frac{n!}{n^n}|\Delta|.$$

Απόδειξη: Το χωρίο $\{x : \prod_{i=1}^{n} |\xi_i| \leq r\}$, $r > 0$, δεν είναι κυρτό, περιέχει όμως το

$$K_r = \{x \in \mathbb{R}^n : \sum_{i=1}^{n} |\xi_i(x)| \leq nr^{1/n}\},$$

γιατί, από την ανισότητα αριθμητικού - γεωμετρικού μέσου, για κάθε $x_1, \ldots, x_n \in \mathbb{R}$,

$$\prod_{i=1}^{n} |\xi_i(x)| \leq \left(\frac{1}{n}\sum_{i=1}^{n} |\xi_i(x)|\right)^n.$$

Αν T είναι ο γραμμικός μετασχηματισμός που ορίζεται από τις ξ_i, τότε $K_r = T^{-1}(K_r^1)$, όπου

$$K_r^1 = \{x : \sum_{i=1}^{n} |x_i| \leq nr^{1/n}\}.$$

Άρα,

$$|K_r| = \frac{|K_r^1|}{|\mathrm{det}T|} = \frac{2^n n^n r}{n!|\Delta|}.$$

Αυτός θα είναι ίσος με 2^n αν $r = r_0 = n!|\Delta|/n^n$, και τότε, το Θεώρημα του Minkowski μάς εξασφαλίζει $x \in K_{r_0} \cap (\mathbb{Z}^n \backslash \{o\})$, δηλαδή, $x \in \mathbb{Z}^n \backslash \{o\}$ για το οποίο

$$\prod_{i=1}^{n} |\xi_i(x)| \leq \left(\frac{1}{n} \sum_{i=1}^{n} |\xi_i(x)| \right)^n \leq r_0 = \frac{n!}{n^n}|\Delta|. \quad \square$$

(δ) Το Θεώρημα του Lagrange

Χρησιμοποιώντας το Θεώρημα του Minkowski, θα αποδείξουμε το εξής Θεώρημα του Lagrange:

Θεώρημα 3.3.4 *Κάθε φυσικός αριθμός n γράφεται στη μορφή $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, όπου $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.*

Για την απόδειξη θα χρειαστούμε ένα λήμμα:

Λήμμα 3.3.1 *Έστω $c_1, \ldots, c_m \in \mathbb{Z}^n$, και $\kappa_1, \ldots, \kappa_m \in \mathbb{N}$. Ορίζουμε*

$$\Lambda = \{x \in \mathbb{Z}^n : \langle x, c_i \rangle \equiv 0 (\mathrm{mod} \kappa_i), i = 1, \ldots, m\}.$$

Τότε, το Λ είναι πλέγμα, και $\mathrm{det}\Lambda \leq \kappa_1 \ldots \kappa_m$.

Απόδειξη: Εύκολα ελέγχουμε ότι το Λ είναι προσθετική υποομάδα του $\mathbb{Z}^n$, άρα είναι και διακριτή υποομάδα του $\mathbb{R}^n$. Αν θέσουμε $\kappa = \kappa_1 \ldots \kappa_m$, τότε το πλέγμα

$$\kappa \mathbb{Z}^n = \{\kappa x : x \in \mathbb{Z}^n\}$$

περιέχεται στο Λ, και αυτό δείχνει ότι το Λ περιέχει n γραμμικώς ανεξάρτητα διανύσματα: για παράδειγμα, τα κe_i, $i = 1, \ldots, n$. Άρα, το Λ είναι υποπλέγμα του $\mathbb{Z}^n$.

Επίσης, $\mathrm{det}\Lambda = |\mathbb{Z}^n : \Lambda|$, άρα, για να δώσουμε φράγμα για την $\mathrm{det}\Lambda$, αρκεί να περιγράψουμε τα σύμπλοκα του $\mathbb{Z}^n$ ως προς το Λ. Θεωρούμε το σύνολο

$$A = \{a = (a_1, \ldots, a_n) \in \mathbb{Z}^m, 0 \leq a_i < \kappa_i\}.$$

Το A έχει πληθάριθμο $\kappa_1 \ldots \kappa_m$. Για κάθε $a \in A$, σταθεροποιούμε $x_a \in \mathbb{Z}^n$ (αν υπάρχει), τέτοιο ώστε

$$\langle x_a, c_i \rangle \equiv a_i (\mathrm{mod} \kappa_i), i = 1, \ldots, m.$$

Τότε,

$$\mathbb{Z}^n = \bigcup (x_a + \Lambda),$$

επομένως, $|\mathbb{Z}^n : \Lambda| \leq |A| = \kappa_1 \dots \kappa_m$. □

Απόδειξη του Θεωρήματος: Εξετάζουμε πρώτα την περίπτωση που ο n είναι ελεύθερος τετραγώνων, δηλαδή, $n = p_1 \dots p_m$, όπου p_k διακεκριμένοι πρώτοι.

Ισχυρισμός: Αν p πρώτος, υπάρχουν $a_p, b_p \in \mathbb{Z}$ τέτοιοι ώστε $a_p^2 + b_p^2 + 1 \equiv 0 (\mathrm{mod} p)$.

Απόδειξη: Αν $p = 2$, παίρνουμε $a_2 = 1$ και $b_2 = 0$. Αν ο p είναι περιττός πρώτος, ελέγχουμε ότι οι a^2, $0 \leq a < p/2$ είναι ανισοϋπόλοιποι mod$p$, και το ίδιο ισχύει για τους $-1 - b^2$, $0 \leq b < p/2$. Αφού το πλήθος των a και b είναι $p + 1$, υπάρχουν δύο από αυτούς που ανήκουν στην ίδια κλάση mod$p$. Αυτό σημαίνει υποχρεωτικά ότι υπάρχουν $0 \leq a_p, b_p < p/2$ με την ιδιότητα

$$a_p^2 \equiv -1 - b_p^2 (\mathrm{mod} p),$$

δηλαδή, $a_p^2 + b_p^2 + 1 \equiv 0 (\mathrm{mod} p)$. □

Ορίζουμε

$$\Lambda = \{x \in \mathbb{Z}^4 : x_1 \equiv a_{p_i} x_3 + b_{p_i} x_4 (\mathrm{mod} p_i),\ x_2 \equiv b_{p_i} x_3 - a_{p_i} x_4 (\mathrm{mod} p_i),\ i \leq m\}.$$

Σύμφωνα με το Λήμμα 3.3.1, το Λ είναι πλέγμα, και

$$\det\Lambda \leq (p_1 \dots p_m)^2 = n^2.$$

Θεωρούμε τη μπάλα $B = \{x : x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n\}$. Ο όγκος της είναι ίσος με

$$|B| = 2n^2\pi^2 > 16n^2 \geq 2^4 \det\Lambda.$$

Από το Θεώρημα του Minkowski, υπάρχει $(x_1, x_2, x_3, x_4) \in \Lambda$ τέτοιο ώστε

$$(*) \qquad 0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n.$$

Όμως,

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &\equiv (a_{p_i} x_3 + b_{p_i} x_4)^2 + (b_{p_i} x_3 - a_{p_i} x_4)^2 + x_3^2 + x_4^2 \ (\mathrm{mod} p_i) \\ &\equiv (a_{p_i}^2 + b_{p_i}^2 + 1) x_3^2 + (a_{p_i}^2 + b_{p_i}^2 + 1) x_4^2 \ (\mathrm{mod} p_i) \\ &\equiv 0 (\mathrm{mod} p_i) \end{aligned}$$

για κάθε $i = 1, \dots, m$, άρα $n | x_1^2 + x_2^2 + x_3^2 + x_4^2$. Από την $(*)$ συμπεραίνουμε ότι $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Στη γενική περίπτωση, γράφουμε τον φυσικό αριθμό n στη μορφή $n = l^2 m$ όπου ο m είναι ελεύθερος τετραγώνων, και εφαρμόζουμε το προηγούμενο για να γράψουμε τον m στη μορφή $m = y_1^2 + y_2^2 + y_3^2 + y_4^2$, $y_i \in \mathbb{Z}$. Τότε,

$$n = (ly_1)^2 + (ly_2)^2 + (ly_3)^2 + (ly_4)^2. \quad \square$$

(ε) Το Θεώρημα προσέγγισης του Dirichlet

Θα εφαρμόσουμε το Θεώρημα του Minkowski στο πρόβλημα της προσέγγισης πραγματικών αριθμών από ρητούς (θεώρημα του Dirichlet):

Θεώρημα 3.3.5 *Υπάρχει σταθερά $c > 0$ με την ιδιότητα: για κάθε $a \in \mathbb{R}$, υπάρχουν $q \in \mathbb{N}$ οσοδήποτε μεγάλος, και $p \in \mathbb{Z}$, τέτοιοι ώστε*

$$|a - \frac{p}{q}| \leq \frac{c}{q^2}.$$

Απόδειξη: Χρησιμοποιούμε την ίδια ιδέα με αυτήν της Εφαρμογής 3.3.1. Μπορούμε να υποθέσουμε ότι ο a είναι άρρητος (αν ο a είναι ρητός, τότε το πρόβλημα δεν έχει καμμία δυσκολία). Έστω $M > 0$. Αφού $a \notin \mathbb{Q}$, υπάρχει $Q > 1$ τέτοιος ώστε

$$t_M := \min\{|aq - p| : q \leq M, q \in \mathbb{N}, p \in \mathbb{Z}\} > \frac{1}{Q}.$$

Ορίζουμε

$$K = \big\{(x,y) \in \mathbb{R}^2 : |ax - y| \leq \frac{1}{Q}, |x| \leq Q\big\}.$$

Το K είναι παραλληλόγραμμο, με εμβαδόν $|K| = (2Q)(2/Q) = 4$. Από το Θεώρημα του Minkowski, υπάρχει $(q,p) \in K \cap (\mathbb{Z}^2 \backslash \{o\})$. Έχουμε $q \neq 0$, γιατί αλλιώς θα είχαμε $|p| \leq 1/Q$, δηλαδή $p = 0$. Επίσης, λόγω της συμμετρίας του K, μπορούμε να υποθέσουμε ότι $q > 0$ (δηλαδή, $q \in \mathbb{N}$). Αυτό σημαίνει ότι $0 < q \leq Q$ και $|aq - p| \leq 1/Q$, άρα

$$|a - \frac{p}{q}| \leq \frac{1}{qQ} \leq \frac{1}{q^2}.$$

Τέλος, από τον ορισμό του t_M, έχουμε

$$|aq - p| \leq \frac{1}{Q} < t_M,$$

άρα, $q > M$. □

Το Θεώρημα 3.3.5 γενικεύεται ως εξής:

Θεώρημα 3.3.6 *Υπάρχει σταθερά $c > 0$ με την ιδιότητα: αν $a_1, \ldots, a_n \in \mathbb{R}$, υπάρχουν $q \in \mathbb{N}$ οσοδήποτε μεγάλος, και $p_1, \ldots, p_n \in \mathbb{Z}$, τέτοιοι ώστε*

$$|a_i - \frac{p_i}{q}| \leq \frac{c}{q^{1+\frac{1}{n}}}.$$

Απόδειξη: Έστω $M > 0$. Η απόδειξη είναι εντελώς ανάλογη με αυτήν του Θεωρήματος 3.3.5: μπορούμε να υποθέσουμε ότι οι $a_1, \ldots, a_n$ δεν είναι όλοι ρητοί. Το παραλληλεπίπεδο στο οποίο εφαρμόζουμε το Θεώρημα του Minkowski, είναι το

$$K = \{(x, y_1, \ldots, y_n) \in \mathbb{R}^{n+1} : |a_i x - y_i| \leq \frac{1}{Q^{1/n}}, |x| \leq Q\},$$

όπου $Q > 1$ τόσο μεγάλος ώστε

$$t_M := \min\{\max_{i \leq n}\{|a_i q - p_i| : q \leq M, q \in \mathbb{N}, p_i \in \mathbb{Z}\}\} > \frac{1}{Q}. \quad \square$$

Κεφάλαιο 4

Το δεύτερο θεώρημα του Minkowski

4.1 Διαδοχικά ελάχιστα συμμετρικού κυρτού σώματος

Στο Κεφάλαιο αυτό θεωρούμε ένα ανοικτό, συμμετρικό ως προς το o κυρτό σώμα K στον $\mathbb{R}^n$. O Minkowski όρισε τα *διαδοχικά ελάχιστα* του K ως εξής: Για κάθε $\lambda > 0$ θεωρούμε το σώμα λK. Το K είναι φραγμένο, αν λοιπόν το λ είναι αρκετά μικρό, τότε $\lambda K \cap \mathbb{Z}^n = \{o\}$. Από την άλλη πλευρά, το K περιέχει μία μπάλα με κέντρο το o. Αν λοιπόν το λ είναι αρκετά μεγάλο, τότε το λK περιέχει n γραμμικώς ανεξάρτητα διανύσματα του $\mathbb{Z}^n$. Επομένως, για κάθε $i = 1, \ldots, n$, υπάρχουν $\lambda > 0$ τέτοια ώστε το λK να περιέχει τουλάχιστον i γραμμικώς ανεξάρτητα διανύσματα του $\mathbb{Z}^n$. Ορίζουμε

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^n) \geq i\}, \quad i = 1, \ldots, n,$$

όπου $\dim(\lambda K \cap \mathbb{Z}^n)$ είναι η διάσταση του υποχώρου που παράγεται από τα ακέραια σημεία του λK.

Λήμμα 4.1.1 *Ισχύει*

$$A_i := \{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^n) \geq i\} = (\lambda_i, \infty).$$

Απόδειξη: Είναι φανερό ότι αν $\lambda \in A_i$ και $\mu > \lambda$, τότε $\mu \in A_i$. Άρα, το A_i είναι διάστημα. Μένει λοιπόν να δούμε ότι $\lambda_i \notin A_i$. Αν το $\lambda_i K$ περιείχε i γραμμικώς ανεξάρτητα ακέραια σημεία, τότε το ίδιο θα ίσχυε και για κάποιο λK με το λ λίγο μικρότερο από το λ_i, γιατί το K έχει υποτεθεί ανοικτό. $\square$

Οι αριθμοί λ_i ονομάζονται **διαδοχικά ελάχιστα** του K (ως προς το πλέγμα $\mathbb{Z}^n$). Είναι φανερό ότι

$$0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n.$$

Μπορεί να συμβεί κάποια από τα λ_i να είναι ίσα. Για παράδειγμα, αν $K = \{x : |x_i| < 1\}$, τότε $\lambda_1 = \ldots = \lambda_n = 1$.

Πρόταση 4.1.1 *Έστω K ανοικτό, συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Υπάρχουν γραμμικώς ανεξάρτητα διανύσματα $u_1, \ldots, u_n \in \mathbb{Z}^n$ που ικανοποιούν τα εξής:*

(α) $u_i \notin \langle u_1, \ldots, u_{i-1} \rangle$, $i = 1, \ldots, n$.

(β) $u_i \notin \lambda_i K$, $i = 1, \ldots, n$.

(γ) $u_i \in \lambda_i \overline{K}$, $i = 1, \ldots, n$.

Απόδειξη: Ορίζουμε επαγωγικά $u_1, \ldots, u_n \in \mathbb{Z}^n$ που ικανοποιούν τα (α)-(γ): Υποθέτουμε ότι έχουν οριστεί τα $u_1, \ldots, u_j$, και ότι $\lambda_j < \lambda_{j+1}$ (θέτουμε $\lambda_0 = 0$ και $u_0 = o$). Τότε $u_1, \ldots, u_j \in \lambda_{j+1} K$, και το Λήμμα 4.1.1 μάς εξασφαλίζει ότι

$$\dim(\lambda_{j+1} K \cap \mathbb{Z}^n) = j.$$

Δείχνουμε πρώτα ότι το $\lambda_{j+1}\overline{K}$ περιέχει τουλάχιστον $j+1$ γραμμικώς ανεξάρτητα ακέραια σημεία: Θεωρούμε $\lambda' > \lambda_{j+1}$. Το $\lambda' K$ περιέχει πεπερασμένα το πλήθος ακέραια σημεία. Έστω B' το σύνολο των ακεραίων σημείων του $\lambda' K$ που δεν ανήκουν στο $\lambda_{j+1} K$. Το B' είναι μη κενό, γιατί $\lambda' > \lambda_{j+1}$. Όλα τα $u \in B'$ που δεν ανήκουν στο $\lambda_{j+1}\overline{K}$ έχουν θετική απόσταση από το $\lambda_{j+1}\overline{K}$, και είναι πεπερασμένα το πλήθος, άρα μπορούμε να βρούμε $\lambda \in (\lambda_{j+1}, \lambda')$ με την ιδιότητα $\lambda K \cap \mathbb{Z}^n = \lambda_{j+1}\overline{K} \cap \mathbb{Z}^n$. Όμως $\lambda > \lambda_{j+1}$, άρα $\dim(\lambda K \cap \mathbb{Z}^n) \geq j + 1$. Έπεται ότι

$$\dim(\lambda_{j+1}\overline{K} \cap \mathbb{Z}^n) = k > j.$$

Υπάρχουν λοιπόν γραμμικώς ανεξάρτητα $u_{j+1}, \ldots, u_k$ στο σύνορο του $\lambda_{j+1} K$, τα οποία δεν ανήκουν στον υπόχωρο $\langle \lambda_{j+1} K \cap \mathbb{Z}^n \rangle$. Τα $u_1, \ldots, u_k$ ικανοποιούν τα (α)-(γ), και από την κατασκευή,

$$\lambda_{j+1} = \ldots = \lambda_k.$$

Συνεχίζουμε με τον ίδιο τρόπο, ορίζοντας τα u_i κατά ομάδες. $\square$

Παρατήρηση Τα λ_i ορίζονται μονοσήμαντα από το K, ενώ το $\{u_1, \ldots, u_n\}$ μπορεί να μην επιλέγεται κατά μοναδικό τρόπο. Τα διανύσματα u_i της Πρότασης 4.1.1 ονομάζονται **ελαχιστικά διανύσματα** του K (ως προς το πλέγμα $\mathbb{Z}^n$).

