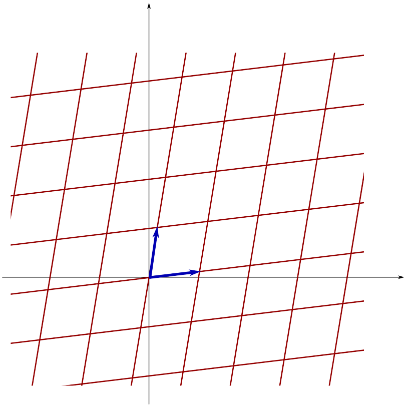
Lattices

Definition

A lattice (of rank d) is a subgroup Γ of $(\mathbb{R}^n; +)$ generated by d linearly independent vectors $\omega_1, \ldots, \omega_d$:

$$\Gamma = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_d = \{c_1\omega_1 + \cdots + c_d\omega_d : c_i \in \mathbb{Z}\}.$$

If $d = n$, then we say that Γ is a full-rank lattice.

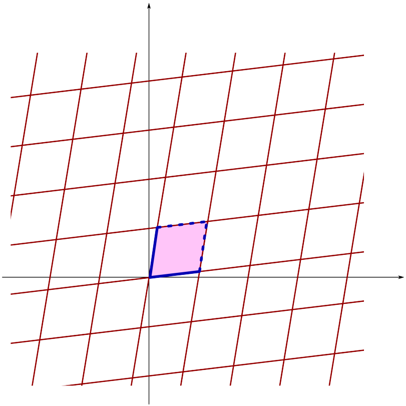


Definition

Let Γ be a full-rank lattice in $\mathbb{R}^n$ with basis $\omega_1, \ldots, \omega_n$. The set

$$P = \{x_1\omega_1 + \cdots + x_n\omega_n : 0 \leq x_i < 1\} \subseteq \mathbb{R}^n$$

is the fundamental parallelotope of L.



Fact

Translates of P cover $\mathbb{R}^n$ without overlaps:

$$\mathbb{R}^n = \dot{\bigcup_{\gamma \in \Gamma}} (\gamma + P) .$$

In other words, each coset of Γ (as a subgroup of $\mathbb{R}^n$) has a unique representative in P.

Fact

Translates of P cover $\mathbb{R}^n$ without overlaps:

$$\mathbb{R}^n = \dot{\bigcup_{\gamma \in \Gamma}} (\gamma + P) .$$

In other words, each coset of Γ (as a subgroup of $\mathbb{R}^n$) has a unique representative in P.

Let Ω be the $n \times n$ matrix obtained by writing $\omega_1, \ldots, \omega_n$ next to each other as column vectors. Then the volume of P is

$$\mathrm{vol}\,(P) = |\det \Omega| = |\det (\omega_1, \ldots, \omega_n)| .$$

Proposition

The volume of the fundamental parallelotope is independent of the choice of the basis.

Proposition

The volume of the fundamental parallelotope is independent of the choice of the basis.

Proof.

Let $\omega_1, \ldots, \omega_n$ and $\omega'_1, \ldots, \omega'_n$ be two bases of with parallelotopes P and P'. Since $\omega_1, \ldots, \omega_n$ is a basis, each ω'_j can be obtained as a linear combination of $\omega_1, \ldots, \omega_n$ with integer coefficients:

$$\omega'_i = c_{1i}\omega_1 + \cdots + c_{ni}\omega_n \quad (i = 1, \ldots, n)\,.$$

In other words, we have $\Omega' = \Omega \cdot C$, where $C = (c_{ij}) \in \mathbb{Z}^{n \times n}$.

Proposition

The volume of the fundamental parallelotope is independent of the choice of the basis.

Proof.

Let $\omega_1, \ldots, \omega_n$ and $\omega'_1, \ldots, \omega'_n$ be two bases of with parallelotopes P and P'. Since $\omega_1, \ldots, \omega_n$ is a basis, each ω'_j can be obtained as a linear combination of $\omega_1, \ldots, \omega_n$ with integer coefficients:

$$\omega'_i = c_{1i}\omega_1 + \cdots + c_{ni}\omega_n \quad (i = 1, \ldots, n)\,.$$

In other words, we have $\Omega' = \Omega \cdot C$, where $C = (c_{ij}) \in \mathbb{Z}^{n\times n}$. Similarly, $\Omega = \Omega' \cdot D$ for some matrix $D \in \mathbb{Z}^{n\times n}$. Therefore,

$$\Omega = \Omega \cdot C \cdot D \implies C \cdot D = I \implies \det C = \det D = \pm 1,$$

Proposition

The volume of the fundamental parallelotope is independent of the choice of the basis.

Proof.

Let $\omega_1, \ldots, \omega_n$ and $\omega'_1, \ldots, \omega'_n$ be two bases of with parallelotopes P and P'. Since $\omega_1, \ldots, \omega_n$ is a basis, each ω'_j can be obtained as a linear combination of $\omega_1, \ldots, \omega_n$ with integer coefficients:

$$\omega'_i = c_{1i}\omega_1 + \cdots + c_{ni}\omega_n \quad (i = 1, \ldots, n)\,.$$

In other words, we have $\Omega' = \Omega \cdot C$, where $C = (c_{ij}) \in \mathbb{Z}^{n \times n}$. Similarly, $\Omega = \Omega' \cdot D$ for some matrix $D \in \mathbb{Z}^{n \times n}$. Therefore,

$$\Omega = \Omega \cdot C \cdot D \implies C \cdot D = I \implies \det C = \det D = \pm 1,$$

and this proves the proposition:

$$\operatorname{vol}(P') = |\det \Omega'| = |\det \Omega| \cdot |\det C| = |\det \Omega| = \operatorname{vol}(P)\,. \qquad \square$$

Proposition

The volume of the fundamental parallelotope is independent of the choice of the basis.

