CHAPTER 2

Geometry of Numbers

In this chapter, we discuss several topics on geometry of numbers, such as Minkowski's theorem, Mahler's inequality, the Brunn-Minkowski theorem and a theorem due to Gillet-Soulé. In particular, an estimate of the number of points in a convex lattice by Gillet-Soulé is very important for later use. It can be viewed as a Riemann-Roch type theorem for normed $\mathbb{Z}$-modules and it will be a fundamental tool for an asymptotic estimate of small sections.

2.1. Convex set and Minkowski's theorem

First, let us recall basic materials on convex sets. For details, see [**72**]. Let V be an n-dimensional real vector space. A subset K of V is called a *convex set* if $tx+(1-t)y \in K$ for any $x, y \in K$ and any real number t with $0 \le t \le 1$. Moreover, K is said to be *symmetric* if $x \in K$ implies $-x \in K$. Note that a convex set K has an interior point if and only if K is not contained in a proper affine subspace of V (cf. [**72**, Corollary 2.3.2]). It is easy to see that if K is a symmetric convex set with an interior point, then the origin is an internal point of K. Further, a compact convex set with an interior point is called a *convex body.*

Let h be an inner product of V. There is a unique Haar measure vol_h such that, for any basis $x_1, \ldots, x_n$ of V,

$$\mathrm{vol}_h\left(\{\lambda_1 x_1 + \cdots + \lambda_n x_n \mid 0 \le \lambda_i \le 1\ (\forall i)\}\right) = \left(\det(h(x_i, x_j))\right)^{1/2}.$$

It is called *the Haar measure induced by h.* The Haar measure of $\mathbb{R}^n$ induced by the standard inner product of $\mathbb{R}^n$ is denoted by vol_n. Here we give a special notation: in the case where $V = \{0\}$, for a subset X of V,

$$\mathrm{vol}(X) = \begin{cases} 1 & \text{if } X = \{0\}, \\ 0 & \text{if } X = \emptyset. \end{cases}$$

Note that a bounded convex set K is Jordan measurable (cf. [**72**, Theorem 6.2.11]). In particular, if we denote the set of interior points of K and the topological closure of K by K° and $\overline{K}$, respectively, then

$$\mathrm{vol}_h(K^\circ) = \mathrm{vol}_h(K) = \mathrm{vol}_h(\overline{K})$$

(cf. [**72**, Theorem 6.2.5]).

Here we consider Minkowski's theorem due to Corput.

THEOREM 2.1 (Minkowski's theorem). *Let K be a bounded and symmetric convex set in $\mathbb{R}^n$. Then we have the following:*

(1) *If k is an integer with $\mathrm{vol}_n(K) > 2^n k$, then $\#(\mathbb{Z}^n \cap K) \ge 2k+1$.*
(2) *We assume that K is closed. If k is an integer with $\mathrm{vol}_n(K) \ge 2^n k$, then $\#(\mathbb{Z}^n \cap K) \ge 2k+1$.*

PROOF. (1) If $k \leq 0$, then the assertion is obvious, so that we may assume that $k > 0$. We set $K' = (1/2)K = \{x/2 \mid x \in K\}$. Then $\mathrm{vol}_n(K') = 2^{-n}\,\mathrm{vol}_n(K) > k$. Since K' is Jordan measurable, we have

$$\lim_{r\to\infty} \#\left(K' \cap \frac{1}{r}\mathbb{Z}^n\right)\frac{1}{r^n} = \mathrm{vol}_n(K').$$

In particular, for a sufficiently large integer r,

$$\#\left(K' \cap \frac{1}{r}\mathbb{Z}^n\right) > kr^n$$

holds. Let $\pi : (1/r)\mathbb{Z}^n \to (1/r)\mathbb{Z}^n/\mathbb{Z}^n$ be the natural homomorphism. As

$$\#((1/r)\mathbb{Z}^n/\mathbb{Z}^n) = r^n,$$

using the pigeon hole principle, there are distinct $k+1$ elements

$$u_1, \ldots, u_{k+1} \in K' \cap \frac{1}{r}\mathbb{Z}^n$$

such that $\pi(u_1) = \cdots = \pi(u_{k+1})$, that is, $u_i - u_j \in \mathbb{Z}^n$ $(\forall i, j)$. Renumbering $u_1, \ldots, u_{k+1}$, we may assume that $u_1, \ldots, u_{k+1}$ is arranged according to the lexicographic order. Here we put $v_i = u_{i+1} - u_1$ $(i = 1, \ldots, k)$. If we choose $x_i \in K$ with $u_i = x_i/2$, then

$$v_i = \frac{x_{i+1} - x_1}{2} = \frac{x_{i+1} + (-x_1)}{2} \in K$$

because K is symmetric. Moreover, as $u_1, \ldots, u_{k+1}$ is arranged according to the lexicographic order, the first non-zero entry of v_i is positive. Thus

$$v_1, \ldots, v_k, -v_1, \ldots, -v_k \in K \cap \mathbb{Z}^n$$

are non-zero distinct elements. Therefore, counting the origin 0, (1) follows.

(2) For a positive integer m, we set $A_m = ((1 + (1/m))K) \cap \mathbb{Z}^n$. Then

$$A_1 \supseteq A_2 \supseteq \cdots \supseteq A_m \supseteq A_{m+1} \supseteq \cdots$$

and A_m is a finite set. Therefore, there are a positive integer m_0 and a finite subset A of $\mathbb{Z}^n$ such that $A_m = A$ for all $m \geq m_0$. Since

$$\mathrm{vol}_n((1 + (1/m))K) > \mathrm{vol}_n(K) \geq 2^n k,$$

we have $\#(A_m) \geq 2k + 1$ by (1). In particular, $\#(A) \geq 2k + 1$. Thus it is sufficient to see that $A \subseteq K \cap \mathbb{Z}^n$. Let a be an element of A. For $m \geq m_0$, as $a \in A = A_m \subseteq (1 + (1/m))K$, there is $x_m \in K$ such that $a = (1 + (1/m))x_m$, and hence $\lim_{m\to\infty} x_m = a$. This implies $a \in K$ because K is closed. □

Let V be an n-dimensional vector space. A $\mathbb{Z}$-submodule Λ of V is called a *lattice* of V if the natural homomorphism $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \to V$ is an isomorphism. Let us fix a Haar measure vol of V. A quantity

$$\mathrm{vol}\left(\{\lambda_1\omega_1 + \cdots + \lambda_n\omega_n \mid 0 \leq \lambda_i \leq 1\ (\forall i)\}\right)$$

does not depend on the choice of a free basis $\omega_1, \ldots, \omega_n$ of Λ, so that it is denoted by $\mathrm{vol}(V/\Lambda)$. If V has an inner product h, then

$$\mathrm{vol}_h(V/\Lambda) = \sqrt{\det(h(\omega_i, \omega_j))},$$

where vol_h is the Haar measure induced by h. For a measurable subset X of V, the quantity $\log(\mathrm{vol}(X)/\mathrm{vol}(V/\Lambda))$ does not depend on the choice of the Haar measure, so that it is denoted by $\widehat{\chi}(X;\Lambda)$, that is, $\exp(\widehat{\chi}(X;\Lambda)) = \mathrm{vol}(X)/\mathrm{vol}(V/\Lambda)$.

Let K be a convex set in V. The set $K \cap \Lambda$ is called a *convex lattice of* V. Minkowski's theorem asserts a good lower bound of the number of points in a convex lattice.

Corollary 2.2. *If K is bounded and symmetric, then we have the following:*
(1) $\#(K \cap \Lambda) \geq 2^{-n} \exp(\widehat{\chi}(K;\Lambda))$.
(2) *If K is closed, then* $\#(K \cap \Lambda) > 2^{-n} \exp(\widehat{\chi}(K;\Lambda))$.

Proof. Let $\omega_1, \ldots, \omega_n$ be a free basis of Λ. Let us consider an isomorphism $\phi : V \to \mathbb{R}^n$ given by $\phi(\omega_i) = e_i$ $(i = 1, \ldots, n)$, where $\{e_1, \ldots, e_n\}$ is the standard basis of $\mathbb{R}^n$. Then, since $\#(K \cap \Lambda) = \#(\phi(K) \cap \mathbb{Z}^n)$ and $\widehat{\chi}(K;\Lambda) = \widehat{\chi}(\phi(K);\mathbb{Z}^n)$, we may assume that $V = \mathbb{R}^n$ and $\Lambda = \mathbb{Z}^n$.

Let vol_n be the standard Haar measure of $\mathbb{R}^n$. Note that $\exp(\widehat{\chi}(K;\Lambda)) = \mathrm{vol}_n(K)$. If $\mathrm{vol}_n(K) < 2^n$, then $2^{-n}\mathrm{vol}_n(K) < 1$. Thus, in this case, (1) and (2) are obvious. Next we assume that $\mathrm{vol}_n(K) = 2^n$. Then (1) is also obvious. Moreover, if K is closed, then, by (2) in Theorem 2.1, $\#(K \cap \Lambda) \geq 3$, so that (2) follows. Finally we suppose that $\mathrm{vol}_n(K) > 2^n$. Let us take a positive integer k and a real number ϵ with

$$2^{-n}\mathrm{vol}_n(K) = k + \epsilon \quad (0 < \epsilon \leq 1).$$

By Theorem 2.1, we have

$$\#(K \cap \mathbb{Z}^n) \geq 2k + 1.$$

As $2^{-n}\mathrm{vol}_n(K) > 1$, we have

$$\#(K \cap \mathbb{Z}^n) \geq 2(2^{-n}\mathrm{vol}_n(K) - \epsilon) + 1 \geq 2(2^{-n}\mathrm{vol}_n(K)) - 1 > 2^{-n}\mathrm{vol}_n(K).$$

□

Finally we consider the following proposition as an application of Minkowski's theorem.

Proposition 2.3. *Let V be an n-dimensional real vector space and let q be a quadratic form on V. If there is a lattice Λ of V such that*

$$\inf\{q(\lambda) \mid \lambda \in \Lambda \setminus \{0\}\} > 0,$$

then q is positive definite.

