TWO FINITENESS THEOREMS IN THE MINKOWSKI THEORY OF REDUCTION

P. W. AITCHISON

(Received 16 March 1970; revised 16 December 1970)

Communicated by E. S. Barnes

1. Introduction

Minkowski proved two important finiteness theorems concerning the reduction theory of positive definite quadratic forms (see [6], p. 285 or [7], §8 and §10). A positive definite quadratic form in n variables may be considered as an ellipsoid in n-dimensional Euclidean space, R^n, and then the two results can be investigated more generally by replacing the ellipsoid by any symmetric convex body in R^n. We show here that when $n \geqq 3$ the two finiteness theorems hold only in the case of the ellipsoid. This is equivalent to showing that Minkowski's results do not hold in a general Minkowski space, namely in a euclidean space where the unit ball is a general symmetric convex body instead of the sphere or ellipsoid.

We denote points and vectors in R^n as $\boldsymbol{a}$, $\boldsymbol{b}_1$, etcetera, and in particular $\mathbf{0}$ is the origin, and $\boldsymbol{u}$ denotes a unit vector always. *An n-dimensional convex body* K is a closed, bounded, and convex subset of a euclidean space, which contains exactly n linearly independent points. In this case, K *is symmetric* means K is a symmetric set about $\mathbf{0}$; gK, for a real number g, is the set $\{g\ \mathrm{x} \mid \boldsymbol{x} \in K\}$, and other concepts associated with K such as *support plane*, *width*, *thickness*, *boundary*, and *interior*, are as defined in [2] for example, except that "supporting" is used there instead of "support". The *distance function* F of a convex body K is defined by $K = \{\boldsymbol{x} \mid F(\boldsymbol{x}) \leqq 1\}$, see [5] or [3], and has the following properties:

interior of $K = \{\boldsymbol{x} \mid \boldsymbol{x}(F) < 1\}$;
boundary of $K = \{\boldsymbol{x} \mid F(\boldsymbol{x}) = 1\}$;
$gK = \{\boldsymbol{x} \mid F(\boldsymbol{x}) \leqq g\}$; $F(t,\boldsymbol{x}) = tF(\boldsymbol{x})$ if $t > 0$ (*homogeneity*);
$F(\boldsymbol{x} + \mathrm{y}) \leqq F(\boldsymbol{x}) + F(\mathrm{y})$ (*convexity*);
K is *symmetric* if and only if $F(\boldsymbol{x}) = F(-\boldsymbol{x})$ for all $\boldsymbol{x}$;
$F(\boldsymbol{x}) = 0$ if and only if $\boldsymbol{x} = \mathbf{0}$ (*boundedness*).

A support plane or support line of K is *regular* if it intersects K in a single point.

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

2. The Finiteness Theorems

A *lattice* L in R^n is a set $\{\sum_{i=1}^{n} \chi_i \boldsymbol{a}_i \mid \chi_i$ is an integer$\}$ with *basis* $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_n\}$ where $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_n$ are linearly independent. The basis $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\}$ of L is called a *K-reduced basis of* L, for an n-dimensional convex body K, if for each j with $1 \leqq j \leqq n$ we have for integers p_i

$$F(\boldsymbol{a}_j) \leqq F(p_1 \boldsymbol{a}_1 + \cdots + p_n \boldsymbol{a}_n)$$

whenever g.c.d. $(p_j, \cdots, p_n) = 1$ (see [7], p. 267, or [5]).

It can easily be shown that when K is an ellipsoid, a K-reducd basis of L corresponds to a reduced positive definite quadratic form in n variables (reduced in the Minkowski sense), and two k-reduced bases of the same lattic correspond to two equivalent quadratic forms.

Minkowski's finiteness theorems may now be stated as in (I) and (II) (see [6] and [7] for more details).

(I). *Let K be a symmetric n-dimensional ellipsoid in R^n with distance function F. There is a finite set P of n-tuples of integers, so that if $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ are linearly independent points satisfying for $j = 1, \cdots, n$,*

$$F(\boldsymbol{a}_j) \leqq F(p_1 \boldsymbol{a}_1 + \cdots + p_n \boldsymbol{a}_n)$$

whenever $\boldsymbol{p} \in P$ and g.c.d. $(p_j, \cdots, p_n) = 1$, then $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\}$ is a K-reduced basis.

In other words, if the coefficients of a positive definite quadratic form satisfy a certain finite set of linear inequalities then that quadratic form is reduced in the Minkowski sense.

(II). *Let K be an n-dimensional ellipsoid in R^n. Considering all K-reduced bases of all n-dimensional lattices in R^n, there are only finitely many different integral unimodular transformations which transform a K-reduced basis again into a K-reduced basis.*

In other words, there are only finitely many integral unimodular transformations which can transform a given reduced positive definite quadratic form into an equivalent such form.

One naturally wonders whether the above results on ellipsoids can be generalized to arbitrary convex bodies. For $n = 2$, this question was investigated by Minkowski, who proved the first and probably also the second of the following two results. (See [8], p. 193.)

(III). *Let K be a symmetric two-dimensional convex body in R^2 with distance function F. If $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ are linearly independent, then $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ is a K-reduced basis if and only if*

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

$$F(\boldsymbol{a}_1 + \boldsymbol{a}_2) \geqq F(\boldsymbol{a}_2),$$

$$F(\boldsymbol{a}_1 - \boldsymbol{a}_2) \geqq F(\boldsymbol{a}_2),$$

and

$$F(\boldsymbol{a}_2) \qquad \geqq F(\boldsymbol{a}_1).$$

(IV). *Let K be a symmetric two-dimensional convex body in R^2 with distance function F. There are finitely many integral unimodular transformations which transform a K-reduced basis again into a K-reduced basis if, and only if, every support line of K is regular.*

However, for $n \geqq 3$ the situation is quite different. Most of the present paper is devoted to the proofs of the theorems (V) and (VI) below, which show that for $n \geqq 3$ the converses of (I) and (II) hold.

(V). *For $n \geqq 3$ let K be an n-dimensional, symmetric convex body which has the distance function F. Suppose there is a finite set P of n-tuples of integers satisfying: if $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ are linearly independent points satisfying, for $j = 1, \cdots, n$,*

$$\text{(A)} \qquad F(\boldsymbol{a}_j) \leqq F(p_1 \boldsymbol{a}_1 + \cdots + p_n \boldsymbol{a}_n)$$

whenever $\boldsymbol{p} \in P$ and g.c.d. $(p_j, \cdots, p_n) = 1$, then $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\}$ is a K-reduced basis. Then K is an ellipsoid.

