Časopis pro pěstování matematiky

Boris Gruber

On the shortest lattice vectors in a three-dimensional translational (Bravais) lattice

*Časopis pro pěstování matematiky*, Vol. 95 (1970), No. 3, 231--239

Persistent URL: http://dml.cz/dmlcz/117688

ČASOPIS PRO PĚSTOVÁNÍ MATEMATIKY

*Vydává Matematický ústav ČSAV, Praha*

SVAZEK 95 * PRAHA 12. 8. 1970 * ČÍSLO 3

# ON THE SHORTEST LATTICE VECTORS IN A THREE-DIMENSIONAL TRANSLATIONAL (BRAVAIS) LATTICE

BORIS GRUBER, Praha

(Received September 9, 1966, in revised form September 3, 1968)

A linear space $\boldsymbol{V}$ over the body of real numbers is given. The elements of the space $\boldsymbol{V}$ (vectors) are denoted by $\boldsymbol{a}, \boldsymbol{b}, \ldots$, integral numbers by $a, b, \ldots$ and real numbers by $\alpha, \beta, \ldots$ (all eventually with various indices). A scalar product $\boldsymbol{a} \,.\, \boldsymbol{b}$ is defined in $\boldsymbol{V}$; $\boldsymbol{a}^2$ is written instead of $\boldsymbol{a} \,.\, \boldsymbol{a}$. By the length of the vector $\boldsymbol{a}$ the number $|\boldsymbol{a}| = \sqrt{\boldsymbol{a}^2}$ is understood.

The set $\boldsymbol{M} \subset \boldsymbol{V}$ is referred to as a (three-dimensional translational or Bravais) *lattice*, if it may be written in the form

$$\boldsymbol{M} = \mathop{\mathscr{E}}_{\boldsymbol{x}}(\boldsymbol{x} = a\boldsymbol{a} + b\boldsymbol{b} + c\boldsymbol{c};\ a, b, c \text{ arbitrary}) \tag{1}$$

where the vectors

$$\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \tag{2}$$

are linearly independent. The vectors belonging to $\boldsymbol{M}$ are also called *lattice vectors* of $\boldsymbol{M}$. If (1) is correct, then the vectors (2) are said to form a *basis* of the lattice $\boldsymbol{M}$.

We call (2) a *fundamental sequence* of lattice vectors of $\boldsymbol{M}$, if

1. (2) are linearly independent lattice vectors of $\boldsymbol{M}$,
2. $|\boldsymbol{a}| \leqq |\boldsymbol{b}| \leqq |\boldsymbol{c}|$,
3. the inequality $|\boldsymbol{a}| + |\boldsymbol{b}| + |\boldsymbol{c}| \leqq |\boldsymbol{x}| + |\boldsymbol{y}| + |\boldsymbol{z}|$ holds for any triplet $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ of linearly independent lattice vectors of $\boldsymbol{M}$.

It is readily seen that (2) is a fundamental sequence of $\boldsymbol{M}$, if and only if

1. $\boldsymbol{a}$ is the shortest non-zero lattice vetor of $\boldsymbol{M}$,
2. $\boldsymbol{b}$ is the shortest of all lattice vectors $\boldsymbol{x}$ such that $\boldsymbol{a}, \boldsymbol{x}$ are linearly independent,
3. $\boldsymbol{c}$ is the shortest of all lattice vectors $\boldsymbol{x}$ such that $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}$ are linearly independent.

If (2) as well as

$$\boldsymbol{a}', \boldsymbol{b}', \boldsymbol{c}' \tag{3}$$

are fundamental sequences of lattice vectors of $\boldsymbol{M}$, then

$$|\boldsymbol{a}| = |\boldsymbol{a}'|\,, \quad |\boldsymbol{b}| = |\boldsymbol{b}'|\,, \quad |\boldsymbol{c}| = |\boldsymbol{c}'|\,. \tag{4}$$

The symbol $[\xi]$ denotes the integer defined by inequalities $0 \leqq \xi - [\xi] < 1$. Consequently,

$$2|\eta - \xi[\eta/\xi + \tfrac{1}{2}]| \leqq \xi \tag{5}$$

holds for $\xi > 0$, $\eta$.

The object of the present paper is the proof of the following theorem.