Proof. Let us choose a basis $e_1, \ldots, e_n$ of V such that

$$q(x_1e_1 + \cdots + x_ne_n) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_{s+t}^2.$$

We set $\epsilon = \inf\{q(\lambda) \mid \lambda \in \Lambda \setminus \{0\}\} > 0$. For a positive real number a, we put

$$K(a) = \{x_1e_1 + \cdots + x_ne_n \in V \mid x_1^2 + \cdots + x_s^2 \leq \epsilon/2,\ x_{s+1}^2 + \cdots + x_n^2 \leq a\}.$$

Note that $q \leq \epsilon/2$ on $K(a)$. Therefore, $K(a) \cap \Lambda = \{0\}$. We assume that $s < n$. Then, for a sufficiently large a, $2^{-n}\exp(\widehat{\chi}(K(a);\Lambda)) \geq 1$. Hence, as $K(a)$ is a bounded and symmetric closed convex set, by Corollary 2.2,

$$\#(K(a) \cap \Lambda) > 2^{-n}\exp(\widehat{\chi}(K(a);\Lambda)) \geq 1.$$

This is a contradiction. Thus $s = n$, that is, q is positive definite. □

2.2. Polar dual set and Mahler's inequality

Let (V, h) be a pair of an n-dimensional real vector space V and an inner product h of V. For a subset X of V, the *polar dual set* X^* of X is defined by

$$X^* = \{x \in V \mid h(x, y) \le 1 \quad (\forall y \in X)\}.$$

It is easy to see that X^* is a closed convex set of V and $X \subseteq (X^*)^*$. Moreover, if X is a convex set with the origin, then $\overline{X} = (X^*)^*$ (cf. [**72**, Theorem 2.8.3]). Note that if X is symmetric, that is, $-x \in X$ for all $x \in X$, then

$$X^* = \{x \in V \mid |h(x, y)| \le 1 \quad (\forall y \in X)\}.$$

Further, if X is a bounded and symmetric convex set with an interior point, then so is X^* (cf. [**72**, Theorem 2.8.4]). Let us begin with the following lemma.

LEMMA 2.4. *Let $\langle , \rangle$ be the standard inner product of $\mathbb{R}^n$. Let X be a subset of $\mathbb{R}^n$ and let A be an $n \times n$ regular real matrix. Then $(AX)^* = {}^tA^{-1}X^*$.*

PROOF. Since $\langle x, Ay\rangle = \langle {}^tAx, y\rangle$ in general, we have

$$\begin{aligned} x \in (AX)^* &\iff \langle x, Ay\rangle \le 1 \ (\forall y \in X) \\ &\iff \langle {}^tAx, y\rangle \le 1 \ (\forall y \in X) \\ &\iff {}^tAx \in X^* \\ &\iff x \in {}^tA^{-1}X^*, \end{aligned}$$

as required. □

The following theorem is important for this book.

THEOREM 2.5 (Mahler's inequality). *Let (V, h) be a pair of an n-dimensional real vector space V and an inner product h of V. For a bounded and symmetric convex set K of V with an interior point, the following two inequalities hold:*

$$\frac{4^n}{(n!)^2} \le \operatorname{vol}_h(K)\operatorname{vol}_h(K^*) \le 4^n.$$

PROOF. Considering an orthonormal basis of V with respect to h, we may assume that $V = \mathbb{R}^n$ and h is the standard inner product of $\mathbb{R}^n$. Clearly we may also assume that K is closed. Let $\phi : K^n \to \mathbb{R}$ be the continuous map given by $\phi(v_1, \ldots, v_n) = |\det(v_1, \ldots, v_n)|$, where $\det(v_1, \ldots, v_n)$ is the determinant of the matrix $(v_1, \ldots, v_n)$ obtained by arranging the vectors $v_1, \ldots, v_n$ as column vectors. Since K is compact, there are $u_1, \ldots, u_n \in K$ such that ϕ takes the maximal value at $(u_1, \ldots, u_n)$. Note that $u_1, \ldots, u_n$ are linearly independent because $\phi(u_1, \ldots, u_n) > 0$. Thus there is a regular $n \times n$ real matrix A with $Au_i = e_i$ $(i = 1, \ldots, n)$, where $e_1, \ldots, e_n$ is the standard basis of $\mathbb{R}^n$. As

$$\begin{cases} \phi(Av_1, \ldots, Av_n) = |\det A|\phi(v_1, \ldots, v_n), \\ \operatorname{vol}_n(K)\operatorname{vol}_n(K^*) = \operatorname{vol}_n(AK)\operatorname{vol}_n((AK)^*) \quad (\because \text{Lemma 2.4}), \end{cases}$$

we may further assume that $u_i = e_i$ $(i = 1, \ldots, n)$. We set

$$W = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid |x_i| \le 1 \ (\forall i)\}.$$

Then it is easy to see that $W^* = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid |x_1| + \cdots + |x_n| \le 1\}$, $\operatorname{vol}_n(W) = 2^n$ and $\operatorname{vol}_n(W^*) = 2^n/n!$. Moreover, we can see that

$$W^* \subseteq K \subseteq W. \tag{2.1}$$

Indeed, as $\pm e_i \in K$, it is obvious that $W^* \subseteq K$. Further, if $x = (x_1, \dots, x_n) \in K$, then, for any i,

$$|x_i| = \phi(e_1, \dots, e_{i-1}, x, e_{i+1}, \dots, e_n) \leq \phi(e_1, \dots, e_n) = 1.$$

Thus $x \in W$.

By (2.1),

$$\frac{2^n}{n!} \leq \operatorname{vol}_n(K) \leq 2^n.$$

On the other hand, considering the polar dual of (2.1), we obtain

$$W^* \subseteq K^* \subseteq (W^*)^* = W,$$

which implies

$$\frac{2^n}{n!} \leq \operatorname{vol}_n(K^*) \leq 2^n.$$

Hence the theorem follows. □

Remark 2.1. By virtue of Blaschke and Santaló, we know the inequality

$$\operatorname{vol}_h(K)\operatorname{vol}_h(K^*) \leq \operatorname{vol}_h\left(\{x \in V \mid h(x,x) \leq 1\}\right)^2.$$

Moreover, it is expected that

$$\frac{4^n}{n!} \leq \operatorname{vol}_h(K)\operatorname{vol}_h(K^*)$$

holds (Mahler's conjecture), and the above theorem is sufficient for this book.

2.3. The Brunn-Minkowski theorem

In this section, we prove the Brunn-Minkowski theorem, which is one of the fundamental theorems in the geometry of convex sets.

Theorem 2.6 (Brunn-Minkowski theorem). *Let (V, h) be a pair of an n-dimensional real vector space V and an inner product h of V. For compact sets X and Y of V, the inequality*

$$\operatorname{vol}_h(X+Y)^{1/n} \geq \operatorname{vol}_h(X)^{1/n} + \operatorname{vol}_h(Y)^{1/n}$$

holds, where $X + Y = \{x + y \mid x \in X,\ y \in Y\}$ (note that $X + Y$ is a compact set).

Proof. Taking an orthonormal basis of V, we may assume that $V = \mathbb{R}^n$ and that h is the standard inner product. Here we introduce several definitions. A subset B of $\mathbb{R}^n$ is called a *compact interval* if there are compact intervals $I_1, \dots, I_n$ of $\mathbb{R}$ such that $B = I_1 \times \cdots \times I_n$. Moreover, a subset X of $\mathbb{R}^n$ is called a *compact elementary set* if there are finitely many compact intervals $B_1, \dots, B_r$ such that $X = B_1 \cup \cdots \cup B_r$ and that $B_i \cap B_j$ has no interior points for all $i \neq j$.

Since X and Y are compact, there are sequences $\{X_l\}$ and $\{Y_l\}$ of compact elementary sets such that

$$\begin{cases} X_1 \supseteq X_2 \supseteq \cdots \supseteq X_l \supseteq \cdots, & X = \bigcap_{l \geq 0} X_l, \\ Y_1 \supseteq Y_2 \supseteq \cdots \supseteq Y_l \supseteq \cdots, & Y = \bigcap_{l \geq 0} Y_l. \end{cases}$$

Then we have the following:

Claim 1. $X + Y = \bigcap_{l \geq 0}(X_l + Y_l)$.

PROOF. It is obvious that $X + Y \subseteq \bigcap_{l \geq 0}(X_l + Y_l)$. Conversely we assume $z \in \bigcap_{l \geq 0}(X_l + Y_l)$. Then we can set $z = x_l + y_l$ ($x_l \in X_l,\ y_l \in Y_l$) for all l. Since $x_l \in X_1$ ($\forall l$) and X_1 is compact, we can find a convergent subsequence $\{x_{l_i}\}$ of $\{x_l\}$. As $y_{l_i} = z - x_{l_i}$, $\{y_{l_i}\}$ is also a convergent sequence. Here we set

$$x = \lim_{i \to \infty} x_{l_i} \quad \text{and} \quad y = \lim_{i \to \infty} y_{l_i}.$$

We assume that $x \notin X$. Then there is l with $x \notin X_l$. Since $\mathbb{R}^n \setminus X_l$ is an open set, we can find i_0 such that, for all $i \geq i_0$, $x_{l_i} \notin X_l$. Here we choose i with $l_i \geq l$ and $i \geq i_0$. Then $x_{l_i} \in X_{l_i} \subseteq X_l$, which is a contradiction. Therefore $x \in X$. In the same way, we can check $y \in Y$. Hence $z = x + y \in X + Y$, as required. □

By the above claim, we have

$$\begin{cases} \operatorname{vol}_n(X) = \lim_{l \to \infty} \operatorname{vol}_n(X_l), \\ \operatorname{vol}_n(Y) = \lim_{l \to \infty} \operatorname{vol}_n(Y_l), \\ \operatorname{vol}_n(X + Y) = \lim_{l \to \infty} \operatorname{vol}_n(X_l + Y_l). \end{cases}$$

Therefore we may assume that X and Y are compact elementary sets in order to show the theorem. Moreover, as

$$\operatorname{vol}_n(X + Y) \geq \max\{\operatorname{vol}_n(X), \operatorname{vol}_n(Y)\},$$

the assertion of the theorem is trivial if either $\operatorname{vol}_n(X) = 0$ or $\operatorname{vol}_n(Y) = 0$. Hence we may further assume that $\operatorname{vol}_n(X) > 0$ and $\operatorname{vol}_n(Y) > 0$.

For a compact elementary set Z, there is no unique way to express Z as a union of compact intervals without sharing an interior point. If the number of compact intervals is minimal among all expressions of Z as above, then such an expression is called a minimal expression of Z and the number of compact intervals in a minimal expression is denoted by $\sigma(Z)$.

First we consider the case where $\sigma(X) + \sigma(Y) = 2$, that is, $\sigma(X) = \sigma(Y) = 1$. In this case, there are compact intervals $I_1, \ldots, I_n, J_1, \ldots, J_n$ in $\mathbb{R}$ such that $X = I_1 \times \cdots \times I_n$ and $Y = J_1 \times \cdots \times J_n$. Then $X + Y = (I_1 + J_1) \times \cdots \times (I_n + J_n)$. If we set

$$a_1 = \operatorname{vol}_1(I_1), \ldots, a_n = \operatorname{vol}_1(I_n), b_1 = \operatorname{vol}_1(J_1), \ldots, b_n = \operatorname{vol}_1(J_n),$$

then

$$\begin{cases} \operatorname{vol}_n(X) = a_1 \cdots a_n, \\ \operatorname{vol}_n(Y) = b_1 \cdots b_n, \\ \operatorname{vol}_n(X + Y) = (a_1 + b_1) \cdots (a_n + b_n). \end{cases}$$

As the arithmetic mean is greater than or equal to the geometric mean, we have

$$\begin{aligned} &\left(\frac{\operatorname{vol}_n(X)}{\operatorname{vol}_n(X+Y)}\right)^{1/n} + \left(\frac{\operatorname{vol}_n(Y)}{\operatorname{vol}_n(X+Y)}\right)^{1/n} \\ &\qquad = \left(\frac{a_1}{a_1 + b_1} \cdots \frac{a_n}{a_n + b_n}\right)^{1/n} + \left(\frac{b_1}{a_1 + b_1} \cdots \frac{b_n}{a_n + b_n}\right)^{1/n} \\ &\qquad \leq \frac{1}{n}\left(\frac{a_1}{a_1 + b_1} + \cdots + \frac{a_n}{a_n + b_n}\right) + \frac{1}{n}\left(\frac{b_1}{a_1 + b_1} + \cdots + \frac{b_n}{a_n + b_n}\right) = 1, \end{aligned}$$

as required.