Σύμφωνα με το πρώτο θεώρημα του Minkowski, αφού $\lambda_1 K \cap \mathbb{Z}^n = \{o\}$, το $\lambda_1 K$ πρέπει να έχει όγκο το πολύ ίσο με 2^n:

Θεώρημα 4.1.1 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε, $\lambda_1^n |K| \leq 2^n$.* $\square$

Παίρνοντας υπ' όψιν του όλα τα διαδοχικά ελάχιστα $\lambda_1, \ldots, \lambda_n$ του K, ο Minkowski [Mi2] απέδειξε κάτι ισχυρότερο (το *δεύτερο θεώρημα του Minkowski*):

Θεώρημα 4.1.2 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε,*

$$\lambda_1\lambda_2 \ldots \lambda_n|K| \leq 2^n. \quad \Box$$

Άμεση γενίκευση του Θεωρήματος 4.1.2 για τυχόν πλέγμα Λ στον $\mathbb{R}^n$ είναι το εξής:

Θεώρημα 4.1.3 *Έστω Λ πλέγμα στον $\mathbb{R}^n$, και K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε,*

$$\lambda_1\lambda_2 \ldots \lambda_n|K| \leq 2^n \det \Lambda,$$

όπου

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda K \cap \Lambda) \geq i\}, \quad i = 1, \ldots, n. \quad \Box$$

Στις επόμενες δύο παραγράφους θα δούμε δύο αρκετά διαφορετικές αποδείξεις του Θεωρήματος 4.1.2.

4.2 Πρώτη απόδειξη του θεωρήματος

Η ιδέα της πρώτης απόδειξης θα γίνει πιό καθαρή από την εξής (λανθασμένη) απόπειρα: Δίνεται το ανοικτό συμμετρικό κυρτό σώμα K στον $\mathbb{R}^n$, υποθέτουμε ότι $u_1, \ldots, u_n$ είναι μία επιλογή ελαχιστικών διανυσμάτων του, και ότι

$$\lambda_1\lambda_2 \ldots \lambda_n|K| > 2^n.$$

Θεωρούμε τον γραμμικό μετασχηματισμό T που ορίζεται από τις $T(u_i) = \lambda_i u_i$, $i = 1, \ldots, n$. Τότε, το $W = T(K)$ έχει όγκο $|W| = \lambda_1 \ldots \lambda_n|K| > 2^n$, οπότε το πρώτο θεώρημα του Minkowski μάς δίνει $a_1, \ldots, a_n \in \mathbb{R}$ τέτοια ώστε

$$o \neq w = a_1\lambda_1 u_1 + \ldots + a_n\lambda_n u_n \in W \cap \mathbb{Z}^n.$$

Αφού $w \neq o$, υπάρχει $k \leq n$ με την ιδιότητα

$$a_k \neq 0, \quad a_{k+1} = \ldots = a_n = 0.$$

Γράφουμε το w στην εξής μορφή:

$$(*) \ w = \lambda_1(a_1u_1 + \ldots + a_ku_k) + (\lambda_2 - \lambda_1)(a_2u_2 + \ldots + a_ku_k) + \ldots + (\lambda_k - \lambda_{k-1})a_ku_k.$$

Αφού $w = T(a_1u_1 + \ldots + a_ku_k)$, γνωρίζουμε ότι $a_1u_1 + \ldots + a_ku_k \in K$. Ας υποθέσουμε πρός στιγμήν ότι τα διανύσματα $a_2u_2 + \ldots + a_ku_k, \ldots, a_ku_k$ είναι όλα μέσα στο K. Τότε, από την κυρτότητα του K και την $(*)$, συμπεραίνουμε ότι

$$w \in \lambda_1 K + (\lambda_2 - \lambda_1)K + \ldots + (\lambda_k - \lambda_{k-1})K = \lambda_k K.$$

Αυτό όμως είναι άτοπο. Θα είχαμε

$$w \in \lambda_k K \backslash \langle u_1, \ldots, u_{k-1} \rangle,$$

δηλαδή το w θα ήταν ακέραιο σημείο του $\lambda_k K$ γραμμικώς ανεξάρτητο προς τα $u_1, \ldots, u_{k-1}$, κάτι που αντιφάσκει προς τον ορισμό του λ_k και των u_i.

Ο Minkowski χρησιμοποίησε αυτήν ακριβώς την ιδέα του «μετασχηματισμού» του σώματος K:

Απόδειξη του Θεωρήματος 4.1.2: Όπως και πριν, θεωρούμε κάποια ελαχιστικά διανύσματα $u_1, \ldots, u_n$ του K, και γράφουμε το τυχόν στοιχείο του K στη μορφή $a = a_1 u_1 + \ldots + a_n u_n$.

Για κάθε $a = a_1 u_1 + \ldots + a_n u_n \in \mathbb{R}^n$ και $k = 1, \ldots, n-1$, ορίζουμε

$$L(a_{k+1}, \ldots, a_n) = \{x = \sum_{i=1}^{n} x_i u_i \in \mathbb{R}^n : x_{k+1} = a_{k+1}, \ldots, x_n = a_n\},$$

τον συσχετισμένο υπόχωρο των σημείων που συμπίπτουν με το a στις συντεταγμένες $x_{k+1}, \ldots, x_n$ (ως προς τη βάση $\{u_1, \ldots, u_n\}$). Για $a \in K$ ορίζουμε $b(a_{k+1}, \ldots, a_n)$ το κέντρο βάρους του $K \cap L(a_{k+1}, \ldots, a_n)$. [Προφανώς, $b(a_1, \ldots, a_n) = a$.] Δηλαδή, η i συντεταγμένη ($i \leq k$) του $b(a_{k+1}, \ldots, a_n)$ δίνεται από το

$$c_i(a_{k+1}, \ldots, a_n) := \int_{K \cap L(a_{k+1}, \ldots, a_n)} x_i dx_k \ldots dx_1.$$

Το $b(a_{k+1}, \ldots, a_n)$ ανήκει στο $K \cap L(a_{k+1}, \ldots, a_n)$, και όλες οι απεικονίσεις $a \mapsto b(a_{k+1}, \ldots, a_n)$ είναι παραγωγίσιμες ως προς a_i στο K.

Λήμμα 4.2.1 *Ο μετασχηματισμός $T : K \to K$ που ορίζεται από την*

$$a = (a_1, \ldots, a_n) \mapsto \lambda_1 b(a_1, \ldots, a_n) + (\lambda_2 - \lambda_1) b(a_2, \ldots, a_n) + \ldots + (\lambda_n - \lambda_{n-1}) b(a_n)$$

είναι ένα προς ένα.

Απόδειξη: Το $b(a_{k+1}, \ldots, a_n)$ γράφεται στη μορφή

$$b(a_{k+1}, \ldots, a_n) = \sum_{j=1}^{k} c_j(a_{k+1}, \ldots, a_n) u_j + \sum_{j=k+1}^{n} a_j u_j,$$

όπου c_j συναρτήσεις που εξαρτώνται μόνο από τα $a_{k+1}, \ldots, a_n$, $j = 1, \ldots, k$.

Έστω $a = \sum_{k=1}^{n} a_k u_k \in K$. Τότε, $T(a) = \sum_{k=1}^{n} d_k u_k$, όπου

$$(*) \quad d_k = \lambda_k a_k + \sum_{j=k}^{n-1} (\lambda_{j+1} - \lambda_j) c_j(a_{k+1}, \ldots, a_n) = \lambda_k a_k + h(a_{k+1}, \ldots, a_n).$$

Για να δείξουμε ότι ο T είναι ένα προς ένα, αρκεί να ελέγξουμε ότι οι συντεταγμένες d_k προσδιορίζουν μονοσήμαντα τις συντεταγμένες a_k. Για $k = n$, η $(*)$ δίνει $d_n = \lambda_n a_n$, άρα $a_n = d_n/\lambda_n$. Τότε,

$$d_{n-1} = \lambda_{n-1}a_{n-1} + h(d_n/\lambda_n),$$

απ' όπου προσδιορίζεται το a_{n-1}, και πηγαίνοντας προς τα πίσω προσδιορίζουμε μονοσήμαντα τα $a_{n-2}, \ldots, a_1$ για τα οποία $T(a) = \sum_{k=1}^n d_k u_k$. □

Λήμμα 4.2.2 *Ο μετασχηματισμός T «πολλαπλασιάζει» τον όγκο του K με τον παράγοντα $\lambda_1 \ldots \lambda_n$:*

$$|T(K)| = \lambda_1 \ldots \lambda_n |K|.$$

Απόδειξη: Αφού ο T είναι ένα προς ένα και διαφορίσιμος, αρκεί να παρατηρήσουμε ότι η ορίζουσα της Ιακωβιανής του T είναι σταθερή και ίση με $\lambda_1 \ldots \lambda_n$ στο K. Αυτό είναι συνέπεια του ορισμού του T. Η Ιακωβιανή του T είναι άνω τριγωνικός πίνακας (το d_k εξαρτάται μόνο από τα $a_k, \ldots, a_n$), και

$$\frac{\partial d_k(a_k, \ldots, a_n)}{\partial a_k} = \lambda_k, \quad k = 1, \ldots, n,$$

από την $(*)$. □

Ας υποθέσουμε τώρα ότι $\lambda_1 \ldots \lambda_n |K| > 2^n$. Από το Λήμμα 4.2.2 και το θεώρημα αντίστροφης απεικόνισης, το $T(K)$ είναι ανοικτό και φραγμένο, και $|T(K)| > 2^n$, οπότε, εφαρμόζοντας το Λήμμα του Blichfeldt για το $\frac{T(K)}{2}$, βρίσκουμε $y^1 \neq y^2 \in T(K)$ τέτοια ώστε

$$\frac{y^1 - y^2}{2} \in \mathbb{Z}^n \backslash \{o\}.$$

Θεωρούμε τα (μοναδικά) $a^1 \neq a^2 \in K$ για τα οποία $T(a^1) = y^1$ και $T(a^2) = y^2$, και γράφουμε

$$a^1 = \sum_{j=1}^n a_j^1 u_j, \quad a^2 = \sum_{j=1}^n a_j^2 u_j.$$

Αφού $a^1 \neq a^2$, υπάρχει $k \leq n$ τέτοιο ώστε $a_k^1 \neq a_k^2$, και $a_j^1 = a_j^2$, $j = k+1, \ldots, n$. Τότε,

$$\begin{aligned} \frac{y^1 - y^2}{2} &= \lambda_1 \frac{1}{2}(b(a_1^1, \ldots, a_n^1) - b(a_1^2, \ldots, a_n^2)) + \ldots \\ &+ (\lambda_k - \lambda_{k-1})\frac{1}{2}(b(a_k^1, \ldots, a_n^1) - b(a_k^2, \ldots, a_n^2)). \end{aligned}$$

Από την κυρτότητα και τη συμμετρία του K, και από το γεγονός ότι όλες οι b παίρνουν τιμές στο K, συμπεραίνουμε ότι

$$\frac{y^1 - y^2}{2} \in \lambda_1 K + \ldots + (\lambda_k - \lambda_{k-1})K = \lambda_k K.$$

Δηλαδή,

$$\frac{y^1 - y^2}{2} \in \lambda_k K \cap (\mathbb{Z}^n \setminus \{o\}).$$

Όμως, η k-στή συντεταγμένη του $(y^1 - y^2)/2$ (ως προς τη βάση $\{u_1, \ldots, u_n\}$) είναι

$$\frac{1}{2}\left(\lambda_k a_k^1 + h(a_{k+1}^1, \ldots, a_n^1) - \lambda_k a_k^2 - h(a_{k+1}^2, \ldots, a_n^2)\right) = \frac{1}{2}\lambda_k (a_k^1 - a_k^2) \neq 0,$$

δηλαδή το $(y^1 - y^2)/2$ είναι γραμμικώς ανεξάρτητο από τα $u_1, \ldots, u_{k-1}$. Αυτό είναι άτοπο, αφού το $\lambda_k K$ δεν μπορεί να περιέχει k γραμμικώς ανεξάρτητα ακέραια σημεία. $\square$

4.3 Δεύτερη απόδειξη του θεωρήματος

Η δεύτερη απόδειξη που θα δώσουμε οφείλεται στον Estermann [Es], και βασίζεται στην πλήρη εκμετάλλευση της τεχνικής του Blichfeldt. Ονομάζουμε $\kappa_1, \ldots, \kappa_n$ τα διαδοχικά ελάχιστα του $\mathcal{D}(K) = K - K$. Αν το K είναι συμμετρικό, τότε $\mathcal{D}(K) = 2K$, οπότε έχουμε $\kappa_i = \lambda_i/2$, $i = 1, \ldots, n$. Αρκεί λοιπόν να δείξουμε ότι

$$(*) \qquad \kappa_1 \kappa_2 \ldots \kappa_n |K| \leq 1.$$

Θεωρούμε μία επιλογή $u_1, \ldots, u_n$ ελαχιστικών διανυσμάτων του $\mathcal{D}(K)$. Τα $u_1, \ldots, u_n$ είναι γραμμικώς ανεξάρτητα, επομένως, από το Θεώρημα 1.1.2 υπάρχει βάση $\{w_1, \ldots, w_n\}$ του $\mathbb{Z}^n$ με την ιδιότητα

$$u_i \in \langle w_1, \ldots, w_i \rangle, \quad i = 1, \ldots, n.$$

Παρατήρηση: Θεωρούμε τον γραμμικό μετασχηματισμό T που ορίζεται από τις $T(e_i) = w_i$, όπου $\{e_i\}_{i \leq n}$ η συνήθης βάση του $\mathbb{Z}^n$. Τότε, $|\det T| = 1$ και ο T αφήνει αναλλοίωτο το $\mathbb{Z}^n$, άρα τα $T^{-1}(K)$ και K έχουν τον ίδιο όγκο και τα ίδια διαδοχικά ελάχιστα, αφού $u \in \lambda K \cap \mathbb{Z}^n$ αν και μόνο αν $T^{-1}(u) \in T^{-1}(\lambda K \cap \mathbb{Z}^n) = \lambda T^{-1}(K) \cap \mathbb{Z}^n$, $\lambda > 0$. Επιπλέον, ισχύει $T^{-1}(\mathcal{D}(K)) = \mathcal{D}(T^{-1}(K))$, αρκεί λοιπόν να δείξουμε την $(*)$ με την επιπλέον υπόθεση ότι $w_i = e_i$, $i = 1, \ldots, n$.

Τότε, αν $a = (a_1, \ldots, a_n) \in \kappa_i \mathcal{D}(K) \cap \mathbb{Z}^n$, ισχύει ότι $a_i = \ldots = a_n = 0$ (το a πρέπει να ανήκει στον υπόχωρο που παράγεται από τα $u_1, \ldots, u_{i-1}$, άρα γράφεται σαν γραμμικός συνδυασμός των $e_1, \ldots, e_{i-1}$). Συνοψίζοντας όλες αυτές τις παρατηρήσεις, βλέπουμε ότι, χωρίς περιορισμό της γενικότητας, το ζητούμενο είναι το εξής:

Θεώρημα 4.3.1 *Έστω K (συμμετρικό) κυρτό σώμα, και $0 < \kappa_1 \leq \ldots \leq \kappa_n \in \mathbb{R}$ τα διαδοχικά ελάχιστα του $\mathcal{D}(K)$. Υποθέτουμε ότι, αν $a = (a_1, \ldots, a_n) \in \kappa_i \mathcal{D}(K) \cap \mathbb{Z}^n$, τότε $a_i = \ldots = a_n = 0$. Τότε,*

$$\kappa_1 \ldots \kappa_n |K| \leq 1.$$

Η συμμετρία του K δεν είναι απαραίτητη για την απόδειξη του Θεωρήματος 4.3.1.

Ορισμός Για κάθε $i = 1, \dots, n$, ορίζουμε $\rho_i : \mathbb{R}^n \to \mathbb{R}^n$, με

$$\rho_i(x_1, \dots, x_i, \dots, x_n) = (x_1, \dots, \{x_i\}, \dots, x_n).$$

Επίσης, ορίζουμε $P_i = \rho_1 \circ \dots \circ \rho_i$, και $P_0 = Id$.