(VI). *For $n \geqq 3$ let K be an n-dimensional, symmetric convex body in R^n. If all K-reduced bases of all n-dimensional lattices in R^n are considered, then suppose there be only finitely many integral unimodular transformations which transform a K-reduced basis again into a K-reduced basis. Then K is an ellipsoid.*

In §3 I give a characterization of the ellipsoid which is needed for the proofs of theorems (IV), (V), (VI). As I have been unable to find proofs of theorem (IV) in the literature, I give a proof of it in §4. In the remainder of the paper I prove (V) and (VI).

3. A characterisation of the ellipsoid

We require some properties of the ellipsoid for the proofs to follow. We define the *width of a convex body K in the direction $\boldsymbol{u}$* to be the distance between the two support planes of K perpendicular to $\boldsymbol{u}$. Two n-dimensional convex bodies K_1 and K_2 in R^n are called *equivalent* if the ratio of the width of K_1 in the direction $\boldsymbol{u}$ to that of K_2 is constant as $\boldsymbol{u}$ varies in R^n. We need the following two results, both of which are proved in [1]. (Result (VII) is Theorem 1 of [1], and (VIII) is contained in Lemma 1 of [1].)

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

(VII) *Let K be a 3-dimensional symmetric convex body in R^3 with all its support planes regular. Suppose there exists a constant h such that $0 < h < 1$, and h has the following property. The 2-dimensional convex bodies $W_1 \cap K$ and $W_2 \cap K$ are equivalent for all pairs of parallel planes W_1 and W_2 which both intersect the interior of K but not the interior of hK. Then K is an ellipsoid.*

(VIII). *Let K_1 and K_2 be 2-dimensional convex bodies lying in parallel planes. Suppose that whenever there is a vector $\boldsymbol{u}$ parallel to the plane of K_1 and K_2 such that all four support lines parallel to $\boldsymbol{u}$ of K_1 and K_2 are regular, then the following property holds. The chord joining the (unique) points of intersection with K_1 of the two support lines of K_1 parallel to $\boldsymbol{u}$, is parallel to the corresponding chord of K_2. Then K_1 is equivalent to K_2.*

Finally we need the result of (IX) to deal with the difficult cases in (V) and (VI) when there are non-regular support planes.

(IX). *Let K be a 3-dimensional symmetric convex body in R^3 such that no support plane of K intersects K in just a segment. Suppose that for each regular support plane T of K there is a constant $h = h(T)$ (depending on T) such that $0 < h < 1$ and h has the following property. If W_0 is the plane through $\mathbf{0}$ parallel to T then $W_0 \cap K$ and $W \cap K$ are equivalent for every plane W which is parallel to T and intersects the interior of K but not that of hK. Then all support planes of K are regular.*

PROOF OF (IX). By hypothesis a support plane of K can intersect K in a single point or a plane face but not a segment. Let D and D' be the intersections of two parallel support planes, T and T', with K, and assume that D (and so by symmetry D') is a plane face. The aim of the proof is to show that for any vector $\boldsymbol{a}$ parallel to the plane of D, there is a plane face of K parallel to $\boldsymbol{a}$ and different from D and D'. This property is then shown to result in a contradiction.

Let $\boldsymbol{a}$ be any vector parallel to the plane of D. Let U be one of the symmetric pair of support planes of K which are parallel to the plane containing L_1 and L_2, where L_1 and L_2 are support lines of D and D' parallel to $\boldsymbol{a}$ and not symmetric about $\mathbf{0}$. There are two cases: (i) U intersects both D and D'; (ii) U does not intersect D or D'. (U cannot intersect just one of D and D', because the intersection of D say and U would lie in L_1, in which case U would also contain L_2 which intersects D'.)

In case (i), $U \cap K$ must contain a segment on the boundary of K (joining a point of D and a point of D'), and so by the hypothesis it must contain a plane face of K parallel to $\boldsymbol{a}$ and different from D and D'.

In case (ii), the plane U_0 parallel to U, through $\mathbf{0}$, clearly intersects the relative interiors of D and D'. We can choose a plane U_1 parallel to U and suf-

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

ficiently close to U such that U_1 does not intersect D or D' or the interior of hK (h is the constant $h(U)$ of the hypothesis). Then by hypothesis $U_1 \cap K$ and $U_0 \cap K$ are equivalent. The boundary of $U_0 \cap K$ contains a straight segment parallel to $\boldsymbol{a}$ in its intersection with D, and a property of equivalence (see [1], Lemma 2) shows that the boundary of $U_1 \cap K$ also contains a segment parallel to $\boldsymbol{a}$. Hence there must be a plane face of K parallel to $\boldsymbol{a}$ and distinct from D and D' which contains this segment.

In both (i) and (ii) we conclude that there is a plane face of K parallel to $\boldsymbol{a}$ and distinct from D and D'. However, there are uncountably many such plane faces corresponding to the mutually non-parallel vectors $\boldsymbol{a}$ which are parallel to the plane T. Any two such plane faces must be distinct since the only plane faces of K parallel to two such vectors are D and D'. Yet a convex body cannot have uncountably many plane faces. This contradicts the assumption that D was a plane face of K. Hence all support planes of K are regular.

4. Proof of Theorem IV

First let every support line of K be regular and $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ be any K-reduced basis of a lattice L, so that $F(\boldsymbol{a}_2) \geqq F(\boldsymbol{a}_1)$ by the definition of K-reduced basis. If $\{\boldsymbol{b}_1, \boldsymbol{b}_2\}$ is any other basis of L, then each of $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ has the form $p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2$ where p_1 and p_2 are integers satisfying g.c.d. $(p_1, p_2) = 1$. If $\{\boldsymbol{b}_1, \boldsymbol{b}_2\}$ is also K-reduced, then $F(\boldsymbol{b}_1) = F(\boldsymbol{a}_1)$, and $F(\boldsymbol{b}_2) = F(\boldsymbol{a}_2)$ (a proof of this is contained in [7]; see in particular pp. 278–286). In the first part of the proof we use the above facts to show that $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ must be one of a finite set of linear combinations of $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$, thus showing that there are only finitely many integral unimodular transformations from a K-reduced basis of L to another K-reduced basis of L (regardless of the choice of L.) .