Next we consider the case where $\sigma(X)+\sigma(Y) \geq 3$. Clearly we may assume that $\sigma(X) \geq 2$. Then there are two compact intervals B and B' in a minimal expression of X.

CLAIM 2. *There are a real number c and an i-th coordinate x_i of $\mathbb{R}^n$ such that B and B' are separated by a hyperplane $\{x_i = c\}$.*

PROOF. We choose compact intervals $T_1, \ldots, T_n, T'_1, \ldots, T'_n$ in $\mathbb{R}$ such that $B = T_1 \times \cdots \times T_n$, $B' = T'_1 \times \cdots \times T'_n$. Then $B \cap B' = (T_1 \cap T'_1) \times \cdots \times (T_n \cap T'_n)$. Since $B \cap B'$ has no interior point, there is i such that $T_i \cap T'_i$ is either empty or a point. Thus our claim follows. □

We set $X_+ = X \cap \{x_i \geq c\}$ and $X_- = X \cap \{x_i \leq c\}$. Then X_+ and X_- are compact elementary sets. Moreover, as B and B' are separated by a hyperplane $\{x_i = c\}$, we can see $\sigma(X_+) \leq \sigma(X) - 1$ and $\sigma(X_-) \leq \sigma(X) - 1$. Here we consider the function $\phi(t)$ given by $\phi(t) = \operatorname{vol}_n(Y \cap \{x_i \leq t\})$. It is easy to see that ϕ is continuous. Thus there is a real number d such that

$$\frac{\operatorname{vol}_n(X_-)}{\operatorname{vol}_n(X)} = \frac{\operatorname{vol}_n(Y_-)}{\operatorname{vol}_n(Y)},$$

where $Y_+ = Y \cap \{x_i \geq d\}$ and $Y_- = Y \cap \{x_i \leq d\}$. Namely, we have

$$\operatorname{vol}_n(X) : \operatorname{vol}_n(Y) = \operatorname{vol}_n(X_-) : \operatorname{vol}_n(Y_-) = \operatorname{vol}_n(X_+) : \operatorname{vol}_n(Y_+).$$

Moreover, we can see that

$$\begin{cases} X_- + Y_- \subseteq (X+Y) \cap \{x_i \leq c+d\}, \\ X_+ + Y_+ \subseteq (X+Y) \cap \{x_i \geq c+d\} \end{cases}$$

and

$$\begin{cases} \sigma(X_-) + \sigma(Y_-) \leq \sigma(X) + \sigma(Y) - 1, \\ \sigma(X_+) + \sigma(Y_+) \leq \sigma(X) + \sigma(Y) - 1. \end{cases}$$

Therefore, using the hypothesis of induction, we obtain

$$\begin{aligned} \operatorname{vol}_n(X+Y) &\geq \operatorname{vol}_n((X_- + Y_-) \cup (X_+ + Y_+)) \\ &= \operatorname{vol}_n(X_- + Y_-) + \operatorname{vol}_n(X_+ + Y_+) \\ &\geq \left(\operatorname{vol}_n(X_-)^{1/n} + \operatorname{vol}(Y_-)^{1/n}\right)^n + \left(\operatorname{vol}_n(X_+)^{1/n} + \operatorname{vol}(Y_+)^{1/n}\right)^n \\ &= \operatorname{vol}_n(X_-)\left(1 + \frac{\operatorname{vol}_n(Y)^{1/n}}{\operatorname{vol}_n(X)^{1/n}}\right)^n + \operatorname{vol}_n(X_+)\left(1 + \frac{\operatorname{vol}_n(Y)^{1/n}}{\operatorname{vol}_n(X)^{1/n}}\right)^n \\ &= \operatorname{vol}_n(X)\left(1 + \frac{\operatorname{vol}_n(Y)^{1/n}}{\operatorname{vol}_n(X)^{1/n}}\right)^n = \left(\operatorname{vol}_n(X)^{1/n} + \operatorname{vol}_n(Y)^{1/n}\right)^n. \end{aligned}$$

□

COROLLARY 2.7. *For bounded convex sets K_1 and K_2 of V, we have*

$$\operatorname{vol}_h(K_1 + K_2)^{1/n} \geq \operatorname{vol}_h(K_1)^{1/n} + \operatorname{vol}_h(K_2)^{1/n}.$$

Proof. Note that K_1, K_2 and $K_1 + K_2$ are bounded convex sets. Moreover, $\overline{K}_1$ and $\overline{K}_2$ are compact, and $\overline{K}_1 + \overline{K}_2 \subseteq \overline{K_1 + K_2}$. By Theorem 2.6, we have

$$\begin{aligned}\mathrm{vol}_h(K_1 + K_2)^{1/n} &= \mathrm{vol}_h(\overline{K_1 + K_2})^{1/n} \geq \mathrm{vol}_h(\overline{K}_1 + \overline{K}_2)^{1/n} \\ &\geq \mathrm{vol}_h(\overline{K}_1)^{1/n} + \mathrm{vol}_h(\overline{K}_2)^{1/n} \\ &= \mathrm{vol}_h(K_1)^{1/n} + \mathrm{vol}_h(K_2)^{1/n}.\end{aligned}$$ □

Corollary 2.8. *Let L be a subspace of V and let K be a bounded and symmetric convex set of V. Let h_L be the subinner product of L induced by h. Then, for any $x \in V$,*

$$\mathrm{vol}_{h_L}(K \cap L) \geq \mathrm{vol}_{h_L}(K \cap (L + x)),$$

where the volume of $K \cap (L + x)$ is measured on L by the natural identification $L \xrightarrow{\sim} L + x$ $(l \mapsto l + x)$.

Proof. Let $\pi : V \to L$ be the orthogonal projection with respect to h. We set

$$K_1 = \pi(K \cap (L + x)) \quad \text{and} \quad K_2 = \pi(K \cap (L - x)).$$

For a subset X of V, we put $-X = \{-x \mid x \in X\}$. Then, since

$$-K_2 = \pi(-(K \cap (L - x))) = \pi(K \cap (L + x)) = K_1,$$

$\mathrm{vol}_{h_L}(K_1) = \mathrm{vol}_{h_L}(K_2)$. Therefore, by Corollary 2.7, if we set $l = \dim L$, then

$$\begin{aligned}\mathrm{vol}_{h_L}((1/2)K_1 + (1/2)K_2) &\geq \left(\mathrm{vol}_{h_L}((1/2)K_1)^{1/l} + \mathrm{vol}_{h_L}((1/2)K_2)^{1/l}\right)^l \\ &= \left((1/2)\,\mathrm{vol}_{h_L}(K_1)^{1/l} + (1/2)\,\mathrm{vol}_{h_L}(K_2)^{1/l}\right)^l \\ &= \mathrm{vol}_{h_L}(K_1).\end{aligned}$$

On the other hand,

$$\frac{1}{2}K_1 + \frac{1}{2}K_2 \subseteq \pi\left(\frac{1}{2}(K \cap (L + x)) + \frac{1}{2}(K \cap (L - x))\right) \subseteq K \cap L,$$

and hence

$$\begin{aligned}\mathrm{vol}_{h_L}(K \cap L) &\geq \mathrm{vol}_{h_L}((1/2)K_1 + (1/2)K_2) \\ &\geq \mathrm{vol}_{h_L}(K_1) = \mathrm{vol}_{h_L}(K \cap (L + x)).\end{aligned}$$ □

2.4. Estimate of the number of points in a convex lattice

Let (V, h) be a pair of an n-dimensional real vector space V and an inner product h of V. Let Λ be a lattice of V. In this section, we prove the following estimate of the number of points in a convex lattice due to Gillet-Soulé [**25**].

Theorem 2.9. *We assume that (V, h, Λ) is unimodular, that is, $h(x, y) \in \mathbb{Z}$ for all $x, y \in \Lambda$, and, for a free basis $\{\omega_1, \ldots, \omega_n\}$ of Λ, $(h(\omega_i, \omega_j)) \in \mathrm{GL}(n, \mathbb{Z})$. Then, for a bounded and symmetric convex set K with an interior point, we have the following inequalities:*

$$6^{-n} \leq \frac{\#(K \cap \Lambda)}{\#(K^* \cap \Lambda)\,\mathrm{vol}_h(K)} \leq \left(\frac{3}{2}\right)^n (n!)^2.$$

For the proof of Theorem 2.9, we need to prepare several lemmas. Let us begin with the following lemma.

LEMMA 2.10. *Let $\phi : V \to V'$ be a surjective homomorphism of finite-dimensional real vector spaces, and let $W = \mathrm{Ker}(\phi)$. Let h_W be the subinner product of W induced by h, and let h' be the quotient inner product of V' induced by ϕ and h. Then, for a bounded and symmetric convex set K with an interior point, we have the following.*

(1) $\mathrm{vol}_h(K) \leq \mathrm{vol}_{h'}(\phi(K)) \, \mathrm{vol}_{h_W}(K \cap W)$.
(2) $\mathrm{vol}_h(K^*) \leq \mathrm{vol}_{h'}(\phi(K)^*) \, \mathrm{vol}_{h_W}((K \cap W)^*)$.

PROOF. (1) Let $W^\perp$ be the orthogonal complement of W with respect to h, and let $p : V \to W^\perp$ be the orthogonal projection to $W^\perp$ with respect to h. Moreover, let $h_{W^\perp}$ be the subinner product of $W^\perp$ induced by h. Then

$$\mathrm{vol}_h(K) = \int_{p(K)} \mathrm{vol}_{h_W}(p^{-1}(x) \cap K) d \, \mathrm{vol}_{h_{W^\perp}}.$$

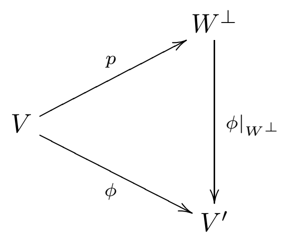
Note that

$$\mathrm{vol}_{h_W}(p^{-1}(x) \cap K) \leq \mathrm{vol}_{h_W}(W \cap K)$$

by Corollary 2.8, and hence

$$\mathrm{vol}_h(K) \leq \mathrm{vol}_{h_{W^\perp}}(p(K)) \, \mathrm{vol}_{h_W}(K \cap W).$$

As the following diagram is commutative:



and $\phi|_{W^\perp}$ gives rise to an isometry $(W^\perp, h_{W^\perp}) \xrightarrow{\sim} (V', h')$, we obtain

$$\mathrm{vol}_{h_{W^\perp}}(p(K)) = \mathrm{vol}_{h'}(\phi(K)).$$

Therefore, (1) follows.

