

Minkowski's Theorem

Manuel Eberl

February 6, 2026

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

1	Minkowski's theorem	2
1.1	Miscellaneous material	2
1.2	Auxiliary theorems about measure theory	3
1.3	Blichfeldt's theorem	5
1.4	Minkowski's theorem	8

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 $(\bigcup_{n \in A}. g (f n)) = (\bigcup_{n \in B}. g n)$
using *assms* **by** (*auto simp: bij-betw-def*)

definition *of-int-vec* **where**
of-int-vec v = (χ i. of-int (v \$ i))

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

lemma *of-int-vec-eq-iff [simp]*:
(of-int-vec a :: ('a :: ring-char-0) ^ 'n) = of-int-vec b \longleftrightarrow a = b
by (*simp add: of-int-vec-def vec-eq-iff*)

lemma *inj-axis*:
assumes *c \neq 0*
shows *inj ($\lambda k. axis k c :: ('a :: \{zero\}) ^ 'n$)*

proof
fix *x y :: 'n*
assume ***: *axis x c = axis y c*
have *axis x c \$ x = axis x c \$ y*
by (*subst **) *simp*
thus *x = y* **using** *assms*
by (*auto simp: axis-def split: if-splits*)
qed

lemma *compactD*:
assumes *compact (A :: 'a :: metric-space set) range f \subseteq A*
shows $\exists h l. strict-mono (h :: nat \Rightarrow nat) \wedge (f \circ h) \longrightarrow l$

using *assms* **unfolding** *compact-def* **by** *blast*

lemma *closed-lattice*:
fixes *A :: (real ^ 'n) set*
assumes $\bigwedge v i. v \in A \implies v $ i \in \mathbb{Z}$
shows *closed A*
proof (*rule discrete-imp-closed[OF zero-less-one], safe, goal-cases*)
case (*1 x y*)
have *x \$ i = y \$ i* **for** *i*
proof –
from *1* **and** *assms* **have** *x \$ i - y \$ i \in \mathbb{Z}*
by *auto*

then obtain m where m : $of-int\ m = (x\ \$\ i - y\ \$\ i)$
by $(elim\ Ints-cases)\ auto$
hence $of-int\ (abs\ m) = abs\ ((x - y)\ \$\ i)$
by $simp$
also have $\dots \leq norm\ (x - y)$
by $(rule\ component-le-norm-cart)$
also have $\dots < of-int\ 1$
using 1 **by** $(simp\ add:\ dist-norm\ norm-minus-commute)$
finally have $abs\ m < 1$
by $(subst\ (asm)\ of-int-less-iff)$
thus $x\ \$\ i = y\ \$\ i$
using m **by** $simp$
qed
thus $y = x$
by $(simp\ add:\ vec-eq-iff)$
qed

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 $(cases\ \forall\ ba \in Basis.\ a \cdot ba \leq b \cdot ba)$

case $True$

hence $emeasure\ lborel\ (cbox\ a\ b) = ennreal\ (prod\ ((\cdot)\ (b - a))\ Basis)$

unfolding $emeasure-lborel-cbox-eq$ **by** $auto$

also have $prod\ ((\cdot)\ (b - a))\ Basis = (\prod\ e \in Basis.\ max\ 0\ ((b - a) \cdot e))$

using $True$ **by** $(intro\ prod.cong\ refl)\ (auto\ simp:\ max-def\ inner-simps)$

finally show $?thesis$.

next

case $False$

hence $emeasure\ lborel\ (cbox\ a\ b) = ennreal\ 0$

by $(auto\ simp:\ emeasure-lborel-cbox-eq)$

also from $False$ **have** $0 = (\prod\ e \in Basis.\ max\ 0\ ((b - a) \cdot e))$

by $(auto\ simp:\ max-def\ inner-simps)$

finally show $?thesis$.

