Chapter 1 - Lattices

Let $b_1, b_2, \ldots, b_m$ be linearly independent vectors in $\mathbb{R}^n$. The lattice $L = L(b_1, b_2, \ldots, b_m)$ is the set of linear integer combinations of $b_1, b_2, \ldots, b_m$ i.e.

$$L = \{ x \in \mathbb{R}^n : x = y_1 b_1 + y_2 b_2 + \cdots + y_m b_m,\ y_1, y_2, \ldots y_m \in \mathbb{Z} \}$$

A linearly independent set such as $b_1, b_2, \ldots, b_m$ which generates L is called a basis of L.

A lattice will have many different bases. Let B be the $m \times n$ basis matrix with rows $b_1, b_2, \ldots, b_m$ and let U be any $m \times m$ unimodular matrix (i.e. $|\det U| = \pm 1$ with integer entries) Note that since U^{-1} is an integer matrix

(1.1) $\quad yU \in \mathbb{Z}^m \Longleftrightarrow y \in \mathbb{Z}^m.$

Now let $b_1', b_2', \ldots, b_m'$ be the rows of $B' = UB$. Then $b_1', b_2', \ldots, b_m'$ is a basis of L. To see this note that if $y \in \mathbb{Z}^m$ and $x = yB$ than $x = y'B'$ where $y' = yU^{-1} \in \mathbb{Z}^m$ by (1.1). This shows that $L(b_1, b_2, \dots b_m) \subseteq L(b'_1, b'_2, \dots, b'_m)$. The reverse containment is proved similarly.

Conversely let $b'_1, b'_2, \dots, b'_{m'}$ be any other basis of L. Since $b_1, b_2, \dots, b_m$ are linear combinations of $b'_1, b'_2, \dots, b'_{m'}$ we have $m' \geq m$, and similarly $m \geq m'$ and so $m' = m$. But now we have $B' = UB$ and $B = U'B'$ for integer $m \times m$ matrices U, U'. So $B = U'UB$ and $U'U = I$ as the rows of B are linearly independent. Thus $\det U' \det U = \underline{1}$ and U, U' are unimodular.

We have thus proved

Theorem 1.1

If B is an $m \times n$ basis matrix of the lattice L then B' is a basis matrix of L iff $B' = UB$ for some unimodular matrix U.

$\square$

Gramme - Schmidt

Given a basis $b_1, b_2, \ldots, b_m$ of L, it will be useful to consider the vectors $b_1^*, b_2^*, \ldots, b_m^*$ obtained by the Gramme-Schmidt orthogonalization process i.e.

(1.2a) $$b_1^* = b_1$$

(1.2b) $$b_i^* = b_i - \sum_{j=1}^{i-1} u_{ij} b_j^* \qquad 2 \le i \le m$$

where $$u_{ij} = \frac{b_i b_j^*}{|b_j^*|^2}.$$

If B^* is the $m \times n$ matrix with rows $b_1^*, b_2^*, \ldots, b_m^*$ then we will denote the matrix form of (1.2) as $B = G B^*$

where G is an $m \times m$ lower triangular matrix with 1's on its diagonal.

We let

$$\Lambda_1(L) = \min\{|x| : x \in L \setminus \{0\}\}$$

denote the length of the shortest vector of L.

Theorem 1.2

$$\Lambda_1(L) \geq \min\{|b_i^*| : 1 \leq i \leq m\}$$

Proof

Let $x = yB \in L$ where $y \in \mathbb{Z}^m$. Then $x = y^* B^*$ where $y^* = yG$. Note that $y^*_t = y_t$ where $t = \max\{i : y_i \neq 0\}$. But then

Nonsense

$$|x| = \sum_{i=1}^{3} |y_i^*| \, |b_i^*|$$ since the b_i^* are mutually orthogonal,

$$\geq |y_r| \, |b_r^*|$$

$$\geq |b_r^*|$$ as $y_r \in \mathbb{Z}$.

$\square$

Determinant of a lattice

We define the determinant $d(L)$ by

$$d(L) = \prod_{i=1}^{n} |b_i^*|.$$

We must show now that $d(L)$ is independent of L. In fact all we need prove is

(1.3) $\quad d(L)^2 = \det(BB^T)$

For suppose $B' = UB$ is any other basis matrix of L. Then

$$\det(B'B'^T) = \det(UBB^TU^T)$$
$$= \det(U)\det(BB^T)\det(U^T)$$
$$= \det(BB^T).$$

Note also that if $m = n$ the (1.3) implies $d(L) = |\det(B)|$ and explains why $d(L)$ is called a determinant.

Proof of (1.3)

Now B^*B^{*T} is an $m \times m$ diagonal matrix with diagonal entries b_i^{*2} for $1 \le i \le m$. Thus

$$
\begin{aligned}
d(L) &= \det(B^* B^{*T}) \\
&= \det(G B B^T G^T) \\
&= \det(G)\det(BB^T)\det(G^T) \\
&= \det(BB^T).
\end{aligned}
$$

$\square$

Fundamental Parallelopipeds

To each basis B of L we associate a fundamental parallelopiped $PP = PP_B(L)$ with 2^m vertices of the form $\delta_1 b_1 + \delta_2 b_2 + \dots + \delta_m b_m$ where $(\delta_1, \delta_2, \dots \delta_m) \in \{0,1\}^m$.

Let vol_m denote m-dimensional volume.

Theorem 1.3

$$\mathrm{vol}_m(PP) = d(L).$$

Proof

By induction on m. The base case $m=1$ is trivial. Let $\tilde{L}$ be the lattice generated by $b_1, b_2, \ldots, b_{m-1}$ and $\widetilde{PP}$ be the corresponding parallelopiped. Then

$$\mathrm{vol}_m(PP) = |b_m^*| \, \mathrm{vol}_{m-1}(\widetilde{PP})$$

since $|b_m^*|$ is the distance between Π and $b_m + \Pi$ where Π is the hyperplane through the origin generated by $b_1, b_2, \ldots, b_{m-1}$. The result now follows by induction.