Proof.

Let $\omega_1, \ldots, \omega_n$ and $\omega'_1, \ldots, \omega'_n$ be two bases of with parallelotopes P and P'. Since $\omega_1, \ldots, \omega_n$ is a basis, each ω'_j can be obtained as a linear combination of $\omega_1, \ldots, \omega_n$ with integer coefficients:

$$\omega'_i = c_{1i}\omega_1 + \cdots + c_{ni}\omega_n \quad (i = 1, \ldots, n)\,.$$

In other words, we have $\Omega' = \Omega \cdot C$, where $C = (c_{ij}) \in \mathbb{Z}^{n\times n}$. Similarly, $\Omega = \Omega' \cdot D$ for some matrix $D \in \mathbb{Z}^{n\times n}$. Therefore,

$$\Omega = \Omega \cdot C \cdot D \implies C \cdot D = I \implies \det C = \det D = \pm 1,$$

and this proves the proposition:

$$\mathrm{vol}\,(P') = |\det \Omega'| = |\det \Omega| \cdot |\det C| = |\det \Omega| = \mathrm{vol}\,(P)\,. \qquad \square$$

Remark

By the above proposition, it makes sense to denote the volume of any/the fundamental parallelotope of Γ by $\mathrm{vol}\,(\Gamma)$.

Theorem

Let $\Gamma_1 \leq \Gamma \leq \mathbb{R}^d$ be full-rank lattices with fundamental parallelotopes P and P_1. Then Γ_1 is of finite index in Γ, and we have

$$[\Gamma : \Gamma_1] = |P_1 \cap \Gamma| = \frac{\mathrm{vol}\,(P_1)}{\mathrm{vol}\,(P)}.$$

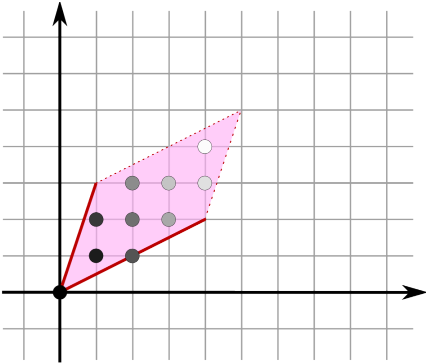
Theorem

Let $\Gamma_1 \leq \Gamma \leq \mathbb{R}^d$ be full-rank lattices with fundamental parallelotopes P and P_1. Then Γ_1 is of finite index in Γ, and we have

$$[\Gamma : \Gamma_1] = |P_1 \cap \Gamma| = \frac{\mathrm{vol}\,(P_1)}{\mathrm{vol}\,(P)}.$$

Proof.

The set $P_1 \cap \Gamma$ is finite (it is a compact discrete set), and it is a complete system of representatives of the cosets of Γ_1, hence $[\Gamma : \Gamma_1] = |P_1 \cap \Gamma| < \infty$.

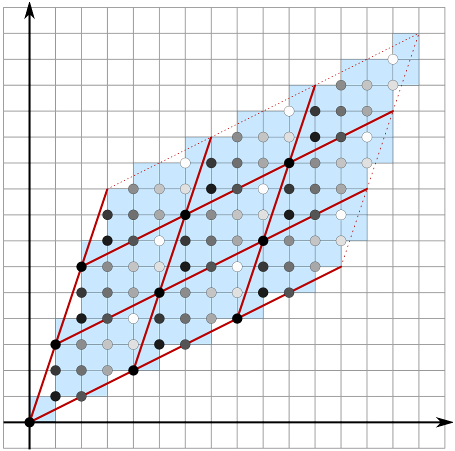


Proof. (cont.)

The union of the translates of P by the elements of $n \cdot P_1 \cap \Gamma$ provides an approximation for $n \cdot P_1$:

$$\mathrm{vol}\,(n \cdot P_1) \approx |n \cdot P_1 \cap \Gamma| \cdot \mathrm{vol}\,(P)\,.$$

(Note that $n \cdot P_1$ is the union of n^d copies of P_1.)



Proof. (cont.)

The error in this approximation is caused by the translates of P protruding and receding around the boundary of $n \cdot P_1$. Therefore, we can give the following estimate:

$$\operatorname{vol}(n \cdot P_1) = |n \cdot P_1 \cap \Gamma| \cdot \operatorname{vol}(P) + O\left(n^{d-1}\right).$$

Proof. (cont.)

The error in this approximation is caused by the translates of P protruding and receding around the boundary of $n \cdot P_1$. Therefore, we can give the following estimate:

$$\mathrm{vol}\left(n \cdot P_1\right) = \left|n \cdot P_1 \cap \Gamma\right| \cdot \mathrm{vol}\left(P\right) + O\left(n^{d-1}\right).$$

Observe that $\mathrm{vol}\left(n \cdot P_1\right) = n^d \cdot \mathrm{vol}\left(P_1\right)$ and $\left|n \cdot P_1 \cap \Gamma\right| = n^d \cdot \left|P_1 \cap \Gamma\right|$. Therefore, after dividing by n^d, we get

$$\mathrm{vol}\left(P_1\right) = \left|P_1 \cap \Gamma\right| \cdot \mathrm{vol}\left(P\right) + O\left(\frac{1}{n}\right).$$

Proof. (cont.)