qed

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

fixes $a\ b :: real\ ^\wedge\ ('n :: finite)$

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

proof $-$

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

unfolding $emeasure-lborel-cbox-eq'$ **..**

also have $(Basis :: (real\ ^\wedge\ 'n)\ set) = range\ (\lambda k.\ axis\ k\ 1)$

unfolding $Basis-vec-def$ **by** $auto$

also have $(\prod\ e \in \dots.\ max\ 0\ ((b - a) \cdot e)) = (\prod\ i \in UNIV.\ max\ 0\ ((b - a)\ \$\ i))$

by $(subst\ prod.reindex)\ (auto\ intro!\: inj-axis\ simp:\ algebra-simps\ inner-axis)$

finally show $?thesis$.

qed

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 –

define *C* **where** $C = (\bigcup_{x \in A}. \bigcup_{y \in (A - \{x\})}. B\ x \cap B\ y)$

have *C*: $C \in \text{null-sets } M$

unfolding *C-def* **using** *assms*

by (*intro null-sets.finite-UN*) (*auto simp: null-sets-def*)

hence [*measurable*]: $C \in \text{sets } M$ **and** [*simp*]: $\text{emeasure } M\ C = 0$

by (*simp-all add: null-sets-def*)

have $(\bigcup_{x \in A}. B\ x) = (\bigcup_{x \in A}. B\ x - C) \cup C$

by (*auto simp: C-def*)

also have $\text{emeasure } M \dots = \text{emeasure } M (\bigcup_{x \in A}. B\ x - C)$

by (*subst emeasure-Un-null-set*) (*auto intro!: sets.Un sets.Diff*)

also from *assms* **have** $\dots = (\sum_{x \in A}. \text{emeasure } M (B\ x - C))$

by (*subst sum-emeasure*)

(*auto simp: disjoint-family-on-def C-def intro!: sets.Diff sets.finite-UN*)

also have $\dots = (\sum_{x \in A}. \text{emeasure } M (B\ x))$

by (*intro sum.cong refl emeasure-Diff-null-set*) *auto*

finally show *?thesis* ..

qed

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 –

define *C* **where** $C = (\bigcup x. \bigcup_{y \in -\{x\}}. B\ x \cap B\ y)$

have *C*: $C \in \text{null-sets } M$

unfolding *C-def* **using** *assms*

by (*intro null-sets-UN'*) (*auto simp: null-sets-def*)

hence [*measurable*]: $C \in \text{sets } M$ **and** [*simp*]: $\text{emeasure } M\ C = 0$

by (*simp-all add: null-sets-def*)

have $(\bigcup x. B\ x) = (\bigcup x. B\ x - C) \cup C$

by (*auto simp: C-def*)

also have $\text{emeasure } M \dots = \text{emeasure } M (\bigcup x. B\ x - C)$

by (*subst emeasure-Un-null-set*) (*auto intro!: sets.Un sets.Diff*)

also from *assms* **have** $(\lambda x. \text{emeasure } M (B\ x - C)) \text{ sums } \dots$

by (*intro sums-emeasure*)

(*auto simp: disjoint-family-on-def C-def intro!: sets.Diff sets.finite-UN*)

also have $(\lambda x. \text{emeasure } M (B\ x - C)) = (\lambda x. \text{emeasure } M (B\ x))$

by (*intro ext emeasure-Diff-null-set*) *auto*

finally show *?thesis* .

qed

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

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 –

– We define for each lattice point in \mathbb{Z}^n the corresponding cell in \mathbb{R}^n .

define $R :: \text{int } ^n \Rightarrow (\text{real } ^n) \text{ set}$

where $R = (\lambda a. \text{cbox } (\text{of-int-vec } a) (\text{of-int-vec } (a + 1)))$

– For each lattice point, we can intersect the cell it defines with our set S to obtain a partitioning of S .

define $T :: \text{int } ^n \Rightarrow (\text{real } ^n) \text{ set}$

where $T = (\lambda a. S \cap R a)$

– We can then translate each such partition into the cell at the origin, i.e. the unit box $R 0$.