Using the convexity, homogeneity and symmetry of F, together with the reduction conditions in (III) we obtain when $p_1 > 0$ and $p_2 > 0$:

$$(1) \qquad \text{for } p_1 > p_2,\; F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) \geqq p_1F(\pm \boldsymbol{a}_1 + \boldsymbol{a}_2) - (p_1 - p_2)F(\boldsymbol{a}_2) \geqq p_2F(\boldsymbol{a}_2);$$

$$(2) \qquad \text{for } p_1 = p_2,\; F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) = p_1F(\pm \boldsymbol{a}_1 + \boldsymbol{a}_2);$$

$$(3) \qquad \text{for } p_1 < p_2,\; F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) \geqq p_2F(\pm \boldsymbol{a}_1 + \boldsymbol{a}_2) - (p_2 - p_1)F(\boldsymbol{a}_1) \geqq p_1F(\boldsymbol{a}\ ).$$

In addition, for $p_1 < p_2$ we find using the convexity, homogeneity and symmetry of F, together with the reduction conditions, that

$$(4) \qquad F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) \geqq p_2F(\boldsymbol{a}_2) - p_1F(\boldsymbol{a}_1) \geqq (p_2 - p_1)F(\boldsymbol{a}_2).$$

From (1), it follows that $F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) > F(\boldsymbol{a}_2)$ unless both $p_2 = 1$ and

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

$F(\pm \boldsymbol{a}_1 + \boldsymbol{a}_2) = F(\boldsymbol{a}_2)$. From (2), we find that $F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) > F(\boldsymbol{a}_2)$ unless $p_1 = p_2 = 1$. From (4), $F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) > F(\boldsymbol{a}_2)$ unless both $p_2 = p_1 + 1$ and $F(\boldsymbol{a}_1) = F(\boldsymbol{a}_2)$, and, from (3), $F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) > F(\boldsymbol{a}_1)$ unless $p_1 = 1$; hence in this case if $F(\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2) \leqq F(\boldsymbol{a}_2)$ we must have $p_1 = 1$, $p_2 = 2$.

If $\pm p_1\boldsymbol{a}_1 + p_2\boldsymbol{a}_2$ is to be part of a k-reduced basis, we need only consider cases where $p_1 > 0$ and $p_2 > 0$, because of the symmetry of F and the fact that $p_1 = 0$, or $p_2 = 0$ can only yield $\pm \boldsymbol{a}_2$ or $\pm \boldsymbol{a}_1$. It follows from these results and the facts mentioned at the beginning of the proof that the only possible candidates for a K-reduced basis of L are

$$\pm \boldsymbol{a}_1 \pm \boldsymbol{a}_2, \ \pm \boldsymbol{a}_1 \pm 2\boldsymbol{a}_2, \ \pm \boldsymbol{a}_1, \ \pm \boldsymbol{a}_2 \quad \text{and}$$

$$\pm p_1\boldsymbol{a}_1 \pm \boldsymbol{a}_2, \text{ where } p_1 \geqq 2.$$

In the last case we also found that $F(\boldsymbol{a}_2) = F(\pm \boldsymbol{a}_1 + \boldsymbol{a}_2)$, and since we also have $F(\boldsymbol{a}_2) = F(\pm p_1\boldsymbol{a}_1 \pm \boldsymbol{a}_2)$ (for appropriate choice of signs), there are three linearly dependent points on the boundary of K. This means that K has a non-regular support line, so this last case must be excluded. We are now left with only a finite number of possibilities for points of other K-reduced bases, namely

$$\pm \boldsymbol{a}_1 \pm \boldsymbol{a}_2, \ \pm \boldsymbol{a}_1 \pm 2\boldsymbol{a}_2, \ \pm \boldsymbol{a}_1, \ \pm \boldsymbol{a}_2.$$

There can only be finitely many transformations between bases composed from these points, regardless of the choice of $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$. This completes the first part of the proof.

Now let us assume that K has a non-regular support line so there is a segment S joining $\boldsymbol{a}$ and $\boldsymbol{b}$ on the boundary of K. Choose a sequence of lattices L_m with respective bases $\{\boldsymbol{a}_1^m, \boldsymbol{a}_2^m\}$ as follows:

$$\boldsymbol{a}_1^m = \frac{1}{m}(\boldsymbol{b} - \boldsymbol{a}), \ \boldsymbol{a}_2^m = \boldsymbol{a}.$$

We now show using the result (III) that $\{\boldsymbol{a}_1^m, \boldsymbol{a}_2^m\}$ is a K-reduced basis for all m sufficiently large. We have first of all

$$F(\boldsymbol{a}) \geqq \frac{1}{m}F(\boldsymbol{b} - \boldsymbol{a})$$

for all m sufficiently large, say $m \geqq m_0$. Hence by the homogeneity of F, we have when $m \geqq m_0$

$$F(\boldsymbol{a}_2^m) \geqq F(\boldsymbol{a}_1^m).$$

Secondly by the convexity, homogeneity and symmetry of F, we have

$$F(\boldsymbol{a}_1^m - \boldsymbol{a}_2^m) = F\left(\left(\frac{m+1}{m}\right)\boldsymbol{a} - \frac{1}{m}\boldsymbol{b}\right)$$

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

$$\geqq \left(\frac{m+1}{m}\right) F(\boldsymbol{a}) - \frac{1}{m} F(\boldsymbol{b}).$$

Since $F(\boldsymbol{a}) = F(\boldsymbol{b}) = F(\boldsymbol{a}_2^m) = 1$, we therefore find for all m,

$$F(\boldsymbol{a}_1^m - \boldsymbol{a}_2^m) \geqq F(\boldsymbol{a}_2^m).$$

Finally, since S lies on the boundary of K and $\boldsymbol{a}_1^m + \boldsymbol{a}_2^m \in S$, we have

$$F(\boldsymbol{a}_1^m + \boldsymbol{a}_2^m) = 1 = F(\boldsymbol{a}_2^m).$$

Hence, the three conditions of (III) are satisfied and $\{\boldsymbol{a}_1^m, \boldsymbol{a}_2^m\}$ is a K-reduced basis of L_m when $m \geqq m_0$.

Similarly, $\{\boldsymbol{a}_1^m, \boldsymbol{b}\}$ is a K-reduced basis of L_m when $m \geqq m_0$. The transformation from the basis $\{\boldsymbol{a}_1^m\ \boldsymbol{a}_2^m\}$ to the basis $\{\boldsymbol{a}_1^m, \boldsymbol{b}\}$ has the matrix

$$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}.$$

Infinitely many of these transformations are different for $m \geqq m_0$. Hence, when the boundary of K contains a segment, there are infinitely many integral unimodular transformations which transform a K-reduced basis into a K-reduced basis of the same lattice.

5. Proof of Theorem V for $n = 3$; regular support planes

The method of proof in this case is to construct a sequence of lattice bases related to K. We show that unless K satisfies conditions which characterize it as an ellipsoid, some of the lattice bases satisfy all of the finite set of inequalities of the hypothesis, yet are not K-reduced.