The error in this approximation is caused by the translates of P protruding and receding around the boundary of $n \cdot P_1$. Therefore, we can give the following estimate:

$$\mathrm{vol}\left(n \cdot P_1\right) = \left|n \cdot P_1 \cap \Gamma\right| \cdot \mathrm{vol}\left(P\right) + O\left(n^{d-1}\right).$$

Observe that $\mathrm{vol}\left(n \cdot P_1\right) = n^d \cdot \mathrm{vol}\left(P_1\right)$ and $\left|n \cdot P_1 \cap \Gamma\right| = n^d \cdot \left|P_1 \cap \Gamma\right|$. Therefore, after dividing by n^d, we get

$$\mathrm{vol}\left(P_1\right) = \left|P_1 \cap \Gamma\right| \cdot \mathrm{vol}\left(P\right) + O\left(\frac{1}{n}\right).$$

Taking the limit as $n \to \infty$ we obtain the desired equality:

$$\mathrm{vol}\left(P_1\right) = \left|P_1 \cap \Gamma\right| \cdot \mathrm{vol}\left(P\right).$$

□

Proof. (cont.)

The error in this approximation is caused by the translates of P protruding and receding around the boundary of $n \cdot P_1$. Therefore, we can give the following estimate:

$$\mathrm{vol}\left(n \cdot P_1\right) = \left|n \cdot P_1 \cap \Gamma\right| \cdot \mathrm{vol}\left(P\right) + O\left(n^{d-1}\right).$$

Observe that $\mathrm{vol}\left(n \cdot P_1\right) = n^d \cdot \mathrm{vol}\left(P_1\right)$ and $\left|n \cdot P_1 \cap \Gamma\right| = n^d \cdot \left|P_1 \cap \Gamma\right|$. Therefore, after dividing by n^d, we get

$$\mathrm{vol}\left(P_1\right) = \left|P_1 \cap \Gamma\right| \cdot \mathrm{vol}\left(P\right) + O\left(\frac{1}{n}\right).$$

Taking the limit as $n \to \infty$ we obtain the desired equality:

$$\mathrm{vol}\left(P_1\right) = \left|P_1 \cap \Gamma\right| \cdot \mathrm{vol}\left(P\right).$$

□

Corollary

If Γ_1 is a sublattice of Γ, then $\mathrm{vol}\left(\Gamma_1\right)$ is a multiple of $\mathrm{vol}\left(\Gamma\right)$, and

$$\Gamma_1 = \Gamma \iff \mathrm{vol}\left(\Gamma_1\right) = \mathrm{vol}\left(\Gamma\right).$$

Definition

A set $S \subseteq \mathbb{R}^n$ is discrete if every element $s \in S$ has a neighborhood that contains no other elements from s. Formally:

$$\forall s \in S \; \exists \varepsilon > 0 : \; B_\varepsilon(s) \cap S = \{s\},$$

where $B_\varepsilon(s) = \{x \in \mathbb{R}^n : |x - s| < \varepsilon\}$ is the open ball of radius ε centered at s.

Definition

A set $S \subseteq \mathbb{R}^n$ is discrete if every element $s \in S$ has a neighborhood that contains no other elements from s. Formally:

$$\forall s \in S \ \exists \varepsilon > 0 : \ B_\varepsilon(s) \cap S = \{s\},$$

where $B_\varepsilon(s) = \{x \in \mathbb{R}^n : |x - s| < \varepsilon\}$ is the open ball of radius ε centered at s.

Proposition

If $G \leq \mathbb{R}^n$ is a discrete group, then G is uniformly discrete, i.e., there exists $\varepsilon > 0$ such that $B_\varepsilon(g) \cap S = \{g\}$ for every $g \in G$.

Definition

A set $S \subseteq \mathbb{R}^n$ is discrete if every element $s \in S$ has a neighborhood that contains no other elements from s. Formally:

$$\forall s \in S \; \exists \varepsilon > 0 : \; B_\varepsilon(s) \cap S = \{s\},$$

where $B_\varepsilon(s) = \{x \in \mathbb{R}^n : |x - s| < \varepsilon\}$ is the open ball of radius ε centered at s.

Proposition

If $G \leq \mathbb{R}^n$ is a discrete group, then G is uniformly discrete, i.e., there exists $\varepsilon > 0$ such that $B_\varepsilon(g) \cap S = \{g\}$ for every $g \in G$.

Proof.

Since G is discrete, $B_\varepsilon(0) \cap G = \{0\}$ for some ε. We claim that $B_\varepsilon(g) \cap G = \{g\}$ for every $g \in G$.

Definition

A set $S \subseteq \mathbb{R}^n$ is discrete if every element $s \in S$ has a neighborhood that contains no other elements from s. Formally:

$$\forall s \in S \; \exists \varepsilon > 0 : \; B_\varepsilon(s) \cap S = \{s\},$$

where $B_\varepsilon(s) = \{x \in \mathbb{R}^n : |x - s| < \varepsilon\}$ is the open ball of radius ε centered at s.

Proposition

If $G \leq \mathbb{R}^n$ is a discrete group, then G is uniformly discrete, i.e., there exists $\varepsilon > 0$ such that $B_\varepsilon(g) \cap S = \{g\}$ for every $g \in G$.

Proof.