$\square$

Minkowski's First Theorem

A set $K \subseteq \mathbb{R}^n$ is <u>convex</u> if $x, y \in K$ and $0 \leq \lambda \leq 1$ implies $\lambda x + (1-\lambda) y \in K$.

A set $S \subseteq \mathbb{R}^n$ is said to be <u>centrally symmetric</u> if $x \in S$ implies $-x \in S$.

For a lattice L we let $lin(L) =$

$$\{ \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k : \lambda_1, \lambda_2, \cdots \lambda_k \in \mathbb{R},\ v_1, v_2, \cdots, v_k \in L \} =$$

vector space generated by L.

$\dim(L) =$ dimension of vector space generated by L

$=$ the number of vectors in a basis of L (Exercise 1.?)

For a lattice L and a closed set $S \subseteq \mathbb{R}^n$ we define

$$\Lambda(S, L) = \inf\{t : tS \cap L \neq \{0\}\}$$

so that $\Lambda_1(L) = \Lambda(B(0,1), L)$.

Theorem 1.4 (Minkowski)

Let L be a lattice of dimension m and let $K \subseteq \mathrm{lin}(L)$ be a centrally symmetric, compact convex set. Then

$$\Lambda^m(K, L)\, \mathrm{vol}_m(K) \leqslant 2^m d(L)$$

Proof

Let $B'(0,r) = B(0,r) \cap \mathrm{lin}(L)$ for $r \geqslant 0$ and let $N(r) = L \cap B'(0,r)$. Choose $\lambda < \Lambda(K, L)$.

We consider copies of $\frac{\lambda}{2}K$ centred at each point of $N(r)$. We show first that

(1.4) $v_1, v_2 \in L$, $v_1 \neq v_2$ implies $(v_1 + \frac{\lambda}{2}K) \cap (v_2 + \frac{\lambda}{2}K) = \emptyset$.

Suppose that (1.4) fails for $v_1, v_2 \in L$. Then there exists $x \in (v + \frac{\lambda}{2}K) \cap (\frac{\lambda}{2}K)$ where $v = v_1 - v_2 \in L$.

Now $x - v \in \frac{\lambda}{2}K$ implies $v - x \in \frac{\lambda}{2}K$ (central symmetry) and then $\frac{1}{2}(x + (v-x)) \in \frac{\lambda}{2}K$ (convexity) i.e. $v \in \lambda K$ — contradiction.

Choose a basis B of L, let $P = PP_B(L)$ and $d_1 = \mathrm{diam}(P)$. Also, let $d_2 = \mathrm{diam}(K)$.

Now

$$\mathrm{vol}_m\Big(\bigcup_{v \in N(r)} (v + \tfrac{\lambda}{2}K)\Big) \leq \mathrm{vol}_m\big(B'(0, r + \tfrac{\lambda}{2}d_2)\big)$$

$$\leqslant |N(r + \tfrac{\lambda}{2} d_2 + d_1)| \; d(L)$$

using Theorem 1.3.

Hence

(1.5) $\quad |N(r)| \left(\frac{\lambda}{2}\right)^m \mathrm{vol}_m(K) \leqslant |N(r+\frac{\lambda}{2}d_2+d_1)| \, d(L)$.

Now it is not difficult to show (Exercise 1.?)

that for any constant d

(1.6) $$\lim_{r\to\infty} \frac{|N(r+d)|}{|N(r)|} = 1 .$$

Hence (1.5) implies

$$\left(\frac{\lambda}{2}\right)^m \mathrm{vol}_m(K) \leqslant d(L)$$

and the theorem follows. $\square$

A subset $S \subseteq \mathbb{R}^n$ is said to be <u>discrete</u> if there exists $\delta = \delta(S) > 0$ such that

$$x, y \in S, x \neq y \text{ implies } |x - y| \geq \delta.$$

The following is a useful characterisation of a lattice.

<u>Theorem 1.5</u>

A set $L \subseteq \mathbb{R}^n$ is a lattice iff

(a) $x, y \in L$ implies $x - y \in L$,

(b) L is discrete.

<u>Proof</u>

A lattice clearly satisfies (a) and (b) follows from Theorem 1.2.

So assume (a) and (b) hold. Let $m = \dim(\mathrm{lin}(L))$. Let $b_1, b_2, \ldots, b_m$ be m linearly independent vectors in L, and let $b_1^*, b_2^*, \ldots, b_m^*$ be computed by Gramm-Schmidt. We claim that

(1.7) $|b_1^*|\,|b_2^*| \cdots |b_m^*| \geq \mathrm{vol}_m(B(0, \frac{\delta}{2}))$.

where $\delta = \delta(L)$.

For let $L' = L(b_1, b_2, \ldots, b_m)$ and $K = B(0,1) \cap \mathrm{lin}(L)$.

Clearly $\Delta(K, L') \geq \delta$ and so (1.7) follows from Theorem 1.4.

Now let

$$\lambda = \inf\left\{ \prod_{i=1}^{m} |b_i^*| : b_1, b_2, \ldots, b_m \text{ are linearly independent vectors in } L \right\}.$$

Now (1.7) implies that $\lambda > 0$ and L

is closed (since it is discrete.) It follows that there exist $b_1, b_2, \ldots, b_m \in L$ for which $\prod_{i=1}^{m} |b_i^*| = \lambda$ (here we use the fact that $\prod_{i=1}^{m} |b_i^*|$ is a continuous function of $b_1, b_2, \ldots, b_m$.)

We claim now that $L = L(b_1, b_2, \ldots, b_m)$. For if $v \in L$ then $v = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_m b_m$ for $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{R}$. We show that $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{Z}$. Suppose not and that w.l.o.g. $\alpha_m \notin \mathbb{Z}$ (the proof of (1.3) shows that the ordering of $b_1, b_2, \ldots, b_m$ is immaterial.) Let $b_m' = v - \lfloor \alpha_m \rfloor b_m \in L$. If we now let $b_i' = b_i$, $1 \leq i \leq m-1$ then $b_1', b_2', \ldots, b_m'$ are linearly independent and we have

$b_i'^* = b_i^*$, $1 \le i \le m-1$ and $b_m'^* = (\alpha_m - \lfloor \alpha_m \rfloor)\, b_m^*$.

