

STATEMENT

SOME CHARACTERISATIONS OF THE ELLIPSOID
AND THE MINKOWSKI THEORY OF REDUCTION

The results presented in this thesis are my own except
where otherwise stated.

by

P. W. Aitchison

P.W. Aitchison

P.W. Aitchison

A thesis presented to the Australian National
University for the degree of Doctor of
Philosophy in the Department of Mathematics.

Canberra. October, 1968

Revised version

PREFACE

The generous support of an Australian National University research scholarship enabled me to write this thesis.

STATEMENT

My sincere thanks go to Professor Kurt Mahler whose inspiration and guidance helped me very much to form and develop my ideas.

The results presented in this thesis are my own except where otherwise stated.

I am indebted to Professor A.C. Woods and Doctor V. Dlab for reading parts of the thesis and for their suggestions, to Mrs Wickland for her excellent typing, and to my wife for her diligent proofreading.

P. W. Aitchison

P.W. Aitchison.

PREFACE

The generous support of an Australian National University research scholarship enabled me to write this thesis.

My sincere thanks go to Professor Kurt Mahler whose inspiration and guidance helped me very much to form and develop my ideas.

Special thanks are also due to Professor A.C. Woods and Doctor V. Dlab for reading parts of the thesis and for their suggestions, to Mrs Wickland for her excellent typing, and to my wife for her diligent proofreading.

Chapter 1. The Ellipsoid.	1
1. The Flats of a Convex Body.	2
2. The Flats of an Ellipsoid.	3
3. The Characterization of the Ellipsoid.	14
4. Some Previous Characterizations of the Ellipsoid.	14
5. A New Characterization of the Ellipsoid.	15
6. Further Results on Ellipsoids.	30
Chapter 2. The Two Finiteness Theorems of the Reduction Theory.	43
7. Lattices.	43
8. The Theory of Reduction.	46
9. The Two Finiteness Theorems.	51
References	74

CONTENTS

Introduction	v
Notation and Terminology	vii
Addenda	viii
Chapter 1. The Theory of Convex Bodies.	1
1. Convex Body.	1
2. Tac Planes of a Convex Body.	2
3. The Tac Function of a Convex Body.	3
4. Equivalent Convex Bodies.	7
Chapter 2. Characterisations of the Ellipsoid.	14
5. Some Previous Characterisations of the Ellipsoid.	14
6. A New Characterisation of the Ellipsoid.	15
7. Further Results on Ellipsoids.	30
Chapter 3. Two Finiteness Theorems of the Reduction Theory.	45
8. Lattices.	45
9. The Theory of Reduction.	46
10. The Two Finiteness Theorems.	51
References	74

Introduction

The theory of reduction of convex bodies is concerned with certain relations between a fixed symmetric convex body K and a variable lattice L in n -dimensional Euclidean space R^n . The fundamental concept in this theory is the K -reduced basis of the lattice L . For the definition of such a basis see [10]a, p.279.

In the special case when K is a Euclidean sphere (or more generally an ellipsoid) in R^n , the reduction theory becomes equivalent to what is known as the Minkowski reduction theory of n -ary, positive definite, quadratic forms. For, a significant equivalence exists in which each lattice basis corresponds to a certain n -ary, positive definite, quadratic form, and in particular, a K -reduced basis corresponds to a reduced form (reduced in the sense of Minkowski). Many properties of positive definite quadratic forms have been found by the study of reduced forms, and van der Waerden in [11] gives a good account of the present knowledge in this field.

Minkowski proved two important finiteness theorems concerning reduced quadratic forms. A geometric formulation of these theorems is as follows: If K is an ellipsoid in R^n with its centre at the origin, then (i) finitely many of the reduction inequalities determine all K -reduced bases of the lattice L ; and (ii) there are only finitely many,

unimodular transformations from one K -reduced basis to another such basis (possibly the same). Minkowski in [7], p.193, showed that if $n = 2$, then (i) also holds for an arbitrary symmetric convex body K ; it is known that if $n = 2$, then (ii) holds for those symmetric K of which the frontier contains no line segments.

The main results of this thesis, established in Theorems 9 and 10 of Chapter 3, assert that for $n > 2$, the properties (i) and (ii) can hold only when K is an ellipsoid, in contrast to the case $n = 2$. Thus, surprisingly, for $n > 2$ the reduction theory loses its finiteness properties when K is not an ellipsoid.