Since G is discrete, $B_\varepsilon(0) \cap G = \{0\}$ for some ε. We claim that $B_\varepsilon(g) \cap G = \{g\}$ for every $g \in G$. Assume that $g' \in B_\varepsilon(g) \cap G$. Then $g' - g \in G$ and $|g' - g| < \varepsilon$, thus $g' - g \in B_\varepsilon(0) \cap G$, and this implies that $g' - g = 0$, i.e., $g' = g$.

$\square$

Definition

A set $S \subseteq \mathbb{R}^n$ is discrete if every element $s \in S$ has a neighborhood that contains no other elements from s. Formally:

$$\forall s \in S\ \exists \varepsilon > 0 :\ B_\varepsilon(s) \cap S = \{s\},$$

where $B_\varepsilon(s) = \{x \in \mathbb{R}^n : |x - s| < \varepsilon\}$ is the open ball of radius ε centered at s.

Proposition

If $G \leq \mathbb{R}^n$ is a discrete group, then G is uniformly discrete, i.e., there exists $\varepsilon > 0$ such that $B_\varepsilon(g) \cap S = \{g\}$ for every $g \in G$.

Proof.

Since G is discrete, $B_\varepsilon(0) \cap G = \{0\}$ for some ε. We claim that $B_\varepsilon(g) \cap G = \{g\}$ for every $g \in G$. Assume that $g' \in B_\varepsilon(g) \cap G$. Then $g' - g \in G$ and $|g' - g| < \varepsilon$, thus $g' - g \in B_\varepsilon(0) \cap G$, and this implies that $g' - g = 0$, i.e., $g' = g$.

□

Corollary

If $G \leq \mathbb{R}^n$ is a discrete group, then every bounded subset of $\mathbb{R}^n$ contains only finitely many elements of G.

Theorem
A subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.

Theorem

A subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.

Proof.

It is clear (?) that lattices are discrete subgroups.

Theorem
A subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.

Proof.
It is clear (?) that lattices are discrete subgroups.

Conversely, let $G \leq \mathbb{R}^n$ be a discrete subgroup. We can assume without loss of generality that G contains n linearly independent vectors, i.e., G spans $\mathbb{R}^n$ (otherwise we can replace $\mathbb{R}^n$ by the subspace spanned by G).

Theorem

A subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.

Proof.

It is clear (?) that lattices are discrete subgroups.

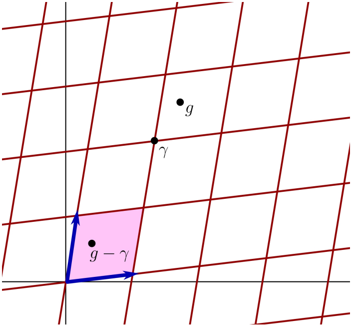
Conversely, let $G \leq \mathbb{R}^n$ be a discrete subgroup. We can assume without loss of generality that G contains n linearly independent vectors, i.e., G spans $\mathbb{R}^n$ (otherwise we can replace $\mathbb{R}^n$ by the subspace spanned by G).

Let us choose linearly independent vectors $\omega_1, \ldots, \omega_n \in G$ with $|\det(\omega_1, \ldots, \omega_n)|$ minimal. Let $\Gamma = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$ and let P be the fundamental parallelotope of the lattice Γ.

In other words, $\Gamma \leq G$ is a sublattice of minimal volume. We claim that $\Gamma = G$.

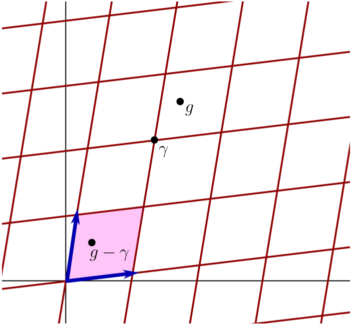
Proof. (cont.)

Assume, on the contrary, that $\exists g \in G \setminus \Gamma$. Since the translates $\gamma + P$ $(\gamma \in \Gamma)$ cover $\mathbb{R}^n$, there exists $\gamma \in \Gamma$ such that $g \in \gamma + P$.



Proof. (cont.)

Assume, on the contrary, that $\exists g \in G \setminus \Gamma$. Since the translates $\gamma + P \ \ (\gamma \in \Gamma)$ cover $\mathbb{R}^n$, there exists $\gamma \in \Gamma$ such that $g \in \gamma + P$. From $g \notin \Gamma$ it follows that $g \neq \gamma$, thus $0 \neq g - \gamma \in P$.

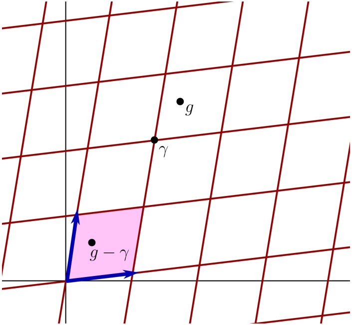


Proof. (cont.)

Assume, on the contrary, that $\exists g \in G \setminus \Gamma$. Since the translates $\gamma + P$ $(\gamma \in \Gamma)$ cover $\mathbb{R}^n$, there exists $\gamma \in \Gamma$ such that $g \in \gamma + P$. From $g \notin \Gamma$ it follows that $g \neq \gamma$, thus $0 \neq g - \gamma \in P$. Therefore, $g - \gamma$ can be written as

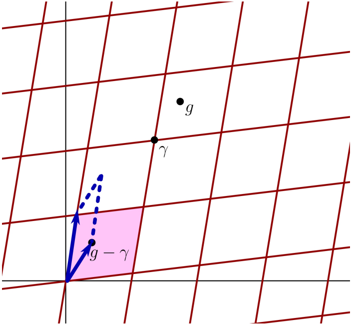
$$g - \gamma = x_1\omega_1 + \cdots + x_n\omega_n \ \ (0 \leq x_i < 1)\,,$$

where at least one of the x_i is nonzero, say (wlog) $x_1 \neq 0$.