Thus $\prod_{i=1}^{m} |b_i'^*| < \lambda$ — contradiction.

$\square$

<u>Corollary 1.6</u>

Let A be a $k \times n$ matrix and q be a positive integer. Then

(a) $\{x \in \mathbb{Z}^n : Ax = 0\}$ is a lattice,

(b) $\{x \in \mathbb{Z}^n : Ax = 0 \bmod q\}$ is a lattice

<u>Corollary 1.7</u>

If L_1, L_2 are lattices then so if $L_1 \cap L_2$.

Primitive Elements

A vector $v \in L$ is <u>primitive</u> if $\alpha v \in L$ implies $\alpha \in \mathbb{Z}$.

Theorem 1.8

If $v \in L$ then there exists $\beta > 0$ such βv is primitive.

Proof

Let $\beta = \min\{\gamma > 0 : \gamma v \in L\}$. $\beta > 0$ as L is discrete. If $\alpha \beta v \in L$ and $\alpha \notin \mathbb{Z}$ then $(\alpha - \lfloor \alpha \rfloor) \beta v \in L$ contradicting the definition of β.

$\square$

Note that if $b_1, b_2, \ldots, b_m$ is a basis of L then $b_1, b_2, \ldots, b_m$ are all primitive.

Theorem 1.9

If $v \in L$ is primitive then there exist $b_2, b_3, \dots, b_m$ such that $v, b_2, b_3, \dots b_m$ is a basis of L.

Proof

Let $b_1 = v$ and $\lambda = \min \{ \prod_{i=1}^{m} |b_i^*| : b_1, b_2, \dots, b_m \in L$ are linearly independent$\}$. Then $\lambda > 0$, as in (1.7), and is achieved by some $b_2, b_3, \dots b_n$.

We claim that $L = L(b_1, b_2, \dots, b_m)$. Suppose $v = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_m b_m \in L$. If $\alpha_i \notin \mathbb{Z}$ for some $i \geq 2$ then w.l.o.g. we can assume $i = m$ and the replace b_m by $v - \lfloor \alpha_m \rfloor b_m$, obtaining the same contradiction as in the proof of Theorem 1.6. If $\alpha_i \in \mathbb{Z}$ for

$i \geq 2$ and $\alpha_1 \notin \mathbb{Z}$ then $(\alpha_1 - \lfloor \alpha_1 \rfloor) b_1 \in L$

contradicting the fact that b_1 is primitive. $\square$

Projection of a lattice

Let $b \in L$. Any $v \in L$ can be expressed

uniquely as

$$v = \alpha b + v' \qquad \text{where } \alpha \in \mathbb{R},\ bv' = 0.$$

The projection $L \backslash b = \{ v' : v \in L \}$

Theorem 1.10

$L \backslash b$ is a lattice.

Proof

Since $L \backslash b = L \backslash \alpha b$ we can assume b

is primitive and so by Theorem 1.9

there is a basis $b = b_1, b_2, \ldots, b_m$ of

L. But if $v = \alpha_1 b_1 + \alpha_2 b_2 + \cdots + \alpha_m b_m$ then $v' = \alpha_2 b_2' + \cdots + \alpha_m b_m'$ and so $L \backslash b = L(b_2', b_3', \ldots, b_m')$ as these $m-1$ vectors are linearly independent.

$\square$

This notion of projection can be generalised.

Let $b_1, b_2, \ldots, b_m$ be a basis of L and let $V = \mathrm{lin}(\{b_1, b_2, \ldots, b_k\})$ where $k \leq m$. Then any $v \in L$ can now be expressed uniquely as $\tilde{v} + \hat{v}$ where $\tilde{v} \in V$ and $\tilde{v}\hat{v} = 0$. We define $L \backslash V = \{ \tilde{v} : v \in V \}$.

<u>Theorem 1.11</u>

$L \backslash V$ is a lattice

Proof

$$L \backslash V = (L \backslash b_1) \setminus \mathrm{lin}(\{b'_2, b'_3, \dots, b'_k\})$$

where $b'_2, b'_3, \dots, b'_m$ are as in Theorem 1.10.

Since $b'_2, b'_3, \dots b'_m$ are a basis of $L \backslash b_1$ we can use induction.

$\square$

Dual Lattice

The dual L^* of a lattice L is defined by

$$L^* = \{ w \in \mathrm{lin}(L) : vw \in \mathbb{Z} \text{ for all } v \in L \}.$$

Theorem 1.12

L^* is a lattice

Proof

We use Theorem 1.5. Clearly property (a) holds. Let $b_1, b_2, \ldots, b_m$ be a basis of L. If $w \in L^*$ and $w \neq 0$ then there exists i such that $wb_i \neq 0$. But then

$$|w|\,|b_i| \geq |wb_i| \geq 1$$

and so

$$|w| \geq \min\{|b_i|^{-1} : 1 \leq i \leq m\}.$$

Since (a) holds this implies L^* is discrete.

$\square$

Theorem 1.13

$$d(L)\,d(L^*) = 1$$

Proof

Let $b_1, b_2, \dots, b_m$ be a basis of L with basis matrix B. Suppose first that $m = n$. Let $b_1^*, b_2^*, \dots, b_n^*$ be the columns of B^{-1}. We claim that $L^* = L(b_1^*, b_2^*, \dots, b_n^*)$ and of course then $d(L^*) = \det(B^{-T}) = \det(B)^{-1} = d(L)^{-1}$. If $v = \alpha_1 b_1 + \dots + \alpha_n b_n \in L$ then $v b_i^* = \alpha_i \in \mathbb{Z}$ and so $b_1^*, b_2^*, \dots, b_n^* \in L^*$.

Conversely, if $v \in L^*$ then $v = B^{-1}Bv$ implies

$$v = (vb_1)\, b_1^* + (vb_2)\, b_2^* + \cdots + (vb_n)\, b_n^*$$

and the theorem follows for $m = n$.