define $T' :: \text{int } ^n \Rightarrow (\text{real } ^n) \text{ set}$

where $T' = (\lambda a. (\lambda x. x - \text{of-int-vec } a) ` T a)$

have $T'\text{-altdef}$: $T' a = (\lambda x. x + \text{of-int-vec } a) - ` T a$ **for** a

unfolding $T'\text{-def}$ **by** *force*

– We need to show measurability of all the defined sets.

have [*measurable, simp*]: $R a \in \text{sets lebesgue}$ **for** a

unfolding $R\text{-def}$ **by** *simp*

have [*measurable, simp*]: $T a \in \text{sets lebesgue}$ **for** a

unfolding $T\text{-def}$ **by** *auto*

have $(\lambda x :: \text{real } ^n. x + \text{of-int-vec } a) \in \text{lebesgue} \rightarrow_M \text{lebesgue}$ **for** a

using *lebesgue-affine-measurable*[*of* $\lambda \cdot 1$ *of-int-vec* a]

by (*auto simp: euclidean-representation add-ac*)

from *measurable-sets*[*OF this, of T a a for a*]

have [*measurable, simp*]: $T' a \in \text{sets lebesgue}$ **for** a

unfolding $T'\text{-altdef}$ **by** *simp*

– Obviously, the original set S is the union of all the lattice point cell partitions.

have $S\text{-decompose}$: $S = (\bigcup a. T a)$ **unfolding** $T\text{-def}$

proof *safe*

fix x **assume** $x: x \in S$

define a **where** $a = (\chi i. \lfloor x \$ i \rfloor)$

have $x \in R a$
unfolding $R\text{-def}$
by (*auto simp: cbox-interval less-eq-vec-def of-int-vec-def a-def*)
with x **show** $x \in (\bigcup a. S \cap R a)$ **by** *auto*
qed

— Translating the partitioned subsets does not change their volume.

have $\text{emeasure } T' a = \text{emeasure } T a$ **for** a
proof –
have $T' a = (\lambda x. 1 *_{R} x + (- \text{of-int-vec } a)) ' T a$
by (*simp add: T'-def*)
also have $\text{emeasure } T' a = \text{emeasure } T a$
by (*subst emeasure-lebesgue-affine auto*)
finally show *?thesis*
by *simp*
qed

— Each translated partition of S is a subset of the unit cell at the origin.

have $T' a \subseteq \text{cbox } 0 1$ **for** a
unfolding $T'\text{-def } T\text{-def } R\text{-def}$
by (*auto simp: algebra-simps cbox-interval of-int-vec-def less-eq-vec-def*)

— It is clear that the intersection of two different lattice point cells is a null set.

have $R a \cap R b \in \text{null-sets lebesgue}$ **if** $a \neq b$ **for** $a b$
proof –
from *that* **obtain** i **where** $a \$ i \neq b \$ i$
by (*auto simp: vec-eq-iff*)
have $R a \cap R b = \text{cbox } (\chi i. \max (a \$ i) (b \$ i)) (\chi i. \min (a \$ i + 1) (b \$ i + 1))$
unfolding $\text{Int-interval-cart } R\text{-def } \text{interval-cbox}$
by (*simp add: of-int-vec-def max-def min-def if-distrib cong: if-cong*)
hence $\text{emeasure } R a \cap R b = \text{emeasure lborel } \dots$
by *simp*
also have $\dots = \text{ennreal } (\prod i \in \text{UNIV}. \max 0 ((\chi x. \text{real-of-int } (\min (a \$ x + 1) (b \$ x + 1))) - (\chi x. \text{real-of-int } (\max (a \$ x) (b \$ x)))) \$ i)$
(is $\dots = \text{ennreal } ?P$ **)**
unfolding $\text{emeasure-lborel-cbox-cart-eq}$ **by** *simp*
also have $?P = 0$
using i **by** (*auto simp: max-def intro!: exI[of - i]*)
finally show *?thesis*
by (*auto simp: null-sets-def R-def*)
qed