Let $\boldsymbol{u}$ be such that the support plane U with outer normal $\boldsymbol{u}$ is regular, let U_0 be the plane parallel to U containing $\mathbf{0}$, and let $D_0 = U_0 \cap K$. We now define a real-valued function j such that if U' is the support plane perpendicular to $\boldsymbol{u}$ of the convex body $(j(\boldsymbol{u})K)$, then U' is "considerably smaller" than D_0. Let $h > 0$, be such that: if $U' \cap K$ is the support plane of hK with outer normal $\boldsymbol{u}$ then the diameter of $U' \cap K$ is equal to $1/4$ of the thickness of D_0. This condition can be satisfied since the diameter of $U' \cap K$ must approach zero continuously as $h \to 1$. This follows because first of all U' is a continuous function of h in terms of the usual metric on convex bodies (see [2], p. 133) (this continuity property can be proved using the boundedness of K and the continuity of F), and secondly because the diameter, as can easily be shown, is a continuous function of U'. Now define

$$j(\boldsymbol{u}) = \max(h, \tfrac{2}{3}), \text{ so } j(\boldsymbol{u}) < 1.$$

Because of the convexity and symmetry of K, the diameter of U' (as defined above) decreases monotonically as h increases. Hence if U_1 is any plane parallel to U, not intersecting the interior of $j(\boldsymbol{u})K$, then the diameter of $(U_1 \cap K)$ is less than or equal to $\frac{1}{4}$ of the thickness of D_0.

Let U_1 be any plane parallel to U not intersecting the interior of $j(\boldsymbol{u})K$ and let $D_1 = U_1 \cap K$. Let V_1 and V_2 be two distinct parallel support lines of D_0 (in U_0) at the points $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$. Let W_1 and W_2 be distinct support lines of D_1 (in U_1) at $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$, which are both parallel to V_1 and V_2 and similarly situated with respect to D_1 and D_0. (See Diagram 1.)

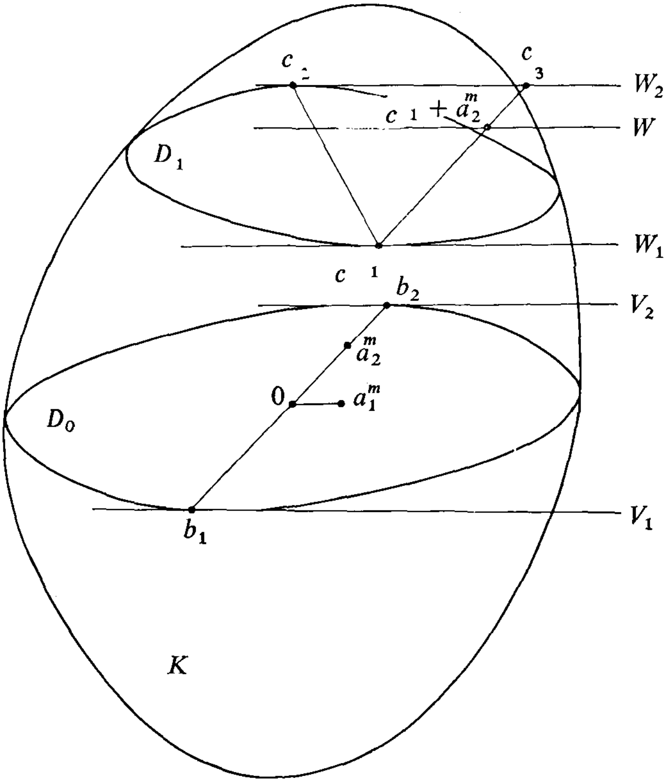

Diagram 1

If the vector $\boldsymbol{b}_1 - \boldsymbol{b}_2$ is parallel to the vector $\boldsymbol{c}_1 - \boldsymbol{c}_2$ for every choice of V_1, V_2, W_1 and W_2 when all four are regular support lines, then D_0 and D_1 are equivalent by (VIII). It is this result we will eventually obtain.

Assume that for some choice of V_1, V_2, W_1 and W_2, all regular, the vector $\boldsymbol{b}_1 - \boldsymbol{b}_2$ is not parallel to $\boldsymbol{c}_1 - \boldsymbol{c}_2$. We now choose a sequence of lattices L_m with respective bases $\{\boldsymbol{a}_1^m, \boldsymbol{a}_2^m, \boldsymbol{a}_3^m\}$. Notice that $\boldsymbol{b}_1 = -\boldsymbol{b}_2$, and any result concerning the plane U_1 also applies to the plane $(-1)U_1$, by the symmetry of K.

Let $\boldsymbol{c}_3$ be the point on W_2 such that the vector $\boldsymbol{c}_1 - \boldsymbol{c}_3$ is parallel to the vector $\boldsymbol{b}_1 - \boldsymbol{b}_2$. By assumption $\boldsymbol{c}_3 \neq \boldsymbol{c}_2$ and by the regularity of W_2, $\boldsymbol{c}_3 \notin K$. We define (independently of m)

$$\boldsymbol{a}_2^m = k(\boldsymbol{c}_3 - \boldsymbol{c}_1)$$

where k is chosen (independently of m) to satisfy:

(i) $\frac{1}{2} < k < 1$; (ii) $\boldsymbol{c}_1 + \boldsymbol{a}_2^m \notin K$. Condition (ii) may be satisfied by choosing k sufficiently close to 1, since $\boldsymbol{c}_3 \notin K$ and $\boldsymbol{c}_1 + \boldsymbol{a}_2^m = k\boldsymbol{c}_3 + \boldsymbol{c}_1(1-k) \to \boldsymbol{c}_3$ a $k \to 1$. Define $\boldsymbol{a}_3^m = \boldsymbol{c}_1$ (again independent of m) and

$$\boldsymbol{a}_1^m = \frac{k}{m}(\boldsymbol{c}_3 - \boldsymbol{c}_2).$$

We will now show that all of the finite number of the inequalities (A) of the hypothesis are satisfied by the linearly independent points $\boldsymbol{a}_1^m$, $\boldsymbol{a}_2^m$ and $\boldsymbol{a}_3^m$ when m is large. First consider $\boldsymbol{a}_1^m$. Every point of L_m, which is not a multiple of $\boldsymbol{a}_1^m$ lies on a line parallel to V_1, though one of the points $p_2\boldsymbol{a}_2^m + p_3\boldsymbol{a}_3^m$ where the integers p_3 and p_2 are not both zero. Since $\boldsymbol{a}_3^m$ and $\boldsymbol{a}_2^m$ are defined independently of m, these lines have a minimum distance from $\boldsymbol{0}$ independent of m. Hence for some $q > 0$

$$F\left(\sum_{i=1}^{3} p_i\boldsymbol{a}_i^m\right) > q,$$

whenever p_2 and p_3 are not both zero. On the other hand,

$$F(\boldsymbol{a}_1^m) = \frac{k}{m}F(\boldsymbol{c}_3 - \boldsymbol{c}_2) \to 0 \text{ as } m \to \infty.$$

Hence, there is an m_0 so that the inequalities (A) hold for $\boldsymbol{a}_1^m$, when $m \geqq m_0$, namely:

$$F(\boldsymbol{a}_1^m) \leqq F(p_1\boldsymbol{a}_1^m + p_2\boldsymbol{a}_2^m + p_3\boldsymbol{a}_3^m)$$

for all integers p_1, p_2, p_3, whenever $m \geqq m_0$.