Λήμμα 4.3.1 *Για κάθε $z \in \mathbb{R}^n$, ισχύει $|P_n(K+z)| = |P_n(K)|$.*

Απόδειξη: Για κάθε $u \in \mathbb{Z}^n$ και $z \in \mathbb{R}^n$, ισχύει $P_n(K+z+u) = P_n(K+z)$. Μπορούμε λοιπόν να υποθέσουμε ότι το $z = z_1 e_1 + \dots + z_n e_n$ ανήκει στο θεμελιώδες παραλληλεπίπεδο του $\mathbb{Z}^n$ ως προς τη συνήθη βάση. Δηλαδή, ότι $0 \leq z_j < 1$, $j = 1, \dots, n$.
Επίσης, αρκεί να αποδείξουμε το ζητούμενο στην περίπτωση $z = z_i e_i$. Γιατί τότε,

$$\begin{aligned} |P_n(K+z)| &= |P_n(K + z_1 e_1 + \dots + z_n e_n)| \\ &= |P_n(K + z_1 e_1 + \dots + z_{n-1} e_{n-1})| = \dots = |P_n(K + z_1 e_1)| \\ &= |P_n(K)|. \end{aligned}$$

Υποθέτουμε λοιπόν, χωρίς περιορισμό της γενικότητας, ότι $z = z_1 e_1$, $0 < z_1 < 1$. Ορίζουμε

$$A = P_n(K) \cap \{x : 0 \leq x_1 < 1 - z_1\}, \quad B = P_n(K) \cap \{x : 1 - z_1 \leq x_1 < 1\}.$$

Τότε,

$$P_n(K+z) = (A + z_1 e_1) \cup (B + (z_1 - 1)e_1) =: A_1 \cup B_1,$$

και αφού $A_1 \cap B_1 = \emptyset$, βλέπουμε ότι

$$|P_n(K+z)| = |A_1| + |B_1| = |A| + |B| = |P_n(K)|. \quad \Box$$

Λήμμα 4.3.2 *Αν $t \geq 1$, τότε $|P_n(tK)| \geq |P_n(K)|$.*

Απόδειξη: Αν $o \in K$, τότε από την κυρτότητα του K έπεται ότι $K \subseteq tK$, οπότε το ζητούμενο είναι προφανές. Αν όχι, επιλέγουμε $z \in \mathbb{R}^n$ τέτοιο ώστε $o \in (K+z)$, και εφαρμόζουμε το Λήμμα 4.3.1:

$$|P_n(tK)| = |P_n(tK + tz)| = |P_n(t(K+z))| \geq |P_n(K+z)| = |P_n(K)|. \quad \Box$$

Πιό γενικά, για κάθε $i = 1, \dots, n$ παίρνουμε:

Λήμμα 4.3.3 *Αν $t \geq 1$, τότε $|P_i(tK)| \geq t^{n-i} |P_i(K)|$.*

Απόδειξη: Σταθεροποιούμε $i \leq n-1$. Για κάθε $x \in \mathbb{R}^n$ γράφουμε $x=(x',x'')$, όπου $x'=(x_1,\ldots,x_i)$, $x''=(x_{i+1},\ldots,x_n)$. Αν $M \subseteq \mathbb{R}^n$, ορίζουμε

$$\langle M;x''\rangle = \{x' \in \mathbb{R}^i : (x',x'') \in M\}, \quad x'' \in \mathbb{R}^{n-i}.$$

Ισχυρισμός: Αν $t>0$, τότε

$$\langle P_i(tM);tx''\rangle = P_i(\langle tM;tx''\rangle) = P_i(t\langle M,x''\rangle).$$

Απόδειξη: Η δεύτερη ισότητα είναι προφανής. Για την πρώτη, θεωρούμε τυχόν $y \in \langle P_i(tM);tx''\rangle$. Τότε, $(y,tx'') \in P_i(tM)$, δηλαδή υπάρχει $(z,w) \in tM$ τέτοιο ώστε $P_i(z,w)=(y,tx'')$. Αφού ο μετασχηματισμός P_i μπορεί να μεταβάλλει μόνο τις πρώτες i συντεταγμένες του (z,w), έπεται ότι $w=tx''$ και $P_i(z)=y$. Δηλαδή, $z \in \langle tM;tx''\rangle$, άρα $y \in P_i(\langle tM;tx''\rangle)$. Έτσι, αποδείχθηκε η

$$\langle P_i(tM);tx''\rangle \subseteq P_i(\langle tM;tx''\rangle).$$

Ο αντίστροφος εγκλεισμός αποδεικνύεται ανάλογα. □

Θα χρησιμοποιήσουμε τον ισχυρισμό, και την παρατήρηση ότι, αν $t \geq 1$ τότε

$$|P_i(t\langle K;x''\rangle)| \geq |P_i(\langle K;x''\rangle)|,$$

η οποία είναι συνέπεια του Λήμματος 4.3.2, αφού κάθε $\langle K;x''\rangle$ είναι κυρτό υποσύνολο του $\mathbb{R}^i$:

Ολοκληρώνοντας πρώτα ως προς $x' \in \mathbb{R}^i$ και μετά ως προς $x'' \in \mathbb{R}^{n-i}$, γράφουμε τον όγκο του $P_i(tK)$ στη μορφή

$$|P_i(tK)| = \int_{\mathbb{R}^{n-i}} |\langle P_i(tK);x''\rangle| dx''.$$

Κάνοντας την αλλαγή μεταβλητής $x''=ty''$ και χρησιμοποιώντας τις παρατηρήσεις μας, έχουμε

$$\begin{aligned} |P_i(tK)| &= t^{n-i}\int_{\mathbb{R}^{n-i}} |\langle P_i(tK);ty''\rangle| dy'' \\ &= t^{n-i}\int_{\mathbb{R}^{n-i}} |P_i(t\langle K;y''\rangle)| dy'' \\ &\geq t^{n-i}\int_{\mathbb{R}^{n-i}} |P_i(\langle K;y''\rangle)| dy'' \\ &= t^{n-i}|P_i(K)|. \end{aligned}$$

Η περίπτωση $i=n$ καλύπτεται από το Λήμμα 4.3.2. □

Λήμμα 4.3.4 *Έστω W κυρτό σώμα στον $\mathbb{R}^n$. Αν $\mathcal{D}(W) \cap \mathbb{Z}^n = \{o\}$, τότε $|\rho_i(W)| = |W|$ για κάθε $i=1,\ldots,n$.*

Απόδειξη: Η απόδειξη είναι εντελώς ανάλογη με αυτήν του Λήμματος του Blichfeldt. Αν θεωρήσουμε τα σύνολα $(u+P)\cap W$ όπου $u \in \mathbb{Z}^n$ και P το σύνηθες θεμελιώδες παραλληλεπίπεδο του $\mathbb{Z}^n$, τότε τα $\rho_i((u+P)\cap W)$ δεν επικαλύπτονται, αλλιώς το $\mathcal{D}(W)$ θα περιείχε μη μηδενικό ακέραιο σημείο, παράλληλο προς το e_i. Άρα,

$$|\rho_i(W)| = \sum_u |\rho_i((u+P)\cap W)| = \sum_u |(u+P)\cap W| = |W|. \quad \square$$

Απόδειξη του Θεωρήματος 4.3.1: Η απόδειξη θα βασιστεί στον ακόλουθο ισχυρισμό:

Ισχυρισμός: Για κάθε $i = 1, \ldots, n$, έχουμε

$$|P_i(\kappa_i K)| = |P_{i-1}(\kappa_i K)|.$$

Απόδειξη: Αφού $P_i = \rho_i \circ P_{i-1}$, σύμφωνα με το Λήμμα 4.3.4 αρκεί να δείξουμε ότι

$$(P_{i-1}(\kappa_i K) - P_{i-1}(\kappa_i K)) \cap \mathbb{Z}^n = \{o\}, \quad i = 1, \ldots, n.$$

Έστω ότι υπάρχουν $x, y \in \kappa_i K$ τέτοια ώστε $o \neq P_{i-1}(x) - P_{i-1}(y) \in \mathbb{Z}^n$. Τότε, $x - y \in (\kappa_i \mathcal{D}(K)) \cap \mathbb{Z}^n$, και από την υπόθεση του Θεωρήματος πρέπει να ισχύει $x_j = y_j$, $j = i, \ldots, n$. Όμως τότε, $P_{i-1}(x) = P_{i-1}(y)$, άτοπο. $\square$

Εφαρμόζοντας τώρα το Λήμμα 4.3.4 για το $P_{i-1}(\kappa_i K)$ με $t = \kappa_i/\kappa_{i-1} \geq 1$, παίρνουμε

$$|P_i(\kappa_i K)| = |P_{i-1}(\kappa_i K)| \geq \left(\frac{\kappa_i}{\kappa_{i-1}}\right)^{n+1-i} |P_{i-1}(\kappa_{i-1} K)|, \quad i = 2, \ldots, n.$$

Για $i = 1$ γράφουμε απλώς

$$|P_1(\kappa_1 K)| = |\kappa_1 K| = \kappa_1^n |K|.$$

Πολλαπλασιάζοντας κατά μέλη, βλέπουμε ότι

$$|P_n(\kappa_n K)| \geq \kappa_1^n \prod_{i=2}^n \left(\frac{\kappa_i}{\kappa_{i-1}}\right)^{n+1-i} |K| = \kappa_1 \kappa_2 \ldots \kappa_n |K|.$$

Όμως $P_n(\kappa_n K) \subseteq P$, άρα $|P_n(\kappa_n K)| \leq 1$. Έπεται ότι

$$\kappa_1 \kappa_2 \ldots \kappa_n |K| \leq 1. \quad \square$$

Δεν είναι δύσκολο να δώσουμε κάτω φράγμα για το γινόμενο $\lambda_1 \ldots \lambda_n$ των διαδοχικών ελαχίστων του K. Ο Minkowski απέδειξε το εξής:

Θεώρημα 4.3.2 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$, και $\lambda_1, \ldots, \lambda_n$ τα διαδοχικά ελάχιστα του K. Τότε,*

$$\lambda_1 \lambda_2 \ldots \lambda_n |K| \geq \frac{2^n}{n!}.$$

Απόδειξη: Υπάρχουν γραμμικώς ανεξάρτητα διανύσματα $u_i \in \mathbb{Z}^n$ τέτοια ώστε κάθε u_i να ανήκει στο σύνορο του $\lambda_i K$. Ορίζουμε

$$v_i = \frac{u_i}{\lambda_i}, \quad i = 1, \dots, n.$$

Τότε, $\pm v_i \in \overline{K}$ για κάθε i, άρα η κυρτή θήκη $A = \mathrm{co}\{\pm v_1, \dots, \pm v_n\}$ των $\pm v_i$ έχει όγκο το πολύ ίσο με $|K|$. Όμως,

$$|A| = |\mathrm{co}\{\pm v_1, \dots, \pm v_n\}| = \frac{2^n |\det(v_1, \dots, v_n)|}{n!},$$

και

$$|\det(v_1, \dots, v_n)| = \frac{|\det(u_1, \dots, u_n)|}{\lambda_1 \lambda_2 \dots \lambda_n} \geq \frac{1}{\lambda_1 \lambda_2 \dots \lambda_n},$$

γιατί τα u_i είναι ακέραια διανύσματα, οπότε $\det(u_1, \dots, u_n) \in \mathbb{Z} \setminus \{0\}$. Συνδυάζοντας τα παραπάνω, έχουμε

$$\lambda_1 \lambda_2 \dots \lambda_n |K| \geq \lambda_1 \lambda_2 \dots \lambda_n |A| \geq \frac{2^n |\det(u_1, \dots, u_n)|}{n!} \geq \frac{2^n}{n!}. \quad \square$$

Κεφάλαιο 5

Το θεώρημα των Minkowski και Hlawka

5.1 Το θεώρημα επιλογής του Mahler

Σκοπός μας σε αυτήν την παράγραφο είναι να αποδείξουμε το Θεώρημα επιλογής του Mahler, το οποίο εξασφαλίζει την ύπαρξη «συγκλίνουσας» υπακολουθίας για κάθε «φραγμένη» ακολουθία πλεγμάτων. Για τη διατύπωση του Θεωρήματος, πρέπει πρώτα να ορίσουμε αυστηρά τι είναι ένα φραγμένο σύνολο πλεγμάτων, καθώς και την έννοια της σύγκλισης που θα χρησιμοποιήσουμε.

Ορισμοί (α) Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Ένα πλέγμα Λ λέγεται **αποδεκτό** για το K, αν το μόνο σημείο του Λ που ανήκει στο εσωτερικό του K είναι το o. Το Λ λέγεται αυστηρά αποδεκτό για το K αν $K \cap \Lambda = \{o\}$.

(β) Για κάθε $\rho > 0$, συμβολίζουμε με ρD_n τη μπάλα με κέντρο το o και ακτίνα ρ:

$$\rho D_n = \{x \in \mathbb{R}^n : \|x\|_2 \leq \rho\}.$$

Ένα σύνολο $\mathcal{L}$ πλεγμάτων του $\mathbb{R}^n$ λέγεται **φραγμένο**, αν υπάρχουν θετικές σταθερές ρ και σ τέτοιες ώστε:

(i) Κάθε $\Lambda \in \mathcal{L}$ είναι αποδεκτό για την ρD_n.

(ii) Για κάθε $\Lambda \in \mathcal{L}$, ισχύει $\det \Lambda \leq \sigma$.

(γ) Για κάθε $n \times n$ πίνακα B, ορίζουμε $\|B\| = \max_{i,j} |b_{ij}|$. Η $\|\cdot\|$ είναι νόρμα στον χώρο των πινάκων (ουσιαστικά, η $\|\cdot\|_\infty$ στον $\mathbb{R}^{n^2}$). Οι βασικές ιδιότητες αυτής της νόρμας περιγράφονται στο εξής Λήμμα:

Λήμμα 5.1.1 *(α) Έστω $A_m, A \in L(\mathbb{R}^n)$. Τότε, $\|A_m - A\| \to 0$ αν και μόνο αν $a_{ij}^{(m)} \to a_{ij}$ για κάθε $i, j \leq n$.*

(β) Για κάθε $A, B \in L(\mathbb{R}^n)$, $\|AB\| \leq n\|A\| \cdot \|B\|$.

(γ) Για κάθε $A \in L(\mathbb{R}^n)$ και κάθε $x \in \mathbb{R}^n$, $\|Ax\|_2 \leq n\|A\| \cdot \|x\|_2$.

Απόδειξη: Το (α) είναι φανερό, αφού

$$\|A_m - A\| = \max_{i,j\leq n} |a_{ij}^{(m)} - a_{ij}|.$$

Για το (β), παρατηρούμε ότι $(AB)_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$. Όμως, για κάθε $i, j \leq n$,

$$|\sum_{k=1}^n a_{ik}b_{kj}| \leq \sum_{k=1}^n |a_{ij}||b_{ij}| \leq \sum_{k=1}^n \|A\| \cdot \|B\| = n\|A\| \cdot \|B\|.$$

άρα,

$$\|AB\| = \max_{i,j\leq n} |\sum_{k=1}^n a_{ik}b_{kj}| \leq n\|A\| \cdot \|B\|.$$

Για το (γ), χρησιμοποιούμε την ανισότητα Cauchy-Schwarz:

$$\begin{aligned}
\|Ax\|_2 &= \left(\sum_{i=1}^n \left(\sum_{j=1}^n a_{ij}x_j\right)^2\right)^{1/2} \\
&\leq \left(\sum_{i=1}^n \left(\sum_{j=1}^n a_{ij}^2\right)\left(\sum_{j=1}^n x_j^2\right)\right)^{1/2} \\
&= \|x\|_2 \left(\sum_{i,j=1}^n a_{ij}^2\right)^{1/2} \\
&\leq \|x\|_2 \left(n^2\|A\|^2\right)^{1/2},
\end{aligned}$$

δηλαδή, $\|Ax\|_2 \leq n\|A\| \cdot \|x\|_2$. □

Με τη βοήθεια αυτής της νόρμας ορίζουμε μία έννοια «περιοχής» για τα πλέγματα του $\mathbb{R}^n$:

Έστω Λ ένα πλέγμα του $\mathbb{R}^n$, και $A = \{u_1, \ldots, u_n\}$ μία βάση του Λ, την οποία ταυτίζουμε με τον πίνακα $A_{ij} = \langle u_j, e_i\rangle$. Για κάθε $\varepsilon > 0$, η (A, ε)-**γειτονιά** του Λ είναι το σύνολο όλων των πλεγμάτων Λ' του $\mathbb{R}^n$ τα οποία έχουν κάποια βάση A' της οποίας ο πίνακας ικανοποιεί την $\|A - A'\| < \varepsilon$.

(δ) Η έννοια της (A, ε)-γειτονιάς μάς επιτρέπει να ορίσουμε σύγκλιση ακολουθιών πλεγμάτων. Λέμε ότι η ακολουθία πλεγμάτων $\{\Lambda_m\}$ **συγκλίνει** στο πλέγμα Λ του $\mathbb{R}^n$ ως προς τη βάση A του Λ, αν για κάθε $\varepsilon > 0$, υπάρχει $m_0(\varepsilon) \in \mathbb{N}$ τέτοιος ώστε: για κάθε $m \geq m_0$, το Λ_m ανήκει στην (A, ε)-γειτονιά του Λ. Λέμε ότι η ακολουθία πλεγμάτων $\{\Lambda_m\}$ **συγκλίνει** στο πλέγμα Λ του $\mathbb{R}^n$, αν συγκλίνει στο Λ ως προς κάθε βάση A του Λ.

Σύμφωνα με αυτόν τον ορισμό, για να ελέγξουμε ότι $\Lambda_m \to \Lambda$, πρέπει να ελέγξουμε τη σύγκλιση για τυχούσα επιλογή της βάσης A του Λ. Όπως θα δούμε όμως, αρκεί να ελεγχθεί η σύγκλιση ως προς **κάποια** βάση A του Λ:

Λήμμα 5.1.2 *Έστω ότι $\Lambda_m \to \Lambda$ ως προς κάποια βάση A του Λ. Τότε, $\Lambda_m \to \Lambda$.*

Απόδειξη: Αφού $\Lambda_m \to \Lambda$ ως προς την A, υπάρχει ακολουθία $\{A_m\}$ βάσεων των Λ_m αντίστοιχα, με

$$\|A_m - A\| \to 0.$$

Έστω B μία άλλη βάση του Λ. Υπάρχει ακέραιος πίνακας U με $\det U = \pm 1$, τέτοιος ώστε $B = AU$. Ορίζουμε $B_m = A_m U$. Τότε, κάθε B_m είναι βάση του Λ_m, και

$$\|B_m - B\| = \|A_m U - AU\| = \|(A_m - A)U\| \leq n\|U\| \cdot \|A_m - A\| \to 0.$$

Άρα, $\Lambda_m \to \Lambda$ ως προς την B. □

Το επόμενο θεώρημα δείχνει ότι αυτός ο ορισμός σύγκλισης είναι «σωστός»: αν $\Lambda_m \to \Lambda$, τότε, για μεγάλα m, τα σημεία του Λ_m βρίσκονται «κοντά» στα σημεία του Λ:

Θεώρημα 5.1.1 *Έστω Λ_m, Λ πλέγματα στον $\mathbb{R}^n$, με $\Lambda_m \to \Lambda$. Τότε,*

(α) Για κάθε $x \in \Lambda$, υπάρχει ακολουθία σημείων $x_m \in \Lambda_m$ με $x_m \to x$.