— Therefore, the intersection of two lattice point cell partitionings of S is also a null set.

have $T a \cap T b \in \text{null-sets lebesgue}$ **if** $a \neq b$ **for** $a b$
proof –
have $T a \cap T b = (R a \cap R b) \cap S$

by (auto simp: T-def)
 also have ... \in null-sets lebesgue
 by (rule null-set-Int2) (insert that, auto intro: R-Int assms)
 finally show ?thesis .
qed
 have emeasure-T-Int: emeasure lebesgue (T a \cap T b) = 0 if $a \neq b$ for $a b$
 using T-Int[OF that] unfolding null-sets-def by blast

— The set of lattice points \mathbb{Z}^n is countably infinite, so there exists a bijection $f : \mathbb{N} \rightarrow \mathbb{Z}^n$. We need this for summing over all lattice points.
 define f :: nat \Rightarrow int n where f = from-nat-into UNIV
 have countable (UNIV :: (int n) set) infinite (UNIV :: (int n) set)
 using infinite-UNIV-char-0 by simp-all
 from bij-betw-from-nat-into [OF this] have f: bij f
 by (simp add: f-def)

— Suppose all the translated cell partitions T' are disjoint.
 {
 assume disjoint: $\bigwedge a b. a \neq b \implies T' a \cap T' b = \{\}$
 — We know by assumption that the volume of S is greater than 1.
 have 1 < emeasure lebesgue S by fact
 also have emeasure lebesgue S = emeasure lebesgue ($\bigcup n. T' (f n)$)
proof —
 — The sum of the volumes of all the T' is precisely the volume of their union,
 which is S .
 have S = ($\bigcup a. T a$) by (rule S-decompose)
 also have ... = ($\bigcup n. T (f n)$)
 by (rule bij-betw-UN [OF f, symmetric])
 also have ($\lambda n. emeasure lebesgue (T (f n))$) sums emeasure lebesgue ...
 by (intro sums-emeasure' emeasure-T-Int) (insert f, auto simp: bij-betw-def inj-on-def)
 also have ($\lambda n. emeasure lebesgue (T (f n))$) = ($\lambda n. emeasure lebesgue (T' (f n))$)
 by (simp add: emeasure-T')
 finally have ($\lambda n. emeasure lebesgue (T' (f n))$) sums emeasure lebesgue S .
 moreover have ($\lambda n. emeasure lebesgue (T' (f n))$) sums emeasure lebesgue ($\bigcup n. T' (f n)$)
 using disjoint by (intro sums-emeasure) (insert f, auto simp: disjoint-family-on-def bij-betw-def inj-on-def)
 ultimately show ?thesis
 by (auto simp: sums-iff)
qed
 — On the other hand, all the translated partitions lie in the unit cell $cbx 0 1$, so their combined volume cannot be greater than 1.
 also have emeasure lebesgue ($\bigcup n. T' (f n)$) \leq emeasure lebesgue (cbx 0 (1 :: real n))
 using T'-subset by (intro emeasure-mono) auto
 also have ... = 1

by (simp add: emeasure-lborel-cbox-cart-eq)
 — This leads to a contradiction.
 finally have *False* by simp
 }
 — Therefore, there exists a point that lies in two different translated partitions,
 which obviously corresponds two two points in the non-translated partitions whose
 difference is the difference between two lattice points and therefore has integer
 components.
 then obtain $a \neq b$ $x \in T' a \cap T' b$
 by auto
 thus ?thesis
 by (intro that[of $x + \text{of-int-vec } a$ $x + \text{of-int-vec } b$])
 (auto simp: T'-def T-def algebra-simps)
 qed

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

assumes *convex* B and *symmetric*: $uminus ' B \subseteq B$

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

assumes *measure-B*: $\text{emeasure lebesgue } B > 2 ^n \text{CARD}(^n)$

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

proof —

— We scale B with $\frac{1}{2}$.