Consider now the inequalities (A) for $\boldsymbol{a}_2^m$. We have

$$|\boldsymbol{a}_2^m| = |k(\boldsymbol{c}_3 - \boldsymbol{c}_1)| < |\boldsymbol{c}_3 - \boldsymbol{c}_1|, \text{ since } k < 1.$$

By our assumption on the widths of D_0 and D_1,

$$|\boldsymbol{c}_3 - \boldsymbol{c}_1| \leqq \tfrac{1}{4}|\boldsymbol{b}_2 - \boldsymbol{b}_1| = \tfrac{1}{2}|\boldsymbol{b}_2|.$$

Hence $F(\boldsymbol{a}_2^m) \leqq \frac{1}{2}F(\boldsymbol{b}_2)$, and since $F(\boldsymbol{b}_2) = 1$,

$$F(\boldsymbol{a}_2^m) \leqq \tfrac{1}{2}.$$

It follows that we need only investigate points $\sum_{i=1}^{3} p_i\boldsymbol{a}_i^m$ in $\frac{1}{2}K$. However U_1 does not intersect the interior of $j(\boldsymbol{u})K$ where $j(\boldsymbol{u}) \geqq \frac{2}{3}$, so $F(\boldsymbol{a}) > \frac{1}{2} \geqq F(\boldsymbol{a}_2^m)$

when $\boldsymbol{a} \in D_1$. Hence we can restrict our attention to D_0. We consider points $(p_1\boldsymbol{a}_1^m + \boldsymbol{a}_2^m)$, since $p_3 = 0$ in U_0, and the inequalities (A) only apply to $\boldsymbol{a}_2^m$ when g.c.d. $(p_2, p_3) = 1$. We know, by the choice of $\boldsymbol{c}_3$, that for some $q > 0$

$$\boldsymbol{b}_2 = qk(\boldsymbol{c}_3 - \boldsymbol{c}_1) = q\boldsymbol{a}_2^m \in V_2$$

By similarity, $q(p_1\boldsymbol{a}_1^m + \boldsymbol{a}_2^m) \in V_2$. Since $F(\boldsymbol{a}) \geqq 1$ when $\boldsymbol{a} \in V_2$,

$$F(q(p_1\boldsymbol{a}_1^m + \boldsymbol{a}_2^m)) \geqq 1$$

and so

$$F(p_1\boldsymbol{a}_1^m + \boldsymbol{a}_2^m) \geqq \frac{1}{q} = F(\boldsymbol{a}_2^m).$$

We have shown that the inequalities (A) hold for $\boldsymbol{a}_2^m$ and for all m, namely: whenever g.c.d. $(p_2, p_3) = 1$,

$$F(\boldsymbol{a}_2^m) \leqq F(p_1\boldsymbol{a}_1^m + p_2\boldsymbol{a}_2^m + p_3\boldsymbol{a}_3^m).$$

We now consider the inequalities (A) for $\boldsymbol{a}_3^m$. In this case the conditions $p_3 = 1$, together with $F(\boldsymbol{a}_3^m) = 1$, restricts our attention to the interior of D_1. Let W be the line through $\boldsymbol{a}_2^m + \boldsymbol{a}_3^m$ parallel to W_1. All points of $L_m \cap U_1$ lie on lines parallel to W_1 through the points

$$\boldsymbol{a}_3^m + p_2\boldsymbol{a}_2^m = \boldsymbol{c}_1 + p_2k(\boldsymbol{c}_3 - \boldsymbol{c}_1).$$

When $p_2 = 0$, this line is W_1 through $\boldsymbol{c}_1$; when $p_2 = 1$, it is W through $\boldsymbol{a}_2^m + \boldsymbol{a}_3^m$; and when $p_2 = 1/k$ (not an integer), it is W_2 through $\boldsymbol{c}_3$. Since W_1 and W_2 are support lines of D_1 and by the construction of k, $(1/k) < 2$, the only such line which intersects the interior of D_1 is W. Therefore we need consider only points of $(W \cap K)$. Since $\boldsymbol{a}_2^m + \boldsymbol{a}_3^m \notin K$, let $\boldsymbol{c}_4$ be the nearest point of $(W \cap K)$ to $\boldsymbol{a}_2^m + \boldsymbol{a}_3^m$. The distance between successive lattice points on W is $|\boldsymbol{a}_1^m|$, so the number of lattice points between $\boldsymbol{a}_2^m + \boldsymbol{a}_3^m$ and $\boldsymbol{c}_4$ is at least $\dfrac{|\boldsymbol{a}_2^m + \boldsymbol{a}_3^m - \boldsymbol{c}_4|}{|\boldsymbol{a}_1^m|} = \dfrac{m|\boldsymbol{a}_2^m + \boldsymbol{a}_3^m - \boldsymbol{c}_4|}{k|\boldsymbol{c}_3 - \boldsymbol{c}_2|} = mt$ say. t is independent of m since $\boldsymbol{a}_2^m$ and $\boldsymbol{a}_3^m$ are independent of m, and also $t > 0$. Hence, all lattice points of L_m in $W \cap D_1$ must be of the form

$$p_1\boldsymbol{a}_1^m + \boldsymbol{a}_2^m + \boldsymbol{a}_3^m, \text{ where } |p_1| \geqq mt.$$

We have shown therefore that

$$F(\boldsymbol{a}_3^m) \leqq F(p_1\boldsymbol{a}_1^m + p_2\boldsymbol{a}_2^m + \boldsymbol{a}_3^m)$$

for all integers p_1 and p_2, except when $p_2 = 1$ and $|p_1| \geqq mt$.