When $m < n$ one can argue (Exercise 1.?) that $L^* = L(b_1^*, b_2^*, \ldots, b_m^*)$ where $b_1^*, b_2^*, \ldots, b_m^*$ are the columns of $B^T(BB^T)^{-1}$ and then, using (1.3),

$$\begin{aligned} d(L^*)^2 &= \det\left(\left(BB^T\right)^{-T} B\, B^T\, (BB^T)^{-1}\right) \\ &= \det\,(BB^T)^{-1} \\ &= d(L)^{-2}. \end{aligned}$$

$\square$

Remark?: we see ~~from~~ the above proof that L^* always has a basis $b_1^*, b_2^*, \ldots b_m^*$ where

(1.7a) $$b_i^*\, b_j = \delta_{ij} \qquad 1 \le i, j \le m$$

[δ_{ij} is the Kronecker delta].

We now consider the interaction between projections and the dual lattice.

Theorem 1.13a

Let $b_1, b_2, \dots, b_m$ be a basis of lattice L and let $b_1^*, b_2^*, \dots, b_m^*$ be a basis of L^* satisfying (1.7a). Then $b_2^*, \dots, b_m^*$ are a basis of $(L \backslash \{b_1\})^*$.

Proof

Let $b_i = \alpha_i b_1 + b_i'$, $2 \leq i \leq m$, so that $b_2', \dots, b_m'$ are a basis of $L \backslash \{b_1\}$. Then

$$b_i' b_j^* = b_i b_j^* = \delta_{ij} \qquad 2 \leq i, j \leq m$$

since $b_1 b_j^* = 0$ for $j \geq 2$

That $b_2^*, \dots b_m^*$ form a basis of $L \backslash \{b_1\}$ follows as in the proof of Theorem 1.13.

$\square$

Sub-lattices

If $a_1, a_2, \ldots, a_m$ are linearly independent vectors in L then $L' = L(a_1, a_2, \ldots, a_m)$ is a sub-lattice of L. The index of L' in L is defined to be $\dfrac{d(L')}{d(L)}$.

Let A have rows $a_1, a_2, \ldots, a_m$. Then we can write $A = MB$ where B is a basis matrix of L and M is a non-singular integer matrix.

Theorem 1.13

$$\text{Index of } L' = |\det(M)|$$

Proof

$$\left(\frac{d(L')}{d(L)}\right)^2 = \frac{\det(AA^T)}{\det(BB^T)} \qquad \text{by (1.3)}$$

$$= \frac{\det(MBB^T M^T)}{\det(BB^T)}$$

$$= \det(M)^2.$$

□

Corollary 1.14

A sublattice L' is the whole of L if and only if its index is 1.

Proof

If L' has index 1 then M is unimodular and we apply Theorem 1.1. The other way round is obvious.

□

Corollary 1.15

$$L^{**} = L$$

Proof

Now $L^{**} \supseteq L$ and Theorem 1.13 implies

$d(L^{**}) = d(L)$. Now apply Corollary 1.14.

$\square$

em is clearly to choose k so that the ole plane. In general one will wish to possible so that it still has this covering trast with the treatment of the homo- the objective was to make the regions rge as possible but so that they did not

y be concerned at first with the homo- ve have a fairly complete theory of the iscuss in Chapter XI the inhomogeneous homogeneous one.

Chapter I

Lattices

I.1. Introduction. In this chapter we introduce the most important concept in the geometry of numbers, that of a lattice, and develop some of its basic properties. The contents of this chapter, except § 2.4 and § 5, are fundamental for almost everything that follows.

In this book we shall be concerned only with lattices over the ring of rational integers. A certain amount of work has been done on lattices over complex quadratic fields, see e.g. MULLENDER (1945 a) and K. ROGERS (1955 a). Many of the concepts should carry over practically unaltered. Again, work on approximation to complex numbers by integers of a complex quadratic field [e.g. MULLENDER (1945 a), CASSELS, LEDERMANN and MAHLER (1951 a), POITOU (1953 a)] and on the minima of hermitian forms when the variables are integers in a quadratic field [e.g. OPPENHEIM (1932a, 1936a, 1953 f) and K. ROGERS (1956a)] may be regarded as a generalization of the geometry of numbers to lattices over complex quadratic fields. We shall not have occasion to mention lattices over complex quadratic fields again in this book; we mention them here only for completeness. For lattices over general algebraic number fields see ROGERS and SWINNERTON-DYER (1958 a).

I.2. Bases and sublattices. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ be linearly independent real vectors in n-dimensional real euclidean space, so that the only set of numbers $t_1, \ldots, t_n$ for which $t_1\boldsymbol{a}_1 + \cdots + t_n\boldsymbol{a}_n = \boldsymbol{o}$ is $t_1 = t_2 = \cdots = t_n = 0$. The set of all points

$$\boldsymbol{x} = u_1\boldsymbol{a}_1 + \cdots + u_n\boldsymbol{a}_n \tag{1}$$

with integral $u_1, \ldots, u_n$ is called the lattice with basis $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$. We note that, since $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ are linearly independent, the expression of any vector $\boldsymbol{x}$ in the shape (1) with real $u_1, \ldots, u_n$ is unique. Hence if $\boldsymbol{x}$ is in Λ and (1) is any expression for $\boldsymbol{x}$ with real $u_1, \ldots, u_n$, then $u_1, \ldots, u_n$ are integers. We shall make use of these remarks frequently, often without explicit reference.