define B' where $B' = (\lambda x. 2 * x) - ' B$

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

using *measurable-sets*[*OF lebesgue-measurable-scaling*[of 2] *meas-B*]

by (simp add: B'-def)

have *B'-altdef*: $B' = (\lambda x. (1/2) * x) - ' B$

unfolding *B'-def* by force

— The volume of the scaled set is 2^n times smaller than the original set, and therefore still has a volume greater than 1.

have $1 < \text{ennreal } ((1 / 2) ^n \text{CARD}(^n)) * \text{emeasure lebesgue } B$

proof (*cases emeasure lebesgue B*)

case (*real x*)

have $\text{ennreal } (2 ^n \text{CARD}(^n)) = 2 ^n \text{CARD}(^n)$

by (*subst ennreal-power* [*symmetric*] *auto*)

also from *measure-B* and *real* have $\dots < \text{ennreal } x$ by *simp*

finally have $(2 ^n \text{CARD}(^n)) < x$

by (*subst (asm) ennreal-less-iff*) *auto*

thus ?thesis

using *real* by (simp add: *ennreal-1* [*symmetric*] *ennreal-mult'* [*symmetric*]
ennreal-less-iff field-simps del: ennreal-1)

qed (*simp-all add: ennreal-mult-top*)

also have ... = *emeasure lebesgue B'*
unfolding *B'-altdef using emeasure-lebesgue-affine[of 1/2 0 B]* **by simp**
finally have *: *emeasure lebesgue B' > 1* .

— We apply Blichfeldt's theorem to get two points whose difference vector has integer coefficients. It only remains to show that that difference vector is itself a point in the original set.

obtain *x y*
where *xy: x ≠ y x ∈ B' y ∈ B' ∧ i. (x - y) \$ i ∈ Z*
by (*erule blichfeldt [OF meas-B' *]*)
hence $2 *_{R} x \in B$ $2 *_{R} y \in B$ **by** (*auto simp: B'-def*)
— Exploiting the symmetric of *B*, the reflection of $2 *_{R} y$ is also in *B*.
moreover from this and symmetric have $-(2 *_{R} y) \in B$ **by blast**
— Since *B* is convex, the mid-point between $2 *_{R} x$ and $-(2 *_{R} y)$ is also in *B*, and that point is simply $x - y$ as desired.
ultimately have $(1 / 2) *_{R} 2 *_{R} x + (1 / 2) *_{R} (- 2 *_{R} y) \in B$
using *<convex B>* **by** (*intro convexD*) *auto*
also have $(1 / 2) *_{R} 2 *_{R} x + (1 / 2) *_{R} (- 2 *_{R} y) = x - y$
by simp
finally show *?thesis using xy*
by (*intro that[of x - y]*) *auto*
qed

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 :: (real ^ 'n) set*
assumes *convex B and compact B and symmetric: uminus ' B ⊆ B*
assumes *measure-B: emeasure lebesgue B ≥ 2 ^ CARD('n)*
obtains *x where x ∈ B and x ≠ 0 and ∧ i. x \$ i ∈ Z*
proof (*cases emeasure lebesgue B = 2 ^ CARD('n)*)
— If the volume is greater than 1, we can just apply the theorem from before.
case False
with *measure-B have less: emeasure lebesgue B > 2 ^ CARD('n)*
by simp
from *<compact B>* **have** *meas: B ∈ sets lebesgue*
by (*intro sets-completionI-sets lborelD borel-closed compact-imp-closed*)
from *minkowski[OF assms(1) symmetric meas less]* **and that**
show *?thesis by blast*

next

case True
— If the volume is precisely one, we look at what happens when *B* is scaled with a factor of $1 + \varepsilon$.

define *B' where B' = (λ ε. (*_R) (1 + ε) ' B)*
from *<compact B>* **have** *compact': compact (B' ε) for ε*
unfolding *B'-def* **by** (*intro compact-scaling*)
have *B'-altdef: B' ε = (*_R) (inverse (1 + ε)) -' B* **if** *ε: ε > 0 for ε*
using *ε unfolding B'-def* **by force**