Collecting all the results we have shown that for each m with $m \geqq m_0$ and for $j = 1, 2, 3$,

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

$$F(\boldsymbol{a}_j) \leqq F(p_1\boldsymbol{a}_1^m + p_2\boldsymbol{a}_2^m + p_3\boldsymbol{a}_3^m)$$

whenever g.c.d. $(p_j, \cdots, p_n) = 1$, except when $p_2 = p_3 = 1$ and $|p_1| \geqq mt$. By choosing m large enough, say $m \geqq m_1 \geqq m_0$, we can ensure that none of the $\boldsymbol{p}$, for which the above inequalities fail, lie in the finite set P of the hypothesis. Hence for $m \geqq m_1$, the basis $\{\boldsymbol{a}_1^m, \boldsymbol{a}_2^m, \boldsymbol{a}_3^m\}$ satisfies all of the finite set of the inequalities (A). However $\{\boldsymbol{a}_1^m, \boldsymbol{a}_2^m, \boldsymbol{a}_3^m\}$ is not K-reduced for $m \geqq m_1$, since the point

$$-m\boldsymbol{a}_1^m + \boldsymbol{a}_2^m + \boldsymbol{a}_3^m = \boldsymbol{c}_1 + k(\boldsymbol{c}_2 - \boldsymbol{c}_1) \text{ for } \tfrac{1}{2} < k < 1$$

lies in the interior of K so that

$$F(\boldsymbol{a}_3^m) > F(-m\boldsymbol{a}_1^m + \boldsymbol{a}_2^m + \boldsymbol{a}_3^m).$$

This violates the reduction conditions. Hence we have a contradiction, and so the initial assumption that the vector $\boldsymbol{b}_1 - \boldsymbol{b}_2$, is not parallel to $\boldsymbol{c}_1 - \boldsymbol{c}_2$ must be false. As previously indicated, this leads us to the conclusion that D_0 is equivalent to D_1. We have shown, for each initial choice of the regular support plane U, that D_0 and D_1 are equivalent whenever U_1 does not intersect the interior of $j(\boldsymbol{u})K$.

If all support planes of K are regular, then $j(\boldsymbol{u})$ is defined for all $\boldsymbol{u}$, and $j(\boldsymbol{u}) < 1$. The supremum, h say, of $j(\boldsymbol{u})$ on the closed set of unit vectors satisfies $h < 1$. For otherwise, there would be a subsequence $\{\boldsymbol{u}_i\}$ of unit vectors so that $j(\boldsymbol{u}_i) \to 1$ as $i \to \infty$ and $j(\boldsymbol{u}_i) > \frac{2}{3}$ for all i. If U_i is the support plane of $j(\boldsymbol{u}_i)K$ and $D_i = U_i \cap K$, then the sequence $\{D_i\}$ has a convergent subsequence, according to the Blaschke Selection Theorem (see [2], p. 134), with a plane limit set D, and then the plane W of D must be a support plane of K. Yet each of the D_i must have a diameter no less than $\frac{1}{4}$ of the minimum thickness of any section of K through $\boldsymbol{0}$. Hence D must have a positive diameter, which is impossible, because W is regular. Hence $j(\boldsymbol{u})$ is bounded above by some constant h with $h < 1$, and this h satisfies the hypothesis of (VII), and so K is an ellipsoid.

This completes the theorem for $n = 3$, when all support planes of K are regular.

6. Completion of proof of Theorem V for $n = 3$

We have to show that every support plane of K is regular, in which case the theorem follows as in §5. We proved in §5 (even when some support planes of K are non-regular) that if $\boldsymbol{u}$ is the outer normal of a regular support plane of K and W_1, W_0 are planes perpendicular to $\boldsymbol{u}$ so that W_0 contains $\boldsymbol{0}$ and W_1 intersects the interior of K but not the interior of $j(\boldsymbol{u})K$, then $(W_0 \cap K)$ and $(W_1 \cap K)$ are equivalent. Hence we can apply Theorem (IX) to K to show that all of its support planes are regular, provided no support plane intersects K in just a segment.

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

Assume that a support plane T with outer normal $\boldsymbol{u}$ intersects K in just a segment S joining $\boldsymbol{d}_1$ and $\boldsymbol{d}_2$ ($\boldsymbol{d}_1 \neq \boldsymbol{d}_2$). Let U_i, $i = 2, 3, \cdots$ be planes parallel to T at a perpendicular distance of $1/i$ from T. We next define points and lines related to each U_i in the same way as we defined points and lines related to U_1 at the beginning of this proof. Let U_0 be the plane parallel to T with $\mathbf{0} \in U_0$, $D_0 = U_0 \cap K$, and, V_1 and V_2 be parallel support lines of D_0 (in U_0). For each i, let $D_i = U_i \cap K$, and let W_{1i} and W_{2i} be support lines of D_i parallel to V_1 and V_2 and respectively, similarly situated about D_i. Let d and d_i be the respective perpendicular distances between, V_1 and V_2, and W_{1i} and W_{2i}. If V_1 is parallel to the vector $\boldsymbol{d}_1 - \boldsymbol{d}_2$ then clearly $d_i \to 0$ as $i \to \infty$. Hence if we choose V_1 sufficiently close in direction to $\boldsymbol{d}_1 - \boldsymbol{d}_2$ yet not parallel to it, then we can find an i_0 so that $d_i \leqq \frac{1}{4}d$ if $i > i_o$. We now take this to be the case and further assume that W_{1i}, W_{2i}, V_1 and V_2 are all regular, which we can do since at most countably many support lines of D_i are not regular. Let $\{\boldsymbol{c}_{1i}\} = W_{1i} \cap D_i$, $\{\boldsymbol{c}_{2i}\} = W_{2i} \cap D_i$, $\{\boldsymbol{b}_1\} = V_1 \cap D_0$, and $\{\boldsymbol{b}_2\} = V_2 \cap D_0$. Finally in addition to the above conditions, we can clearly assume that $\boldsymbol{b}_1 - \boldsymbol{b}_2$ is not parallel to $\boldsymbol{d}_1 - \boldsymbol{d}_2$. V_1 and V_2 are now fixed. Note that $U_i \cap \operatorname{Int}(\frac{2}{3}K)$ is empty when i is sufficiently large, say $i > i_1 \geqq i_0$. In this case D_i, with $i > i_1$, now satisfies conditions by which we can show (with $j(\boldsymbol{u}) = \frac{2}{3}$) that $\boldsymbol{c}_{1i} - \boldsymbol{c}_{2i}$ is parallel to $\boldsymbol{b}_1 - \boldsymbol{b}_2$ in exactly the same way as we previously showed that the vector $\boldsymbol{c}_1 - \boldsymbol{c}_2$ in D_1 (in the previous notation) is parallel to $\boldsymbol{b}_1 - \boldsymbol{b}_2$ in D_0. (Even though $j(\boldsymbol{u})$ here does not satisfy the complete condition satisfied by $j(\boldsymbol{u})$ in the previous proof, the condition $d_i \leqq \frac{1}{4}d$ is sufficient to follow through the proof for the particular choice of V_1 and V_2.)