Proof. (cont.)

Let Γ_1 be the lattice obtained by replacing ω_1 by $g-\gamma$ in the basis: $\Gamma_1 = \mathbb{Z}(g-\gamma) + \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n$. We will prove that $\mathrm{vol}(\Gamma_1) < \mathrm{vol}(\Gamma)$.



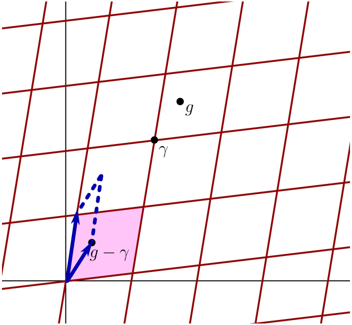
Proof. (cont.)

Let Γ_1 be the lattice obtained by replacing ω_1 by $g-\gamma$ in the basis: $\Gamma_1 = \mathbb{Z}(g-\gamma) + \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n$. We will prove that $\mathrm{vol}(\Gamma_1) < \mathrm{vol}(\Gamma)$.

$$\mathrm{vol}(\Gamma_1) = |\det(g-\gamma, \omega_2, \ldots, \omega_n)| = \left|\det\left(\sum_{i=1}^{n} x_i\omega_i, \omega_2, \ldots, \omega_n\right)\right|$$

$$= \left|\sum_{i=1}^{n} x_i \det(\omega_i, \omega_2, \ldots, \omega_n)\right| = |x_1 \cdot \det(\omega_1, \omega_2, \ldots, \omega_n)| = x_1 \cdot \mathrm{vol}(\Gamma).$$

Hence $\mathrm{vol}(\Gamma_1) = x_1 \cdot \mathrm{vol}(\Gamma) < \mathrm{vol}(\Gamma)$, contradicting the minimality of $\mathrm{vol}(\Gamma)$. $\square$



Question

Where is the mistake in this proof?

Question

Where is the mistake in this proof?

Answer

We did not prove that there is a sublattice of minimal volume.

Lemma

Let $G \leq \mathbb{R}^n$ be a discrete group and let $\Delta \leq G$ be a sublattice of G. Then there exists a positive integer h such that $G \leq \frac{1}{h} \cdot \Delta$.

Lemma

Let $G \leq \mathbb{R}^n$ be a discrete group and let $\Delta \leq G$ be a sublattice of G. Then there exists a positive integer h such that $G \leq \frac{1}{h} \cdot \Delta$.

Proof.

If P is the fundamental parallelotope of Δ, then every coset of Δ has a representative in $P \cap G$. Since G is discrete, this is a finite set, hence $h := [G : \Delta] < \infty$.

Lemma

Let $G \leq \mathbb{R}^n$ be a discrete group and let $\Delta \leq G$ be a sublattice of G. Then there exists a positive integer h such that $G \leq \frac{1}{h} \cdot \Delta$.

Proof.

If P is the fundamental parallelotope of Δ, then every coset of Δ has a representative in $P \cap G$. Since G is discrete, this is a finite set, hence $h := [G : \Delta] < \infty$.

By Lagrange's theorem, the h-th power of any element of G/Δ is the identity,

Lemma

Let $G \leq \mathbb{R}^n$ be a discrete group and let $\Delta \leq G$ be a sublattice of G. Then there exists a positive integer h such that $G \leq \frac{1}{h} \cdot \Delta$.

Proof.

If P is the fundamental parallelotope of Δ, then every coset of Δ has a representative in $P \cap G$. Since G is discrete, this is a finite set, hence $h := [G : \Delta] < \infty$.

By Lagrange's theorem, the h-th power of any element of G/Δ is the identity, i.e., $h \cdot g \in \Delta$ for all $g \in G$. This shows that $G \leq \frac{1}{h} \cdot \Delta$. $\square$

Lemma

Let $G \leq \mathbb{R}^n$ be a discrete group and let $\Delta \leq G$ be a sublattice of G. Then there exists a positive integer h such that $G \leq \frac{1}{h} \cdot \Delta$.

Proof.

If P is the fundamental parallelotope of Δ, then every coset of Δ has a representative in $P \cap G$. Since G is discrete, this is a finite set, hence $h := [G : \Delta] < \infty$.

By Lagrange's theorem, the h-th power of any element of G/Δ is the identity, i.e., $h \cdot g \in \Delta$ for all $g \in G$. This shows that $G \leq \frac{1}{h} \cdot \Delta$. $\square$

Now we can fix our proof:

Lemma
Let $G \leq \mathbb{R}^n$ be a discrete group and let $\Delta \leq G$ be a sublattice of G. Then there exists a positive integer h such that $G \leq \frac{1}{h} \cdot \Delta$.

Proof.
If P is the fundamental parallelotope of Δ, then every coset of Δ has a representative in $P \cap G$. Since G is discrete, this is a finite set, hence $h := [G : \Delta] < \infty$.

By Lagrange's theorem, the h-th power of any element of G/Δ is the identity, i.e., $h \cdot g \in \Delta$ for all $g \in G$. This shows that $G \leq \frac{1}{h} \cdot \Delta$. □

Now we can fix our proof: Let $\Delta \leq G$ be any sublattice of G. Then the lemma shows that $G \leq \frac{1}{h} \cdot \Delta$. Therefore, for every sublattice $\Gamma \leq G$, we have $\Gamma \leq \frac{1}{h} \cdot \Delta$.