**Theorem.** *The vectors* (2) *constitute a fundamental sequence of lattice vectors of* $\boldsymbol{M}$, *if and only if they form a basis of* $\boldsymbol{M}$ *and satisfy the following inequalities*:

$$|\boldsymbol{a}| \leqq |\boldsymbol{b}| \leqq |\boldsymbol{c}|\,, \tag{6}$$

$$2|\boldsymbol{a}\,.\,\boldsymbol{b}| \leqq \boldsymbol{a}^2\,, \tag{7}$$

$$2|(s\boldsymbol{a} + t\boldsymbol{b})\,.\,\boldsymbol{c}| \leqq (s\boldsymbol{a} + t\boldsymbol{b})^2 \quad \textit{for} \quad \mathrm{Max}\,(|s|, |t|) = 1\,. \tag{8}$$

The proof of this theorem is preceded by six lemmas.

**Lemma 1.** *Let*

$$2|\boldsymbol{a}\,.\,\boldsymbol{b}| > \boldsymbol{a}^2 > 0\,. \tag{9}$$

*Then, denoting*

$$r = [\boldsymbol{a}\,.\,\boldsymbol{b}/\boldsymbol{a}^2 + \tfrac{1}{2}]\,, \quad \boldsymbol{b}' = \boldsymbol{b} - r\boldsymbol{a}\,, \tag{10}$$

*the inequalities*

$$\begin{gathered} |\boldsymbol{b}'| < |\boldsymbol{b}|\,, \\ |\boldsymbol{b}'| \leqq |\boldsymbol{b} - s\boldsymbol{a}| \quad (s \textit{ arbitrary}) \end{gathered} \tag{11}$$

*hold.*

Proof. The relations (9), (10) and (5) imply

$$r \neq 0 \tag{12}$$

$$2|\boldsymbol{a}\,.\,\boldsymbol{b}'| \leqq \boldsymbol{a}^2\,. \tag{13}$$

Bearing in mind that

$$\boldsymbol{b} - s\boldsymbol{a} = \boldsymbol{b}' + (r - s)\,\boldsymbol{a} \quad (s \text{ arbitrary})\,,$$

inequality (11) is equivalent to

$$(r - s)^2\,\boldsymbol{a}^2 + 2(r - s)\,\boldsymbol{a}\,.\,\boldsymbol{b}' \geqq 0\,.$$

Here (see (13)) the left-hand side is at least $(r-s)^2\,\boldsymbol{a}^2 - |r-s|\,\boldsymbol{a}^2$ which is non-negative. Thus (11) is proved. If $|\boldsymbol{b}'|$ were equal to $|\boldsymbol{b}|$, we should get $r\boldsymbol{a}^2 = -2\boldsymbol{a}\,.\,\boldsymbol{b}'$ from (10), (12). This would necessitate $|\boldsymbol{a}\,.\,\boldsymbol{b}| = |\boldsymbol{a}\,.\,\boldsymbol{b}'|$ and (9) would contradict (13).

In the next five lemmas the following assumptions are made. Linearly independent vectors (3) satifying

$$|\boldsymbol{a}'| \leqq |\boldsymbol{b}'| \leqq |\boldsymbol{c}'| \tag{14}$$

$$2|\boldsymbol{a}'\,.\,\boldsymbol{b}'| \leqq \boldsymbol{a}'^2 \tag{15}$$

$$2|(s\boldsymbol{a}' + t\boldsymbol{b}')\,.\,\boldsymbol{c}'| \leqq (s\boldsymbol{a}' + t\boldsymbol{b}')^2 \quad \text{for} \quad \operatorname{Max}(|s|, |t|) = 1 \tag{16}$$

are given. Further the linearly independent vectors (2) satifying (4) are given. The following equalities hold:

$$\boldsymbol{x} = a\boldsymbol{a}' + b\boldsymbol{b}' + c\boldsymbol{c}',$$

$$\boldsymbol{a} = a_1\boldsymbol{a}' + b_1\boldsymbol{b}' + c_1\boldsymbol{c}', \quad \boldsymbol{b} = a_2\boldsymbol{a}' + b_2\boldsymbol{b}' + c_2\boldsymbol{c}',$$