(2) Let $q : V \to W$ be the orthogonal projection to W with respect to h. Here we claim the following:

CLAIM 3. (a) $\phi(K^* \cap W^\perp) \subseteq \phi(K)^*$.
(b) $q(K^*) \subseteq (K \cap W)^*$.

PROOF. Let $x \in K^* \cap W^\perp$ and $y \in K$. We put

$$y = y' + y'' \quad (y' \in W^\perp, y'' \in W).$$

Then $h(x, y) = h(x, y') = h'(\phi(x), \phi(y))$. On the other hand, as $x \in K^*$ and $y \in K$, we obtain $|h(x, y)| \leq 1$. Thus $|h'(\phi(x), \phi(y))| \leq 1$, which shows (a).

Next let $x \in K^*$ and $y \in K \cap W$. We set

$$x = x' + x'' \quad (x' \in W, x'' \in W^\perp).$$

Then $h(x, y) = h(x', y) = h_W(q(x), y)$. On the other hand, as $x \in K^*$ and $y \in K$, we have $|h(x, y)| \leq 1$. Thus $|h_W(q(x), y)| \leq 1$, which shows (b). □

Let us go back to the proof of (2). Note that $\operatorname{Ker}(q) = W^{\perp}$ and that h_W coincides with the quotient inner product of W induced by $q : V \to W$ and h. Thus, applying (1) to K^* and $q : V \to W$, we obtain

$$\begin{aligned}\operatorname{vol}_h(K^*) &\leq \operatorname{vol}_{h_{W^\perp}}(K^* \cap W^{\perp}) \operatorname{vol}_{h_W}(q(K^*)) \\ &= \operatorname{vol}_{h'}(\phi(K^* \cap W^{\perp})) \operatorname{vol}_{h_W}(q(K^*)).\end{aligned}$$

Therefore, (2) follows from the above claim. □

Next we consider the following lemma.

LEMMA 2.11. (1) *Let $0 \to V' \xrightarrow{\phi} V \xrightarrow{\psi} V'' \to 0$ be an exact sequence of finite-dimensional real vector spaces. Let h be an inner product of V. Let h' be the subinner product of V' induced by $\phi : V' \to V$ and h, and let h'' be the quotient inner product of V'' induced by $\psi : V \to V''$ and h. Let Λ', Λ and Λ'' be lattices of V', V and V'', respectively. We assume that the above exact sequence gives rise to an exact sequence $0 \to \Lambda' \to \Lambda \to \Lambda'' \to 0$ as $\mathbb{Z}$-modules. Then we have*

$$\operatorname{vol}_h(V/\Lambda) = \operatorname{vol}_{h'}(V'/\Lambda') \operatorname{vol}_{h''}(V''/\Lambda'').$$

(2) *Let V be a finite-dimensional real vector space, h an inner product of V and $h^{\vee}$ the dual inner product of h. Let Λ be a lattice of V and $\Lambda^{\vee} = \operatorname{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$. Then $\Lambda^{\vee}$ is a lattice of $V^{\vee}$ and $\operatorname{vol}_{h^\vee}(V^{\vee}/\Lambda^{\vee}) = \operatorname{vol}_h(V/\Lambda)^{-1}$.*

PROOF. (1) Let $\{e'_1, \ldots, e'_m\}$, $\{e_1, \ldots, e_n\}$ and $\{e''_1, \ldots, e''_{n-m}\}$ be free bases of Λ', Λ and Λ'' such that

$$\phi(e'_i) = e_i \quad (i = 1, \ldots, m) \quad \text{and} \quad \psi(e_{m+j}) = e''_j \quad (j = 1, \ldots, n-m).$$

Then, by Lemma 1.1,

$$\det(h(e_i, e_j)) = \det(h'(e'_i, e'_j)) \det(h''(e''_i, e''_j)).$$

Thus we obtain (1).

(2) Let $e_1, \ldots, e_n$ be a free basis of Λ, and let $e_1^{\vee}, \ldots, e_n^{\vee}$ be the dual basis of $e_1, \ldots, e_n$ in $V^{\vee}$. Then $e_1^{\vee}, \ldots, e_n^{\vee}$ form a free basis of $\Lambda^{\vee}$. On the other hand, by Lemma 1.4, $(h(e_i, e_j))(h^{\vee}(e_i^{\vee}, e_j^{\vee})) = I_n$, and hence (2) follows. □

From now on, let Λ be a lattice of V.

LEMMA 2.12. *Let K be a bounded and symmetric convex set with an interior point. If $K \cap \Lambda$ generates V as a real vector space, then*

$$\#(K \cap \Lambda) \operatorname{vol}_h(K^*) \operatorname{vol}_h(V/\Lambda) \leq 6^n.$$

Note that we do not assume that (V, h, Λ) is unimodular.

PROOF. First, let us recall the primitivity of a lattice point. For $x \in \Lambda \setminus \{0\}$, x is said to be *primitive* if there are no integer $l \geq 2$ and $y \in \Lambda \setminus \{0\}$ such that $x = ly$. Note that x is primitive if and only if $\Lambda/\mathbb{Z}x$ has no torsion. Moreover, as K is a symmetric convex set, we can find a primitive lattice point in K if $K \cap \Lambda \neq \{0\}$.

Let Λ' be a $\mathbb{Z}$-module generated by $K \cap \Lambda$. Then $\Lambda' \subseteq \Lambda$ and $\operatorname{rk} \Lambda' = \operatorname{rk} \Lambda$. Thus $\operatorname{vol}_h(V/\Lambda') \geq \operatorname{vol}_h(V/\Lambda)$. Note that $\#(K \cap \Lambda') = \#(K \cap \Lambda)$. Therefore, if the assertion of the lemma holds for Λ', then it also holds for Λ, so that we may assume that $K \cap \Lambda$ generates Λ as a $\mathbb{Z}$-module.

We prove the lemma by induction on n under the assumption that $K \cap \Lambda$ generates Λ as a $\mathbb{Z}$-module. First we have the case where $n = 1$. Clearly we may assume that $V = \mathbb{R}$, h is the standard inner product, $\Lambda = \mathbb{Z}a$ ($a > 0$) and K is a symmetric interval. It is easy to see the following claim.

Claim 4. *Let a be a positive real number and let I be an interval in $\mathbb{R}$. Then*

$$\#(I \cap \mathbb{Z}a) \leq \frac{\mathrm{vol}_1(I)}{a} + 1.$$

Using the above claim, $\#(K \cap \Lambda) \leq \mathrm{vol}_1(K)/a + 1$. Moreover, since $[-a, a] \subseteq K$, $2a \leq \mathrm{vol}_1(K)$. On the other hand, $\mathrm{vol}_1(K)\,\mathrm{vol}_1(K^*) = 4$. Thus we obtain

$$\#(K \cap \Lambda)\,\mathrm{vol}_1(K^*)\,\mathrm{vol}_1(\mathbb{R}/\Lambda) \leq 4 + \frac{4a}{\mathrm{vol}_1(K)} \leq 6.$$

Next we assume that $n \geq 2$. We choose a primitive lattice point ω in K. Let $V'' = V/\mathbb{R}\omega$, $\psi : V \to V''$ the natural homomorphism, $\Lambda'' = \psi(\Lambda)$ and $K'' = \psi(K)$. Moreover, we set $V' = \mathbb{R}\omega$, $\Lambda' = \mathbb{Z}\omega$ and $K' = K \cap V'$. Let h'' be the quotient inner product of V'' induced by $\psi : V \to V''$ and h, and let h' be the subinner product of V' induced by h. Then, as $K'' \cap \Lambda''$ generates Λ'' as a $\mathbb{Z}$-module, by using the hypothesis of induction,

$$\#(K'' \cap \Lambda'')\,\mathrm{vol}_{h''}(K''^*)\,\mathrm{vol}_{h''}(V''/\Lambda'') \leq 6^{n-1} \tag{2.2}$$

holds. Moreover, we can see

$$\#(K \cap \Lambda) \leq \#(K'' \cap \Lambda'') \cdot \sup_{y \in \Lambda''} \#(\psi^{-1}(y) \cap K \cap \Lambda).$$

For $y \in \Lambda''$, let us fix $x \in \Lambda$ with $\psi(x) = y$. Since

$$\#(\psi^{-1}(y) \cap K \cap \Lambda) = \#(\psi^{-1}(0) \cap (K - x) \cap \Lambda)$$

and

$$\mathrm{vol}_{h'}(\psi^{-1}(y) \cap K) = \mathrm{vol}_{h'}(\psi^{-1}(0) \cap (K - x)),$$

using Claim 4, we have

$$\#(\psi^{-1}(y) \cap K \cap \Lambda) \leq \frac{\mathrm{vol}_{h'}(\psi^{-1}(y) \cap K)}{\mathrm{vol}_{h'}(V'/\Lambda')} + 1.$$

On the other hand, by Corollary 2.8,

$$\mathrm{vol}_{h'}(\psi^{-1}(y) \cap K) \leq \mathrm{vol}_{h'}(\psi^{-1}(0) \cap K) = \mathrm{vol}_{h'}(K').$$

Note that $\pm\omega \in K'$. Thus $\mathrm{vol}_{h'}(K')/\mathrm{vol}_{h'}(V'/\Lambda') \geq 2$, so that

$$\frac{\mathrm{vol}_{h'}(K')}{\mathrm{vol}_{h'}(V'/\Lambda')} + 1 \leq (3/2)\frac{\mathrm{vol}_{h'}(K')}{\mathrm{vol}_{h'}(V'/\Lambda')}.$$

Hence

$$\#(K \cap \Lambda) \leq \#(K'' \cap \Lambda'')(3/2)\frac{\mathrm{vol}_{h'}(K')}{\mathrm{vol}_{h'}(V'/\Lambda')}. \tag{2.3}$$

Moreover, by Lemma 2.10,

$$\mathrm{vol}_h(K^*) \leq \mathrm{vol}_{h'}(K'^*)\,\mathrm{vol}_{h''}(K''^*). \tag{2.4}$$

Therefore, by (2.2), (2.3) and (2.4), we obtain

$$\begin{aligned}&\#(K\cap\Lambda)\operatorname{vol}_h(K^*)\operatorname{vol}_h(V/\Lambda)\\&\qquad\le 6^n\frac{\operatorname{vol}_{h'}(K')\operatorname{vol}_{h'}(K'^*)}{4}\frac{\operatorname{vol}_h(V/\Lambda)}{\operatorname{vol}_{h'}(V'/\Lambda')\operatorname{vol}_{h''}(V''/\Lambda'')}.\end{aligned}$$