We now show that the condition that $\boldsymbol{c}_{1i} - \boldsymbol{c}_{2i}$ is parallel to $\boldsymbol{b}_1 - \boldsymbol{b}_2$ leads to a contradiction. The sequence $\{\boldsymbol{c}_{1i}\}$ clearly has a limit point $\boldsymbol{d}$ in the segment S and we show that $\boldsymbol{d} = \boldsymbol{d}_1$ or $\boldsymbol{d}_2$. Project all of the sets in question from $\mathbf{0}$ onto T, and denote the projected sets by an asterisk. Then clearly $D_1^* \supseteq D_2^* \supseteq \cdots \supseteq S$, and $\boldsymbol{c}_{1i}^* \to \boldsymbol{d}$ as $i \to \infty$. Now W_{1i}^* cannot intersect the interior of S since $D_i \supseteq S$ and consequently $\boldsymbol{d} = \boldsymbol{d}_1$ or $\boldsymbol{d}_2$, say $\boldsymbol{d} = \boldsymbol{d}_1$. Similarly $\boldsymbol{c}_{2i} \to \boldsymbol{d}_2$ as $i \to \infty$. Hence the direction of the vector $\boldsymbol{c}_{1i} - \boldsymbol{c}_{2i}$ approaches that of $\boldsymbol{d}_1 - \boldsymbol{d}_2$ as $i \to \infty$, yet $\boldsymbol{c}_{1i} - \boldsymbol{c}_{2i}$ is parallel to $\boldsymbol{b}_1 - \boldsymbol{b}_2$ for $i > i_1$ and $\boldsymbol{b}_1 - \boldsymbol{b}_2$, is not parallel to $\boldsymbol{d}_1 - \boldsymbol{d}_2$. This is a contradiction. Hence $T \cap K$ is not just a segment.

Now we can apply (IX) to show all support planes of K are regular. Hence we can prove K is an ellipsoid as in §5 and the proof of Theorem V is complete for the case $n = 3$.

6. Proof of Theorem V for all n

For $n > 3$ we proceed by induction on n. Assume that the theorem is true for dimension $(n-1)$ and that K is an n-dimensional convex body satisfying the hypothesis. Let U be any hyperplane through $\mathbf{0}$, and let $J = K \cap U$. Clearly U can be identified with R^{n-1} so that J is an $(n-1)-$ dimensional convex body. Let

$$P' = \{(p_1, \cdots, p_{n-1}) \mid (p_1, \cdots, p_{n-1}, 0) \in P\}.$$

We now show that J satisfies the hypothesis of this theorem with P replaced by P'. Let $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_{n-1}$ be linearly independent points in U satisfying for $j = 1, \cdots, n-1$,

$$F(\boldsymbol{a}_j) \leqq F(p_1\boldsymbol{a}_1 + \cdots + p_{n-1}\boldsymbol{a}_{n-1}) \tag{1}$$

whenever $(p_1, \cdots, p_{n-1}) \in P'$ and g.c.d. $(p_j, \cdots, p_{n-1}) = 1$. We must show that *$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_{n-1}$ is a J-reduced basis. Choose a hyperplane V in R^n, parallel to U,* which does not intersect the set $F(\boldsymbol{x}) \leqq F(\boldsymbol{a}_i)$ for $\boldsymbol{x} \in R^n$, and $i = 1, \cdots, n-1$. Define $\boldsymbol{a}_n \in V$ by

$$F(\boldsymbol{a}_n) = \min_{\boldsymbol{a} \in V} F(\boldsymbol{a}).$$

By the construction of V, none of the planes parallel to V, through points $p\boldsymbol{a}_n$, for an integer p, can intersect the sets $F(\boldsymbol{x}) \leqq F(\boldsymbol{a}_i)$, for $i = 1, \cdots, n-1$. Hence, for $j = 1, \cdots, n$,

$$F(\boldsymbol{a}_j) \leqq F(p_1\boldsymbol{a}_1 + \cdots + p_n\boldsymbol{a}_n) \tag{2}$$

for all $(p_1, \cdots, p_n)$ with $p_n \neq 0$. From equations (1) and (2) we find, for $j = 1, \cdots, n$,

$$F(\boldsymbol{a}_j) \leqq F(p_1\boldsymbol{a}_1 + \cdots + p_n\boldsymbol{a}_n)$$

for all $\boldsymbol{p} \in P$, with g.c.d. $(p_j, \cdots, p_n) = 1$. Since K satisfies the hypothesis of this theorem, it follows that $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\}$ is a K-reduced basis. Hence we have, in particular, by the definition of a K-reduced basis, for $j = 1, \cdots, n-1$,

$$F(\boldsymbol{a}_j) \leqq F(p_1\boldsymbol{a}_1 + \cdots + p_{n-1}\boldsymbol{a}_{n-1})$$

whenever g.c.d. $(p_j, \cdots, p_{n-1}) = 1$. This shows that $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_{n-1}\}$ is a J-reduced basis.

We have now shown that J satisfies the hypothesis of this theorem, and so by the induction hypothesis, J is an ellipsoid. This result is true for each choice of the hyperplane U through $\mathbf{0}$, so every section of K through $\mathbf{0}$ is an ellipsoid. It follows from a well-known result, see [4], p. 91, that K is an ellipsoid. Hence the theorem follows for all n by the induction principle.

7. Proof of Theorem VI

The proof of this theorem is very similar to the proof of (V) and many of the details of this proof are referred to the proof of (V). We first consider the case where $n = 3$.

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

Let U be a regular support plane of K and let U_0, $j(\boldsymbol{u})$, U_1 D_0, D_1, W_1, W_2, V_1, V_2, $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, $\boldsymbol{c}_1$, $\boldsymbol{c}_2$ and $\boldsymbol{c}_3$ be defined as in (V) (see Diagram 2). We assume that, as in (V), for some choice of V_1, V_2, W_1 and W_2, all regular, we have $\boldsymbol{c}_2 \neq \boldsymbol{c}_3$. We now define a sequence of lattices L_m with respective bases $\{\boldsymbol{a}_1^m, \boldsymbol{a}_2^m, \boldsymbol{a}_3^m\}$.

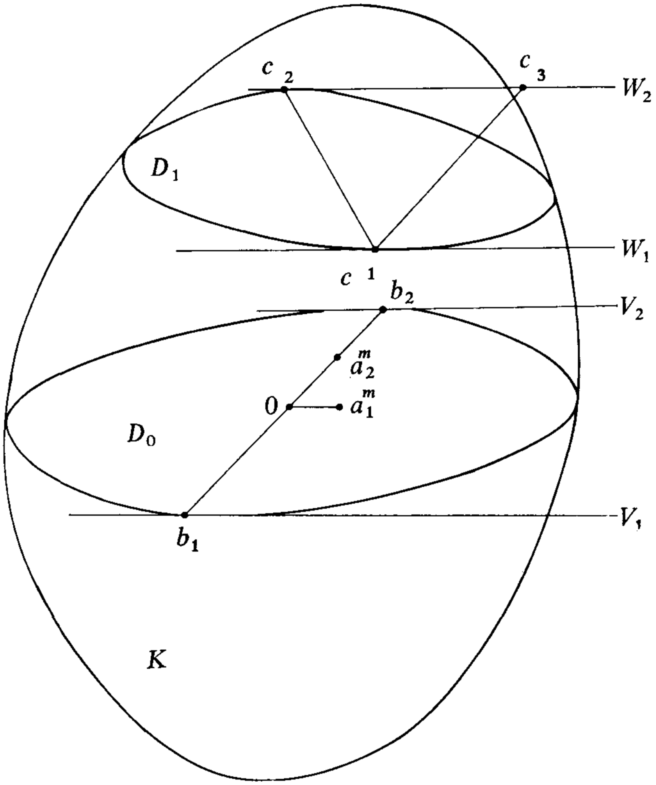

Diagram 2

Define

$$\boldsymbol{a}_1^m = \frac{1}{m}(\boldsymbol{c}_2 - \boldsymbol{c}_3), \quad \boldsymbol{a}_2^m = \boldsymbol{c}_3 - \boldsymbol{c}_1 \text{ and } \boldsymbol{a}_3^m = \boldsymbol{c}_1 .$$