— Since the scaled sets are convex, they are stable under scaling.

have *B-scale*: $a *_R x \in B$ **if** $x \in B$ $a \in \{0..1\}$ **for** a x

proof —

have $((a + 1) / 2) *_R x + (1 - ((a + 1) / 2)) *_R (-x) \in B$
using that and $\langle \text{convex } B \rangle$ **and symmetric by** (*intro convexD*) *auto*
also have $((a + 1) / 2) *_R x + (1 - ((a + 1) / 2)) *_R (-x) =$
 $(1 + a) *_R ((1/2) *_R (x + x)) - x$
by (*simp add: algebra-simps del: scaleR-half-double*)
also have $\dots = a *_R x$
by (*subst scaleR-half-double*) (*simp add: algebra-simps*)
finally show $\dots \in B$.

qed

— This means that B' is monotonic.

have *B'-subset*: $B' a \subseteq B' b$ **if** $0 \leq a \leq b$ **for** a b

proof

fix x **assume** $x \in B' a$
then obtain y **where** $x = (1 + a) *_R y$ $y \in B$
by (*auto simp: B'-def*)
moreover then have $(inverse (1 + b) * (1 + a)) *_R y \in B$
using that by (*intro B-scale*) (*auto simp: field-simps*)
ultimately show $x \in B' b$
using that by (*force simp: B'-def*)

qed

— We obtain some upper bound on the norm of B .

from $\langle \text{compact } B \rangle$ **have** *bounded B*

by (*rule compact-imp-bounded*)

then obtain C **where** C : *norm* $x \leq C$ **if** $x \in B$ **for** x

unfolding *bounded-iff* **by** *blast*

— We can then bound the distance of any point in a scaled set to the original set.

have *setdist-le*: *setdist* $\{x\} B \leq \varepsilon * C$ **if** $x \in B' \varepsilon$ **and** $\varepsilon \geq 0$ **for** x ε

proof —

from that obtain y **where** $y: y \in B$ **and** [*simp*]: $x = (1 + \varepsilon) *_R y$
by (*auto simp: B'-def*)
from y **have** *setdist* $\{x\} B \leq \text{dist } x y$
by (*intro setdist-le-dist*) *auto*
also from that have $\text{dist } x y = \varepsilon * \text{norm } y$
by (*simp add: dist-norm algebra-simps*)
also from y **have** $\text{norm } y \leq C$
by (*rule C*)
finally show *setdist* $\{x\} B \leq \varepsilon * C$
using that by (*simp add: mult-left-mono*)

qed

— By applying the standard Minkowski theorem to the a scaled set, we can see that any scaled set contains a non-zero point with integer coordinates.

have $\exists v. v \in B' \varepsilon - \{0\} \wedge (\forall i. v \$ i \in \mathbb{Z})$ **if** $\varepsilon: \varepsilon > 0$ **for** ε

proof –

from $\langle \text{convex } B \rangle$ **have** convex' : $\text{convex } (B' \varepsilon)$
unfolding B' -def **by** (rule *convex-scaling*)
from $\langle \text{compact } B \rangle$ **have** meas : $B' \varepsilon \in \text{sets lebesgue}$ **unfolding** B' -def
by (intro *sets-completionI-sets lborelD borel-closed compact-imp-closed compact-scaling*)
from *symmetric* **have** $\text{symmetric}'$: $\text{uminus } ' B' \varepsilon \subseteq B' \varepsilon$
by (auto *simp: B'-altdef[OF ε]*)