The basis is not uniquely determined by the lattice. For let $\boldsymbol{a}_i'$ be the points

$$\boldsymbol{a}_i' = \sum_j v_{ij}\boldsymbol{a}_j \qquad (1 \leqq i,\ j \leqq n), \tag{2}$$

where v_{ij} are any integers with

$$\det(v_{ij}) = \pm 1. \tag{3}$$

Then

$$\boldsymbol{a}_i = \sum_j w_{ij} \boldsymbol{a}'_j \tag{4}$$

with integral w_{ij}. It follows easily that the set of points (1) is precisely the set of points

$$u'_1 \boldsymbol{a}'_1 + \cdots + u'_n \boldsymbol{a}'_n$$

where $u'_1, \ldots, u'_n$ run through all integers; that is $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ and $\boldsymbol{a}'_1, \ldots, \boldsymbol{a}'_n$ are bases of the same lattice. We show now that every basis $\boldsymbol{a}'_i$ of a lattice Λ may be obtained from a given basis $\boldsymbol{a}_i$ in this way. For since $\boldsymbol{a}'_i$ belongs to the lattice with basis $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ there are integers v_{ij} such that (2) holds: and since $\boldsymbol{a}_i$ belongs to the lattice with basis $\boldsymbol{a}'_1, \ldots, \boldsymbol{a}'_n$ there are integers w_{ij} such that (4) holds. On substituting (2) in (4) and making use of the linear independence of the $\boldsymbol{a}_i$, we have

$$\sum w_{ij} v_{jl} = \begin{cases} 1 & \text{if} \quad i = l \\ 0 & \text{otherwise}. \end{cases}$$

Hence

$$\det(w_{ij}) \det(v_{jl}) = 1$$

and so each of the integers $\det(w_{ij})$ and $\det(v_{jl})$ must be ± 1; that is (3) holds as required.

We denote lattices by capital sanserif Greek letters, and in particular by Λ, M, N, Γ.

If $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ and $\boldsymbol{a}'_1, \ldots, \boldsymbol{a}'_n$ are bases of the same lattice, so that they are related by (2) and (3), then we have

$$\det(\boldsymbol{a}'_1, \ldots, \boldsymbol{a}'_n) = \det(v_{ij}) \det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) = \pm \det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n),$$

where, for example, $\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ denotes the determinant of the $n \times n$ array whose j-th row is the vector $\boldsymbol{a}_j$. Hence

$$d(\Lambda) = |\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)|$$

is independent of the particular choice of basis for Λ. Because of the linear independence of $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ we have

$$d(\Lambda) > 0.$$

We call $d(\Lambda)$ the determinant of Λ.

An example of a lattice is the set Λ_0 of all vectors with integral coordinates. A basis for Λ_0 is clearly the set of vectors

$$\boldsymbol{e}_j = (\overbrace{0, \ldots, 0}^{j-1 \text{ zeros}}, 1, \overbrace{0, \ldots, 0}^{n-j \text{ zeros}}) \quad (1 \leqq j \leqq n);$$

and so

$$d(\Lambda_0) = 1.$$

We note that the vectors of a lattice Λ form a group under addition: if $\boldsymbol{a}\in\Lambda$ then $-\boldsymbol{a}\in\Lambda$; and if $\boldsymbol{a}, \boldsymbol{b}\in\Lambda$ then $\boldsymbol{a}\pm\boldsymbol{b}\in\Lambda$. We shall see later (Chapter III, § 4) that a lattice is the most general group of vectors in n-dimensional space which contains n linearly independent vectors and which satisfies the further property that there is some sphere about the origin $\boldsymbol{o}$ which contains no other vector of the group except $\boldsymbol{o}$.

I.2.2. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ be vectors of a lattice M with basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$, so that

$$\boldsymbol{a}_i = \sum_j v_{ij}\boldsymbol{b}_j \tag{1}$$

with integers v_{ij}. The integer

$$I = |\det(v_{ij})| = \frac{|\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)|}{|\det(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)|} = \frac{|\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)|}{d(\mathsf{M})}$$

is called the index of the vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ in M. From the last expression it is independent of the particular choice of basis for M. By definition, $I\geqq 0$; and $I=0$ only if $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ are linearly dependent.

If every point of the lattice Λ is also a point of the lattice M then we say that Λ is a sublattice of M. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ and $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ be bases of Λ and M respectively. Then there are integers v_{ij} such that (1) holds, since $\boldsymbol{a}_i\in\mathsf{M}$. The index of $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ in M, namely

$$D = |\det(v_{ij})| = \frac{|\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)|}{|\det(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)|} = \frac{d(\Lambda)}{d(\mathsf{M})} \tag{2}$$

is called the index of Λ in M. From the last expression the index depends only on Λ and M, not on the choice of bases. Since $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ are linearly independent, we have $D>0$. On solving (1) for the $\boldsymbol{b}_i$ and using (2), we have

$$D\,\boldsymbol{b}_i = \sum_j w_{ij}\boldsymbol{a}_j,$$

where the w_{ij} are integers. Hence

$$D\mathsf{M} \subset \Lambda \subset \mathsf{M}, \tag{3}$$

where $D\mathsf{M}$ is the lattice of $D\boldsymbol{b}$, $\boldsymbol{b}\in\mathsf{M}$.

It is often convenient to choose particular bases for Λ and M so that (1) takes a particularly simple shape.

Theorem I. *Let Λ be a sublattice of M.*

A. *To every base $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ of M there can be found a base $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ of Λ of the shape*

$$\left.\begin{aligned} \boldsymbol{a}_1 &= v_{11}\boldsymbol{b}_1 \\ \boldsymbol{a}_2 &= v_{21}\boldsymbol{b}_1 + v_{22}\boldsymbol{b}_2 \\ &\cdots\cdots\cdots\cdots \\ \boldsymbol{a}_n &= v_{n1}\boldsymbol{b}_1 + \cdots + v_{nn}\boldsymbol{b}_n, \end{aligned}\right\} \tag{4}$$

where the v_{ij} are integers and $v_{ii}\neq 0$ for all i.