$$\boldsymbol{c} = a_3\boldsymbol{a}' + b_3\boldsymbol{b}' + c_3\boldsymbol{c}', \tag{17}$$

$$n = \operatorname{Max}(|a|, |b|, |c|), \quad m_i = \operatorname{Max}(|a_i|, |b_i|, |c_i|) \quad (i = 1, 2, 3),$$

$$m = \operatorname{Max}(m_1, m_2, m_3),$$

$$\boldsymbol{D} = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}, \tag{18}$$

$$D = |\boldsymbol{D}|\,. \tag{19}$$

**Lemma 2.**

$$b \neq 0, \quad c = 0 \Rightarrow |\boldsymbol{x}| \geqq |\boldsymbol{b}'|, \tag{20b}$$

$$c \neq 0 \Rightarrow |\boldsymbol{x}| \geqq |\boldsymbol{c}'|\,. \tag{20c}$$

**Lemma 3.**

$$b \neq 0, \quad c = 0, \quad |\boldsymbol{x}| = |\boldsymbol{b}'| \Rightarrow n = 1 \tag{21b}$$

$$c \neq 0, \quad |\boldsymbol{x}| = |\boldsymbol{c}'| \Rightarrow n = 1\,. \tag{21c}$$

These two lemmas are proved simultaneously. Let us denote by $\boldsymbol{K}$ the set of all points $[\xi, \eta, \zeta]$ satisfying the inequalities

$$|\xi| \leqq \boldsymbol{b}'^2, \quad |\eta| \leqq \boldsymbol{a}'^2, \quad |\zeta| \leqq \boldsymbol{a}'^2,$$

$$r\xi + s\eta + t\zeta \leqq \boldsymbol{a}'^2 + \boldsymbol{b}'^2 \quad \text{for} \quad rst = -1\,.$$

$\boldsymbol{K}$ is a convex dodecahedron. Therefore the linear form

$$L(\xi, \eta, \zeta) = bc\xi + ac\eta + ab\zeta$$

assumes its minimum $\mu$ on $\boldsymbol{K}$ in one of the 16 vertices of $\boldsymbol{K}$. Comparing the corresponding values, we find that

$$\mu = (|bc| - |ac| - |ab|)\,\boldsymbol{a}'^2 - |bc|\,\boldsymbol{b}'^2\,, \quad \text{if} \quad n = |a|\,,$$

$$\mu = -|ab|\,\boldsymbol{a}'^2 - |bc|\,\boldsymbol{b}'^2\,, \quad \text{if} \quad n = |b|\,,$$

$$\mu = -|ac|\,\boldsymbol{a}'^2 - |bc|\,\boldsymbol{b}'^2\,, \quad \text{if} \quad n = |c|\,.$$

Let us denote $v = a^2\boldsymbol{a}'^2 + b^2\boldsymbol{b}'^2 + c^2\boldsymbol{c}'^2 + \mu$. Since $\boldsymbol{x}^2 = a^2\boldsymbol{a}'^2 + b^2\boldsymbol{b}'^2 + c^2\boldsymbol{c}'^2 + L(2\boldsymbol{b}' \,.\, \boldsymbol{c}', 2\boldsymbol{a}' \,.\, \boldsymbol{c}', 2\boldsymbol{a}' \,.\, \boldsymbol{b}')$ and $[2\boldsymbol{b}' \,.\, \boldsymbol{c}', 2\boldsymbol{a}' \,.\, \boldsymbol{c}', 2\boldsymbol{a}' \,.\, \boldsymbol{b}'] \in \boldsymbol{K}$ according to (7), (8), we have $\boldsymbol{x}^2 \geqq v$.

Later the implications

$$\text{Max}\,(s, t) \geqq 1 \Rightarrow s^2 + t^2 \geqq st + 1\,, \tag{22}$$

$$s^2 + t^2 = st + 1 \Rightarrow \text{Max}\,(s, t) = 1$$

referring to non-negative integers $s$, $t$ will be applied.