have $2 \wedge \text{CARD}('n) = \text{ennreal } (2 \wedge \text{CARD}('n))$
by (*subst ennreal-power [symmetric] auto*)
hence $1 * \text{emeasure lebesgue } B < \text{ennreal } ((1 + \varepsilon) \wedge \text{CARD}('n)) * \text{emeasure lebesgue } B$
using *True and ε by (intro ennreal-mult-strict-right-mono) (auto)*
also have $\dots = \text{emeasure lebesgue } (B' \varepsilon)$
using *emeasure-lebesgue-affine[of $1 + \varepsilon$ 0 B] and ε by (simp add: B' -def)*
finally have $\text{measure-}B'$: $\text{emeasure lebesgue } (B' \varepsilon) > 2 \wedge \text{CARD}('n)$
using *True by simp*

obtain v **where** $v \in B' \varepsilon$ $v \neq 0$ $\wedge i. v \$ i \in \mathbf{Z}$
by (*erule minkowski[OF convex' $\text{symmetric}'$ $\text{meas measure-}B'$]*)
thus *?thesis*
by *blast*

qed

hence $\forall n. \exists v. v \in B' (1/\text{Suc } n) - \{0\} \wedge (\forall i. v \$ i \in \mathbf{Z})$
by *auto*

— In particular, this means we can choose some sequence tending to zero – say $\frac{1}{n+1}$ – and always find a lattice point in the scaled set.
hence $\exists v. \forall n. v n \in B' (1/\text{Suc } n) - \{0\} \wedge (\forall i. v n \$ i \in \mathbf{Z})$
by (*subst (asm) choice-iff*)
then obtain v **where** $v n \in B' (1/\text{Suc } n) - \{0\}$ $v n \$ i \in \mathbf{Z}$ **for** $i n$
by *blast*

— By the Bolzano–Weierstraß theorem, there exists a convergent subsequence of v .

have $\exists h l. \text{strict-mono } (h::\text{nat} \Rightarrow \text{nat}) \wedge (v \circ h) \longrightarrow l$
proof (*rule compactD*)
show *compact* $(B' 1)$ **by** (*rule compact'*)
show $\text{range } v \subseteq B' 1$
using *B'-subset[of $1/\text{Suc } n$ 1 for n] and v by auto*

qed

then obtain $h l$ **where** h : *strict-mono* h **and** l : $(v \circ h) \longrightarrow l$
by *blast*

— Since the convergent subsequence tends to l , the distance of the sequence elements to B tends to the distance of l and B . Furthermore, the distance of the sequence elements is bounded by $(1 + \varepsilon)C$, which tends to 0, so the distance of l to B must be 0.
have *setdist* $\{l\} B \leq 0$

```

proof (rule tendsto-le)
  show (( $\lambda x. \text{setdist } \{x\} B$ )  $\circ$  ( $v \circ h$ ))  $\longrightarrow$   $\text{setdist } \{l\} B$ 
    by (intro continuous-imp-tendsto l continuous-at-setdist)
  show ( $\lambda n. \text{inverse } (\text{Suc } (h n)) * C$ )  $\longrightarrow$  0
    by (intro tendsto-mult-left-zero filterlim-compose[OF - filterlim-subseq[OF h]]
        LIMSEQ-inverse-real-of-nat)
  show  $\forall_F x$  in sequentially. (( $\lambda x. \text{setdist } \{x\} B$ )  $\circ$  ( $v \circ h$ ))  $x$ 
     $\leq$   $\text{inverse } (\text{real } (\text{Suc } (h x))) * C$ 
    using setdist-le and v unfolding o-def
    by (intro always-eventually allI setdist-le) (auto simp: field-simps)
qed auto
hence  $\text{setdist } \{l\} B = 0$ 
  by (intro antisym setdist-pos-le)
with assms and  $\langle \text{compact } B \rangle$  have  $l \in B$ 
  by (subst (asm) setdist-eq-0-closed) (auto intro: compact-imp-closed)

— It is also easy to see that, since the lattice is a closed set and all sequence
elements lie on it, the limit  $l$  also lies on it.
moreover have  $l \in \{l. \forall i. l \$ i \in \mathbb{Z}\} - \{0\}$ 
  using  $v$  by (intro closed-sequentially[OF closed-lattice - l]) auto
ultimately show ?thesis using that by blast
qed

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, 2014.