The only difference between the situation here and that of (V) is that the line W defined in (V) has now become W_2. Hence we can show, as in (V). (But without the exceptional points on the line W), that for $m \geqq m_0$ and for $j = 1,2,3$,

$$F(\boldsymbol{a}_j^m) \leqq F(p_1\boldsymbol{a}_1^m + p_2\boldsymbol{a}_2^m + p_3\boldsymbol{a}_3^m)$$

whenever g.c.d. $(p_j, \cdots, p_3) = 1$. Hence $\{\boldsymbol{a}_1^m, \boldsymbol{a}_2^m, \boldsymbol{a}_3^m\}$ is a K-reduced basis of L_m when $m \geqq m_0$. However, $\boldsymbol{c}_2 \in L_m$, since $\boldsymbol{c}_2 = m\boldsymbol{a}_1^m + \boldsymbol{a}_2^m + \boldsymbol{a}_3^m$, and it is easily

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press

shown that $\{a_1^m, a_2^m, c_2\}$ is also a basis of L_m. Yet $F(c_2) = F(a_3^m) = 1$, so $\{a_1^m, a_2^m, c_2\}$ is also a K-reduced basis of L_m, for $m \geqq m_0$. The transformation from the basis $\{a_1^m, a_2^m, a_3^m\}$ to the basis $\{a_1^m, a_2^m, c_2\}$ has the matrix

$$\begin{bmatrix} 1 & 0 & m \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Hence infinitely many of these transformations are different for $m \geqq m_0$. This contradicts the hypothesis, so in fact we must have $c_2 = c_3$. As in (V) we deduce D_0 and D_1 are equivalent, and that K is an ellipsoid provided no support plane intersects K in a segment.

Assume therefore that the support plane U of K intersects K in a segment S from d_1 to d_2. We define U_0, D_0, V_1, V_2, b_1 and b_2 with V_1 and V_2 regular, as in the first part of this proof. We define a sequence of lattices L_m with respective bases $\{a_1^m, a_2^m, a_3^m\}$. Define

$$a_1^m = \frac{1}{m}(d_2 - d_1), \quad a_2^m = b_2, \text{ and } a_3^m = d_1 .$$

It is easy to show, as in the first part of the proof of this theorem, that for some m_0, $\{a_1^m, a_2^m, a_3^m\}$ is a K-reduced basis of L_m for $m \geqq m_0$. Similarly $\{a_1^m, a_2^m, d_2\}$ is a K-reduced basis of L_m for $m \geqq m_0$, and $d_2 = m a_1^m + a_3^m$. The transformation from the basis $\{a_1^m, a_2^m, a_3^m\}$ to the basis $\{a_1^m, a_2^m, d_2\}$ has the matrix

$$\begin{bmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Infinitely many of these transformations are different for $m \geqq m_0$. This contradicts the hypothesis. Hence U cannot intersect K in a segment. As previously noted, this result together with the preceding results leads us to the conclusion that K is an ellipsoid. This completes the discussion of the three-dimensional case.

We now prove the theorem for $n > 3$ by an induction proof. Assume that the theorem holds for dimension $(n - 1)$, and let K be an n-dimensional convex body satisfying the hypothesis of the theorem. Let U be a hyperplane through $\mathbf{0}$ and let $J = U \cap K$. We now show that the $(n-1)$-dimensional convex body J satisfies the hypothesis of this theorem.

Let $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_{n-1}\}$ and $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{n-1}\}$ be any two J-reduced bases of some lattice L. Let the unimodular transformation from the first basis to the second one have coefficients f_{ij}. We choose a hyperplane V in R^n which is parallel to U and does not intersect the sets $F(\boldsymbol{x}) \leqq F(\boldsymbol{a}_{n-1})$ and $F(\boldsymbol{x}) \leqq F(\boldsymbol{b}_{n-1})$ for $\boldsymbol{x} \in R^n$ and define $\boldsymbol{a}_n$ by

$$F(\boldsymbol{a}_n) = \min_{\boldsymbol{a} \in V} F(\boldsymbol{a}).$$

Then, as in the previous proof of (V), $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\}$ and $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{n-1}, \boldsymbol{a}_n\}$ are both K-reduced bases of the same lattice. The transformation from the first basis to the second has the matrix

$$\begin{bmatrix} f_{11} & \cdots & f_{1,n-1} & 0 \\ \vdots & & \vdots & \vdots \\ f_{n-1,1} & \cdots & f_{n,n} & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}$$

However, since K satisfies the hypothesis of this theorem, there can only be finitely many of these transformations which are different. Hence only finitely many of the original transformations with the coefficients f_{ij} are different. Therefore J satisfies the hypothesis of this theorem, and so J must be an ellipsoid by the induction hypothesis. It follows as in (V) that K is an ellipsoid, and so the theorem is proved for all n by the induction principle.

References

[1] P. W. Aitchison 'A Characterisation of the Ellipsoid.' *J. Australian Math. Soc.* 11 (1970), 385–394.

[2] R. V. Benson, *Euclidean Geometry and Convexity* (McGraw-Hill, U.S.A., 1966).

[3] T. Bonnesen, and W. Fenchel *Theorie der konvexen Körper* (Reprint by Chelsea, New York, 1948).

[4] H. Busemann, *Geometry of Geodesics* (Academic Press, New York, 1955).

[5] J. W. S. Cassels, *An Introduction to the Geometry of Numbers* (Springer-Verlag, Berlin, 1959).

[6] H.Weyl, 'On Geometry of Numbers'. *Proc. Lond. Math. Soc.* 47 (1942), 268–289.

[7] B. L. van der Waerden, 'Die Redukionstheorie der positiven quadratischen Formen.' *Acta Math.* 96 (1956), 265–309.

[8] H. Minkowski, *Geometrie der Zahlen* (Reprint by Chelsea, New York, 1953).

Department of Mathematics,
University of Manitoba
Winnipeg
Canada

https://doi.org/10.1017/S1446788700010818 Published online by Cambridge University Press