(β) Αν για κάποιο $x \in \mathbb{R}^n$ υπάρχει ακολουθία σημείων $x_m \in \Lambda_m$ με $x_m \to x$, τότε $x \in \Lambda$.

Απόδειξη: (α) Έστω $x \in \Lambda$. Αν A είναι μία βάση του Λ, το x γράφεται στη μορφή $x = Au$, όπου $u \in \mathbb{Z}^n$. Αφού $\Lambda_m \to \Lambda$, υπάρχουν βάσεις A_m των Λ_m αντίστοιχα, με $\|A_m - A\| \to 0$. Ορίζουμε $x_m = A_m u$. Τότε, $x_m \in \Lambda_m$ και

$$\|x_m - x\|_2 = \|(A_m - A)u\|_2 \leq n\|A_m - A\| \cdot \|u\|_2 \to 0.$$

Δηλαδή, $x_m \to x$.

(β) Σταθεροποιούμε βάσεις A_m, A των Λ_m, Λ. Κάθε x_m γράφεται $x_m = A_m u_m$ όπου $u_m \in \mathbb{Z}^n$. Αφού η βάση A του Λ είναι βάση του $\mathbb{R}^n$, το x γράφεται $x = Ay$ για κάποιο $y \in \mathbb{R}^n$. Σκοπός μας είναι να δείξουμε ότι $y \in \mathbb{Z}^n$.

Ο A είναι αντιστρέψιμος, και η $z \mapsto \|Az\|_2$ είναι συνεχής στην S^{n-1}. Άρα, παίρνει ελάχιστη γνήσια θετική τιμή a. Δηλαδή,

$$\|Az\|_2 \geq a, \quad z \in S^{n-1}.$$

Αφού $A_m \to A$, υπάρχει $m_0 \in \mathbb{N}$ με την ιδιότητα: για κάθε $m \geq m_0$, $\|A_m - A\| < a/2n$. Τότε, χρησιμοποιώντας το Λήμμα 5.1.1, βλέπουμε ότι για κάθε $m \geq m_0$ και κάθε $z \in S^{n-1}$,

$$\|A_m z\|_2 \geq \|Az\|_2 - \|(A_m - A)z\|_2 \geq a - n\|A_m - A\| \cdot \|z\|_2 > \frac{a}{2}.$$

Δηλαδή, αν $m \geq m_0$, έχουμε

$$\|A_m z\|_2 \geq \frac{a}{2}\|z\|_2, \quad z \in \mathbb{R}^n.$$

Από τις $A_m u_m = x_m \to x = Ay$ και $A_m y \to Ay$, έπεται ότι $A_m(u_m - y) \to o$. Άρα, για $m \geq m_0$,

$$\|u_m - y\|_2 \leq \frac{2}{a}\|A_m(u_m - y)\|_2 \to 0,$$

δηλαδή, $u_m \to y$. Αφού $u_m \in \mathbb{Z}^n$ για κάθε m, συμπεραίνουμε ότι $y \in \mathbb{Z}^n$. Έπεται ότι $x = Ay \in \Lambda$. $\square$

Για την απόδειξη του Θεωρήματος του Mahler θα χρειαστούμε επίσης το εξής:

Θεώρημα 5.1.2 *Για κάθε $n \in \mathbb{N}$ υπάρχει σταθερά $C(n) > 0$ με την ακόλουθη ιδιότητα: Αν Λ είναι ένα πλέγμα στον $\mathbb{R}^n$, τότε υπάρχει βάση $A = \{u_1, \ldots, u_n\}$ του Λ τέτοια ώστε*

$$\prod_{i=1}^{n} \|u_i\|_2 \leq C(n) \det \Lambda.$$

Η ύπαρξη τέτοιων «ανηγμένων βάσεων», καθώς και διάφορα φράγματα για τη σταθερά $C(n)$, θα συζητηθούν λεπτομερώς στο Κεφάλαιο 7.

Θεώρημα 5.1.3 *Κάθε φραγμένη ακολουθία πλεγμάτων έχει συγκλίνουσα υπακολουθία.*

Απόδειξη: Έστω $\{\Lambda_m\}$ φραγμένη ακολουθία πλεγμάτων στον $\mathbb{R}^n$. Δηλαδή, υπάρχουν θετικές σταθερές ρ και σ τέτοιες ώστε: για κάθε $m \in \mathbb{N}$, $(\rho D_n)^\circ \cap \Lambda_m = \{o\}$ και $\det \Lambda_m \leq \sigma$. Παρατηρούμε ότι

$$|\rho D_n| = \omega_n \rho^n \leq 2^n \det \Lambda_m$$

από το πρώτο θεώρημα του Minkowski, δηλαδή

$$\inf_{m \in \mathbb{N}} \det \Lambda_m = a > 0.$$

Για κάθε m, επιλέγουμε βάση $A_m = \{u_1^{(m)}, \ldots, u_n^{(m)}\}$ του Λ_m, με την ιδιότητα

$$\prod_{i=1}^{n} \|u_i^{(m)}\|_2 \leq C(n) \det \Lambda_m \leq C(n)\sigma.$$

Αφού κάθε Λ_m είναι επιτρεπτό για την ρD_n, συμπεραίνουμε ότι $\|u_i^{(m)}\|_2 \geq \rho$ για κάθε $m \in \mathbb{N}$, $i = 1, \ldots, n$. Άρα,

$$\|u_i^{(m)}\|_2 \leq \frac{C(n)\sigma}{\rho^{n-1}}, \quad m \in \mathbb{N}, i = 1, \ldots, n.$$

Από το θεώρημα Bolzano-Weierstrass, υπάρχουν αύξουσα ακολουθία φυσικών k_m και $u_1, \ldots, u_n \in \mathbb{R}^n$, τέτοια ώστε

$$u_i^{(k_m)} \to u_i, \quad i = 1, \ldots, n.$$

Το $A = \{u_1, \ldots, u_n\}$ είναι γραμμικώς ανεξάρτητο, γιατί $\det A = \lim \det A_{k_m} = \lim \det \Lambda_{k_m} \geq a$. Θεωρούμε το πλέγμα Λ που παράγεται από το A. Τότε, $\det \Lambda = \lim \det \Lambda_{k_m} \leq \sigma$, και $\|u_i\|_2 = \lim \|u_i^{(k_m)}\|_2 \geq \rho$, δηλαδή το Λ είναι αποδεκτό για την ρD_n. Τέλος,

$$\|A_{k_m} - A\| \leq \max_{i \leq n} \|u_i^{k_m} - u_i\|_2 \to 0,$$

επομένως, $\Lambda_{k_m} \to \Lambda$. □

5.2 Η κρίσιμη ορίζουσα

Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Η **κρίσιμη ορίζουσα** $\Delta(K)$ του K είναι το $\inf \det \Lambda$, όπου το infimum παίρνεται πάνω από όλα τα πλέγματα Λ που είναι αποδεκτά (ισοδύναμα, αυστηρά αποδεκτά) για το K.

Το πρώτο θεώρημα του Minkowski μάς δίνει αμέσως ένα κάτω φράγμα για την κρίσιμη ορίζουσα του K:

Πρόταση 5.2.1 *Για κάθε συμμετρικό κυρτό σώμα K στον $\mathbb{R}^n$, έχουμε*

$$\Delta(K) \geq 2^{-n}|K|.$$

Απόδειξη: Έστω Λ ένα πλέγμα, αποδεκτό για το K. Αφού το K δεν περιέχει μη μηδενικό στοιχείο του Λ, το πρώτο θεώρημα του Minkowski μάς λέει ότι

$$|K| \leq 2^n \det \Lambda.$$

Παίρνοντας infimum ως προς όλα τα K-αποδεκτά πλέγματα, καταλήγουμε στο ζητούμενο. □

Παρατήρηση Απλές συνέπειες του ορισμού της κρίσιμης ορίζουσας είναι οι εξής:
(α) Αν $K \subseteq W$, τότε $\Delta(K) \leq \Delta(W)$.
(β) Για κάθε $t > 0$, $\Delta(tK) = t^n \Delta(K)$.
(γ) Αν $A \in GL(n)$, τότε $\Delta(AK) = |\det A|\Delta(K)$.

Ο Mahler απέδειξε ότι για κάθε συμμετρικό κυρτό σώμα K υπάρχει τουλάχιστον ένα K-αποδεκτό πλέγμα με την ελάχιστη δυνατή ορίζουσα (δηλαδή, το infimum στον ορισμό της $\Delta(K)$ είναι minimum). Αυτός ήταν και ένας από τους λόγους για τους οποίους απέδειξε το θεώρημα επιλογής της Παραγράφου 5.1:

Πρόταση 5.2.2 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Υπάρχει πλέγμα Λ το οποίο είναι αποδεκτό για το K και έχει ορίζουσα*

$$\det \Lambda = \Delta(K).$$

Απόδειξη: Το K περιέχει μία μπάλα με κέντρο το o και ακτίνα $\rho > 0$. Έπεται ότι, κάθε πλέγμα που είναι αποδεκτό για το K είναι αποδεκτό για την ρD_n. Θεωρούμε ακολουθία Λ_m αποδεκτών για το K πλεγμάτων, με

$$\det \Lambda_m \to \Delta(K).$$

Η $\{\Lambda_m\}$ είναι φραγμένη ακολουθία: κάθε Λ_m είναι αποδεκτό για την ρD_n, και η $\{\det \Lambda_m\}$ είναι συγκλίνουσα ακολουθία, άρα φραγμένη. Από το Θεώρημα επιλογής του Mahler, περνώντας σε υπακολουθία, μπορούμε να υποθέσουμε ότι υπάρχει πλέγμα Λ στον $\mathbb{R}^n$, τέτοιο ώστε $\Lambda_m \to \Lambda$. Προφανώς,

$$\det \Lambda = \lim_{m\to\infty} \det \Lambda_m = \Delta(K).$$

Μένει να δείξουμε ότι το Λ είναι αποδεκτό για το K. Υποθέτουμε το αντίθετο. Τότε, υπάρχει $x \in \Lambda$, το οποίο είναι εσωτερικό σημείο του K. Από το Θεώρημα 5.1.1, υπάρχει ακολουθία $\{x_m\}$, $x_m \in \Lambda_m$, με $x_m \to x$. Αφού το x είναι εσωτερικό σημείο του K, για μεγάλα m το x_m θα είναι εσωτερικό σημείο του K. Αυτό όμως είναι άτοπο, γιατί όλα τα Λ_m είναι K-αποδεκτά. □

Το ερώτημα το οποίο προκύπτει από τα παραπάνω, είναι αν ο λόγος $\Delta(K)/|K|$ είναι άνω φραγμένος. Ο Minkowski [Mi1] ισχυρίστηκε ότι για κάθε συμμετρικό κυρτό σώμα K με όγκο $|K| < 2\zeta(n) = 2(1 + 2^{-n} + 3^{-n} + \ldots)$, υπάρχει K-αποδεκτό πλέγμα Λ με ορίζουσα $\det \Lambda = 1$. Δηλαδή,

$$\frac{\Delta(K)}{|K|} \leq \frac{1}{2\zeta(n)}.$$

Αυτή η εικασία του Minkowski αποδείχθηκε το 1944 από τον Hlawka [Hl]. Την απόδειξη αυτού του θεωρήματος (το οποίο αναφέρεται ως Θεώρημα Minkowski-Hlawka), θα συζητήσουμε στην επόμενη παράγραφο.

5.3 Το θεώρημα των Minkowski και Hlawka

Θα αποδείξουμε το Θεώρημα των Minkowski-Hlawka, για συμμετρικά κυρτά σώματα. Το ίδιο αποτέλεσμα ισχύει για μία ευρύτερη κλάση συμμετρικών υποσυνόλων του $\mathbb{R}^n$ (τα λεγόμενα **αστρόμορφα χωρία**).

Θεώρημα 5.3.1 *Έστω K συμμετρικό κυρτό σώμα στον $\mathbb{R}^n$. Τότε,*

$$\frac{\Delta(K)}{|K|} \leq \frac{1}{2\zeta(n)}.$$

Η απόδειξη θα βασιστεί σε δύο γενικότερα λήμματα για Riemann-ολοκληρώσιμες συναρτήσεις με συμπαγή φορέα. Το πρώτο οφείλεται στους Davenport και Rogers [DR], ενώ το δεύτερο είναι το βασικό λήμμα του Hlawka [Hl]:

Λήμμα 5.3.1 *Έστω $f:\mathbb{R}^n \to \mathbb{R}$ μία συνεχής συνάρτηση που μηδενίζεται έξω από ένα φραγμένο σύνολο (έχει **συμπαγή φορέα**). Για κάθε $\gamma \in \mathbb{R}$, ορίζουμε*

$$V_f(\gamma) = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} f(x_1, \dots, x_{n-1}, \gamma) dx_1 \dots dx_{n-1}.$$

Έστω Λ' ένα πλέγμα στον $\mathbb{R}^{n-1}$ με ορίζουσα $\det \Lambda'$, και έστω $\delta > 0$. Για κάθε $y = (y_1, \dots, y_{n-1}) \in \mathbb{R}^{n-1}$, συμβολίζουμε με Λ_y το πλέγμα που παράγεται από τα Λ' και (y, δ). Δηλαδή,

$$\Lambda_y = \{x + m(y, \delta) : x \in \Lambda', m \in \mathbb{Z}\}.$$

Τότε, υπάρχει $z = (z_1, \dots, z_{n-1})$ με την ιδιότητα

$$(*) \qquad \sum_{x \in \Lambda_z, x_n \neq 0} f(x) \leq \frac{1}{\det \Lambda'} \sum_{i \in \mathbb{Z} \setminus \{0\}} V_f(i\delta).$$

Απόδειξη: Υπάρχει αντιστρέψιμος γραμμικός μετασχηματισμός T_0 του $\mathbb{R}^{n-1}$ τέτοιος ώστε $\Lambda' = T_0(\mathbb{Z}^{n-1})$. Τον επεκτείνουμε σε έναν $T \in GL(n)$, ορίζοντας $T(e_n) = e_n$. Παρατηρούμε ότι

$$V_f(\gamma) = (\det \Lambda') V_{f \circ T}(\gamma)$$

και

$$\sum_{x \in \Lambda_y, x_n \neq 0} f(x) = \sum_{x \in \langle \mathbb{Z}^{n-1}, T^{-1}y \rangle, x_n \neq 0} (f \circ T)(x)$$

όπου $\langle \mathbb{Z}^{n-1}, T^{-1}(y) \rangle$ το πλέγμα που παράγεται από τον $\mathbb{Z}^{n-1}$ και το $T^{-1}(y)$. Αν λοιπόν υποθέσουμε ότι το Λήμμα ισχύει στην περίπτωση $\Lambda' = \mathbb{Z}^{n-1}$, περνάμε στη γενική περίπτωση ως εξής: αν μάς δώσουν $f:\mathbb{R}^n \to \mathbb{R}$ συνεχή, με συμπαγή φορέα, βρίσκουμε $w \in \mathbb{R}^{n-1}$ τέτοιο ώστε

$$\sum_{x \in \langle \mathbb{Z}^{n-1}, (w, \delta) \rangle, x_n \neq 0} (f \circ T)(x) \leq \sum_{i \in \mathbb{Z} \setminus \{0\}} V_{f \circ T}(i\delta),$$

και θέτοντας $z = T_0(w)$ έχουμε

$$\begin{aligned} \sum_{x \in \Lambda_z, x_n \neq 0} f(x) &= \sum_{x \in \langle \mathbb{Z}^{n-1}, w \rangle, x_n \neq 0} (f \circ T)(x) \\ &\leq \sum_{i \in \mathbb{Z} \setminus \{0\}} V_{f \circ T}(i\delta) \\ &= \frac{1}{\det \Lambda'} \sum_{i \in \mathbb{Z} \setminus \{0\}} V_f(i\delta). \end{aligned}$$

Μπορούμε λοιπόν να υποθέσουμε ότι $\Lambda' = \mathbb{Z}^{n-1}$.