Note that $\operatorname{vol}_{h'}(K')\operatorname{vol}_{h'}(K'^*) = 4$ ($\because \dim V' = 1$), and that

$$\operatorname{vol}_h(V/\Lambda) = \operatorname{vol}_{h'}(V'/\Lambda')\operatorname{vol}_{h''}(V''/\Lambda'')$$

by Lemma 2.11. Hence the lemma follows. □

LEMMA 2.13. *We assume that (V, h, Λ) is unimodular. Let T be a saturated $\mathbb{Z}$-submodule of Λ, that is, T is a $\mathbb{Z}$-submodule of Λ and Λ/T has no torsion. We set*

$$T^{\perp} = \{x\in\Lambda \mid h(x,y) = 0 \text{ for all } y\in T\}.$$

Let W be a vector subspace of V generated by T, and let $W^{\perp}$ be the orthogonal complement of W. Then we have the following:

(1) *$T^{\perp}$ is a lattice of $W^{\perp}$.*
(2) *Let h_W and $h_{W^{\perp}}$ be the subinner products of W and $W^{\perp}$ induced by h, respectively. Then*

$$\operatorname{vol}_{h_W}(W/T) = \operatorname{vol}_{h_{W^{\perp}}}(W^{\perp}/T^{\perp}).$$

PROOF. Let us consider a homomorphism

$$\alpha : T^{\perp} \to \operatorname{Hom}_{\mathbb{Z}}(\Lambda/T, \mathbb{Z})$$

given by $\alpha(x) = h(x,\cdot)$. First let us see that α is an isomorphism. Clearly α is injective. Let us choose $\phi \in \operatorname{Hom}_{\mathbb{Z}}(\Lambda/T,\mathbb{Z})$. A homomorphism $\Lambda \to \Lambda/T \xrightarrow{\phi} \mathbb{Z}$ is denoted by $\widetilde{\phi}$. Since (V,h,Λ) is unimodular, there is $x\in\Lambda$ such that $\widetilde{\phi}(\cdot) = h(x,\cdot)$. Note that $\widetilde{\phi}(y) = 0$ for all $y \in T$. Thus $x\in T^{\perp}$, which show the surjectivity of α.

(1) Since α is bijective,

$$\operatorname{rk} T^{\perp} = \dim_{\mathbb{R}} V - \dim_{\mathbb{R}} W = \dim_{\mathbb{R}} W^{\perp}.$$

On the other hand, as $T^{\perp}\subseteq W^{\perp}$, $T^{\perp}$ is a lattice of $W^{\perp}$.

(2) Let $h_{V/W}$ be the quotient inner product of V/W induced by h, and let $h_{V/W}^{\vee}$ be the dual inner product of $\operatorname{Hom}_{\mathbb{R}}(V/W,\mathbb{R})$ induced by $h_{V/W}$. Let $x_1,\ldots,x_n$ be an orthonormal basis of V such that $x_1,\ldots,x_l \in W^{\perp}$ and $x_{l+1},\ldots,x_n\in W$. Moreover, let $x_1^{\vee},\ldots,x_n^{\vee}$ be the dual basis of $x_1,\ldots,x_n$. Then $x_1^{\vee},\ldots,x_l^{\vee}$ give rise to an orthonormal basis of $\operatorname{Hom}_{\mathbb{R}}(V/W,\mathbb{R})$ with respect to $h_{V/W}^{\vee}$. Let $\alpha_{\mathbb{R}} : W^{\perp}\to \operatorname{Hom}_{\mathbb{R}}(V/W,\mathbb{R})$ be a homomorphism given by $\alpha_{\mathbb{R}}(x) = h(x,\cdot)$. Then we can see that $\alpha_{\mathbb{R}}(x_i) = x_i^{\vee}$ $(i=1,\ldots,l)$. Thus $\alpha_{\mathbb{R}}$ yields an isometry

$$\alpha_{\mathbb{R}} : \left(W^{\perp}, h_{W^{\perp}}\right) \to \left(\operatorname{Hom}_{\mathbb{R}}(V/W,\mathbb{R}), h_{V/W}^{\vee}\right).$$

Therefore,

$$\operatorname{vol}_{h_{W^{\perp}}}(W^{\perp}/T^{\perp}) = \operatorname{vol}_{h_{V/W}^{\vee}}(\operatorname{Hom}_{\mathbb{R}}(V/W,\mathbb{R})/\operatorname{Hom}_{\mathbb{Z}}(\Lambda/T,\mathbb{Z})),$$

which implies that

$$\operatorname{vol}_{h_{W^{\perp}}}(W^{\perp}/T^{\perp}) = \operatorname{vol}_{h_{V/W}}((V/W)/(\Lambda/T))^{-1}$$

by (2) in Lemma 2.11. On the other hand, by using (1) in Lemma 2.11,

$$\mathrm{vol}_h(V/\Lambda) = \mathrm{vol}_{h_W}(W/T)\,\mathrm{vol}_{h_{V/W}}((V/W)/(\Lambda/T)).$$

Note that $\mathrm{vol}_h(V/\Lambda) = 1$ because (V, h, Λ) is unimodular. Thus (2) follows. □

PROOF OF THEOREM 2.9. First let us show the inequality

$$6^{-n} \le \frac{\#(K \cap \Lambda)}{\#(K^* \cap \Lambda)\,\mathrm{vol}_h(K)}, \tag{2.5}$$

which is the left side inequality in Theorem 2.9. Let T be the saturation of a $\mathbb{Z}$-submodule of Λ generated by $K^* \cap \Lambda$, that is, T is the minimal saturated $\mathbb{Z}$-submodule of Λ containing $K^* \cap \Lambda$. Let W be the vector subspace generated by T, and let $W^\perp$ be the orthonormal complement of W with respect to h. Moreover, let vol_W be the Haar measure of W induced by $h|_{W \times W}$. Then, since $\#(K^* \cap \Lambda) = \#(K^* \cap T)$, by Lemma 2.12,

$$\#(K^* \cap \Lambda) = \#(K^* \cap T) \le \frac{6^{n_0}}{\mathrm{vol}_W((K^* \cap W)^*)\,\mathrm{vol}_W(W/T)}, \tag{2.6}$$

where $n_0 = \dim W$. Let $p : V \to W$ be the orthogonal projection to W with respect to h. Let us see that $p(K) \subseteq (K^* \cap W)^*$. Indeed, let $x \in K$ and $y \in K^* \cap W$. We set $x = x' + x''$ ($x' \in W$, $x'' \in W^\perp$). Then

$$h(x, y) = h(x', y) = h(p(x), y).$$

On the other hand, as $x \in K$ and $y \in K^*$, we have $|h(x, y)| \le 1$. Thus $|h(p(x), y)| \le 1$, which shows that $p(K) \subseteq (K^* \cap W)^*$. Therefore, (2.6) implies

$$\#(K^* \cap \Lambda) \le \frac{6^{n_0}}{\mathrm{vol}_W(p(K))\,\mathrm{vol}_W(W/T)}. \tag{2.7}$$

CLAIM 5. *Let K° be the set of interior points of K. Then, for all $x \in K^\circ$ and $y \in K^*$, $|h(x, y)| < 1$.*

PROOF. We assume the contrary. Since K^* is symmetric, there are $x \in K^\circ$ and $y \in K^*$ with $h(x, y) = 1$. In particular, $y \ne 0$. As x is an interior point of K, for a sufficiently small positive real number ϵ, $x + \epsilon y \in K$. Therefore, $h(x + \epsilon y, y) \le 1$. On the other hand, $h(x + \epsilon y, y) = 1 + \epsilon h(y, y) > 1$. This is a contradiction. □

For $x \in K^\circ \cap \Lambda$ and $y \in K^* \cap \Lambda$, $h(x, y) \in \mathbb{Z}$ and $|h(x, y)| < 1$ by the above claim. Thus $h(x, y) = 0$. This means that $K^\circ \cap \Lambda \subseteq W^\perp$. Therefore,

$$\#(K \cap \Lambda) \ge \#(K^\circ \cap \Lambda) = \#(K^\circ \cap W^\perp \cap \Lambda).$$

Here we set

$$T^\perp = \{x \in \Lambda \mid h(x, y) = 0 \text{ for all } y \in T\},$$

that is, $W^\perp \cap \Lambda = T^\perp$. By Lemma 2.13, $T^\perp$ is a lattice of $W^\perp$. By Corollary 2.2,

$$\#(K^\circ \cap T^\perp) \ge 2^{n_0 - n} \frac{\mathrm{vol}_{W^\perp}(K^\circ \cap W^\perp)}{\mathrm{vol}_{W^\perp}(W^\perp/T^\perp)},$$

where $\mathrm{vol}_{W^\perp}$ is the Haar measure induced by $h|_{W^\perp \times W^\perp}$. Therefore, as $2^{n_0-n} \ge 6^{n_0-n}$,

$$\#(K^\circ \cap \Lambda) \ge 6^{n_0 - n} \frac{\mathrm{vol}_{W^\perp}(K^\circ \cap W^\perp)}{\mathrm{vol}_{W^\perp}(W^\perp/T^\perp)}. \tag{2.8}$$

By the inequalities (2.7), (2.8), $K^\circ \subseteq K$ and Lemma 2.13, we obtain

$$\frac{\#(K \cap \Lambda)}{\#(K^* \cap \Lambda)} \geq 6^{-n} \operatorname{vol}_{W^\perp}(K^\circ \cap W^\perp) \operatorname{vol}_W(p(K^\circ)).$$

Therefore, by virtue of Lemma 2.10, we have

$$\frac{\#(K \cap \Lambda)}{\#(K^* \cap \Lambda)} \geq 6^{-n} \operatorname{vol}_h(K^\circ) = 6^{-n} \operatorname{vol}_h(K).$$

Hence the inequality (2.5) follows.

Next let us consider the right side inequality in Theorem 2.9:

$$\frac{\#(K \cap \Lambda)}{\#(K^* \cap \Lambda) \operatorname{vol}_h(K)} \leq \left(\frac{3}{2}\right)^n (n!)^2. \tag{2.9}$$

Applying the inequality (2.5) to K^*, we have

$$6^{-n} \leq \frac{\#(K^* \cap \Lambda)}{\#((K^*)^* \cap \Lambda) \operatorname{vol}(K^*)}.$$

On the other hand, $K \subseteq (K^*)^*$ and $4^n (n!)^{-2} \leq \operatorname{vol}(K) \operatorname{vol}(K^*)$ by Mahler's inequality. Therefore,

$$\begin{aligned} 6^{-n} &\leq \frac{\#(K^* \cap \Lambda)}{\#((K^*)^* \cap \Lambda) \operatorname{vol}(K^*)} \leq \frac{\#(K^* \cap \Lambda)}{\#(K \cap \Lambda) \operatorname{vol}(K^*)} \\ &\leq \frac{(n!)^2 \#(K^* \cap \Lambda) \operatorname{vol}(K)}{4^n \#(K \cap \Lambda)}, \end{aligned}$$

which shows (2.9). □

As an application of Theorem 2.9, we can see that

$$\#((aK) \cap \Lambda) \leq a^n 9^n (n!)^2 \#(K \cap \Lambda)$$

for a real number a with $a \geq 1$. Indeed, as $(aK)^* \subseteq K^*$ and $\operatorname{vol}(aK) = a^n \operatorname{vol}(K)$, applying Theorem 2.9 to aK,

$$\begin{aligned} \#((aK) \cap \Lambda) &\leq \left(\frac{3}{2}\right)^n (n!)^2 \#((aK)^* \cap \Lambda) \operatorname{vol}(aK) \\ &\leq a^n \left(\frac{3}{2}\right)^n (n!)^2 \#(K^* \cap \Lambda) \operatorname{vol}(K). \end{aligned}$$

Moreover, by Theorem 2.9,

$$\#(K^* \cap \Lambda) \operatorname{vol}(K) \leq 6^n \#(K \cap \Lambda),$$

as required.