Lemma

Let $G \leq \mathbb{R}^n$ be a discrete group and let $\Delta \leq G$ be a sublattice of G. Then there exists a positive integer h such that $G \leq \frac{1}{h} \cdot \Delta$.

Proof.

If P is the fundamental parallelotope of Δ, then every coset of Δ has a representative in $P \cap G$. Since G is discrete, this is a finite set, hence $h := [G : \Delta] < \infty$.

By Lagrange's theorem, the h-th power of any element of G/Δ is the identity, i.e., $h \cdot g \in \Delta$ for all $g \in G$. This shows that $G \leq \frac{1}{h} \cdot \Delta$. □

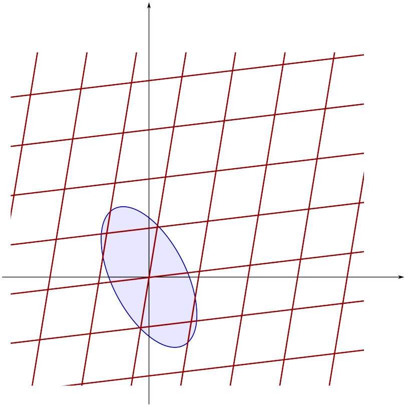
Now we can fix our proof: Let $\Delta \leq G$ be any sublattice of G. Then the lemma shows that $G \leq \frac{1}{h} \cdot \Delta$. Therefore, for every sublattice $\Gamma \leq G$, we have $\Gamma \leq \frac{1}{h} \cdot \Delta$. This implies that $\operatorname{vol}(\Gamma)$ is a multiple of $v := \operatorname{vol}\left(\frac{1}{h} \cdot \Delta\right)$. Thus the possible volumes of sublattices come from the set $\{v, 2v, 3v, \dots\}$, and now it is clear that there is a sublattice of minimal volume.

Theorem (Minkowski)

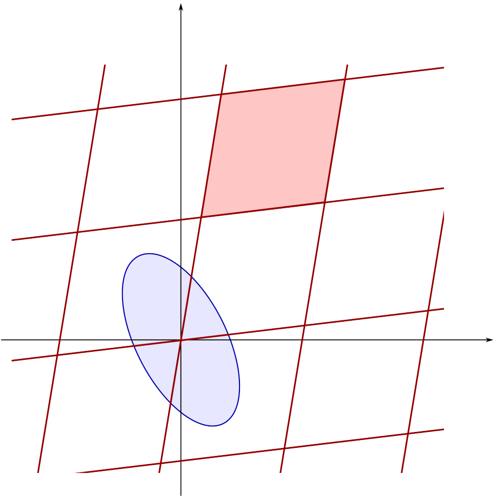
Let $\Gamma \leq \mathbb{R}^n$ be a full-rank lattice, and let $S \subseteq \mathbb{R}^n$ be a set such that

1. S is convex,
2. S is centrally symmetric with respect to the origin ($x \in S \implies -x \in S$),
3. $\mathrm{vol}\,(S) > 2^n \cdot \mathrm{vol}\,(\Gamma)$.

Then $S \cap \Gamma \neq \{0\}$, i.e., S contains at least one lattice point other than the origin.

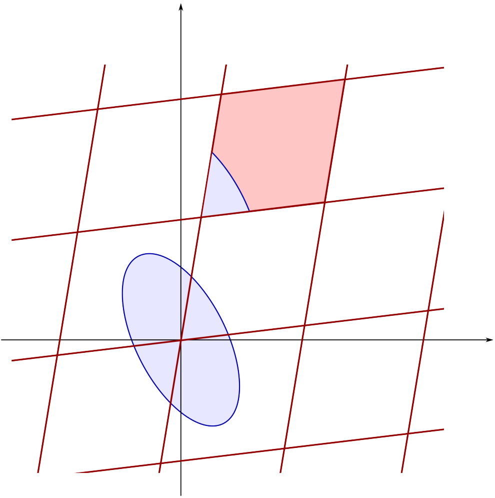


Proof of Minkowski's theorem



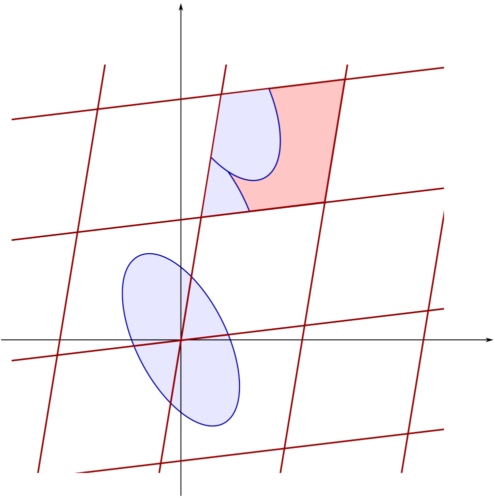
Let us pick one of the parallelotopes of 2Γ (its volume is $2^n \cdot \mathrm{vol}(\Gamma)$),

Proof of Minkowski's theorem



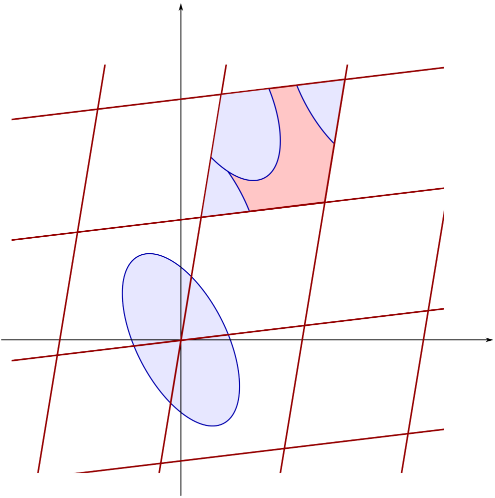
Let us pick one of the parallelotopes of 2Γ (its volume is $2^n \cdot \mathrm{vol}(\Gamma)$), and translate here all parallelotopes that intersect S.