Ισχυρισμός: Ισχύει η ισότητα

$$\int_0^1 \dots \int_0^1 \left(\sum_{x\in\Lambda_y, x_n\neq 0} f(x) \right) dy_1 \dots dy_{n-1} = \sum_{i\in\mathbb{Z}\setminus\{0\}} V_f(i\delta).$$

Απόδειξη του ισχυρισμού: Έχουμε υποθέσει ότι

$$\Lambda' = \{(m_1, \dots, m_{n-1}) : m_1, \dots, m_{n-1} \in \mathbb{Z}\}.$$

Άρα,

$$\sum_{x\in\Lambda_y, x_n\neq 0} f(x) = \sum_{i\neq 0} \sum_{m_1,\dots,m_{n-1}\in\mathbb{Z}} f(m_1 + iy_1, \dots, m_{n-1} + iy_{n-1}, i\delta).$$

Κρατάμε σταθερό το $i \in \mathbb{Z}\setminus\{0\}$, και θεωρούμε το

$$J(i,\delta) = \int_0^1 \dots \int_0^1 \sum_{m_1,\dots,m_{n-1}\in\mathbb{Z}} f(m_1 + iy_1, \dots, m_{n-1} + iy_{n-1}, i\delta) dy_1 \dots dy_{n-1}.$$

Το ολοκλήρωμα αυτό υπάρχει, γιατί η f είναι συνεχής και έχει συμπαγή φορέα, οπότε το άθροισμα που ολοκληρώνουμε είναι ουσιαστικά άθροισμα πεπερασμένων το πλήθος συνεχών συναρτήσεων. Κάνοντας την αλλαγή μεταβλητής $z_k = iy_k$, $k = 1, \dots, n-1$, έχουμε

$$J(i,\delta) = \frac{1}{i^{n-1}} \int_0^i \dots \int_0^i \sum_{m_1,\dots,m_{n-1}\in\mathbb{Z}} f(m_1 + z_1, \dots, m_{n-1} + z_{n-1}, i\delta) dz_1 \dots dz_{n-1}.$$

Όμως, η προς ολοκλήρωση συνάρτηση είναι περιοδική ως προς κάθε μία από τις πρώτες $(n-1)$ συντεταγμένες, με περίοδο 1 (γιατί, τα $m_1, \dots, m_{n-1}$ διατρέχουν το $\mathbb{Z}$, και αθροίζουμε ως προς όλες τις επιλογές τους). Έπεται ότι

$$\begin{aligned} J(i,\delta) &= \int_0^1 \dots \int_0^1 \sum_{m_1,\dots,m_{n-1}\in\mathbb{Z}} f(m_1 + z_1, \dots, m_{n-1} + z_{n-1}, i\delta) dz_1 \dots dz_{n-1} \\ &= \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} f(z_1, \dots, z_{n-1}, i\delta) dz_1 \dots dz_{n-1} \\ &= V_f(i\delta). \end{aligned}$$

Αθροίζοντας ως προς $i \in \mathbb{Z}\setminus\{0\}$, παίρνουμε το ζητούμενο. $\square$

Από τον ισχυρισμό έπεται άμεσα ότι υπάρχουν $z_1, \dots, z_{n-1} \in [0,1]$ τέτοια ώστε

$$\sum_{x\in\Lambda_z, x_n\neq 0} f(x) \leq \sum_{i\in\mathbb{Z}\setminus\{0\}} V_f(i\delta),$$

και η απόδειξη του λήμματος είναι πλήρης, σύμφωνα με τις αρχικές μας παρατηρήσεις. $\square$

Λήμμα 5.3.2 *Έστω $g : \mathbb{R}^n \to \mathbb{R}$ Riemann-ολοκληρώσιμη συνάρτηση, με συμπαγή φορέα, και έστω $\varepsilon > 0$. Τότε, υπάρχει πλέγμα Λ στον $\mathbb{R}^n$, με ορίζουσα $\det \Lambda = 1$, τέτοιο ώστε*

$$\sum_{x\in\Lambda\setminus\{o\}} g(x) < \int_{\mathbb{R}^n} g(x)dx + \varepsilon.$$

Απόδειξη: Μπορούμε να βρούμε συνεχή $f : \mathbb{R}^n \to \mathbb{R}$ με συμπαγή φορέα, τέτοια ώστε: $f \geq g$ παντού, και

$$\int_{\mathbb{R}^n} f(x)dx < \int_{\mathbb{R}^n} g(x)dx + \frac{\varepsilon}{2}.$$

Ισχυρισμός: Αν το $\delta > 0$ είναι αρκετά μικρό, τότε

$$\delta\sum_{i\neq 0}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} f(x_1,\ldots,x_{n-1},i\delta)dx_1\ldots dx_{n-1} < \int_{\mathbb{R}^n} f(x)dx + \frac{\varepsilon}{2}.$$

Απόδειξη του ισχυρισμού: Υπάρχει κύβος $Q = [-M,M]^n$ τέτοιος ώστε $f(x) = 0$ αν $x \notin Q$. Η f είναι συνεχής στο Q, άρα ομοιόμορφα συνεχής. Υπάρχει λοιπόν $\delta_0 > 0$ τέτοιο ώστε: αν $0 < \delta < \delta_0$, τότε

$$\|x - x'\|_2 < \delta \Longrightarrow |f(x) - f(x')| < \frac{\varepsilon}{2(2M)^{n-1}(2M+2)}.$$

Έστω $0 < \delta < \min\{\delta_0, 1\}$. Θέτουμε $Q_1 = [-M,M]^{n-1} \subset \mathbb{R}^{n-1}$, και $k = [M/\delta] + 1$. Τότε,

$$\begin{aligned}\int_{\mathbb{R}^n} f(x)dx &= \int_Q f(x_1,\ldots,x_n)dx_1\ldots dx_n\\ &= \sum_{i=1}^{k}\int_{(i-1)\delta}^{i\delta}\int_{Q_1} f(x_1,\ldots,x_{n-1},x_n)dx_1\ldots dx_n\\ &+ \sum_{i=-k}^{-1}\int_{i\delta}^{(i+1)\delta}\int_{Q_1} f(x_1,\ldots,x_{n-1},x_n)dx_1\ldots dx_n,\end{aligned}$$

και

$$\begin{aligned}\delta\sum_{i\neq 0} V_f(i\delta) &= \delta\sum_{i\neq 0}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} f(x_1,\ldots,x_{n-1},i\delta)dx_1\ldots dx_{n-1}\\ &= \delta\sum_{i=1}^{k}\int_{Q_1} f(x_1,\ldots,x_{n-1},i\delta)dx_1\ldots dx_{n-1}\\ &+ \delta\sum_{i=-k}^{-1}\int_{Q_1} f(x_1,\ldots,x_{n-1},i\delta)dx_1\ldots dx_{n-1}\end{aligned}$$

$$\begin{aligned} &= \sum_{i=1}^{k} \int_{(i-1)\delta}^{i\delta} \int_{Q_1} f(x_1, \ldots, x_{n-1}, i\delta) dx_1 \ldots dx_n \\ &+ \sum_{i=-k}^{-1} \int_{i\delta}^{(i+1)\delta} \int_{Q_1} f(x_1, \ldots, x_{n-1}, i\delta) dx_1 \ldots dx_n. \end{aligned}$$

Αφαιρώντας, βλέπουμε ότι

$$\begin{aligned} \delta \quad &\cdot \quad \sum_{i\neq 0} V_f(i\delta) - \int_{\mathbb{R}^n} f(x)dx \\ &= \sum_{i=1}^{k} \int_{(i-1)\delta}^{i\delta} \int_{Q_1} [f(x_1, \ldots, x_{n-1}, i\delta) - f(x_1, \ldots, x_{n-1}, x_n)] dx_1 \ldots dx_{n-1} \\ &+ \sum_{i=-k}^{-1} \int_{i\delta}^{(i+1)\delta} \int_{Q_1} [f(x_1, \ldots, x_{n-1}, i\delta) - f(x_1, \ldots, x_{n-1}, x_n)] dx_1 \ldots dx_n \\ &< \frac{2k\delta\varepsilon(2M)^{n-1}}{2(2M)^{n-1}(2M+2)} < \frac{\varepsilon}{2}. \qquad \square \end{aligned}$$

Επιλέγουμε το $\delta < \delta_0$ να είναι τόσο μικρό ώστε, ταυτόχρονα, να ισχύει ότι $f(x) = 0$ αν $|x| \geq 1/\delta^{1/(n-1)}$. Θεωρούμε το πλέγμα

$$\Lambda' = \frac{1}{\delta^{1/(n-1)}} \mathbb{Z}^{n-1}$$

στον $\mathbb{R}^{n-1}$. Τότε, για κάθε $z = (z_1, \ldots, z_{n-1}) \in \mathbb{R}^{n-1}$, έχουμε $\det \Lambda_z = 1$.

Παρατηρούμε ότι $x_n \neq 0$ για κάθε $x \in \Lambda_z \setminus \{o\}$ με $f(x) \neq 0$. Από το Λήμμα 5.3.1, υπάρχει $z = (z_1, \ldots, z_{n-1})$ με την ιδιότητα

$$\begin{aligned} \sum_{x\in\Lambda_z\setminus\{o\}} f(x) &= \sum_{x\in\Lambda_z, x_n\neq 0} f(x) \\ &\leq \frac{1}{\det \Lambda'} \sum_{i\in\mathbb{Z}\setminus\{0\}} V_f(i\delta) \\ &= \delta \sum_{i\in\mathbb{Z}\setminus\{0\}} V_f(i\delta), \end{aligned}$$

και, χρησιμοποιώντας τον ισχυρισμό, συμπεραίνουμε ότι

$$\sum_{x\in\Lambda_z\setminus\{o\}} f(x) < \int_{\mathbb{R}^n} f(x)dx + \frac{\varepsilon}{2}.$$

Παίρνοντας υπ' όψιν τον τρόπο ορισμού της f, βλέπουμε ότι

$$\sum_{x\in\Lambda_z\setminus\{o\}} g(x) < \int_{\mathbb{R}^n} g(x)dx + \varepsilon.$$

Από την κατασκευή, $\det \Lambda_z = 1$. Άρα, παίρνοντας $\Lambda = \Lambda_z$ έχουμε αποδείξει το Λήμμα. □

Απόδειξη του Θεωρήματος Minkowski-Hlawka: Αρκεί να δείξουμε τη συνεπαγωγή

$$|K| < 2\zeta(n) \Longrightarrow \Delta(K) \leq 1.$$

Θεωρούμε τη συνάρτηση

$$g(x) = \sum_{i=1}^{\infty} \mu(i)\chi_K(ix),$$

όπου μ είναι η συνάρτηση του Möbius, η οποία ορίζεται ως εξής: $\mu(i) = 1$ αν $i = 1$, $\mu(i) = 0$ αν υπάρχει πρώτος p με $p^2|i$, και $\mu(i) = (-1)^k$ αν $i = p_1 \dots p_k$, όπου p_j διαφορετικοί ανά δύο πρώτοι.

Για κάθε πλέγμα Λ, ονομάζουμε ένα $x \in \Lambda\backslash\{o\}$ **πρωταρχικό για το** Λ, αν το ανοιχτό ευθύγραμμο τμήμα που συνδέει τα o και x δεν περιέχει σημείο του Λ. Τότε, αν M είναι το σύνολο των πρωταρχικών σημείων του Λ, έχουμε

$$\begin{aligned}
\sum_{x\in\Lambda\backslash\{o\}} g(x) &= \sum_{x\in M}\sum_{j=1}^{\infty} g(jx) \\
&= \sum_{x\in M}\sum_{j=1}^{\infty}\sum_{i=1}^{\infty} \mu(i)\chi_K(ijx) \\
&= \sum_{x\in M}\sum_{k=1}^{\infty} \chi_K(kx)\sum_{i|k}\mu(i) \\
&= \sum_{x\in M} \chi_K(x),
\end{aligned}$$

όπου χρησιμοποιήσαμε το γεγονός ότι

$$\sum_{i|k}\mu(k) = 0, \quad k \geq 2.$$

Η ταυτότητα αυτή είναι άμεση συνέπεια του ορισμού της μ: αν $k = p_1^{a_1}\dots p_s^{a_s}$, τότε οι μη μηδενικοί όροι στο παραπάνω άθροισμα προέρχονται μόνο από τους ελεύθερους τετραγώνων διαιρέτες του k. Πιό συγκεκριμένα,

$$\sum_{i|k}\mu(i) = \mu(1) + \binom{s}{1}(-1)^1 + \binom{s}{2}(-1)^2 + \dots \binom{s}{s}(-1)^s = (1 + (-1))^s = 0.$$

Το K είναι συμμετρικό, άρα το

$$\sum_{x\in\Lambda\backslash\{o\}} g(x) = \sum_{x\in M} \chi_K(x)$$

είναι **άρτιος** φυσικός ή 0. Από την άλλη πλευρά, από την υπόθεσή μας για τον όγκο του K,

$$\int_{\mathbb{R}^n} g(x)dx = \sum_{i=1}^{\infty} \mu(i) \int_{\mathbb{R}^n} \chi_K(ix)dx = \sum_{i=1}^{\infty} \mu(i) \frac{|K|}{i^n} = \frac{|K|}{\zeta(n)} < 2,$$

όπου χρησιμοποιήσαμε την

$$\int_{\mathbb{R}^n} \chi_K(ix)dx = \frac{1}{i^n} \int_{\mathbb{R}^n} \chi_K(y)dy = \frac{|K|}{i^n}, \quad i \in \mathbb{N},$$

και την ταυτότητα

$$\begin{aligned} \zeta(n) \sum_{i=1}^{\infty} \frac{\mu(i)}{i^n} &= \left(\sum_{k=1}^{n} \frac{1}{k^n} \right) \left(\sum_{i=1}^{\infty} \frac{\mu(i)}{i^n} \right) \\ &= \sum_{l=1}^{\infty} \sum_{k \cdot i = l} \frac{\mu(i)}{l^n} \\ &= \sum_{l=1}^{\infty} \frac{1}{l^n} \sum_{i|l} \mu(i) = \frac{1}{1^n} = 1. \end{aligned}$$

Από το Λήμμα του Hlawka, για κατάλληλα μικρό $\varepsilon > 0$, υπάρχει πλέγμα Λ του $\mathbb{R}^n$ με ορίζουσα $\det \Lambda = 1$, τέτοιο ώστε

$$\sum_{x \in M} \chi_K(x) = \sum_{x \in \Lambda \setminus \{o\}} g(x) < \int_{\mathbb{R}^n} g(x)dx + \varepsilon < 2,$$

το οποίο σημαίνει ότι $M \cap K = \emptyset$. Αφού το K δεν περιέχει πρωταρχικά σημεία του Λ, συμπεραίνουμε ότι $\Lambda \cap K = \{o\}$. Άρα,

$$\Delta(K) \leq \det \Lambda = 1. \quad \square$$

Κεφάλαιο 6

Packings της σφαίρας

6.1 Ορισμοί

Συμβολίζουμε με $\mathcal{E}_n$ την κλάση όλων των ελλειψοειδών του $\mathbb{R}^n$ που δεν περιέχουν στο εσωτερικό τους κανένα σημείο του $\mathbb{Z}^n \setminus \{o\}$. Το πρόβλημα που θα μάς απασχολήσει σε αυτό το Κεφάλαιο είναι να δοθούν ακριβείς εκτιμήσεις για την ποσότητα

$$\alpha_n = \sup\{|E| : E \in \mathcal{E}_n\}.$$

Δεν είναι δύσκολο να δεί κανείς ότι το πρόβλημα αυτό είναι ισοδύναμο με το πρόβλημα του υπολογισμού της κρίσιμης ορίζουσας $\Delta(D_n)$ της μπάλας (το οποίο συζητήσαμε για γενικό συμμετρικό κυρτό σώμα K στο προηγούμενο Κεφάλαιο).

Πρόταση 6.1.1 $\Delta(D_n)\alpha_n = \omega_n$.

Απόδειξη: Υπάρχει πλέγμα $\Lambda = T(\mathbb{Z}^n)$ το οποίο είναι D_n-αποδεκτό, και έχει ορίζουσα $\det \Lambda = \det T = \Delta(D_n)$. Τότε, το ελλειψοειδές $T^{-1}(D_n) \in \mathcal{E}_n$, άρα

$$\alpha_n \geq |T^{-1}(D_n)| = \frac{\omega_n}{\det T} = \frac{\omega_n}{\Delta(D_n)}.$$

Για την αντίστροφη ανισότητα, παρατηρούμε ότι αν $E = S(D_n)$ είναι ένα ελλειψοειδές που ικανοποιεί την $S(D_n) \cap \mathbb{Z}^n = \{o\}$, τότε το πλέγμα $\Lambda = S^{-1}(\mathbb{Z}^n)$ είναι D_n-αποδεκτό. Άρα,

$$|E| = \frac{\omega_n}{\det S^{-1}} = \frac{\omega_n}{\det \Lambda} \leq \frac{\omega_n}{\Delta(D_n)}.$$

Έπεται ότι

$$\alpha_n = \sup\{|E| : E \in \mathcal{E}_n\} \leq \frac{\omega_n}{\Delta(D_n)},$$

το οποίο ολοκληρώνει την απόδειξη. □

Μία έννοια που συνδέεται στενά με το πρόβλημα, είναι η έννοια του **packing** από μπάλες στον $\mathbb{R}^n$. Μία οικογένεια $P = \{x_i + rD_n : i \in I\}$ από μπάλες ακτίνας $r > 0$, λέγεται packing αν οι $x_i + rD_n$ έχουν ξένα εσωτερικά.

Ορίζουμε άνω και κάτω **πυκνότητα** του P ως εξής: για κάθε $R > 0$, θεωρούμε την RD_n, και τις $x_i + rD_n$ οι οποίες τέμνουν την RD_n. Αν $N(R)$ είναι το πλήθος των στοιχείων του $\{i \in I : (x_i + rD_n) \cap (RD_n) \neq \emptyset\}$, ορίζουμε

$$\overline{\delta}(P) = \limsup_{R\to\infty} \frac{N(R)\omega_n r^n}{\omega_n R^n}$$

και

$$\underline{\delta}(P) = \liminf_{R\to\infty} \frac{N(R)\omega_n r^n}{\omega_n R^n}.$$

Οι αριθμοί $\overline{\delta}(P)$ και $\underline{\delta}(P)$ είναι η άνω και κάτω πυκνότητα του P, αντίστοιχα. Αν $\overline{\delta}(P) = \underline{\delta}(P)$, τότε αυτή η κοινή τιμή είναι η πυκνότητα $\delta(P)$ του P.

Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$. Ένα **packing με κέντρα στο** Λ είναι ένα packing της μορφής

$$P = \{x + rD_n : x \in \Lambda\}.$$

Πρόταση 6.1.2 *Έστω $P = \{x + rD_n : x \in \Lambda\}$ ένα packing με κέντρα στο πλέγμα Λ. Τότε,*

$$\delta(P) = \frac{\omega_n r^n}{\det \Lambda}.$$

Απόδειξη: Έστω $R > 0$. Το πλήθος $N(R)$ των $x + rD_n$, $x \in \Lambda$, που τέμνουν την RD_n, ικανοποιεί την ανισότητα

$$|RD_n \cap \Lambda| \leq N(R) \leq |(R + r)D_n \cap \Lambda|.$$

Άρα,

$$\frac{|RD_n \cap \Lambda|}{|RD_n|} \leq \frac{N(R)}{|RD_n|} \leq \frac{|(R + r)D_n \cap \Lambda|}{|RD_n|}.$$

Παίρνοντας όριο καθώς $R \to \infty$, και χρησιμοποιώντας την Πρόταση 1.2.4, βλέπουμε ότι

$$\frac{1}{\det \Lambda} = \lim_{R\to\infty} \frac{N(R)}{\omega_n R^n}.$$

Άρα, υπάρχει το

$$\delta(P) = \lim_{R\to\infty} \frac{N(R)\omega_n r^n}{\omega_n R^n} = \frac{\omega_n r^n}{\det \Lambda}. \quad \square$$

Ορίζουμε δ_n το supremum των $\delta(P)$, όπου P packing με μπάλες ακτίνας 1 και κέντρα σε κάποιο πλέγμα Λ του $\mathbb{R}^n$. Τότε,

$$\delta_n = \sup_{\Lambda} \frac{\omega_n}{\det \Lambda},$$

όπου το sup είναι πάνω από όλα τα πλέγματα Λ για τα οποία η οικογένεια $P = \{x + D_n : x \in \Lambda\}$ είναι packing. Παρατηρούμε ότι ένα πλέγμα Λ επιδέχεται packing από μπάλες ακτίνας 1 αν και μόνο αν είναι $2D_n$-αποδεκτό. Άρα,

$$(*) \qquad \delta_n = \frac{\omega_n}{2^n \Delta(D_n)}.$$

Η $(*)$ και η Πρόταση 6.1.1 μάς δίνουν το εξής:

Θεώρημα 6.1.1 $\alpha_n = 2^n \delta_n$. □

6.2 Η μέθοδος του Blichfeldt

Στην προηγούμενη παράγραφο είδαμε ότι $\alpha_n = 2^n \delta_n$. Θα περιγράψουμε την μέθοδο του Blichfeldt [Bl2] για την εκτίμηση της δ_n από πάνω. Σε συνδυασμό με την παραπάνω ισότητα, το αποτέλεσμα του Blichfeldt δίνει το εξής:

Θεώρημα 6.2.1 *Για κάθε $n \in \mathbb{N}$, ισχύει η ανισότητα*

$$\alpha_n \leq \frac{n+2}{2} 2^{n/2}.$$

Η απόδειξη αυτής της ανισότητας βασίζεται σε δύο λήμματα.

Λήμμα 6.2.1 *Έστω $D : [0, +\infty) \to [0, +\infty)$ συνεχής συνάρτηση, και $t_0 > 0$ με την ιδιότητα: $D(t) = 0$, για κάθε $t > t_0$. Υποθέτουμε ότι για κάθε packing $P = \{x_i + D_n : i \in \mathbb{N}\}$ του $\mathbb{R}^n$ από μπάλες ακτίνας 1, και για κάθε $y \in \mathbb{R}^n$, ισχύει*

$$\sum_{i=1}^{\infty} D(\|y - x_i\|_2) \leq 1.$$

Τότε,

$$\delta_n \leq \frac{1}{n \int_0^{t_0} t^{n-1} D(t) dt}.$$

Απόδειξη: Έστω P ένα packing του $\mathbb{R}^n$ από μπάλες ακτίνας 1. Θεωρούμε τυχόν (μεγάλο) $R > 0$. Οι μπάλες του P που τέμνουν την RD_n είναι πεπερασμένες το πλήθος, και χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι είναι οι $x_i + D_n$, $i = 1, \ldots, N$.

Θεωρούμε την $(R+1)D_n$. Αφού $(x_i + D_n) \cap RD_n \neq \emptyset$, $i \leq N$, συμπεραίνουμε ότι

$$x_i \in (R+1)D_n, \quad i = 1, \ldots, N.$$

Επομένως, από την υπόθεσή μας ότι $D(t) = 0$ αν $t > t_0$, βλέπουμε ότι: για κάθε $i = 1, \ldots, N$, έχουμε $D(\|y - x_i\|_2) = 0$ αν $y \notin (R + t_0 + 1)D_n$. Δηλαδή,

$$\int_{\mathbb{R}^n} D(\|y - x_i\|_2)dy = \int_{(R+t_0+1)D_n} D(\|y - x_i\|_2)dy, \quad i = 1, \ldots, N.$$

Χρησιμοποιώντας και την $\sum_{i=1}^{\infty} D(\|y - x_i\|_2) \leq 1$, έχουμε

$$\begin{aligned} \omega_n(R + t_0 + 1)^n &= \int_{(R+t_0+1)D_n} 1dy \\ &\geq \int_{(R+t_0+1)D_n} \sum_{i=1}^{N} D(\|y - x_i\|_2)dy \\ &= \sum_{i=1}^{N} \int_{(R+t_0+1)D_n} D(\|y - x_i\|_2)dy \\ &= \sum_{i=1}^{N} \int_{\mathbb{R}^n} D(\|y - x_i\|_2)dy \\ &= N \int_{\mathbb{R}^n} D(\|w\|_2)dw. \end{aligned}$$

Υπολογίζουμε το τελευταίο ολοκλήρωμα σε πολικές συντεταγμένες: χρησιμοποιώντας το γεγονός ότι η $D(\|w\|_2)$ εξαρτάται μόνο από το μήκος του w, και μηδενίζεται αν $\|w\|_2 > t_0$, παίρνουμε

$$\int_{\mathbb{R}^n} D(\|w\|_2)dw = \int_{S^{n-1}} \int_0^{t_0} t^{n-1} D(t)dtd\theta = n\omega_n \int_0^{t_0} t^{n-1} D(t)dt,$$

γιατί το «εμβαδόν» της S^{n-1} είναι ίσο με $n\omega_n$. Συνδυάζοντας τα παραπάνω, παίρνουμε

$$(R + t_0 + 1)^n \geq Nn \int_0^{t_0} t^{n-1} D(t)dt.$$

Υποθέτουμε τώρα ότι το P έχει κέντρα σε ένα πλέγμα Λ. Τότε,

$$\begin{aligned} \delta(P) &= \lim_{R\to\infty} \frac{N(R)\omega_n}{\omega_n R^n} \leq \lim_{R\to\infty} \left(\frac{R + t_0 + 1}{R}\right)^n \frac{1}{n\int_0^{t_0} t^{n-1} D(t)dt} \\ &= \frac{1}{n\int_0^{t_0} t^{n-1} D(t)dt}. \end{aligned}$$

Από τον ορισμό του δ_n,

$$\delta_n \leq \frac{1}{n\int_0^{t_0} t^{n-1} D(t)dt}. \qquad \square$$

Ο Blichfeldt επέλεξε κατάλληλη συνάρτηση D, χρησιμοποιώντας την εξής παρατήρηση (ανισότητα του Blichfeldt):

Λήμμα 6.2.2 *Αν* $y, x_1, \ldots, x_m \in \mathbb{R}^n$, *τότε*

$$\sum_{i=1}^m \sum_{j=1}^m \|x_i - x_j\|_2^2 \leq 2m \sum_{i=1}^m \|y - x_i\|_2^2.$$

Απόδειξη: Παρατηρούμε πρώτα ότι αρκεί να αποδείξουμε την ανισότητα στην περίπτωση $y = 0$:

$$(*) \qquad \sum_{i=1}^m \sum_{j=1}^m \|x_i - x_j\|_2^2 \leq 2m \sum_{i=1}^m \|x_i\|_2^2.$$

(Κατόπιν εφαρμόζουμε αυτήν την ειδική περίπτωση για τα $o, y - x_1, \ldots, y - x_m$.)

Για την απόδειξη της $(*)$, γράφουμε

$$\begin{aligned} \sum_{i=1}^m \sum_{j=1}^m \|x_i - x_j\|_2^2 &= \sum_{i=1}^m \sum_{j=1}^m \left(\|x_i\|_2^2 - 2\langle x_i, x_j\rangle + \|x_j\|_2^2\right) \\ &= 2m \sum_{i=1}^m \|x_i\|_2^2 - 2\langle \sum_{i=1}^m x_i, \sum_{j=1}^m x_j\rangle \\ &\leq 2m \sum_{i=1}^m \|x_i\|_2^2. \quad \square \end{aligned}$$

Θεώρημα 6.2.2 $\delta_n \leq \frac{n+2}{2} 2^{-n/2}$.

Απόδειξη: Θεωρούμε τη συνάρτηση

$$D(t) = \begin{cases} 1 - \frac{t^2}{2} & , \quad 0 \leq t \leq \sqrt{2} \\ 0 & , \quad t > \sqrt{2}. \end{cases}$$

Έστω $P = \{x_i + D_n : i \in I\}$ ένα packing του $\mathbb{R}^n$. Για κάθε $y \in \mathbb{R}^n$, θεωρούμε τα x_i για τα οποία $\|y - x_i\|_2 \leq \sqrt{2}$. Είναι φανερό ότι το πλήθος τους είναι πεπερασμένο, μπορούμε λοιπόν να τα αριθμήσουμε σαν $x_1, \ldots, x_m$, όπου $m = m(y)$. Για όλα τα υπόλοιπα x_i, έχουμε $D(\|y - x_i\|_2) = 0$, από τον ορισμό της D. Άρα,

$$\sum_{i\in I} D(\|y - x_i\|_2) = \sum_{i=1}^m D(\|y - x_i\|_2) = \sum_{i=1}^m \left(1 - \frac{\|y - x_i\|_2^2}{2}\right) = m - \frac{1}{2}\sum_{i=1}^m \|y - x_i\|_2^2.$$

Από την ανισότητα του Blichfeldt, χρησιμοποιώντας και το γεγονός ότι $\|x_i - x_j\|_2 \geq 2$ αν $i \neq j$, παίρνουμε

$$\sum_{i=1}^m \|y - x_i\|_2^2 \geq \frac{1}{2m} \sum_{i=1}^m \sum_{i=1}^m \|x_i - x_j\|_2^2 \geq \frac{1}{2m} 4m(m-1) = 2(m-1).$$

Άρα,

$$\sum_{i\in I} D(\|y-x_i\|_2) \leq m - \frac{1}{2}2(m-1) = 1.$$

Υπολογίζουμε το

$$\int_0^{\sqrt{2}} t^{n-1}(1-t^2/2)dt = \left[\frac{t^n}{n} - \frac{t^{n+2}}{2(n+2)}\right]_0^{\sqrt{2}} = \frac{2^{n/2}}{n} - \frac{2^{n/2}}{n+2} = \frac{2}{n(n+2)}2^{n/2}.$$

Αφού η D ικανοποιεί τις υποθέσεις του Λήμματος 6.2.1, συμπεραίνουμε ότι

$$\delta_n \leq \frac{1}{n\int_0^{\sqrt{2}} t^{n-1}(1-t^2/2)dt} = \frac{n+2}{2}2^{-n/2}. \quad \square$$

Αφού $\alpha_n = 2^n\delta_n$, η απόδειξη του Θεωρήματος 6.2.1 είναι πλήρης.

6.3 Ελλειψοειδή χωρίς ακέραια σημεία

Σε αυτήν την παράγραφο εξετάζουμε το αντίστροφο πρόβλημα: να βρεθεί ελλειψοειδές με όσο γίνεται μεγαλύτερο όγκο, το οποίο δεν περιέχει ακέραια σημεία στο εσωτερικό του. Το καλύτερο γνωστό αποτέλεσμα οφείλεται στον K. Ball [Ba], και χρησιμοποιεί το Λήμμα του Bang [Ban]:

Λήμμα 6.3.1 *Έστω $x_1,\dots,x_m$ μοναδιαία διανύσματα στον $\mathbb{R}^n$, και $w_1,\dots,w_m$ θετικοί πραγματικοί αριθμοί. Υπάρχει επιλογή προσήμων $\varepsilon_1,\dots,\varepsilon_m \in \{-1,1\}$, τέτοια ώστε το $u=\sum_{i=1}^m \varepsilon_i w_i x_i$ να ικανοποιεί τις*

$$|\langle u, x_i\rangle| \geq w_i, \quad i=1,\dots,m.$$

Απόδειξη: Για κάθε $\varepsilon=(\varepsilon_1,\dots,\varepsilon_m)\in\{-1,1\}^m$, θέτουμε $u(\varepsilon)=\sum_{i=1}^m \varepsilon_i w_i x_i$. Επιλέγουμε εκείνο το $u=u(\varepsilon^*)$ που έχει το μεγαλύτερο μήκος (αν υπάρχουν περισσότερα από ένα τέτοια $u(\varepsilon)$, επιλέγουμε οποιοδήποτε από αυτά).

Για κάθε $j=1,\dots,m$, ορίζουμε

$$u_j = u(\varepsilon^*) - 2\varepsilon_j^* w_j x_j.$$

Κάθε u_j είναι της μορφής $u(\varepsilon)$, με $\varepsilon_i=\varepsilon_i^*$ αν $i\neq j$, και $\varepsilon_j = -\varepsilon_j^*$. Άρα,

$$\begin{aligned}\|u(\varepsilon^*)\|_2^2 &\geq \|u_j\|_2^2 = \|u(\varepsilon^*) - 2\varepsilon_j^* w_j x_j\|_2^2\\ &= \|u(\varepsilon^*)\|_2^2 - 4w_j\varepsilon_j^*\langle u(\varepsilon^*), x_j\rangle + 4w_j^2\|x_j\|_2^2.\end{aligned}$$

Έπεται ότι

$$|\langle u(\varepsilon^*), x_j\rangle| \geq \varepsilon_j^*\langle u(\varepsilon^*), x_j\rangle \geq \frac{4w_j^2\|x_j\|_2^2}{4w_j} = w_j,$$

για κάθε $j=1,\dots,m$. $\square$

Η ακριβής διατύπωση του θεωρήματος του Ball είναι η εξής:

Θεώρημα 6.3.1 *Για κάθε $\varepsilon > 0$ υπάρχει ελλειψοειδές E στον $\mathbb{R}^n$ που δεν περιέχει σημεία του $\mathbb{Z}^n \setminus \{o\}$, και έχει όγκο*

$$|E| > 2(n-1) - \varepsilon.$$

Απόδειξη: Θεωρούμε την κλάση όλων των ελλειψοειδών της μορφής

$$E_R = \{x \in \mathbb{R}^n : \langle u, x\rangle^2 + \|x\|_2^2 \leq R^2\}, \quad u \in \mathbb{R}^n, R > 0.$$

Για κάθε $R > 0$, προσπαθούμε αρχικά να βρούμε $u = u_R \in \mathbb{R}^n$, τέτοιο ώστε το E_R να μην περιέχει ακέραια σημεία εκτός από το o. Δηλαδή, ζητάμε για κάθε $z \in \mathbb{Z}^n \setminus \{o\}$ να ισχύει

$$\langle u, z\rangle^2 + \|z\|_2^2 \geq R^2.$$

Η ανισότητα αυτή ικανοποιείται προφανώς αν $\|z\|_2 \geq R$. Περιοριζόμαστε λοιπόν στα $0 < \|z\|_2 < R$, και ζητάμε

$$|\langle u, \frac{z}{\|z\|_2}\rangle| \geq \sqrt{\frac{R^2}{\|z\|_2^2} - 1}.$$

Θέτουμε $w_z = \sqrt{(R/\|z\|_2)^2 - 1}$, κρατάμε ένα μόνο $\tilde{z}$ από τα $\pm z$ για κάθε $0 < \|z\|_2 < R$, και εφαρμόζουμε το Λήμμα του Bang: υπάρχουν $\varepsilon_{\tilde{z}} \in \{-1, 1\}$, τέτοια ώστε

$$|\langle \sum_{\tilde{z}} \varepsilon_{\tilde{z}} w_{\tilde{z}} \frac{\tilde{z}}{\|\tilde{z}\|_2}, \frac{\tilde{z}}{\|\tilde{z}\|_2}\rangle \geq w_{\tilde{z}}, \quad 0 < \|z\|_2 < R.$$

Ισοδύναμα, υπάρχουν $\varepsilon_z \in \{-1, 1\}$, τέτοια ώστε το διάνυσμα

$$u = u(R) = \frac{1}{2} \sum_{0 < \|z\|_2 < R} \varepsilon_z w_z \frac{z}{\|z\|_2}$$