Now let us suppose $c \neq 0$, $n = |a|$. Then the inequality $v \geqq \boldsymbol{c}'$ can be written in the form

$$(n - |b|)(n - |c|)\,\boldsymbol{a}'^2 + b^2\boldsymbol{b}'^2 + (c^2 - 1)\,\boldsymbol{c}'^2 \geqq |bc|\,\boldsymbol{b}'^2 \tag{23}$$

and it is enough to prove

$$b^2\boldsymbol{b}'^2 + (c^2 - 1)\,\boldsymbol{b}'^2 \geqq |bc|\,\boldsymbol{b}'^2\,. \tag{24}$$

But this is true according to (22). If $|\boldsymbol{x}| = |\boldsymbol{c}'|$ (our assumptions being fulfilled), then the equality occurs in (23) and consequently (see (24)) $|c| > 1$, $|\boldsymbol{c}'| > |\boldsymbol{b}'|$ cannot hold. If $|c| = 1$, then

$$(n - |b|)(n - 1)\,\boldsymbol{a}'^2 + |b|\,(|b| - 1)\,\boldsymbol{b}'^2 = 0$$

which necessitates $n = 1$. If $|\boldsymbol{c}'| = |\boldsymbol{b}'|$ we have

$$(n - |b|)(n - |c|)\,\boldsymbol{a}'^2 + (b^2 + c^2 - |bc| - 1)\,\boldsymbol{b}'^2 = 0\,.$$

Here both terms on the left-hand side are non-negative again. To nullify the second of them $\text{Max}\,(|b|, |c|) = 1$ must hold and then the first term vanishes only if $n = 1$. Thus (20c), (21c) are proved for $n = |a|$. Other cases as well as the implications (20b), (21b) are analogous.

**Lemma 4.** $m = 1$.

Proof. If $c_1 \neq 0$, then (20c), (4) and (14) imply $|\boldsymbol{c}'| \leqq |\boldsymbol{a}| = |\boldsymbol{a}'| \leqq |\boldsymbol{c}'|$ and according to (21c) $m_1 = 1$. If $b_2 = c_2 = 0$, then either $c_1 \neq 0$, which implies $|\boldsymbol{a}| \geqq |\boldsymbol{c}'|$, or $b_1 \neq 0, c_1 = 0$, and then $|\boldsymbol{a}| \geqq |\boldsymbol{b}'|$. In both cases $|\boldsymbol{b}| = |\boldsymbol{a}'|$, which necessitates $|a_2| = m_2 = 1$. If $b_3 \neq 0$, $c_3 = 0$, then either $c_1 \neq 0$ with the consequence $|\boldsymbol{a}| \geqq |\boldsymbol{c}'|$, or $c_2 \neq 0$ resulting in $|\boldsymbol{b}| \geqq |\boldsymbol{c}'|$. In both cases $|\boldsymbol{c}| = |\boldsymbol{b}'|$ and (21b) is applied. If $b_3 = c_3 = 0$, then either $c_1 \neq 0$ and then $|\boldsymbol{a}| \geqq |\boldsymbol{c}'|$, or $c_1 = 0$, $b_1 \neq 0$, $c_2 \neq 0$ and then $|\boldsymbol{a}| \geqq |\boldsymbol{b}'|$, $|\boldsymbol{b}| \geqq |\boldsymbol{c}'|$. Thus $|\boldsymbol{c}| = |\boldsymbol{a}'|$ always holds and $|a_3| = m_3 = 1$. The remaining cases are analogous.

**Lemma 5.** $|D^*| \leqq 1$ *for any second-order subdeterminant* $D^*$ *of the matrix* $\boldsymbol{D}$.

Proof. Let

$$r_1\boldsymbol{a}' + s_1\boldsymbol{b}' + t_1\boldsymbol{c}', \quad r_2\boldsymbol{a}' + s_2\boldsymbol{b}' + t_2\boldsymbol{c}' \tag{25}$$

be any two of the vectors (17), let us denote

$$D' = \begin{vmatrix} s_1 & t_1 \\ s_2 & t_2 \end{vmatrix}.$$

The inequality

$$|D'| \leqq 1 \tag{26}$$

is obvious if $s_1t_1s_2t_2 = 0$. Further let this product be different from zero. From the inequalities (15) and

$$2|\boldsymbol{a}' \,.\, \boldsymbol{c}'| \leqq \boldsymbol{a}'^2 \,^{1})$$

it follows

$$-2r_1s_1\boldsymbol{a}' \,.\, \boldsymbol{b}' \leqq r_1^2\boldsymbol{a}'^2, \quad -2r_1t_1\boldsymbol{a}' \,.\, \boldsymbol{c}' \leqq r_1^2\boldsymbol{a}'^2 . \tag{27}$$