Proof of Minkowski's theorem



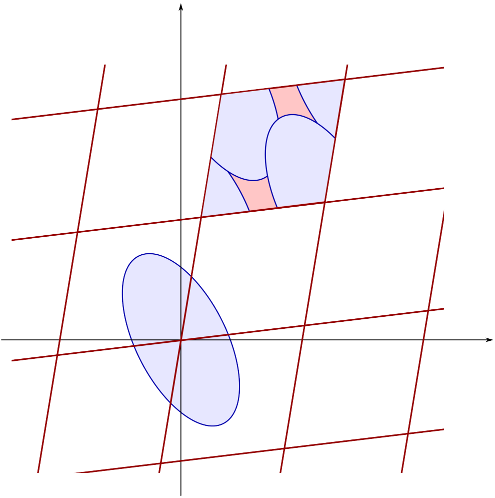
Let us pick one of the parallelotopes of 2Γ (its volume is $2^n \cdot \mathrm{vol}(\Gamma)$), and translate here all parallelotopes that intersect S.

Proof of Minkowski's theorem



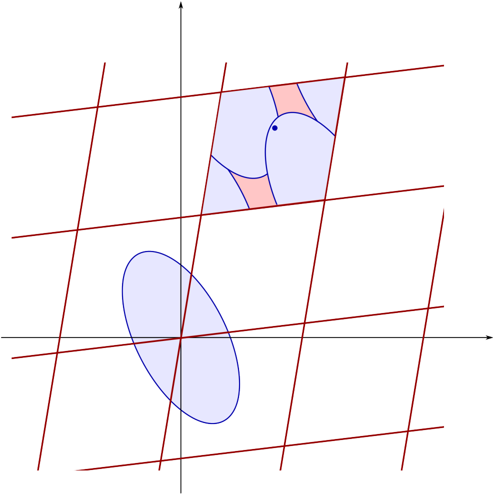
Let us pick one of the parallelotopes of 2Γ (its volume is $2^n \cdot \mathrm{vol}\,(\Gamma)$), and translate here all parallelotopes that intersect S.

Proof of Minkowski's theorem



Let us pick one of the parallelotopes of 2Γ (its volume is $2^n \cdot \mathrm{vol}(\Gamma)$), and translate here all parallelotopes that intersect S.

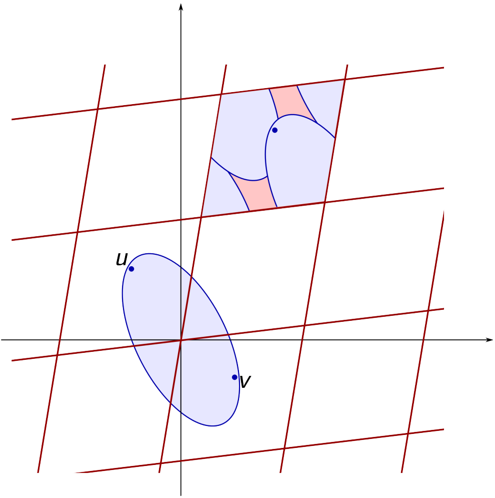
Proof of Minkowski's theorem



Let us pick one of the parallelotopes of 2Γ (its volume is $2^n \cdot \mathrm{vol}(\Gamma)$), and translate here all parallelotopes that intersect S.

Since $\mathrm{vol}(S) > 2^n \cdot \mathrm{vol}(\Gamma)$, there will be a point that is covered at least twice.

Proof of Minkowski's theorem

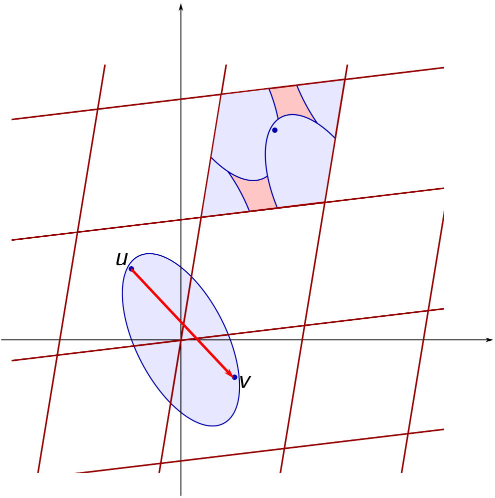


Let us pick one of the parallelotopes of 2Γ (its volume is $2^n \cdot \mathrm{vol}(\Gamma)$), and translate here all parallelotopes that intersect S.

Since $\mathrm{vol}(S) > 2^n \cdot \mathrm{vol}(\Gamma)$, there will be a point that is covered at least twice.

Let u and v denote two different preimages of such a doubly covered point.

