Το θεώρημα του Minkowski

Άγγελος Μαντζαφλάρης, amantzaf@math.uoa.gr

Προαπαιτούμενα

Ορισμός 1. *Ένα υποσύνολο $X \subseteq \mathbb{R}^n$ ονομάζεται κυρτό σύνολο αν για κάθε $x, y \in X$ το ευθύγραμμο τμήμα $\overline{xy}$ που ενώνει τα x, y περιέχεται στο σύνολο, δηλαδή $\overline{xy} \subseteq X$.*

Ορισμός 2. *Αν $x, y \in \mathbb{R}^n$ τότε κάθε διάνυσμα της μορφής $(1-\rho)x + \rho y$ όπου $\rho \in [0,1]$ καλείται κυρτός συνδυασμός των x, y.*

Κάθε κυρτός συνδυασμός δυο στοιχείων x, y ενός κυρτού συνόλου ανήκει στο σύνολο, επειδή βρίσκεται πάνω στο ευθύγραμμο τμήμα $\overline{xy}$.

Ορισμός 3. *Θεωρούμε $e_1, e_2, \ldots, e_m \in \mathbb{R}^n$ γραμμικά ανεξάρτητα διανύσματα, $m \leq n$. Η προσθετική υποομάδα της $(\mathbb{R}^n, +)$ που παράγεται από τα $e_1, e_2, \ldots, e_m$ καλείται πλέγμα διάστασης m.*

Αποδεικνύεται πως κάθε διακριτή υποομάδα του $\mathbb{R}^n$ αποτελεί πλέγμα του $\mathbb{R}^n$.

Ορισμός 4. *Έστω L πλέγμα παραγόμενο από τα διανύσματα $e_1, e_2, \ldots, e_m$. Καλούμε θεμελιώδη περιοχή του L το σύνολο*

$$\Theta := \left\{ \sum_{i=1}^{m} a_i e_i \quad | \quad 0 \leq a_i < 1 \right\}$$

Ορισμός 5. *Έστω S η πολλαπλασιαστική ομάδα των μιγαδικών αριθμών μέτρου 1. Το ευθύ γινόμενο $T^n := \underbrace{S \times S \times \cdots \times S}_{n \text{ φορές}}$ ονομάζεται σπείρα διάστασης n.*

Πρόταση 1. *Έστω ένα πλέγμα L διάστασης n. Το πηλίκο $\mathbb{R}^n / L$ είναι ισόμορφο με τη $n-$διάστατη σπείρα T^n, δηλαδή υπάρχει επιμορφισμός $f : \mathbb{R}^n \to T^n$ με πυρήνα το L.*

Πρόταση 2. *Ο περιορισμός $\phi := f|_\Theta$, με $\phi : \Theta \to T^n$ είναι αμφιμονοσήμαντη συνάρτηση.*

Αν $X \subseteq \mathbb{R}^n$ είναι γνωστό ότι ο όγκος του X με την ευρύτερη έννοια είναι $v(X) = \int_X dx_1 \ldots dx_n$. Εισάγουμε μια έννοια όγκου σε υποσύνολα της $n-$διάστατης σπείρας:

Ορισμός 6. *Έστω $Y \subseteq T^n$. Καλούμε όγκο του Y το $v(Y) := v(\phi^{-1}(Y)) = \int_{\phi^{-1}(Y)} dx_1 \ldots dx_n$.*

Πρόταση 3. *Αν $X \subseteq \mathbb{R}^n$ φραγμένο, και $v(f(X)) \neq v(X)$, τότε ο περιορισμός $f|_X$ δεν είναι ένα-προς-ένα.*

Το Θεώρημα

Θεώρημα Minkowski. *Έστω L ένα πλέγμα διάστασης n στο $\mathbb{R}^n$ με θεμελιώδη περιοχή Θ, και $X \subset \mathbb{R}^n$ ένα κυρτό, συμμετρικό και φραγμένο σύνολο. Αν*

$$v(X) > 2^n v(\Theta)$$

τότε υπάρχει μη μηδενικό στοιχείο του πλέγματος L το οποίο ανήκει στο X, δηλαδή $L \cap X - \{0\} \neq \emptyset$.