B. *Conversely, to every basis* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ *of* Λ *there exists a basis* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ *of* M *such that* (4) *holds.*

Proof of A. For each i $(1 \leqq i \leqq n)$ there certainly exist points $\boldsymbol{a}_i$ in Λ of the shape

$$\boldsymbol{a}_i = v_{i1}\boldsymbol{b}_1 + \cdots + v_{ii}\boldsymbol{b}_i$$

where $v_{i1}, \ldots, v_{ii}$ are integers and $v_{ii} \neq 0$, since, as we have seen, $D\boldsymbol{b}_i \in \Lambda$. We choose for $\boldsymbol{a}_i$ such an element of Λ for which the positive integer $|v_{ii}|$ is as small as possible (but not 0), and will show that $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ are in fact a basis for Λ. Since $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ are in Λ, by construction, so is every vector

$$w_1\boldsymbol{a}_1 + \cdots + w_n\boldsymbol{a}_n, \tag{5}$$

where $w_1, \ldots, w_n$ are integers. Suppose, if possible, that $\boldsymbol{c}$ is a vector of Λ not of the shape (5). Since $\boldsymbol{c}$ is in M, it certainly can be expressed in terms of $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$, and so can be written in the shape

$$\boldsymbol{c} = t_1\boldsymbol{b}_1 + \cdots + t_k\boldsymbol{b}_k,$$

where $1 \leqq k \leqq n$, $t_k \neq 0$ and $t_1, \ldots, t_k$ are integers. If there are several such $\boldsymbol{c}$, then we choose one for which the integer k is as small as possible. Now, since $v_{kk} \neq 0$, we may choose an integer s such that

$$|t_k - s\,v_{kk}| < |v_{kk}|. \tag{6}$$

The vector

$$\boldsymbol{c} - s\,\boldsymbol{a}_k = (t_1 - s\,v_{11})\,\boldsymbol{b}_1 + \cdots + (t_k - s\,v_{kk})\,\boldsymbol{b}_k$$

is in Λ since $\boldsymbol{c}$ and $\boldsymbol{a}_k$ are; but it is not of the shape (5) since $\boldsymbol{c}$ is not. Hence $t_k - s v_{kk} \neq 0$ by the assumption that k was chosen as small as possible. But then (6) contradicts the assumption that the non-zero integer v_{kk} was chosen as small as possible. The contradiction shows that there are no $\boldsymbol{c}$ in Λ which cannot be put in the form (5), and so proves part A of the theorem.

Proof of B. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ be some fixed basis of Λ. Since $D\mathsf{M}$ is a sublattice of Λ by (3), where D is the index of Λ in M, there exists by Part A a basis $D\boldsymbol{b}_1, \ldots, D\boldsymbol{b}_n$ of $D\mathsf{M}$ of the type

$$\left.\begin{aligned} D\boldsymbol{b}_1 &= w_{11}\boldsymbol{a}_1 \\ D\boldsymbol{b}_2 &= w_{21}\boldsymbol{a}_1 + w_{22}\boldsymbol{a}_2 \\ &\cdots\cdots\cdots\cdots \\ D\boldsymbol{b}_n &= w_{n1}\boldsymbol{a}_1 + \cdots + w_{nn}\boldsymbol{a}_n, \end{aligned}\right\} \tag{7}$$

with integral w_{ij} and $w_{ii} \neq 0$ $(1 \leqq i \leqq n)$. On solving (7) for $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ in succession we obtain a series of equations of the type (4) but where at first we know only that the v_{ij} are rational. But clearly $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ are a basis for M and so the v_{ij} are in fact integers, since the $\boldsymbol{a}_i$ are in M, and since the representation of any vector $\boldsymbol{a}$ in the shape

$$\boldsymbol{a} = t_1 \boldsymbol{b}_1 + \cdots + t_n \boldsymbol{b}_n \qquad (t_1, \ldots, t_n, \text{ real numbers})$$

is unique by the independence of $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$.

From this theorem we have a number of simple but useful corollaries.

Corollary 1. *In theorem I we may suppose further that*

$$v_{ii} > 0 \tag{8}$$

and that

$$0 \leqq v_{ij} < v_{jj} \qquad \textit{in case } A\,, \tag{9}$$

$$0 \leqq v_{ij} < v_{ii} \qquad \textit{in case } B\,. \tag{10}$$

Proof of A. To obtain (8) it is necessary only to replace $\boldsymbol{a}_i$ or $\boldsymbol{b}_i$ by $-\boldsymbol{a}_i, -\boldsymbol{b}_i$ respectively if originally $v_{ii} < 0$. To obtain (9) we replace the $\boldsymbol{a}_i$ by

$$\boldsymbol{a}_i' = t_{i1} \boldsymbol{a}_1 + \cdots + t_{i,i-1} \boldsymbol{a}_{i-1} + \boldsymbol{a}_i,$$

where the t_{ij} are integers to be determined. For any choice of the t_{ij} the $\boldsymbol{a}_i'$ are a basis for Λ. We have

$$\boldsymbol{a}_i' = v_{i1}' \boldsymbol{b}_1 + \cdots + v_{ii}' \boldsymbol{b}_i,$$

where

$$v_{ii}' = v_{ii};$$

and, for $j < i$, we have

$$v_{ij}' = t_{ij} v_{jj} + t_{i,j+1} v_{j+1,j} + \cdots + t_{i,i-1} v_{i-1,j} + v_{ij}.$$

For each i we may now choose $t_{i-1,i}, t_{i-2,i}, \ldots, t_{i1}$ in that order so that

$$0 \leqq v_{ij}' < v_{jj} = v_{jj}',$$

as was required.

Proof of B. Similar.

Corollary 2. *Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ be linearly independent vectors of a lattice M. Then there is a basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ of M such that*

$$\begin{aligned} \boldsymbol{a}_1 &= v_{11} \boldsymbol{b}_1 \\ \boldsymbol{a}_2 &= v_{21} \boldsymbol{b}_1 + v_{22} \boldsymbol{b}_2 \\ &\cdots\cdots\cdots\cdots \\ \boldsymbol{a}_m &= v_{m1} \boldsymbol{b}_1 + \cdots + v_{mm} \boldsymbol{b}_m, \end{aligned}$$

with integers v_{ij} such that

$$v_{jj} > 0 \qquad 0 \leqq v_{ij} < v_{ii} \qquad (1 \leqq j < i \leqq m)\,. \tag{11}$$

VIII.1.2. For later purposes we shall often need the following two simple lemmas.

