

# Minkowski's Theorem

Manuel Eberl

December 14, 2021

## Abstract

Minkowski's theorem relates a subset of  $\mathbb{R}^n$ , the Lebesgue measure, and the integer lattice  $\mathbb{Z}^n$ : It states that any convex subset of  $\mathbb{R}^n$  with volume greater than  $2^n$  contains at least one lattice point from  $\mathbb{Z}^n \setminus \{0\}$ , i. e. a non-zero point with integer coefficients.

A related theorem which directly implies this is Blichfeldt's theorem, which states that any subset of  $\mathbb{R}^n$  with a volume greater than 1 contains two different points whose difference vector has integer components.

The entry contains a proof of both theorems.

## Contents

<b>1</b>	<b>Minkowski's theorem</b>	<b>2</b>
1.1	Miscellaneous material . . . . .	2
1.2	Auxiliary theorems about measure theory . . . . .	2
1.3	Blichfeldt's theorem . . . . .	3
1.4	Minkowski's theorem . . . . .	3

# 1 Minkowski's theorem

**theory** *Minkowskis-Theorem*

**imports** *HOL-Analysis.Equivalence-Lebesgue-Henstock-Integration*  
**begin**

## 1.1 Miscellaneous material

**lemma** *bij-betw-UN*:

**assumes** *bij-betw f A B*

**shows**  $(\bigcup n \in A. g (f n)) = (\bigcup n \in B. g n)$

*<proof>*

**definition** *of-int-vec where*

*of-int-vec v = ( $\chi$  i. of-int (v \$ i))*

**lemma** *of-int-vec-nth [simp]: of-int-vec v \$ n = of-int (v \$ n)*

*<proof>*

**lemma** *of-int-vec-eq-iff [simp]:*

*(of-int-vec a :: ('a :: ring-char-0) ^ 'n) = of-int-vec b  $\longleftrightarrow$  a = b*

*<proof>*

**lemma** *inj-axis:*

**assumes** *c  $\neq$  0*

**shows** *inj ( $\lambda k. axis k c :: ('a :: \{zero\}) ^ 'n$ )*

*<proof>*

**lemma** *compactD:*

**assumes** *compact (A :: 'a :: metric-space set) range f  $\subseteq$  A*

**shows**  $\exists h l. strict-mono (h :: nat  $\Rightarrow$  nat)  $\wedge$  (f  $\circ$  h)  $\longrightarrow$  l$

*<proof>*

**lemma** *closed-lattice:*

**fixes** *A :: (real ^ 'n) set*

**assumes**  $\bigwedge v i. v \in A \implies v $ i \in \mathbf{Z}$

**shows** *closed A*

*<proof>*

## 1.2 Auxiliary theorems about measure theory

**lemma** *emeasure-lborel-cbox-eq'*:

*emeasure lborel (cbox a b) = ennreal ( $\prod e \in Basis. max 0 ((b - a) \cdot e)$ )*

*<proof>*

**lemma** *emeasure-lborel-cbox-cart-eq:*

**fixes** *a b :: real ^ ('n :: finite)*

**shows** *emeasure lborel (cbox a b) = ennreal ( $\prod i \in UNIV. max 0 ((b - a) $ i)$ )*

*<proof>*

**lemma** *sum-emeasure'*:

**assumes** [*simp*]: *finite A*

**assumes** [*measurable*]:  $\bigwedge x. x \in A \implies B\ x \in \text{sets } M$

**assumes**  $\bigwedge x\ y. x \in A \implies y \in A \implies x \neq y \implies \text{emeasure } M\ (B\ x \cap B\ y) = 0$

**shows**  $(\sum_{x \in A. \text{emeasure } M\ (B\ x)}) = \text{emeasure } M\ (\bigcup_{x \in A. B\ x})$

*<proof>*

**lemma** *sums-emeasure'*:

**assumes** [*measurable*]:  $\bigwedge x. B\ x \in \text{sets } M$

**assumes**  $\bigwedge x\ y. x \neq y \implies \text{emeasure } M\ (B\ x \cap B\ y) = 0$

**shows**  $(\lambda x. \text{emeasure } M\ (B\ x)) \text{ sums } \text{emeasure } M\ (\bigcup x. B\ x)$

*<proof>*

### 1.3 Blichfeldt's theorem

Blichfeldt's theorem states that, given a subset of  $\mathbb{R}^n$  with  $n > 0$  and a volume of more than 1, there exist two different points in that set whose difference vector has integer components.

This will be the key ingredient in proving Minkowski's theorem.

Note that in the HOL Light version, it is additionally required – both for Blichfeldt's theorem and for Minkowski's theorem – that the set is bounded, which we do not need.

**proposition** *blichfeldt*:

**fixes**  $S :: (\text{real } ^n)$  *set*

**assumes** [*measurable*]:  $S \in \text{sets lebesgue}$

**assumes** *emeasure lebesgue S > 1*

**obtains**  $x\ y$  **where**  $x \neq y$  **and**  $x \in S$  **and**  $y \in S$  **and**  $\bigwedge i. (x - y)\ \$\ i \in \mathbb{Z}$

*<proof>*

### 1.4 Minkowski's theorem

Minkowski's theorem now states that, given a convex subset of  $\mathbb{R}^n$  that is symmetric around the origin and has a volume greater than  $2^n$ , that set must contain a non-zero point with integer coordinates.

**theorem** *minkowski*:

**fixes**  $B :: (\text{real } ^n)$  *set*

**assumes** *convex B and symmetric: uminus ' B ⊆ B*

**assumes** *meas-B* [*measurable*]:  $B \in \text{sets lebesgue}$

**assumes** *measure-B: emeasure lebesgue B > 2 ^ CARD('n)*

**obtains**  $x$  **where**  $x \in B$  **and**  $x \neq 0$  **and**  $\bigwedge i. x\ \$\ i \in \mathbb{Z}$

*<proof>*

If the set in question is compact, the restriction to the volume can be weakened to “at least 1” from “greater than 1”.

**theorem** *minkowski-compact*:

**fixes**  $B :: (\text{real } ^n)$  *set*

**assumes** *convex B and compact B and symmetric:  $u \in B \implies -u \in B$*   
**assumes** *measure-B:  $\text{emeasure lebesgue } B \geq 2^{-n} \text{CARD}(B)$*   
**obtains** *x where  $x \in B$  and  $x \neq 0$  and  $\forall i. x \cdot i \in \mathbb{Z}$*   
*<proof>*

**end**

## References

- [1] E. Dummit. Number Theory: The Geometry of Numbers.  
[https://web.math.rochester.edu/people/faculty/edummit/docs/numthy\\_7\\_geometry\\_of\\_numbers.pdf](https://web.math.rochester.edu/people/faculty/edummit/docs/numthy_7_geometry_of_numbers.pdf), 2014.