Απόδειξη. Έστω $e_1, e_2, \ldots, e_n \in \mathbb{R}^n$ διανύσματα που παράγουν το L. Θεωρούμε το πλέγμα $2L$ που παράγεται από τα $2e_1, 2e_2, \ldots, 2e_n$. Αυτό έχει θεμελιώδη περιοχή

$$2\Theta = \left\{ 2\sum_{i=1}^{n} a_i e_i \quad | \quad 0 \leq a_i < 1 \right\}$$

με όγκο

$$v(2\Theta) = 2^n v(\Theta)$$

Σύμφωνα με την *Πρόταση 1*

$$T^n \cong {\mathbb{R}^n}/{2L}$$

Από τον ορισμό (6) του όγκου είναι

$$v(T^n) = v(\phi^{-1}(T^n)) = v(2\Theta) = 2^n v(\Theta)$$

Θεωρούμε τη συνάρτηση $f : \mathbb{R}^n \to T^n$ που ορίστηκε στην *Πρόταση 1*. Τότε $f(X) \subseteq T^n$ και

$$v(f(X)) \leq v(T^n) = 2^n v(\Theta) < v(X)$$

λόγω της υπόθεσης $v(X) > 2^n v(\Theta)$.

Έπεται από την *Πρόταση 3* ότι ο περιορισμός $f|_X$ δεν είναι ένα-προς-ένα, δηλαδή υπάρχουν $x_1, x_2 \in X,\ x_1 \neq x_2$ με

$$f(x_1) = f(x_2) \Longrightarrow f(x_1) - f(x_2) = 0 \Longrightarrow f(x_1 - x_2) = 0$$

επειδή η f είναι ομοιομορφισμός. Τελικά το $x_1 - x_2$ ανήκει στον πυρήνα της f δηλαδή $x_1 - x_2 \in 2L$. Άρα υπάρχουν συντελεστές $\lambda_i \in \mathbb{Z}$ ώστε

$$x_1 - x_2 = \sum_{i=1}^{n} \lambda_i \cdot 2e_i$$

όμως τότε

$$\frac{x_1 - x_2}{2} = \sum_{i=1}^{n} \lambda_i \cdot e_i \quad \Longrightarrow \quad \frac{1}{2}(x_1 - x_2) \in L \qquad (*)$$

Το X είναι συμμετρικό, άρα $-x_2 \in X$. Επίσης ο κυρτός συνδυασμός $\frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in X$ άρα

$$\frac{1}{2}(x_1 - x_2) \in X \qquad (\dagger)$$

Τελικά από $(*)$ και $(\dagger)$ έχουμε $0 \neq \frac{1}{2}(x_1 - x_2) \in X \cap L$.

□

Εφαρμογές του θεωρήματος

- Κάθε πρώτος της μορφής $4k + 1$ είναι άθροισμα δυο τετραγώνων.
- Κάθε φυσικός είναι άθροισμα τεσσάρων τετραγώνων.
- Θεώρημα Hesse-Minkowski
- Η ομάδα κλάσης $\mathfrak{H}$ ενός αριθμητικού σώματος είναι πεπερασμένη(όριο Minkowski).
- Προσέγγιση άρρητου από ρητό: Αν $a \in \mathbb{R}$ τότε υπάρχουν $m, n \in \mathbb{Z}$ με $\frac{m}{n}$ να προσεγγίζει το a με όση ακρίβεια θέλουμε. Δηλαδή $\forall\ N \in \mathbb{N} \quad \exists m, n \in \mathbb{N}$ ώστε $|a - \frac{m}{n}| < \frac{1}{nN}$.