Using Yuan's idea [**74**] or [**53**], we have the following better estimation.

LEMMA 2.14. *Let V be a finite-dimensional real vector space and K a bounded symmetric convex set in V (note that K does not necessarily generate V). Let Λ be a lattice of V, Λ' a $\mathbb{Z}$-submodule of Λ and $r : \Lambda \to \Lambda/\Lambda'$ the natural homomorphism. Then we have the following estimation:*

$$\log \#r(K \cap \Lambda) \geq \log \#(K \cap \Lambda) - \log \#(2K \cap \Lambda'), \tag{2.10}$$

$$\log \#r(K \cap \Lambda) \leq \log \#(2K \cap \Lambda) - \log \#(K \cap \Lambda'). \tag{2.11}$$

Moreover, if a is a real number with $a \geq 1$,

$$0 \leq \log \#(aK \cap \Lambda) - \log \#(K \cap \Lambda) \leq \log(\lceil 2a \rceil) \dim V. \tag{2.12}$$

PROOF. (2.10) Let $t \in r(K \cap \Lambda)$ and fix $s_0 \in K \cap \Lambda$ with $r(s_0) = t$. Then, for any $s \in r^{-1}(t) \cap K \cap \Lambda$,

$$s - s_0 = s + (-s_0) \in 2K \cap \Lambda'.$$

Thus

$$\#(r^{-1}(t) \cap K \cap \Lambda) \leq \#(2K \cap \Lambda').$$

Therefore,

$$\#(K \cap \Lambda) = \sum_{t \in r(K \cap \Lambda)} \#(r^{-1}(t) \cap K \cap \Lambda) \leq \#(r(K \cap \Lambda))\#(2K \cap \Lambda'),$$

as required.

(2.11) We set $S = K \cap \Lambda + K \cap \Lambda'$. Then $r(S) = r(K \cap \Lambda)$ and $S \subseteq 2K \cap \Lambda$. Moreover, for all $t \in r(S)$,

$$\#(K \cap \Lambda') \leq \#(S \cap r^{-1}(t)).$$

Indeed, if we choose $s_0 \in K \cap \Lambda$ with $r(s_0) = t$, then

$$s_0 + K \cap \Lambda' \subseteq S \cap r^{-1}(t).$$

Therefore,

$$\begin{aligned}\#(2K \cap \Lambda) \geq \#(S) = \sum_{t \in r(S)} \#(r^{-1}(t) \cap S) &\geq \#(r(S))\#(K \cap \Lambda') \\ &= \#(r(K \cap \Lambda))\#(K \cap \Lambda')\end{aligned}$$

as required.

(2.12) We set $n = \lceil 2a \rceil$. Applying (2.10) to the case where $(n/2)K$ and $\Lambda' = n\Lambda$, we have

$$\log \#((n/2)K \cap \Lambda) - \log \#(nK \cap n\Lambda) \leq \log \#\Lambda/n\Lambda = \log(n) \dim V.$$

Note that $a \leq n/2$ and $\#(nK \cap n\Lambda) = \#(K \cap \Lambda)$. Hence we obtain

$$\begin{aligned}0 &\leq \log \#(aK \cap \Lambda) - \log \#(K \cap \Lambda) \\ &\leq \log \#((n/2)K \cap \Lambda) - \log \#(nK \cap n\Lambda) \leq \log(n) \dim V.\end{aligned}$$

□

2.5. Normed finitely generated ℤ-module

A pair $(M, \|\cdot\|)$ is called a *normed finitely generated ℤ-module* if M is a finitely generated ℤ-module and $\|\cdot\|$ is a norm of $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$. For a normed finitely generated ℤ-module $(M, \|\cdot\|)$, we define $\hat{H}^0(M, \|\cdot\|)$ to be

$$\hat{H}^0(M, \|\cdot\|) := \{x \in M \mid \|x\| \leq 1\},$$

and the logarithm of the number of $\hat{H}^0(M, \|\cdot\|)$ is denoted by $\hat{h}^0(M, \|\cdot\|)$, that is,

$$\hat{h}^0(M, \|\cdot\|) := \log \#\hat{H}^0(M, \|\cdot\|).$$

Moreover, we set

$$\hat{H}^0_{<1}(M, \|\cdot\|) := \{x \in M \mid \|x\| < 1\} \quad \text{and} \quad \hat{h}^0_{<1}(M, \|\cdot\|) := \log \#\hat{H}^0_{<1}(M, \|\cdot\|).$$

Let M_{tor} be the torsion part of M. By its definition, it is easy to see that

$$\hat{h}^0(M, \|\cdot\|) = \hat{h}^0(M/M_{tor}, \|\cdot\|) + \log \#(M_{tor}).$$

Note that M/M_{tor} is a lattice of $M_{\mathbb{R}}$. We define $\widehat{\chi}(M, \|\cdot\|)$ to be

$$\widehat{\chi}(M, \|\cdot\|) := \log\left(\frac{\operatorname{vol}(B(M, \|\cdot\|))}{\operatorname{vol}(M_{\mathbb{R}}/(M/M_{tor}))}\right) + \log \#(M_{tor}),$$

where $B(M, \|\cdot\|) = \{x \in M_{\mathbb{R}} \mid \|x\| \leq 1\}$. Note that $\widehat{\chi}(M, \|\cdot\|)$ does not depend on the choice of a Haar measure of $M_{\mathbb{R}}$. In terms of the notation in Section 2.1, if M is free, then

$$\widehat{\chi}(M, \|\cdot\|) = \widehat{\chi}(B(M, \|\cdot\|); M).$$

Let $M^{\vee}$ be the dual space of M over $\mathbb{Z}$, that is, $M^{\vee} = \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$. Note that $M^{\vee}$ has no torsion elements. As $(M^{\vee})_{\mathbb{R}}$ is naturally isomorphic to $(M_{\mathbb{R}})^{\vee}$, we denote $(M^{\vee})_{\mathbb{R}}$ by $M_{\mathbb{R}}^{\vee}$. The dual norm of the norm $M_{\mathbb{R}}$ of $\|\cdot\|$ is denoted by $\|\cdot\|^{\vee}$ (cf. Section 1.2). Then $\hat{H}^1(M, \|\cdot\|)$ and $\hat{h}^1(M, \|\cdot\|)$ are defined by

$$\hat{H}^1(M, \|\cdot\|) := \hat{H}^0(M^{\vee}, \|\cdot\|^{\vee}) \quad \text{and} \quad \hat{h}^1(M, \|\cdot\|) := \hat{h}^0(M^{\vee}, \|\cdot\|^{\vee}).$$

If $M = \{0\}$, then $\hat{h}^0(M, \|\cdot\|)$, $\hat{h}^1(M, \|\cdot\|)$ and $\widehat{\chi}(M, \|\cdot\|)$ are defined to be 0.

Let $\Sigma = \{e_1, \ldots, e_r\}$ be a free basis of M/M_{tor}, and let $\langle\ ,\ \rangle_{\Sigma}$ be the standard inner product with respect to Σ, that is, for $x = a_1e_1, + \cdots + a_re_r$, $y = b_1e_1 + \cdots + b_re_r \in M/M_{tor}$,

$$\langle x, y\rangle_{\Sigma} = a_1b_1 + \cdots + a_rb_r.$$

Then we have the following.

Lemma 2.15. *We can calculate $\hat{h}^1(M, \|\cdot\|)$ by the following formula:*

$$\hat{h}^1(M, \|\cdot\|) = \log \# \left\{x \in M/M_{tor} \mid |\langle x, y\rangle_{\Sigma}| \leq 1 \quad (\forall y \in B(M, \|\cdot\|)\right\}.$$

Proof. Let $e_1^{\vee}, \ldots, e_r^{\vee}$ be the dual basis of $e_1, \ldots, e_r$. For $\phi \in \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$, there are unique $a_1, \ldots, a_r \in \mathbb{Z}$ with $\phi = a_1e_1^{\vee} + \cdots + a_re_r^{\vee}$. Since

$$\phi(y) = a_1b_1 + \cdots + a_rb_r = \langle a_1e_1 + \cdots + a_re_r, y\rangle_{\Sigma}$$

for $y = b_1e_1 + \cdots + b_re_r \in M_{\mathbb{R}}$,

$$\begin{aligned} \|\phi\|^{\vee} \leq 1 \quad &\iff \quad |\phi(y)| \leq 1 \ (\forall y \in B(M, \|\cdot\|)) \\ &\iff \quad |\langle a_1e_1 + \cdots + a_re_r, y\rangle_{\Sigma}| \leq 1 \ (\forall y \in B(M, \|\cdot\|)). \end{aligned}$$

Thus the lemma follows. □

Here let us consider the following two propositions. The second one is an important tool to estimate $\hat{h}^0$ of normed finitely generated $\mathbb{Z}$-modules.