να ικανοποιεί τις

$$|\langle u, \frac{z}{\|z\|_2}\rangle| \geq w_z, \quad 0 < \|z\|_2 < R.$$

Γι' αυτήν την επιλογή του u έχουμε εξασφαλίσει ότι $E_R \cap \mathbb{Z}^n = \{o\}$. Για τον υπολογισμό του όγκου του E_R, χρειαζόμαστε μία εκτίμηση για το μήκος του u. Για το σκοπό αυτό, θεωρούμε το μοναδιαίο διάνυσμα θ στη διεύθυνση του u. Αν $K(R)$ είναι το μήκος του u, έχουμε

$$\begin{aligned} K(R) = \|u\|_2 = \langle u, \theta\rangle &= \frac{1}{2} \sum_{0 < \|z\|_2 < R} \varepsilon_z \frac{\langle z, \theta\rangle}{\|z\|_2} w_z \\ &\leq \frac{1}{2} \sum_{0 < \|z\|_2 < R} \frac{|\langle z, \theta\rangle|}{\|z\|_2} \sqrt{\frac{R^2}{\|z\|_2^2} - 1} =: \tilde{K}(R). \end{aligned}$$

Θέτουμε $v = z/R$. Τότε,

$$\tilde{K}(R) = \frac{1}{2} \sum_{v \in \frac{1}{R}\mathbb{Z}^n \cap D_n \setminus \{o\}} \frac{|\langle v, \theta \rangle|}{\|v\|_2} \sqrt{\frac{1}{\|v\|_2^2} - 1}.$$

Καθώς το $R \to \infty$, το παραπάνω άθροισμα (πολλαπλασιασμένο επί R^{-n}) είναι ένα άθροισμα Riemann για το

$$\frac{1}{2} \int_{D_n} \frac{|\langle v, \theta \rangle|}{\|v\|_2} \sqrt{\frac{1}{\|v\|_2^2} - 1} dv.$$

Δηλαδή,

$$\lim_{R \to \infty} \frac{\tilde{K}(R)}{\omega_n R^n} = \frac{1}{2\omega_n} \int_{D_n} \frac{|\langle v, \theta \rangle|}{\|v\|_2} \sqrt{\frac{1}{\|v\|_2^2} - 1} dv.$$

Για τον υπολογισμό του τελευταίου ολοκληρώματος, παίρνουμε πολικές συντεταγμένες:

$$\begin{aligned} \lim_{R \to \infty} \frac{\tilde{K}(R)}{\omega_n R^n} &= \frac{n\omega_n}{2\omega_n} \int_{S^{n-1}} \int_0^1 |\langle \phi, \theta \rangle| \rho^{n-1} \sqrt{\frac{1}{\rho^2} - 1} d\rho \sigma(d\phi) \\ &= \frac{n}{2} \int_{S^{n-1}} |\langle \phi, \theta \rangle| \sigma(d\phi) \cdot \int_0^1 \rho^{n-2} \sqrt{1 - \rho^2} d\rho. \end{aligned}$$

Παρατηρούμε ότι το πρώτο ολοκλήρωμα είναι ανεξάρτητο του $\theta \in S^{n-1}$. Μπορούμε λοιπόν να υποθέσουμε ότι $\theta = e_1$. Γράφουμε

$$\int_{D_n} |z_1| dz = n\omega_n \int_{S^{n-1}} |\langle \phi, e_1 \rangle| \sigma(d\phi) \cdot \int_0^1 \rho^n d\rho = \frac{n\omega_n}{n+1} \int_{S^{n-1}} |\langle \phi, e_1 \rangle| \sigma(d\phi),$$

και

$$\int_{D_n} |z_1| dz = 2 \int_0^1 \omega_{n-1} t (1 - t^2)^{(n-1)/2} dt,$$

οπότε,

$$\begin{aligned} \int_{S^{n-1}} |\langle \phi, \theta \rangle| \sigma(d\phi) &= \frac{2\omega_{n-1} \int_0^1 t(1-t^2)^{(n-1)/2} dt}{(n\omega_n)/(n+1)} \\ &= \frac{2(n+1)\omega_{n-1}}{n\omega_n} \left[-\frac{1}{n+1} (1 - t^2)^{(n+1)/2} \right]_0^1 \\ &= \frac{2\omega_{n-1}}{n\omega_n}. \end{aligned}$$

Τέλος,

$$\begin{aligned} \int_0^1 \rho^{n-2} \sqrt{1 - \rho^2} d\rho &= \frac{1}{2} \int_0^1 t^{\frac{n-1}{2} - 1} (1 - t)^{\frac{3}{2} - 1} dt \\ &= \frac{\Gamma((n-1)/2)\Gamma(3/2)}{2\Gamma((n+2)/2)}. \end{aligned}$$

Παίρνοντας υπ' όψιν την $\omega_k = \pi^{k/2}/\Gamma((k/2)+1)$, καταλήγουμε στην

$$\begin{aligned}\lim_{R\to\infty}\frac{\tilde{K}(R)}{\omega_n R^n} &= \frac{2\omega_{n-1}}{n\omega_n}\frac{\Gamma(\frac{n-1}{2})\frac{\sqrt{\pi}}{2}}{\Gamma(\frac{n}{2})}\\ &= \frac{2}{n}\frac{\pi^{(n-1)/2}\Gamma(\frac{n}{2}+1)}{\pi^{n/2}\Gamma(\frac{n-1}{2}+1)}\frac{\Gamma(\frac{n-1}{2})\frac{\sqrt{\pi}}{2}}{2\Gamma(\frac{n}{2})}\\ &= \frac{1}{2(n-1)}.\end{aligned}$$

Αυτό σημαίνει ότι, για μεγάλα R,

$$\frac{\omega_n R^n}{\tilde{K}(R)} > 2(n-1) - \frac{\varepsilon}{2}.$$

Παρατηρούμε επίσης ότι $\lim \tilde{K}(R) = +\infty$, αλλιώς θα είχαμε

$$\lim_{R\to\infty}\frac{\tilde{K}(R)}{\omega_n R^n} = 0.$$

Από την άλλη πλευρά, ο όγκος του E_R είναι ίσος με τον όγκο του

$$E_R' = \{x \in \mathbb{R}^n : \langle K(R)e_1, x\rangle^2 + \|x\|_2^2 \leq R^2\},$$

ο οποίος υπολογίζεται εύκολα: το E_R' έχει $(n-1)$ ημιάξονες ίσους με R, και έναν ίσο με $R/\sqrt{1+K^2(R)}$. Άρα,

$$|E_R| = \frac{\omega_n R^n}{\sqrt{1+K^2(R)}} \geq \frac{\omega_n R^n}{\sqrt{1+\tilde{K}^2(R)}},$$

το οποίο για μεγάλα R είναι μεγαλύτερο από

$$\frac{\omega_n R^n}{\tilde{K}(R)} - \frac{\varepsilon}{2} > 2(n-1) - \varepsilon.$$

Έτσι, έχουμε αποδείξει ότι υπάρχουν ελλειψοειδή χωρίς μη τετριμμένα ακέραια σημεία, τα οποία έχουν όγκο οσοδήποτε κοντά στο $2(n-1)$. □

Άμεση συνέπεια είναι το ακόλουθο κάτω φράγμα για το α_n:

Θεώρημα 6.3.2 *Για κάθε $n \in \mathbb{N}$, $\alpha_n \geq 2(n-1)$.* □

Παρατηρήσεις (α) Μελετώντας μόνο τα πρωταρχικά σημεία του $\mathbb{Z}^n$ και χρησιμοποιώντας τη συνάρτηση του Möbius όπως στην απόδειξη του Θεωρήματος Minkowski-Hlawka, μπορεί κανείς να αποδείξει κάτι λίγο ισχυρότερο:

$$\alpha_n \geq 2(n-1)\zeta(n).$$

(β) Στην κατεύθυνση του Θεωρήματος του Blichfeldt, το καλύτερο γνωστό αποτέλεσμα είναι αυτό των Kabatjanskii και Levenstein [KL]:

$$\alpha_n \leq (1.32)^n \simeq 2^{[0.401+o_n(1)]n}.$$

Κεφάλαιο 7

Ανηγμένες βάσεις

7.1 Το πρόβλημα

Στην απόδειξη του Θεωρήματος Επιλογής του Mahler, χρησιμοποιήσαμε το εξής θεώρημα:

Θεώρημα 7.1.1 *Για κάθε $n \in \mathbb{N}$ υπάρχει σταθερά $C(n) > 0$ που ικανοποιεί το εξής: Αν Λ είναι ένα πλέγμα στον $\mathbb{R}^n$, τότε υπάρχει βάση $A = \{u_1, \ldots, u_n\}$ του Λ με την ιδιότητα*

$$\prod_{i=1}^{n} \|u_i\|_2 \leq C(n) \det \Lambda.$$

Τέτοιες βάσεις ονομάζονται **ανηγμένες**. Το γενικό πρόβλημα της «αναγωγής» διατυπώνεται ως εξής: Δίνεται ένα πλέγμα Λ στον $\mathbb{R}^n$, και ζητάμε έναν αλγόριθμο ο οποίος να προσδιορίζει μία βάση $\{u_1, \ldots, u_n\}$ του Λ (ανηγμένη βάση), η οποία να έχει «καλές» γεωμετρικές ή αριθμητικές ιδιότητες.

Το πρόβλημα αυτό απασχόλησε τους Lagrange, Seeber, Gauss, Dirichlet, Hermite, Korkin και Zolotarev, και άλλους. Συνήθως η προσπάθεια ήταν να βρεθεί βάση του Λ η οποία να ικανοποιεί φράγμα της μορφής

$$\prod_{i=1}^{n} \|u_i\|_2 \leq C(n) \det \Lambda,$$

για μία όσο γίνεται καλύτερη σταθερά $C(n)$. Αξίζει να αναφέρουμε δύο τέτοιους «αλγόριθμους αναγωγής»:

(α) **Αναγωγή κατά Minkowski**. Παίρνουμε σαν u_1 το διάνυσμα $u \in \Lambda \setminus \{o\}$ που έχει το μικρότερο μήκος:

$$\|u_1\|_2 = \min\{\|u\|_2 : u \in \Lambda \setminus \{o\}\}.$$

Αν τα $u_1, \ldots, u_k$ έχουν επιλεγεί, το u_{k+1} επιλέγεται έτσι ώστε το $\{u_1, \ldots, u_{k+1}\}$ να είναι πρωταρχικό σύνολο (βλέπε Κεφάλαιο 1), και το u_{k+1} να έχει το μικρότερο δυνατό μήκος. Με αυτόν τον τρόπο ορισμού των u_i, μπορεί κανείς να αποδείξει ότι

$$C(n) \leq \left(\frac{4}{\pi}\right)^{n/2} \Gamma\left(\frac{n+1}{2}\right) \left(\frac{3}{2}\right)^{\frac{(n-1)(n-2)}{2}}.$$

(β) **Αναγωγή κατά Korkin-Zolotarev**. Όπως πρίν, u_1 είναι μη μηδενικό διάνυσμα του Λ που έχει ελάχιστο μήκος. Αν τα $u_1, \ldots, u_k$ έχουν επιλεγεί, το u_{k+1} επιλέγεται έτσι ώστε να ελαχιστοποιεί την προβολή στον $\langle u_1, \ldots, u_k\rangle^{\perp}$ ανάμεσα σε όλα τα $v \in \Lambda$ για τα οποία το $\{u_1, \ldots, u_k, v\}$ είναι πρωταρχικό σύνολο. Ο Schnorr [Sc] απέδειξε ότι, σε αυτήν την περίπτωση,

$$C(n) \leq n^n,$$

το οποίο είναι και το καλύτερο αποτέλεσμα για την $C(n)$ (πάνω από όλες τις γνωστές μεθόδους αναγωγής).

Δεν είναι γνωστό αν ο αλγόριθμος των Korkin και Zolotarev [KZ] εκτελείται σε πολυωνυμικό χρόνο. Στην επόμενη παραγραφο θα παρουσιάσουμε τον αλγόριθμο των Lenstra, Lenstra και Lovász: ο αλγόριθμος αυτός ξεκινάει με τυχούσα βάση του πλέγματος και την μετασχηματίζει σε ανηγμένη. Δεν δίνει τόσο ισχυρή εκτίμηση για την $C(n)$, είναι όμως πολύ χρήσιμος στις εφαρμογές, γιατί απαιτεί $O(n^4 s)$ αριθμητικές πράξεις, όπου s το μέγιστο μήκος (σε ψηφία) των συντεταγμένων των διανυσμάτων της αρχικής βάσης.

7.2 Ο αλγόριθμος των Lenstra, Lenstra και Lovász

Σε αυτήν την παράγραφο παρουσιάζουμε τον αλγόριθμο αναγωγής των Lenstra, Lenstra και Lovasz [LLL]. Για την περιγραφή του αλγορίθμου θα χρειαστούμε την ορθογωνιοποίηση Gram-Schmidt:

Έστω $u_1, \ldots, u_n$ γραμμικώς ανεξάρτητα διανύσματα στον $\mathbb{R}^n$. Ορίζουμε ορθογώνια διανύσματα $w_1, \ldots, w_n$ αναδρομικά, ως εξής: Θέτουμε $w_1 = u_1$, και

$$(*) \qquad w_k = u_k - \sum_{j=1}^{k-1} \frac{\langle u_k, w_j\rangle}{\langle w_j, w_j\rangle} w_j, \quad k = 2, \ldots, n.$$

Εύκολα ελέγχουμε ότι τα $w_1, \ldots, w_n$ είναι ανά δύο κάθετα, και

$$\langle w_1, \ldots, w_k\rangle = \langle u_1, \ldots, u_k\rangle, \quad k = 1, \ldots, n.$$

Ειδικότερα, κάθε u_i γράφεται στη μορφή

$$u_i = w_i + \sum_{j=1}^{i-1} a_{ij} w_j$$

για κάποιους $a_{ij} \in \mathbb{R}$, $j = 1, \ldots, i-1$.

Παρατηρήσεις (α) Τα παραλληλεπίπεδα που ορίζονται από τα $\{u_1, \ldots, u_n\}$ και $\{w_1, \ldots, w_n\}$ έχουν τον ίδιο όγκο:

$$|\det(u_1, \ldots, u_n)| = |\det(w_1, \ldots, w_n)| = \prod_{j=1}^{n} \|w_j\|_2.$$

(β) Αν $j < i$ και $t \in \mathbb{R}$, τότε τα διανύσματα $u_1, \ldots, u_{i-1}, u_i - tu_j, \ldots, u_n$ είναι γραμμικώς ανεξάρτητα, και το σύνολο διανυσμάτων που προκύπτει με ορθογωνιοποίηση Gram-Schmidt από αυτά, είναι πάλι το $\{w_1, \ldots, w_n\}$.
(γ) Αν αντιμεταθέσουμε τα u_i, u_{i+1}, αν δηλαδή θεωρήσουμε το σύνολο διανυσμάτων

$$u_1' = u_1, \ldots, u_{i-1}' = u_{i-1}, u_i' = u_{i+1}, u_{i+1}' = u_i, \ldots, u_n' = u_n,$$

τότε το σύνολο διανυσμάτων $\{w_1', \ldots, w_n'\}$ που προκύπτει με την ορθογωνιοποίηση Gram-Schmidt από τα u_j' ικανοποιεί τις

$$w_1' = w_1, \ldots, w_{i-1}' = w_{i-1}, w_{i+2}' = w_{i+2}, \ldots, w_n' = w_n.$$

Δηλαδή, αν κάποια από τα w_j μεταβληθούν, αυτά θα είναι μόνο τα w_i, w_{i+1}.

Οι ισχυρισμοί (α)-(γ) προκύπτουν άμεσα από την $(*)$.

Ορισμός Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, $\{u_1, \ldots, u_n\}$ βάση του Λ, και $\{w_1, \ldots, w_n\}$ η ορθογωνιοποίηση Gram-Schmidt της βάσης. Για κάθε $u \in \mathbb{R}^n$, γράφουμε $u(i)$ για την ορθογώνια προβολή του u στον υπόχωρο $\langle w_j : j \geq i \rangle$. Ειδικότερα, $u_i(i) = w_i$, $i = 1, \ldots, n$.

Λέμε ότι η βάση $\{u_1, \ldots, u_n\}$ είναι **LLL-ανηγμένη** αν ικανοποιεί τα εξής:
(α) Για κάθε $i \leq n$, στην ανάλυση

$$u_i = w_i + \sum_{j=1}^{i-1} a_{ij} w_j$$

του u_i έχουμε $|a_{ij}| \leq 1/2$, $j = 1, \ldots, i-1$.
(β) Για κάθε $i = 1, \ldots, n$,

$$\|u_i(i)\|_2^2 = \|w_i\|_2^2 \leq \frac{4}{3}\|u_{i+1}(i)\|_2^2 = \frac{4}{3}\|w_{i+1} + a_{i+1,i}w_i\|_2^2.$$

Θεώρημα 7.2.1 *Κάθε πλέγμα Λ στον $\mathbb{R}^n$ έχει μία LLL-ανηγμένη βάση.*

Απόδειξη: Ξεκινάμε με τυχούσα βάση $\{u_1, \ldots, u_n\}$ του Λ, και εκτελούμε τα εξής βήματα:

Βήμα 1: Θεωρούμε την ορθογωνιοποίηση Gram-Schmidt $\{w_1, \ldots, w_n\}$ και ελέγχουμε αν ισχύει η συνθήκη (α).