Since

$$|r_1\boldsymbol{a}' + s_1\boldsymbol{b}' + t_1\boldsymbol{c}'| = |\boldsymbol{c}'|, \tag{28}$$

we have according to (27)

$$\begin{aligned} 2s_1t_1\boldsymbol{b}' \,.\, \boldsymbol{c}' &= -r_1^2\boldsymbol{a}'^2 - \boldsymbol{b}'^2 - 2r_1s_1\boldsymbol{a}' \,.\, \boldsymbol{b}' - 2r_1t_1\boldsymbol{a}' \,.\, \boldsymbol{c}' \leqq \\ &\leqq -r_1^2\boldsymbol{a}'^2 - \boldsymbol{b}'^2 + r_1^2\boldsymbol{a}'^2 + r_1^2\boldsymbol{a}'^2 \leqq 0 . \end{aligned} \tag{29}$$

Analogously

$$\begin{aligned} -2s_2t_2\boldsymbol{b}' \,.\, \boldsymbol{c}' &= r_2^2\boldsymbol{a}'^2 + \boldsymbol{b}'^2 + 2r_2s_2\boldsymbol{a}' \,.\, \boldsymbol{b}' + 2r_2t_2\boldsymbol{a}' \,.\, \boldsymbol{c}' \geqq \\ &\geqq r_2^2\boldsymbol{a}'^2 + \boldsymbol{b}'^2 - r_2^2\boldsymbol{a}'^2 - r_2^2\boldsymbol{a}'^2 \geqq 0 . \end{aligned} \tag{30}$$

[1]) This is the inequality (16) for $s = 1$, $t = 0$.

Let us suppose now that (26) is not true. Then

$$s_1t_1s_2t_2 = -1\,, \tag{31}$$

the left-hand sides in (29), (30) are equal and equality sign is valid throughout. If $r_1r_2 = 0$, the contradiction is obvious. If $r_1r_2 \neq 0$, we have according to (29), (27)

$$-2r_1s_1\boldsymbol{a}' \,.\, \boldsymbol{b}' = \boldsymbol{a}'^2\,, \quad -2r_1t_1\boldsymbol{a}' \,.\, \boldsymbol{c}' = \boldsymbol{a}'^2$$

and also according to (30), (27)

$$2r_2s_2\boldsymbol{a}' \,.\, \boldsymbol{b}' = -\boldsymbol{a}'^2\,, \quad 2r_2t_2\boldsymbol{a}' \,.\, \boldsymbol{c}' = -\boldsymbol{a}'^2\,.$$

Consequently $s_1t_1 = s_2t_2$ in contradiction to (31). Thus (26) is proved. For the determinant $\begin{vmatrix} r_1 & t_1 \\ r_2 & t_2 \end{vmatrix}$ a slight modification is necessary, for $\begin{vmatrix} r_1 & s_1 \\ r_2 & s_2 \end{vmatrix}$ the equality

$$(r_1\boldsymbol{a}' + s_1\boldsymbol{b}' + t_1\boldsymbol{c}')^2 = \boldsymbol{b}'^2 + t_1^2(\boldsymbol{c}'^2 - \boldsymbol{b}'^2) \tag{32}$$

is to be applied instead of (28). Proving (32), we need only pay attention to the case $t_1 = 0$, $r_1\boldsymbol{a}' + s_1\boldsymbol{b}' = \boldsymbol{c}$. Here one of the vectors $\boldsymbol{a}$, $\boldsymbol{b}$ has the form $r\boldsymbol{a}' + s\boldsymbol{b}' + t\boldsymbol{c}'$, $t \neq 0$, so that

$$|\boldsymbol{c}'| \leqq |r\boldsymbol{a}' + s\boldsymbol{b}' + t\boldsymbol{c}'| \leqq |\boldsymbol{b}| \leqq |\boldsymbol{c}'|$$

and consequently $|r_1\boldsymbol{a}' + s_1\boldsymbol{b}'| = |\boldsymbol{b}'|$ which was to be proved.