Proposition 2.16. *For a finitely generated $\mathbb{Z}$-module M, the following hold.*

(1) *Let $\|\cdot\|_1$ and $\|\cdot\|_2$ be norms of $M_{\mathbb{R}}$ with $\|\cdot\|_1 \leq \|\cdot\|_2$. Then*

$$\widehat{\chi}(M, \|\cdot\|_1) \geq \widehat{\chi}(M, \|\cdot\|_2).$$

(2) *Let $\|\cdot\|$ be a norm of M. For a real number λ,*

$$\widehat{\chi}(M, \exp(-\lambda)\|\cdot\|) = \lambda \operatorname{rk}(M) + \widehat{\chi}(M, \|\cdot\|).$$

Proof. (1) is obvious because $B(M, \|\cdot\|_1) \supseteq B(M, \|\cdot\|_2)$. (2) follows from the fact that $B(M, \exp(-\lambda)\|\cdot\|) = \exp(\lambda)B(M, \|\cdot\|)$. □

Proposition 2.17. *The following* (1)–(5) *hold.*

(1) *For a normed finitely generated $\mathbb{Z}$-module $(M, \|\cdot\|)$,*

$$-\log(6)\operatorname{rk} M \leq \hat{h}^0(M, \|\cdot\|) - \hat{h}^1(M, \|\cdot\|) - \widehat{\chi}(M, \|\cdot\|) \\ \leq \log(3/2)\operatorname{rk} M + 2\log((\operatorname{rk} M)!)$$

(2) *Let $\|\cdot\|_1$ and $\|\cdot\|_2$ be norms of a finitely generated $\mathbb{Z}$-module M with $\|\cdot\|_1 \leq \|\cdot\|_2$. Then we have*

$$\hat{h}^0(M, \|\cdot\|_1) \geq \hat{h}^0(M, \|\cdot\|_2) \quad \text{and} \quad \hat{h}^1(M, \|\cdot\|_1) \leq \hat{h}^1(M, \|\cdot\|_2).$$

Moreover,

$$\widehat{\chi}(M, \|\cdot\|_2) - \widehat{\chi}(M, \|\cdot\|_1) \leq \hat{h}^0(M, \|\cdot\|_2) - \hat{h}^0(M, \|\cdot\|_1) \\ + \log(9)\operatorname{rk} M + 2\log((\operatorname{rk} M)!).$$

(3) *For a non-negative real number λ,*

$$0 \leq \hat{h}^0(M, \exp(-\lambda)\|\cdot\|) - \hat{h}^0(M, \|\cdot\|) \leq \lambda \operatorname{rk} M + \log(3)\operatorname{rk} M.$$

(4) *Let*

$$0 \to (M', \|\cdot\|') \xrightarrow{f} (M, \|\cdot\|) \xrightarrow{g} (M'', \|\cdot\|'') \to 0$$

be an exact sequence of normed finitely generated $\mathbb{Z}$-modules, that is,

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

is an exact sequence of finitely generated $\mathbb{Z}$-modules, $\|\cdot\|'$ is the subnorm induced by $M'_{\mathbb{R}} \to M_{\mathbb{R}}$ and $\|\cdot\|$, and $\|\cdot\|''$ is the quotient norm induced by $M_{\mathbb{R}} \to M''_{\mathbb{R}}$ and $\|\cdot\|$. Then

$$\hat{h}^0(M, \|\cdot\|) \leq \hat{h}^0(M', \|\cdot\|') + \hat{h}^0(M'', \|\cdot\|'') + \log(6)\operatorname{rk} M'.$$

(5) *If there is a free basis $\{e_1, \ldots, e_{\operatorname{rk} M}\}$ of M/M_{tor} with $\|e_i\| \leq 1$ for all i, then*

$$\hat{h}^1(M, \|\cdot\|) \leq \log(3)\operatorname{rk} M.$$

Proof. (1) Since

$$\hat{h}^0(M, \|\cdot\|) - \hat{h}^1(M, \|\cdot\|) - \widehat{\chi}(M, \|\cdot\|) \\ = \hat{h}^0(M/M_{tor}, \|\cdot\|) - \hat{h}^1(M/M_{tor}, \|\cdot\|) - \widehat{\chi}(M/M_{tor}, \|\cdot\|),$$

we may assume that M is torsion free. If we put $K = \{x \in M_{\mathbb{R}} \mid \|x\| \leq 1\}$, then $\hat{h}^0(M, \|\cdot\|) = \log \#(K \cap M)$ and $\hat{h}^1(M, \|\cdot\|) = \log \#(K^* \cap M)$ by Lemma 2.15. Moreover, if h is a metric of $M_{\mathbb{R}}$ such that a free basis of M is an orthogonal basis with respect to h, then $\widehat{\chi}(M, \|\cdot\|) = \log \operatorname{vol}_h(K)$. Thus (1) follows from Theorem 2.9.

(2) The inequalities

$$\hat{h}^0(M, \|\cdot\|_1) \geq \hat{h}^0(M, \|\cdot\|_2) \quad \text{and} \quad \hat{h}^1(M, \|\cdot\|_1) \leq \hat{h}^1(M, \|\cdot\|_2)$$

are obvious. The third inequality follows from (1).

(3) Since

$$\hat{h}^0(M, \exp(-\lambda)\|\cdot\|) - \hat{h}^0(M, \|\cdot\|) = \hat{h}^0(M/M_{tor}, \exp(-\lambda)\|\cdot\|) - \hat{h}^0(M/M_{tor}, \|\cdot\|),$$

we may assume that M is torsion free. Note that $\lceil 2a \rceil \leq 3a$ for $a \geq 1$. Thus (3) follows from Lemma 2.14.

(4) We may assume that M' is a submodule of M. We choose $x_1, \ldots, x_l \in M$ as follows:

(i) $\|x_i\| \leq 1$ $(\forall i)$.
(ii) $g(x_i) \neq g(x_j)$ $(\forall i \neq j)$.
(iii) For any $x \in M$ with $\|x\| \leq 1$, there is x_i with $g(x) = g(x_i)$.

Using (ii) and (iii), for $x \in M$ with $\|x\| \leq 1$, there is a unique x_i with $g(x) = g(x_i)$. Moreover, $x - x_i \in M'$ and $\|x - x_i\| \leq 2$. On the other hand, $\log(l) \leq \hat{h}^0(M'', \|\cdot\|'')$ because $\|g(x_i)\|'' \leq 1$ for all $i = 1, \ldots, l$. Therefore, we have

$$\hat{h}^0(M, \|\cdot\|) \leq \hat{h}^0(M'', \|\cdot\|'') + \log \#\{x' \in M' \mid \|x'\| \leq 2\}.$$

Thus (4) is a consequence of (3).

(5) Let $\langle\ ,\ \rangle$ be the standard inner product with respect to the basis $\{e_1, \ldots, e_{\operatorname{rk} M}\}$. Then, for $x = a_1 e_1 + \cdots + a_{\operatorname{rk} M} e_{\operatorname{rk} M}$, if $|\langle x, e_i \rangle| \leq 1$ holds for every i, then $|a_i| \leq 1$ $(\forall i)$. Thus (5) follows from Lemma 2.15. □

2.6. $\lambda_{\mathbb{Q}}$ and $\lambda_{\mathbb{Z}}$

In this section, we consider basic properties of $\lambda_{\mathbb{Q}}$ and $\lambda_{\mathbb{Z}}$ treated in [**75**], [**76**] and [**54**].

For a normed finitely generated $\mathbb{Z}$-module $(M, \|\cdot\|)$, we introduce $\lambda_{\mathbb{Q}}(M, \|\cdot\|)$ and $\lambda_{\mathbb{Z}}(M, \|\cdot\|)$ as follows: If M is not a torsion module, then

$$\lambda_{\mathbb{Q}}(M, \|\cdot\|) = \min \left\{ \lambda \in \mathbb{R}_{\geq 0} \;\middle|\; \begin{array}{l} \exists\ x_1, \ldots, x_n \in M \text{ such that } \{x_1, \ldots, x_n\} \text{ gives} \\ \text{a basis of } M_{\mathbb{Q}} = M \otimes_{\mathbb{Z}} \mathbb{Q} \text{ and } \max_i\{\|x_i\|\} \leq \lambda \end{array} \right\}$$

and

$$\lambda_{\mathbb{Z}}(M, \|\cdot\|) = \min \left\{ \lambda' \in \mathbb{R}_{\geq 0} \;\middle|\; \begin{array}{l} \exists\ x_1, \ldots, x_n \in M \text{ such that } \{x_1, \ldots, x_n\} \text{ gives} \\ \text{a free basis of } M/M_{tor} \text{ and } \max_i\{\|x_i\|\} \leq \lambda' \end{array} \right\}.$$

In the case where M is a torsion module,

$$\lambda_{\mathbb{Q}}(M, \|\cdot\|) = \lambda_{\mathbb{Z}}(M, \|\cdot\|) = 0.$$

We have the following inequalities on $\lambda_{\mathbb{Q}}(M, \|\cdot\|)$ and $\lambda_{\mathbb{Z}}(M, \|\cdot\|)$.

Lemma 2.18.

$$\lambda_{\mathbb{Q}}(M, \|\cdot\|) \leq \lambda_{\mathbb{Z}}(M, \|\cdot\|) \leq \operatorname{rk}(M) \lambda_{\mathbb{Q}}(M, \|\cdot\|).$$

Proof. Considering M/M_{tor}, we may assume that M is free. The inequality $\lambda_{\mathbb{Q}}(M, \|\cdot\|) \leq \lambda_{\mathbb{Z}}(M, \|\cdot\|)$ is obvious, so that we only need to show the inequality

$$\lambda_{\mathbb{Z}}(M, \|\cdot\|) \leq \operatorname{rk}(M) \lambda_{\mathbb{Q}}(M, \|\cdot\|).$$

For this purpose, let us claim the following.

Claim 6. *Let $s_1, \ldots, s_n \in M$ such that $s_1, \ldots, s_n$ give rise to a basis of $M_{\mathbb{Q}}$. Then there is an $n \times n$-matrix (a_{ij}) such that a_{ij} is a rational number with $|a_{ij}| \leq 1$ for all i, j, and that if we set $e_i = \sum_j a_{ij} s_j$, then $e_1, \ldots, e_n \in M$ and $e_1, \ldots, e_n$ form a free basis of M.*

Proof. We prove it by induction on n. If $n = 0$, the assertion is obvious. Let us choose a positive integer a such that if we set $e_n = (1/a)s_n$, then $e_n \in M$ and $M' = M/\mathbb{Z}e_n$ has no torsion. Let $s'_1, \ldots, s'_{n-1}$ be the image of $s_1, \ldots, s_{n-1}$ in M'. Then, by the hypothesis of induction, there is an $(n-1) \times (n-1)$-matrix

(a'_{ij}) such that a'_{ij} is a rational number with $|a'_{ij}| \leq 1$ for all i, j, and that if we set $e'_i = \sum_j a'_{ij} s'_j$, then $e'_1, \ldots, e'_{n-1} \in M'$ and $e'_1, \ldots, e'_{n-1}$ form a free basis of M'. Let us choose $f_1, \ldots, f_{n-1} \in M$ such that the images of $f_1, \ldots, f_{n-1}$ in M' are $e'_1, \ldots, e'_{n-1}$, respectively. Since $\sum_j a'_{ij} s_j - f_i \in \mathbb{Q}e_n$, there is a rational number c_i with $\sum_j a'_{ij} s_j - f_i = c_i e_n$. Here we put $e_i = f_i + \lceil c_i \rceil e_n$ $(i = 1, \ldots, n-1)$, where $\lceil x \rceil = \min\{b \in \mathbb{Z} \mid x \leq b\}$ for $x \in \mathbb{R}$. Then $e_1, \ldots, e_{n-1}, e_n$ yield a free basis of M. Moreover,

$$e_i = \sum\nolimits_j a'_{ij} s_j + \frac{(\lceil c_i \rceil - c_i)}{a} s_n \ (1 \leq i \leq n-1), \quad e_n = (1/a) s_n.$$

Thus we get the claim. □

By the above claim,

$$\|e_i\| \leq \operatorname{rk}(M) \max\{\|s_1\|, \ldots, \|s_n\|\}$$

holds, and hence the lemma follows. □

Moreover, the following two lemmas hold for $\lambda_{\mathbb{Q}}$.