Αν υπάρχουν συντελεστές a_{ij} με $|a_{ij}| > 1/2$ στην $(*)$, επιλέγουμε ζευγάρι (i,j) με $|a_{ij}| > 1/2$ και το j μέγιστο. Θεωρούμε τον πλησιέστερο προς τον a_{ij} ακέραιο t_{ij}, και τροποποιούμε τη βάση, παίρνοντας τα διανύσματα

$$u_1, \ldots, u_{i-1}, u_i' = u_i - t_{ij}u_j, u_{i+1}, \ldots, u_n.$$

Η ορθογωνιοποίηση των u_j' είναι τα w_j, και τώρα

$$u_i' = w_i + \sum_{j=1}^{i-1} a_{ij}' w_j,$$

με $a_{ij}' = a_{ij} - t_{ij}$, δηλαδή $|a_{ij}'| \leq 1/2$. Επαναλαμβάνοντας αυτήν τη διαδικασία το πολύ $\binom{n}{2}$ φορές, παίρνουμε μία νέα βάση $\{u_1, \ldots, u_n\}$ του Λ, η ορθογωνιοποίηση της οποίας ικανοποιεί το (α).

Βήμα 2: Έστω $i \leq n$ (το ελάχιστο δυνατό) για το οποίο δεν ικανοποιείται η συνθήκη (β). Μεταβάλλουμε τη βάση αντιμεταθέτοντας τα u_i και u_{i+1}:

$$u_1' = u_1, \ldots, u_{i-1}' = u_{i-1}, u_i' = u_{i+1}, u_{i+1}' = u_i, u_{i+2}' = u_{i+2}, \ldots, u_n' = u_n.$$

Τότε, για την ορθογωνιοποίηση w_j' των u_j' έχουμε

$$u_i'(i) = u_{i+1}(i), \quad u_{i+1}'(i) = u_i(i),$$

δηλαδή ικανοποιείται η (β).

Συνεχίζουμε την εκτέλεση αυτών των δύο βημάτων όσο είναι δυνατόν. Αν κάποια στιγμή δεν μπορούμε να εκτελέσουμε κανένα από τα δύο, τότε αυτό σημαίνει ότι έχουμε καταλήξει σε LLL-ανηγμένη βάση του Λ. Αυτό που πρέπει να δείξουμε είναι ότι ο αλγόριθμος που περιγράψαμε θα τερματίσει οπωσδήποτε.

Για το σκοπό αυτό, θεωρούμε την ποσότητα

$$D(u_1, \ldots, u_n) = \prod_{i=1}^{n} \|w_i\|_2^{n-i+1},$$

όπου $\{w_1, \ldots, w_n\}$ είναι η ορθογωνιοποίηση της βάσης στην οποία βρισκόμαστε τη δεδομένη στιγμή. Το Βήμα 1 δεν μεταβάλλει την ποσότητα $D(u_1, \ldots, u_n)$ γιατί αφήνει αναλλοίωτη την ορθογωνιοποίηση της βάσης. Αρκεί λοιπόν να εξετάσουμε τη μεταβολή που προκαλεί η εκτέλεση του Βήματος 2. Το βήμα αυτό μεταβάλλει τα διανύσματα w_i, w_{i+1}, άρα

$$\frac{D(u_1', \ldots, u_n')}{D(u_1, \ldots, u_n)} = \frac{\|w_i'\|_2^{n-i+1}\|w_{i+1}'\|_2^{n-i}}{\|w_i\|_2^{n-i+1}\|w_{i+1}\|_2^{n-i}}.$$

Ισχυρισμός: Ισχύουν οι ανισότητες

$$\frac{\|w_i'\|_2}{\|w_i\|_2} = \frac{\|w_{i+1}\|_2}{\|w_{i+1}'\|_2} < \frac{\sqrt{3}}{2}.$$

Απόδειξη του ισχυρισμού: Για την πρώτη ανισότητα παρατηρούμε ότι, αφού εκτελούμε το Βήμα 2, έχουμε

$$\|u_i(i)\|_2^2 = \|w_i\|_2^2 > \frac{4}{3}\|u_{i+1}(i)\|_2^2 = \frac{4}{3}\|w_{i+1} + a_{i+1,i}w_i\|_2^2.$$

Με την αντιμετάθεση όμως των u_i, u_{i+1}, θα έχουμε $w_i' = u_{i+1}'(i+1) = u_i(i+1)$, άρα

$$\|w_i'\|_2^2 = \|u_{i+1}'(i+1)\|_2^2 = \|u_i(i+1)\|_2^2 < \frac{3}{4}\|w_i\|_2^2.$$

Για τη δεύτερη ανισότητα, θεωρούμε το διδιάστατο υπόχωρο $H = \langle w_i, w_{i+1}\rangle$. Παρατηρούμε ότι τα διανύσματα $w_i = u_i(i) = u_{i+1}'(i)$, w_{i+1}, $w_i' = u_{i+1}(i)$, και w_{i+1}' ανήκουν στον H. Τα ορθογώνια τρίγωνα $ow_{i+1}w_i'$ και ow_iw_{i+1}' είναι όμοια, άρα

$$\frac{\|w_{i+1}'\|_2}{\|w_i\|_2} = \frac{\|w_{i+1}\|_2}{\|w_i'\|_2},$$

απ' όπου έπεται ότι

$$\frac{\|w_{i+1}'\|_2}{\|w_{i+1}\|_2} = \frac{\|w_i\|_2}{\|w_i'\|_2}. \quad \square$$

Χρησιμοποιώντας τον ισχυρισμό, βλέπουμε ότι

$$\frac{D(u_1',\dots,u_n')}{D(u_1,\dots,u_n)} = \frac{\|w_i'\|_2^{n-i+1}\|w_{i+1}'\|_2^{n-i}}{\|w_i\|_2^{n-i+1}\|w_{i+1}\|_2^{n-i}} = \frac{\|w_i'\|_2}{\|w_i\|_2} < \frac{\sqrt{3}}{2},$$

δηλαδή, κάθε φορά που εκτελούμε το Βήμα 2, η $D(u_1,\dots,u_n)$ μειώνεται «γεωμετρικά».

Ισχυρισμός: Θέτουμε $\lambda = \min\{\|u\|_2 : u \in \Lambda\setminus\{o\}\}$. Σε κάθε βήμα, ισχύει η ανισότητα

$$D(u_1,\dots,u_n) \geq c,$$

όπου $c = c(\lambda, n) > 0$.

Απόδειξη του ισχυρισμού: Έστω Λ_k το πλέγμα που παράγεται από τα $u_1,\dots,u_k$. Η μπάλα ακτίνας λ στον υπόχωρο $\langle u_1,\dots,u_k\rangle$ δεν περιέχει μη μηδενικό σημείο του Λ_k, οπότε το πρώτο θεώρημα του Minkowski μάς δίνει

$$\omega_k\lambda^k \leq 2^k \det\Lambda_k = 2^k\prod_{i=1}^k \|w_i\|_2.$$

Πολλαπλασιάζοντας κατά μέλη, παίρνουμε

$$\begin{aligned} D(u_1,\dots,u_n) &= \prod_{i=1}^n \|w_i\|_2^{n-i+1} \\ &= \prod_{k=1}^n \det\Lambda_k \end{aligned}$$

$$\begin{aligned} &\geq \prod_{k=1}^{n} \frac{\omega_k \lambda^k}{2^k} \\ &= \left(\frac{\lambda}{2}\right)^{n(n+1)/2} \prod_{k=1}^{n} \omega_k. \quad \square \end{aligned}$$

Αυτό σημαίνει ότι δεν μπορεί να συμβεί επ' άπειρον επανάληψη του Βήματος 2. Αν D_0 είναι η αρχική τιμή της $D(u_1, \ldots, u_n)$, τότε μετά από m επαναλήψεις του Βήματος 2, θα έχουμε

$$D(u_1, \ldots, u_n) < D_0 \left(\frac{\sqrt{3}}{2}\right)^m < c$$

αν το m υπερβεί κάποιο m_0. Δεδομένου ότι έχουμε και ένα άνω φράγμα για το πλήθος των αλλαγών βάσης σε κάθε εφαρμογή του Βήματος 1, μπορούμε να δώσουμε άνω φράγμα για το πλήθος των αλλαγών βάσης που απαιτούνται για τον τερματισμό του αλγορίθμου. Αυτό ολοκληρώνει την απόδειξη του θεωρήματος. $\square$

Δείχνουμε τώρα ότι κάθε LLL-ανηγμένη βάση ικανοποιεί ανισότητα της μορφής

$$\prod_{i=1}^{n} \|u_i\|_2 \leq C(n) \det \Lambda.$$

Θα χρειαστούμε ένα λήμμα:

Λήμμα 7.2.1 *Έστω Λ ένα πλέγμα στον $\mathbb{R}^n$, $\{u_1, \ldots, u_n\}$ τυχούσα βάση του Λ, και $\{w_1, \ldots, w_n\}$ η ορθογωνιοποίηση Gram-Schmidt της βάσης. Τότε,*

$$\min\{\|u\| : u \in \Lambda \backslash \{o\}\} \geq \min\{\|w_1\|_2, \ldots, \|w_n\|_2\}.$$

Απόδειξη: Έστω $u \in \Lambda \backslash \{o\}$. Το u γράφεται στη μορφή

$$u = \sum_{i=1}^{k} \lambda_i u_i$$

όπου $\lambda_k \in \mathbb{Z} \backslash \{0\}$ και $k \leq n$. Γνωρίζουμε ότι

$$u_i = w_i + \sum_{j=1}^{i-1} a_{ij} w_j, \quad i \leq n,$$

άρα

$$u = \sum_{i=1}^{k} \beta_i w_i,$$

και $\beta_k \in \mathbb{Z}$, $\beta_k \neq 0$. Από την καθετότητα των w_i παίρνουμε

$$\|u\|_2^2 = \beta_1^2 \|w_1\|_2^2 + \ldots + \beta_k \|w_k\|_2^2 \geq \|w_k\|_2^2,$$

δηλαδή,

$$\|u\|_2 \geq \min\{\|w_1\|_2, \ldots, \|w_n\|_2\}. \quad \square$$

Θεώρημα 7.2.2 *Έστω Λ πλέγμα στον $\mathbb{R}^n$, και $\{u_1, \ldots, u_n\}$ μία LLL-ανηγμένη βάση του Λ. Τότε,*

(α) $\|u_1\|_2 \leq 2^{(n-1)/2} \min\{\|u\|_2 : u \in \Lambda \setminus \{o\}\}$.

(β) $\|u_1\|_2 \leq 2^{(n-1)/4} (\det \Lambda)^{1/n}$.

(γ) $\|u_1\|_2 \ldots \|u_n\|_2 \leq 2^{\frac{1}{2}\binom{n}{2}} \det \Lambda$.

Απόδειξη: (α) Θα δείξουμε ότι

$$(*) \qquad \|u_1\|_2 \leq 2^{(i-1)/2} \|w_i\|_2, \quad i = 1, \ldots, n.$$

Τότε,

$$\|u_1\|_2 \leq \min\{2^{(i-1)/2} \|w_i\|_2, i \leq n\} \leq 2^{(n-1)/2} \min\{\|w_i\|_2, i \leq n\},$$

και ο ισχυρισμός έπεται από το Λήμμα 7.2.1. Για την απόδειξη της $(*)$, παρατηρούμε ότι η βάση μας ικανοποιεί τις συνθήκες (α) και (β) του ορισμού της LLL-ανηγμένης βάσης, άρα

$$\begin{aligned} \|w_i\|_2^2 &\leq \frac{4}{3} \|w_{i+1} + a_{i+1,i} w_i\|_2^2 \\ &= \frac{4}{3} \|w_{i+1}\|_2^2 + \frac{4}{3} a_{i+1,i}^2 \|w_i\|_2^2 \\ &\leq \frac{4}{3} \|w_{i+1}\|_2^2 + \frac{1}{3} \|w_i\|_2^2, \end{aligned}$$

επομένως, $\|w_{i+1}\|_2^2 \geq (1/2) \|w_i\|_2^2$. Πολλαπλασιάζοντας κατά μέλη και παίρνοντας υπ' όψιν την $w_1 = u_1$, παίρνουμε

$$(**) \qquad \|w_i\|_2^2 \geq 2^{1-i} \|w_1\|_2^2 = 2^{1-i} \|u_1\|_2^2.$$

(β) Πολλαπλασιάζοντας την $(**)$ κατά μέλη, έχουμε

$$\|u_1\|_2^{2n} \leq \prod_{i=1}^{n} 2^{i-1} \prod_{i=1}^{n} \|w_i\|_2^2 = 2^{n(n-1)/2} (\det \Lambda)^2$$

γιατί

$$\det \Lambda = |\det(u_1, \ldots, u_n)| = |\det(w_1, \ldots, w_n)| = \prod_{i=1}^{n} \|w_i\|_2.$$

Αυτό αποδεικνύει το (β).

(γ) Χρησιμοποιώντας τη συνθήκη (α) του ορισμού της LLL-ανηγμένης βάσης, έχουμε

$$\begin{aligned} \|u_i\|_2^2 &= \|w_i\|_2^2 + \sum_{j=1}^{i-1} a_{ij}^2 \|w_j\|_2^2 \leq \|w_i\|_2^2 + \frac{1}{4} \sum_{j=1}^{i-1} \|w_j\|_2^2 \\ &\leq \|w_i\|_2^2 + \sum_{j=1}^{i-1} 2^{j-1} \|w_i\|_2^2 = 2^{i-1} \|w_i\|_2^2, \end{aligned}$$

και, πολλαπλασιάζοντας κατά μέλη, παίρνουμε

$$\prod_{i=1}^{n} \|u_i\|_2^2 \leq 2^{n(n-1)/2} \prod_{i=1}^{n} \|w_i\|_2^2 = 2^{\binom{n}{2}} (\det \Lambda)^2. \quad \square$$

Βιβλιογραφία

[Bar] A. Barvinok, *Lattice Points in Geometry, Combinatorics and Optimization*, Lecture Notes, 1996.

[Ca] J.W.S. Cassels, *An introduction to the Geometry of Numbers*, Springer-Verlag, Berlin, 1959.

[EGH] P. Erdös, P.M. Gruber and J. Hammer, *Lattice Points*, Longman Scientific & Technical, Essex, 1989.

[Gr] P.M. Gruber, *Geometry of Numbers*, Handbook of Convex Geometry, North-Holland, Amsterdam (1993), 739-763.

[GL] P.M. Gruber and C.G. Lekkerkerker, *Geometry of numbers*, North-Holland Math. Library **37**, North-Holland, Amsterdam, 1987.

[PA] J. Pach and P.K. Agarwal, *Combinatorial Geometry*, John Wiley & Sons, New York, 1995.

[Ro] C.A. Rogers, *Packing and Covering*, Cambridge University Press, Cambridge, 1964.

[Sie] C.L. Siegel, *Lectures on the Geometry of Numbers*, Springer-Verlag, Berlin, 1989.

[Z] C. Zong, *Sphere packings*, Universitext, Springer-Verlag, New York, 1999.

[Ba] K.M. Ball, *A lower bound for the optimal density of lattice packings*, Internat. Math. Res. Notices **10** (1992), 217-221.

[Ban] T. Bang, *A solution of the Plank problem*, Proc. Amer. Math. Soc. **2** (1951), 990-993.

[Bl1] H.F. Blichfeldt, *A new principle in the geometry of numbers, with some applications*, Trans. Amer. Math. Soc. **15** (1914), 227-235.

[Bl2] H.F. Blichfeldt, *The minimum value of quadratic forms and the closest packing of spheres*, Math. Ann. **101** (1929), 605-608.

[vdC] J.G. van der Corput, *Verallgemeinerung einer Mordellschen Beweismethode in der Geometrie der Zahlen II*, Acta Arithm. **2** (1936), 145-146.

[Di] G.L. Dirichlet, *Über die Reduktion der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen*, J. reine angew. Math. **40** (1850), 209-227.

[DR] H. Davenport and C.A. Rogers, *Hlawka's theorem in the geometry of numbers*, Duke Math. J. **14** (1947), 367-375.

[Es] T. Estermann, *Note on a theorem of Minkowski*, J. London Math. Soc. **21** (1946), 179-182.

[Ga] C.F. Gauss, *Recursion der "Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen" von Ludwig August Seeber*, J. reine angew. Math. **20** (1840), 312-320.

[Ha] G. Hajos, *Ein neuer Beweis eines Satzes von Minkowski*, Acta Litt. Sci. (Szeged) **6** (1934), 224-225.

[Her] C. Hermite, *Première lettre à M. Jacobi*, Oeuvres I, Paris, Gauthier-Villars (1905), 100-121.

[Hl] E. Hlawka, *Zur Geometrie der Zahlen*, Math. Zeitschr. **49** (1943), 285-312.

[J] F. John, *Extremum problems with inequalities as subsidiary conditions*, Courant Anniversary Volume, Interscience, New York (1948), 187-204.

[KL] G.A. Kabatjanski and V.I. Levenstein, *Bounds for packing on a sphere and in space*, translated in Problems of Information Transmission **14** (1978), 1-17.

[KZ] A. Korkin and G. Zolotarev, *Sur les formes quadratiques*, Math. Annalen **5** (1873), 366-389.

[LLL] A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Annalen **261** (1982), 515-534.

[Mah1] K. Mahler, *Ein Übertragungsprinzip für konvexe Körper*, Casopis Pest. Mat. Fyz. **68** (1939), 93-102.

[Mi1] H. Minkowski, *Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen*, Gesammelte Abhandlungen I (1911), 243-260.

[Mi2] H. Minkowski, *Geometrie der Zahlen*, Leipzig-Berlin 1896 and 1910, Chelsea 1953.

[Mor] L.J. Mordell, *On some arithmetical results in the geometry of numbers*, Compositio Math. **1** (1934), 248-253.

[Sc] C.P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theoret. Comput. Sci. **53** (1987), 201-224.

[Si] C.L. Siegel, *Über Gitterpunkte in konvexen Körpern und ein damit zusammenhängendes Extremalproblem*, Acta Math. **65** (1935), 307-323.