**Lemma 6.** $|D| = 1$.

Proof. If the matrix $\boldsymbol{D}$ involves two zeros in one row or in one column, then the result is obvious. Let us suppose further that there is no more than one zero in any row and any column of $\boldsymbol{D}$.

a) Every row of $\boldsymbol{D}$ involves a zero. Then $\boldsymbol{D}$ has the form (except, perhaps, for the order or the rows)

$$\begin{bmatrix} s_1 & s_2 & 0 \\ s_3 & 0 & s_4 \\ 0 & s_5 & s_6 \end{bmatrix} \quad (|s_1 \dots s_6| = 1)$$

so that

$$|D| = |s_2s_3s_6 + s_1s_4s_5|\,. \tag{33}$$

It is

$$|s_1\boldsymbol{a}' + s_2\boldsymbol{b}'| = |\boldsymbol{b}'|\,, \quad |s_3\boldsymbol{a}' + s_4\boldsymbol{c}'| = |\boldsymbol{c}'|\,, \quad |s_5\boldsymbol{b}' + s_6\boldsymbol{c}'| = |\boldsymbol{c}'|\,. \tag{34}$$

This may be shown in a similar way as (32). From (34) it follows

$$\boldsymbol{a}'^2 = -2s_1s_2\boldsymbol{a}' \,.\, \boldsymbol{b}'\,, \quad \boldsymbol{a}'^2 = -2s_3s_4\boldsymbol{a}' \,.\, \boldsymbol{c}'\,, \quad \boldsymbol{b}'^2 = -2s_5s_6\boldsymbol{b}' \,.\, \boldsymbol{c}'\,,$$

and summing we get

$$2a'^2 + b'^2 = -2(s_1 s_2 a' \,.\, b' + s_3 s_4 a' \,.\, c' + s_5 s_6 b' \,.\, c') \,. \tag{35}$$

Putting $s = t = 1$ and $s = -t = 1$ in the inequalities (16) we obtain

$$2(t_1 a' \,.\, b' + t_2 a' \,.\, c' + t_3 b' \,.\, c') \leqq a'^2 + b'^2 \quad \text{for} \quad t_1 t_2 t_3 = -1.$$

Thus if

$$s_1 \ldots s_6 = 1 \,, \tag{36}$$

then

$$2a'^2 + b'^2 \leqq a'^2 + b'^2$$

according to (35); if (36) is not true, then $D = 0$ by (33). This results in a contradiction in both cases. The matrix $\boldsymbol{D}$ cannot have a zero in every row.

b) Just two rows of $\boldsymbol{D}$ involve a zero. Let us suppose these zeros be in the first and second columns, other cases being analogous. Then $\boldsymbol{D}$ has the form (except, perhaps, for the order of the rows)

$$\begin{bmatrix} 0 & s_1 & s_2 \\ s_3 & 0 & s_4 \\ s_5 & s_6 & s_7 \end{bmatrix} \qquad (|s_1 \ldots s_7| = 1)$$

and

$$|D| = |s_1 s_4 s_5 + s_2 s_3 s_6 - s_1 s_3 s_7| \,. \tag{37}$$

Lemma 5 implies

$$\begin{vmatrix} s_1 & s_2 \\ s_6 & s_7 \end{vmatrix} = \begin{vmatrix} s_3 & s_4 \\ s_5 & s_7 \end{vmatrix} = 0$$

so that

$$s_1 s_2 s_6 s_7 = s_3 s_4 s_5 s_7 = 1 \,. \tag{38}$$

According to (37) and (38)

$$|D| = \frac{|s_1^2 s_3 s_4 s_5 s_7 + s_1 s_2 s_3^2 s_6 s_7 - s_1^2 s_3^2 s_7^2|}{|s_1 s_3 s_7|} = 1 \,.$$

c) Two rows of $\boldsymbol{D}$ are without zeros. Then two of the vectors (17) have the form (25) where

$$|r_1 s_1 t_1 r_2 s_2 t_2| = 1 \,.$$

Applying lemma 5 once more we get

$$\begin{vmatrix} r_1 & s_1 \\ r_2 & s_2 \end{vmatrix} = \begin{vmatrix} r_1 & t_1 \\ r_2 & t_2 \end{vmatrix} = \begin{vmatrix} s_1 & t_1 \\ s_2 & t_2 \end{vmatrix} = 0 \,;$$

but (25) are linearly independent. Thus eventuality c) cannot occur and lemma 6 is proved.