LEMMA 2.19. *Let $(M_1, \|\cdot\|_1)$ and $(M_2, \|\cdot\|_2)$ be normed $\mathbb{Z}$-modules, and let $\phi : M_1 \to M_2$ be a homomorphism such that ϕ yields an isomorphism over $\mathbb{Q}$. Then we have the following:*

(1) *$\lambda_{\mathbb{Q}}(M_2, \|\cdot\|_2) \leq \|\phi\| \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1)$.*
(2) *We further assume that ϕ is surjective and that ϕ yields an isometry*

$$((M_1)_{\mathbb{R}}, \|\cdot\|_1) \xrightarrow{\sim} ((M_2)_{\mathbb{R}}, \|\cdot\|_2).$$

Then $\lambda_{\mathbb{Q}}(M_2, \|\cdot\|_2) = \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1)$.

PROOF. (1) Let $e_1, \ldots, e_n \in M_1$ such that $e_1, \ldots, e_n$ form a basis of M_1 over $\mathbb{Q}$ and $\max\{\|e_1\|_1, \ldots, \|e_n\|_1\} = \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1)$. Note that $\phi(e_1), \ldots, \phi(e_n)$ form a basis of M_2 over $\mathbb{Q}$ and

$$\|\phi(e_i)\|_2 \leq \|\phi\| \cdot \|e_i\|_1 \leq \|\phi\| \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1)$$

for all i, as required.

(2) By (1), we have $\lambda_{\mathbb{Q}}(M_2, \|\cdot\|_2) \leq \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1)$. On the other hand, let us choose $y_1, \ldots, y_n \in M_2$ such that $y_1, \ldots, y_n$ form a basis of M_2 over $\mathbb{Q}$ and

$$\max\{\|y_1\|_2, \ldots, \|y_n\|_2\} = \lambda_{\mathbb{Q}}(M_2, \|\cdot\|_2).$$

By our assumption, for each i, we can choose $x_i \in M_1$ with $\phi(x_i) = y_i$. Then $\|x_i\|_1 = \|y_i\|_2$ for all i. Thus $\lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1) \leq \lambda_{\mathbb{Q}}(M_2, \|\cdot\|_2)$. □

LEMMA 2.20. *Let $(M_1, \|\cdot\|_1), \ldots, (M_n, \|\cdot\|_n)$ be normed $\mathbb{Z}$-modules. Let*

$$M_1 \xrightarrow{\alpha_2} M_2 \xrightarrow{\alpha_3} M_3 \longrightarrow \cdots \longrightarrow M_{i-1} \xrightarrow{\alpha_i} M_i \longrightarrow \cdots \longrightarrow M_{n-1} \xrightarrow{\alpha_n} M_n$$

be a sequence of homomorphisms such that $\alpha_i : M_{i-1} \to M_i$ yields an injective homomorphism over $\mathbb{Q}$ for each i with $2 \leq i \leq n$. If we set $\phi_i = \alpha_n \circ \cdots \circ \alpha_{i+1} : M_i \to M_n$ for $i = 1, \ldots, n-1$, and

$$Q_i = \begin{cases} \operatorname{Coker}(\alpha_i : M_{i-1} \to M_i) & \text{if } i \geq 2, \\ M_1 & \text{if } i = 1, \end{cases}$$

for $i = 1, \ldots, n$*, then we have*

$$\lambda_{\mathbb{Q}}(M_n, \|\cdot\|_n) \leq \lambda_{\mathbb{Q}}(Q_n, \|\cdot\|_{n, M_n \twoheadrightarrow Q_n}) + \sum_{i=1}^{n-1} \|\phi_i\| \lambda_{\mathbb{Q}}(Q_i, \|\cdot\|_{i, M_i \twoheadrightarrow Q_i}) \operatorname{rk} Q_i.$$

PROOF. We prove this lemma by induction on n. First we consider the case where $n = 2$. We need to show that

$$\lambda_{\mathbb{Q}}(M_2, \|\cdot\|_2) \leq \lambda_{\mathbb{Q}}(Q_2, \|\cdot\|_{2, M_2 \twoheadrightarrow Q_2}) + \|\alpha_2\| \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1) \operatorname{rk} M_1.$$

Let $e_1, \ldots, e_s \in M_1$ and $f_1, \ldots, f_t \in Q_2$ such that $e_1, \ldots, e_s$ and $f_1, \ldots, f_t$ form bases of M_1 and Q_2 over $\mathbb{Q}$, respectively, and that

$$\begin{cases} \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1) = \max\{\|e_1\|_1, \ldots, \|e_s\|_1\}, \\ \lambda_{\mathbb{Q}}(Q_2, \|\cdot\|_{2, M_2 \twoheadrightarrow Q_2}) = \max\{\|f_1\|_{2, M_2 \twoheadrightarrow Q_2}, \ldots, \|f_t\|_{2, M_2 \twoheadrightarrow Q_2}\}. \end{cases}$$

We choose $f'_j \in M_2$ and $f''_j \in (M_2)_{\mathbb{R}}$ such that $f'_j = f_j$ on Q_2, $f''_j = f_j$ on $(Q_2)_{\mathbb{R}}$ and that $\|f''_j\|_2 = \|f_j\|_{2, M_2 \twoheadrightarrow Q_2}$. Since $f'_j \otimes 1 - f''_j \in \alpha_2(M_1)_{\mathbb{R}}$, there are $a_{ji} \in \mathbb{R}$ such that $f'_j \otimes 1 - f''_j = \sum_i a_{ji}(\alpha_2(e_i) \otimes 1)$. If we set $g_j = f'_j - \sum_i \lfloor a_{ji} \rfloor \alpha_2(e_i)$, then $\alpha_2(e_1), \ldots, \alpha_2(e_s), g_1, \ldots, g_t \in M_2$ form a basis of M_2 over $\mathbb{Q}$, where

$$\lfloor x \rfloor = \max\{a \in \mathbb{Z} \mid a \leq x\}$$

for $x \in \mathbb{R}$. Moreover, as $g_j \otimes 1 = f''_j + \sum_i (a_{ji} - \lfloor a_{ji} \rfloor)(\alpha_2(e_i) \otimes 1)$, we have

$$\begin{aligned} \|g_j\|_2 &\leq \|f''_j\|_2 + \sum_i \|\alpha_2(e_i)\|_2 \leq \|f''_j\|_2 + \sum_i \|\alpha_2\| \cdot \|e_i\|_1 \\ &\leq \lambda_{\mathbb{Q}}(Q_2, \|\cdot\|_{2, M_2 \twoheadrightarrow Q_2}) + \|\alpha_2\| \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1) \operatorname{rk} M_1, \end{aligned}$$

which implies the assertion for $n = 2$ because $\|\alpha_2(e_i)\|_2 \leq \|\alpha_2\| \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1)$.

Here we assume that $n \geq 3$. We set

$$\widetilde{M}_i = \operatorname{Coker}(\alpha_i \circ \cdots \circ \alpha_2 : M_1 \longrightarrow M_i)$$

for $i = 2, \ldots, n$. Let $\tilde{\alpha}_i : \widetilde{M}_{i-1} \to \widetilde{M}_i$ be the induced homomorphism by α_i for $i = 3, \ldots, n$. Note that $\tilde{\alpha}_i$ yields an injective homomorphism over $\mathbb{Q}$. Here we put $\tilde{\phi}_i = \tilde{\alpha}_n \circ \cdots \circ \tilde{\alpha}_{i+1} : \widetilde{M}_i \to \widetilde{M}_n$ for $i = 2, \ldots, n-1$, and

$$\widetilde{Q}_i = \begin{cases} \operatorname{Coker}(\tilde{\alpha}_i : \widetilde{M}_{i-1} \to \widetilde{M}_i) & \text{if } i \geq 3, \\ \widetilde{M}_2 & \text{if } i = 2. \end{cases}$$

Then, by the hypothesis of induction, we have

$$\begin{aligned} \text{(2.13)} \quad \lambda_{\mathbb{Q}}(\widetilde{M}_n, \|\cdot\|_{n, M_n \twoheadrightarrow \widetilde{M}_n}) &\leq \lambda_{\mathbb{Q}}\left(\widetilde{Q}_n, \left(\|\cdot\|_{n, M_n \twoheadrightarrow \widetilde{M}_n}\right)_{\widetilde{M}_n \twoheadrightarrow \widetilde{Q}_n}\right) \\ &\quad + \sum_{i=2}^{n-1} \|\tilde{\phi}_i\| \lambda_{\mathbb{Q}}\left(\widetilde{Q}_i, \left(\|\cdot\|_{i, M_i \twoheadrightarrow \widetilde{M}_i}\right)_{\widetilde{M}_i \twoheadrightarrow \widetilde{Q}_i}\right) \operatorname{rk} \widetilde{Q}_i. \end{aligned}$$

By (1) in Lemma 1.2, $\left(\|\cdot\|_{i, M_i \twoheadrightarrow \widetilde{M}_i}\right)_{\widetilde{M}_i \twoheadrightarrow \widetilde{Q}_i} = \|\cdot\|_{i, M_i \twoheadrightarrow \widetilde{Q}_i}$ for $i = 2, \ldots, n$. Moreover, the natural homomorphism $h_i : Q_i \to \widetilde{Q}_i$ is surjective and $(Q_i)_{\mathbb{Q}} \to (\widetilde{Q}_i)_{\mathbb{Q}}$ is an isomorphism. Therefore, by (2) in Lemma 2.19,

$$\lambda_{\mathbb{Q}}\left(\widetilde{Q}_i, \left(\|\cdot\|_{i, M_i \twoheadrightarrow \widetilde{M}_i}\right)_{\widetilde{M}_i \twoheadrightarrow \widetilde{Q}_i}\right) = \lambda_{\mathbb{Q}}\left(Q_i, \|\cdot\|_{i, M_i \twoheadrightarrow Q_i}\right)$$

for $i = 2, \ldots, n$. On the other hand, by Lemma 1.5, $\|\tilde{\phi}_i\| \leq \|\phi_i\|$ for $i = 2, \ldots, n-1$. Thus, (2.13) implies that

$$\lambda_{\mathbb{Q}}\left(\widetilde{M}_n, \|\cdot\|_{n, M_n \twoheadrightarrow \widetilde{M}_n}\right) \leq \lambda_{\mathbb{Q}}\left(Q_n, \|\cdot\|_{n, M_n \twoheadrightarrow Q_n}\right) + \sum_{i=2}^{n-1} \|\phi_i\| \lambda_{\mathbb{Q}}\left(Q_i, \|\cdot\|_{i, M_i \twoheadrightarrow Q_i}\right) \operatorname{rk} Q_i. \tag{2.14}$$

Further, applying the induction hypothesis to $M_1 \xrightarrow{\phi_1} M_n$, we obtain

$$\lambda_{\mathbb{Q}}(M_n, \|\cdot\|_n) \leq \lambda_{\mathbb{Q}}\left(\widetilde{M}_n, \|\cdot\|_{n, M_n \twoheadrightarrow \widetilde{M}_n}\right) + \|\phi_1\| \lambda_{\mathbb{Q}}(M_1, \|\cdot\|_1) \operatorname{rk} M_1. \tag{2.15}$$

Therefore, the assertion of the lemma follows from (2.14) and (2.15). $\square$