Proof of Minkowski's theorem



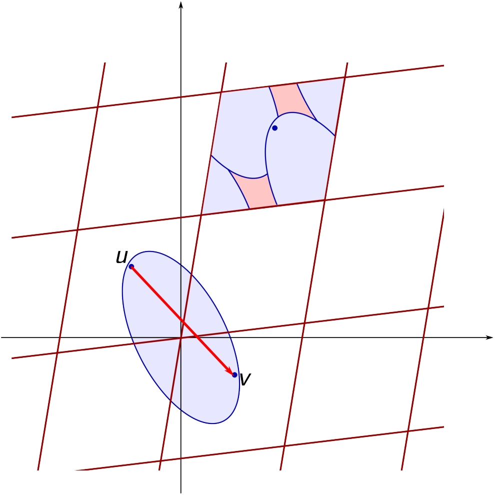
Let us pick one of the parallelotopes of 2Γ (its volume is $2^n \cdot \mathrm{vol}(\Gamma)$), and translate here all parallelotopes that intersect S.

Since $\mathrm{vol}(S) > 2^n \cdot \mathrm{vol}(\Gamma)$, there will be a point that is covered at least twice.

Let u and v denote two different preimages of such a doubly covered point.

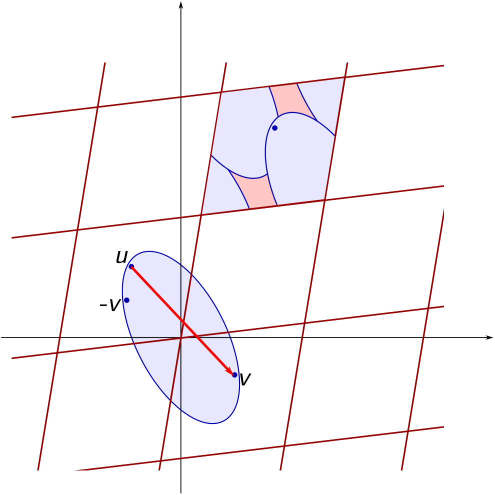
Then u and v are in the same coset of 2Γ, i.e., $u - v \in 2\Gamma$.

Proof of Minkowski's theorem



$$u, v \in S, \quad u - v \in 2\Gamma$$

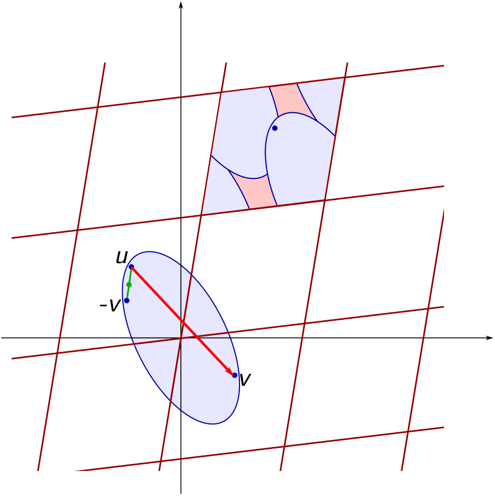
Proof of Minkowski's theorem



$u, v \in S, \quad u - v \in 2\Gamma$

S is symmetric $\implies -v \in K$

Proof of Minkowski's theorem

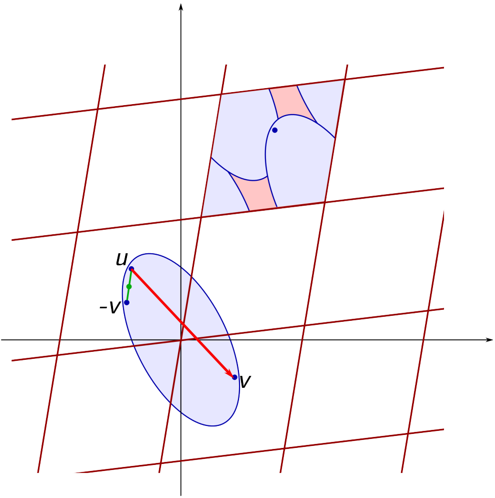


$u, v \in S, \quad u - v \in 2\Gamma$

S is symmetric $\implies -v \in K$

S is convex $\implies \dfrac{u-v}{2} \in S$

Proof of Minkowski's theorem



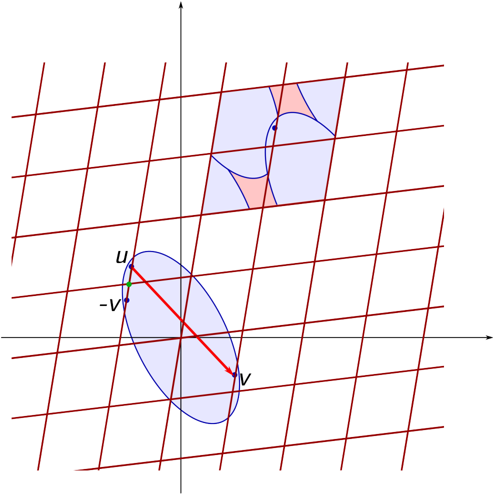
$$u, v \in S, \quad u - v \in 2\Gamma$$

$$S \text{ is symmetric} \implies -v \in K$$

$$S \text{ is convex} \implies \frac{u-v}{2} \in S$$

$$u - v \in 2\Gamma \implies \frac{u-v}{2} \in \Gamma$$

Proof of Minkowski's theorem



$u, v \in S, \quad u - v \in 2\Gamma$

S is symmetric $\implies -v \in K$

S is convex $\implies \dfrac{u-v}{2} \in S$

$u - v \in 2\Gamma \implies \dfrac{u-v}{2} \in \Gamma$

Conclusion: $\dfrac{u-v}{2} \in S \cap \Gamma.$ $\square$