Proof of the theorem. a) Let us assume that (2) is a basis of $\boldsymbol{M}$, that inequalities (6), (7), (8) are correct and that $\boldsymbol{x}$ is an arbitrary lattice vector of $\boldsymbol{M}$. Then integral numbers $a, b, c$ exist in such a way that $\boldsymbol{x} = a\boldsymbol{a} + b\boldsymbol{b} + c\boldsymbol{c}$. To prove that (2) is a fundamental sequence of $\boldsymbol{M}$ we must show that

$$|a| + |b| + |c| > 0 \Rightarrow |\boldsymbol{x}| \geqq |\boldsymbol{a}|,$$
$$|b| + |c| > 0 \Rightarrow |\boldsymbol{x}| \geqq |\boldsymbol{b}|,$$
$$|c| > 0 \Rightarrow |\boldsymbol{x}| \geqq |\boldsymbol{c}|.$$

For this purpose it is sufficient (see (6)) to show that

$$a \neq 0, \quad b = 0, \quad c = 0 \Rightarrow |\boldsymbol{x}| \geqq |\boldsymbol{a}|,$$
$$b \neq 0, \quad c = 0 \Rightarrow |\boldsymbol{x}| \geqq |\boldsymbol{b}|,$$
$$c \neq 0 \Rightarrow |\boldsymbol{x}| \geqq |\boldsymbol{c}|.$$

But this follows from lemma 2.

b) Let us assume that (2) is a fundamental sequence of lattice vectors of $\boldsymbol{M}$. Then inequality (6) is fulfilled. If any of the inequalities (8) do not hold, a lattice vector $\boldsymbol{c}'$ may be found according to lemma 1 in such a way that $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}'$ are linearly independent and $|\boldsymbol{c}'| < |\boldsymbol{c}|$. But this contradicts the fact that (2) is a fundamental sequence. In the same way inequality (7) can be proved.

Thus the only thing which remains to complete the proof is to show that (2) is a basis of $\boldsymbol{M}$. Let us construct a sequence of bases

$$\boldsymbol{a}_i, \boldsymbol{b}_i, \boldsymbol{c}_i \quad (|\boldsymbol{a}_i| \leqq |\boldsymbol{b}_i| \leqq |\boldsymbol{c}_i|) \tag{39}$$

($i = 1, \ldots, s$) in the following way. For $i = 1$ (39) is an arbitrary basis. If (39) is known for a certain $i \geqq 1$, we proceed as follows. If the inequalities

$$2|\boldsymbol{a}_i \,.\, \boldsymbol{b}_i| \leqq \boldsymbol{a}_i^2, \tag{40}$$

$$2|(s\boldsymbol{a}_i + t\boldsymbol{b}_i) \,.\, \boldsymbol{c}_i| \leqq (s\boldsymbol{a}_i + t\boldsymbol{b}_i)^2 \quad \text{for} \quad \operatorname{Max}(|s|, |t|) = 1 \tag{41}$$

are fulfilled, we put $s = i$. If (40) does not hold we find the vector $\boldsymbol{b}' = \boldsymbol{b}_i - r\boldsymbol{a}_i$ fulfilling $|\boldsymbol{b}'| < |\boldsymbol{b}_i|$ according to lemma 1. If (40) holds but (41) does not for a certain pair of numbers $s, t$, we find the vector $\boldsymbol{c}' = \boldsymbol{c}_i - r(s\boldsymbol{a}_i + t\boldsymbol{b}_i)$ fulfilling $|\boldsymbol{c}'| < |\boldsymbol{c}_i|$. In the first case the vectors $\boldsymbol{a}_i, \boldsymbol{b}', \boldsymbol{c}_i$ are relabelled

$$\boldsymbol{a}_{i+1}, \boldsymbol{b}_{i+1}, \boldsymbol{c}_{i+1} \tag{42}$$

in such a way that $|\boldsymbol{a}_{i+1}| \leqq |\boldsymbol{b}_{i+1}| \leqq |\boldsymbol{c}_{i+1}|$ is correct; in the second case the same is done with the vectors $\boldsymbol{a}_i, \boldsymbol{b}_i, \boldsymbol{c}'$. Thus (42) is a basis of $\boldsymbol{M}$ and the inequality