LEMMA 1. *Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of a lattice Λ with respect to a distance function F associated with a bounded star-body $F(\boldsymbol{x})<1$. Then there exist n linearly independent points $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \in \Lambda$ such that*

$$F(\boldsymbol{a}_j) = \lambda_j \qquad (1 \leqq j \leqq n).$$

If $\boldsymbol{a} \in \Lambda$ and $F(\boldsymbol{a})<\lambda_j$, then $\boldsymbol{a}$ is linearly dependent on $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{j-1}$.

For by the definition of λ_n there are n linearly independent points of Λ in

$$F(\boldsymbol{x}) < \lambda_n + 1. \tag{1}$$

By Lemma 2 of Chapter IV, the set (1) is bounded and so contains only a finite number of lattice points. Only these points need be considered in the definition of the λ_j. The truth of the lemma is now obvious.

LEMMA 2. *Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of the distance function F with respect to the lattice Λ. Then there is a basis*

$$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$$

of Λ such that, for each $j=1, 2, \ldots, n$, the inequality

$$F(\boldsymbol{x}) < \lambda_j$$

implies that

$$\boldsymbol{x} = u_1 \boldsymbol{b}_1 + \cdots + u_{j-1} \boldsymbol{b}_{j-1}$$

for integers $u_1, \ldots, u_{j-1}$.

When $F(\boldsymbol{x})=0$ only for $\boldsymbol{x}=\boldsymbol{o}$, this is a trivial consequence of Lemma 1, since we may choose $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ so that $\boldsymbol{a}_j$ for each j is dependent only on $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_j$, by Theorem I of Chapter I.

Otherwise a slightly more refined argument is needed. In general, the λ_j will not be all unequal, but there are numbers

$$\mu_1 < \mu_2 < \cdots < \mu_s,$$

for some s in $1 \leqq s \leqq n$, such that

$$\lambda_k = \mu_t \quad \text{if} \quad k_{t-1} < k \leqq k_t,$$

where

$$0 = k_0 < k_1 < \cdots < k_s = n.$$

By the definition of successive minima, there is no point of Λ with $F(\boldsymbol{a})<\mu_1$ except, possibly[1], $\boldsymbol{o}$. Since

$$\mu_2 > \lambda_{k_1},$$

[1] For a general distance function $F(\boldsymbol{x})$ there is, of course, no reason why λ_1 should not be 0. Indeed, if $F(\boldsymbol{x}) = |x_1 \ldots x_n|^{1/n}$, we have $\lambda_1 = \cdots = \lambda_n = 0$ for the lattice Λ_0 of points with integer coordinates.

the are k_1 linearly independent points

$$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{k_1} \tag{2}$$

of Λ in $F(\boldsymbol{x}) < \mu_2$, and, since

$$\mu_2 = \lambda_{k_1+1},$$

every other point of Λ in $F(\boldsymbol{x}) < \mu_2$ is linearly dependent on them. Similarly, we may find k_2 linearly independent points of Λ in $F(\boldsymbol{x}) < \mu_3$ such that every other point of Λ in $F(\boldsymbol{x}) < \mu_3$ is linearly dependent on them. Since $\mu_2 < \mu_3$ we may suppose that k_1 of these k_2 points are $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k_1}$ already determined. We may thus denote by

$$\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k_2}$$

the maximal linearly independent set of points of Λ in $F(\boldsymbol{x}) < \mu_3$ without disturbing the notation (2). And so on. In this way we obtain $k_{s-1} < n$ points

$$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{k_{s-1}}$$

of Λ such that

$$F(\boldsymbol{a}_j) < \mu_t \quad \text{if} \quad j \leqq k_{t-1} \qquad (t \leqq s).$$

By Theorem I of Chapter I there is a basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ of Λ such that, for each $j = 1, \ldots, k_{s-1}$, the vector $\boldsymbol{a}_j$ is linearly dependent on $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_j$ only. This basis clearly has all the properties required.

VIII.2. Spheres. We first prove the results for spheres, since they are simplest and the treatment forms the model for what follows.

THEOREM I. *Let*

$$F_0(\boldsymbol{x}) = |\boldsymbol{x}| \tag{1}$$

and let $\lambda_1, \ldots, \lambda_n$ be the successive minima of a lattice Λ with respect to F_0. Then

$$d(\Lambda) \leqq \lambda_1 \ldots \lambda_n \leqq \delta(F_0)\, d(\Lambda). \tag{2}$$

The left-hand side of (2) was substantially proved in Theorem XIII of Chapter V. We have on the one hand

$$|\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)| = I\, d(\Lambda) \geqq d(\Lambda),$$

where I is the index of $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ in Λ, and, on the other hand,

$$|\det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)| \leqq |\boldsymbol{a}_1| \ldots |\boldsymbol{a}_n|$$

by HADAMARD's Lemma 9 of Chapter V. If now the $\boldsymbol{a}_j$ are the linearly independent vectors of Λ with $F(\boldsymbol{a}_j) = \lambda_j$ given by Lemma 1, the required inequality follows at once.

It remains to prove the second part of (2). As in the proof of Lemma 9 of Chapter V, there is a set of mutually orthogonal[1] vectors $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n$ such that

$$\boldsymbol{b}_j = t_{j1}\boldsymbol{c}_1 + \cdots + t_{jj}\boldsymbol{c}_j$$

for some real numbers t_{ji} $(n \geqq j)$, where $\boldsymbol{b}_j$ is the basis given by Lemma 2. By incorporating a factor in $\boldsymbol{c}_i$ we may suppose, without loss of generality, that

$$|\boldsymbol{c}_i|^2 = 1 \qquad (1 \leqq i \leqq n).$$

Then

$$\sum_j u_j \boldsymbol{b}_j = \sum_i \sum_{j \geqq i} u_j t_{ji} \boldsymbol{c}_i;$$

and so

$$|\sum u_j \boldsymbol{b}_j|^2 = \sum_i \big(\sum_{j \geqq i} u_j t_{ji}\big)^2. \tag{3}$$