$$|\boldsymbol{a}_{i+1}| + |\boldsymbol{b}_{i+1}| + |\boldsymbol{c}_{i+1}| < |\boldsymbol{a}_i| + |\boldsymbol{b}_i| + |\boldsymbol{c}_i|$$

holds so that the sequence (39) must be a finite one. Further on the notation

$$\boldsymbol{a}' = \boldsymbol{a}_s\,, \quad \boldsymbol{b}' = \boldsymbol{b}_s\,, \quad \boldsymbol{c}' = \boldsymbol{c}_s$$

is applied.

The vectors (3) form a basis of $\boldsymbol{M}$ and fulfil the inequalities (14), (15), (16). According to the part a) of this proof (3) is a fundamental sequence of $\boldsymbol{M}$. Equalities (4) are true and integers $a_1 \ldots c_3$ may be found in such a way that (17) holds. Then $|D| = 1$, using the notation of (18), (19). Accordingly the vectors (3) may be expressed as integral linear combinations of the vectors (2). But this means – (3) being a basis of $\boldsymbol{M}$ – that (2) is also its basis. Thus the proof of the theorem is completed.

**Corollary 1.** The above proof involves, moreover, an algorithm for determining a fundamental sequence of lattice vectors of $\boldsymbol{M}$, if an arbitrary basis of $\boldsymbol{M}$ is known. Inequality (11) guarantees a good efficiency of this procedure.

**Corollary 2.** *If* (2) *is a fundamental sequence of lattice vectors of* $\boldsymbol{M}$, *then inequalities*

$$|\cos\alpha| \leqq \tfrac{1}{2}\,, \quad |\cos\beta| \leqq \tfrac{1}{2}\,, \quad |\cos\gamma| \leqq \tfrac{1}{2}$$

*hold where*

$$\alpha = \arccos\left(\boldsymbol{b}\,.\,\boldsymbol{c}/|\boldsymbol{b}|\,|\boldsymbol{c}|\right), \quad \textit{etc.}$$

In other words the angle between two vectors of a fundamental sequence cannot be smaller than 60° and greater than 120°. This follows from inequalities (7), (8).

**Corollary 3.** *The system of inequalities* (6), (7), (8) *is the best one in the following sense. Let us choose real numbers*

$$\varrho, \sigma, \tau, \xi, \eta, \zeta \tag{43}$$

*in such a way that*

$$0 < \varrho \leqq \sigma \leqq \tau\,, \tag{44}$$

$$2|\xi| \leqq \sigma^2\,, \quad 2|\eta| \leqq \varrho^2\,, \quad 2|\zeta| \leqq \varrho^2\,, \tag{45}$$

$$2(r\xi + s\eta + t\zeta) \leqq \varrho^2 + \sigma^2 \quad \textit{for} \quad rst = -1\ ^2) \tag{46}$$

*are fulfilled* (*but otherwise arbitrarily*). *Then there exists a lattice* $\boldsymbol{M}$ *with fundamental sequence* (2) *satisfying*

$$|\boldsymbol{a}| = \varrho\,, \quad |\boldsymbol{b}| = \sigma\,, \quad |\boldsymbol{c}| = \tau\,,$$

$$\boldsymbol{b}\,.\,\boldsymbol{c} = \xi\,, \quad \boldsymbol{a}\,.\,\boldsymbol{c} = \eta\,, \quad \boldsymbol{a}\,.\,\boldsymbol{b} = \zeta\,.$$

This may be shown by an example of the arithmetical vector space.

*Author's address:* Praha 2, Ke Karlovu 3 (Matematicko-fyzikální fakulta UK).

[2]) (44), (45), (46) are inequalities (6), (7), (8), where (43) are written instead of $|\boldsymbol{a}|$, $|\boldsymbol{b}|$, $|\boldsymbol{c}|$, $\boldsymbol{b}\,.\,\boldsymbol{c}$, $\boldsymbol{a}\,.\,\boldsymbol{c}$, $\boldsymbol{a}\,.\,\boldsymbol{b}$, respectively.