We now show that

$$\sum_i \lambda_i^{-2} \big(\sum_{j \geqq i} u_j t_{ji}\big)^2 \geqq 1 \tag{4}$$

for all sets of integers $\boldsymbol{u} \neq \boldsymbol{o}$. For let $u_1, \ldots, u_n$ be integers, and suppose that

$$u_J \neq 0, \quad u_j = 0 \qquad (j > J). \tag{5}$$

Then $u_1\boldsymbol{b}_1 + \cdots + u_n\boldsymbol{b}_n$ is not dependent on $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{J-1}$; and so

$$|\sum u_j \boldsymbol{b}_j|^2 \geqq \lambda_J^2. \tag{5'}$$

Further, (5) implies that all the summands in (3) and (4) with $i > J$ are 0. Hence, and since $\lambda_j \leqq \lambda_J$ if $j \leqq J$, the left-hand side of (4) is

$$\sum_{i \leqq J} \lambda_i^{-2} \big(\sum_{j \geqq i} u_j t_{ji}\big)^2 \geqq \sum_{i \leqq J} \lambda_J^{-2} \big(\sum_{j \geqq i} u_j t_{ji}\big)^2 = \lambda_J^{-2} \Big|\sum_j u_j \boldsymbol{b}_j\Big|^2 \geqq 1,$$

by (3) and (5'). Hence if Λ' is the lattice with basis

$$\boldsymbol{b}_j' = t_{j1}\lambda_1^{-1}\boldsymbol{c}_1 + \cdots + t_{jj}\lambda_j^{-1}\boldsymbol{c}_j, \qquad (1 \leqq j \leqq n),$$

we have

$$|\sum u_j \boldsymbol{b}_j'|^2 \geqq 1$$

for every point $\sum u_j \boldsymbol{b}_j' \neq \boldsymbol{o}$ of Λ'; that is

$$F_0(\Lambda') = |\Lambda'| \geqq 1. \tag{6}$$

On the other hand,

$$d(\Lambda') = \lambda_1^{-1} \ldots \lambda_n^{-1} d(\Lambda). \tag{7}$$

But now

$$\frac{|\Lambda'|^n}{d(\Lambda')} \leqq \sup_{\mathsf{M}} \frac{|\mathsf{M}|^n}{d(\mathsf{M})} = \delta(F_0), \tag{8}$$

[1] We say that two vectors $\boldsymbol{a}, \boldsymbol{b}$ are orthogonal if their scalar product $\boldsymbol{a}\boldsymbol{b}$ vanishes.

Lemma

Let L be a lattice of dimension n. Let $v_1, v_2, \dots, v_n$ be linearly independent members of L. Then there exists a basis $b_1, b_2, \dots, b_n$ such that

$$v_1 = t_{1,1} b_1$$

$$v_2 = t_{1,2} b_1 + t_{2,2} b_2$$

where the t_{ij} are integers.

$$\vdots$$

Mahler's Theorem

$0 < \lambda_1 \le \dots \le \lambda_d$ are the successive minima of lattice L.

$v_1, v_2, \dots, v_d$ are associated "directional basis".

$\exists$ basis $w_1, \dots, w_d$ of L such that (i) $|w_i| \le \frac{i\lambda_i}{2}$, $1 \le i \le d$

(ii) $V_i = \mathrm{span}[v_1, \dots, v_i] \Rightarrow w_1, \dots, w_i$ is a basis for $L \cap V_i$

Proof

$w_1 = v_1$; suppose inductively we have chosen $w_1, \dots, w_{i-1}$.

Define $\hat{w}_j$, $j = 1, 2, \dots, i$, via Lemma, $v_1, \dots, v_i$ and $L \cap V_i$.

Then $x \in L \cap V_i \Rightarrow$ $x = \underbrace{n_1 \hat{w}_1 + \dots + n_{i-1} \hat{w}_{i-1}}_{\in L \cap V_{i-1}} + n_i \hat{w}_i$ ($\hat{w}_j$) basis for $L \cap V_i$

$= n_1' w_1 + \dots + n_{i-1}' w_{i-1} + n_i \hat{w}_i$ (w_j) basis for $L \cap V_{i-1}$

$w_1, w_2, \dots, w_{i-1}, \hat{w}_i$ is a basis for $L \cap V_i$

~~$\hat{w}_i = \xi_{i,1} v_1 + \dots + \xi_{i,i} v_i$ where $\xi_{i,i} = \frac{1}{\text{integer}}$~~

~~(Comes from $v_i = \underline{m_1 \hat{w}_1 + \dots + m_{i-1} \hat{w}_{i-1}} + m_i \hat{w}_i$~~

~~now re-express in terms of $w_1, \dots, w_{i-1}$~~

~~$v_1, v_2, \dots, v_i$: integer ; $w_1, \dots, w_{i-1}, \hat{w}_i$~~

Now let $\hat{\omega}_i = t_1 v_1 + \dots + t_{i-1} v_{i-1} + t_i v_i$

$v_i \in (L \cap V_{i-1}) + \{n \hat{\omega}_i\}$ and so

$$\hat{\omega}_i = t_1 v_1 + \dots + t_{i-1} v_{i-1} + [\alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} + n v_i] t_i$$

$$\Rightarrow \quad t_i = \tfrac{1}{n} \quad \text{where } n \text{ is integer.}$$

If $|t_i| = 1$ we take $\omega_i = v_i$.

[We get $v_i = \hat{\omega}_i - \sum_{j=1}^{i-1} t_j v_j = \hat{\omega}_i - \sum_{j=1}^{i-1} t'_j \omega_j$, where $t'_1, \dots, t'_{i-1}$ must be integral. v_i has an integral expression in terms of $\hat{\omega}_i, \omega_1, \dots, \omega_{i-1}$ & is unique]

So v_i can replace $\hat{\omega}_i$ in basis of $L \cap V_i$

If $|t_i| \leq \frac{1}{2}$ then we can assume $|t_j| \leq \frac{1}{2}$ for $1 \leq j \leq i-1$ too.

For example $\hat{\omega}_i - v_1, \omega_1, \dots, \omega_{i-1}$ is a basis for V_i.

Now $|v_j| \leq \lambda_j \leq \lambda_i$ and so $|\hat{\omega}_i| \leq \frac{i \lambda_i}{2}$ and we take $\omega_i = \hat{\omega}_i$.