In Chapter 2 several new characterisations of the ellipsoid are proved, one of which is used to establish the results mentioned above. The principal result of Chapter 2 is: Let K be a convex body in $\mathbb{R}^3$, symmetric or not. If any two parallel planes "sufficiently close" to a tac plane of K intersect K in equivalent convex bodies, then K is an ellipsoid. Here, two convex bodies are called equivalent if for some Minkowski metric both have constant width.

This generalises some previously known results, for example:

(a) K is an ellipsoid if every plane intersects K in a body of constant width; (b) K is an ellipsoid if any two parallel planes intersect K in homothetic convex bodies.

The results (a) and (b) are mentioned in [2], p.142.

Notation and Terminology

In this thesis R^n denotes the n -dimensional Euclidean space of all n -tuples of real numbers. These n -tuples are called points, and $\underline{a}$, $\underline{x}$, $\underline{c}_1$, etc., and in particular $\underline{o}$, are abbreviations for the points $(a_1, a_2, \dots, a_n)$, $(x_1, x_2, \dots, x_n)$, $(c_{11}, c_{12}, \dots, c_{1n})$, etc., and $(o, o, \dots, o)$. The scalar product is written $\underline{a} \cdot \underline{b} = \sum_{i=1}^n a_i b_i$ and the Euclidean metric is written $|\underline{a}| = (\underline{a} \cdot \underline{a})^{1/2}$. The notation $\underline{w}$ will always be used for a point for which $|\underline{w}| = 1$. The integers, positive integers, n -tuples of integers, reals, and positive reals are denoted respectively I , I^+ , I^n , R , R^+ . The usual notations $[r, s]$ and (r, s) are used for closed and open intervals of real numbers. The closed line segment determined by $\underline{a}$ and $\underline{b}$ is denoted $\overline{\underline{a} \underline{b}}$ and its length by $|\underline{a} \underline{b}|$. A p -flat in R^n for $0 \leq p \leq n$ is a p -dimensional subspace of R^n or a translation of one. The 0 -, 1 -, $(n-1)$ - flats are also called points, lines, hyperplanes respectively. Two sets in R^n are called parallel if a translation of one is contained in a dilation of the other. Geometric entities other than points are regarded as sets and are usually denoted by capital letters. The usual set theory notation is used.

CHAPTER 1.

Addenda.The Theory of Convex Bodies.

A number of mistakes were found by the examiners in the original version of this thesis. Consequently pages 12, 16, 17, 21 - 27, 32, 38 - 41, 50, 59, and 65 - 67, have been revised in order to rectify the errors, and pages 42 - 44 are now omitted from the thesis. A number of minor errors on other pages were corrected.

that $\bar{a} \in K$ whenever $a, b \in K$. The *boundary* of K , written $\text{Fr}K$, is the set of all boundary (or frontier points) of the set K . The *interior* of K , written $\text{Int}K$, is the set of points of K which are not in $\text{Fr}K$.

An n -dimensional convex body is transformed into an n -dimensional convex body by an affine transformation of $\mathbb{R}^n$, so in fact a convex body is of a geometric nature. It is clear that an n -dimensional convex body can be embedded in an n -flat in any higher dimensional space so that it is meaningful to talk of n -dimensional convex bodies in $\mathbb{R}^m$ for $m \geq n$.

An n -dimensional convex body is called *symmetric* if $a \in K$ entails $-a \in K$.

Further information on convex bodies may be found in

[2] p. 2 ff..

CHAPTER 1.

The Theory of Convex Bodies.1. Convex Body.

An n -dimensional convex body K in $\mathbb{R}^n$ for $n \geq 2$ is a set of points of $\mathbb{R}^n$ which is closed, bounded, convex, and contains n -linearly independent points. Here convex means that $\overline{ab} \subseteq K$ whenever $a, b \in K$. The frontier of K , written $\text{Fr}K$, is the set of all boundary (or frontier points) of the set K . The interior of K , written $\text{Int}K$, is the set of points of K which are not in $\text{Fr}K$.

An n -dimensional convex body is transformed into an n -dimensional convex body by an affine transformation of $\mathbb{R}^n$, so in fact a convex body is of a geometric nature. It is clear that an n -dimensional convex body can be embedded in an n -flat in any higher dimensional space so that it is meaningful to talk of n -dimensional convex bodies in $\mathbb{R}^m$ for $m \geq n$.

An n -dimensional convex body is called symmetric if $a \in K$ entails $-a \in K$.

Further information on convex bodies may be found in

[2] p.2 ff..

2. Tac Planes of a Convex Body.

Let K be an n -dimensional convex body in R^n . Through each point $\underline{a} \in \text{Fr}K$ there is at least one $(n-1)$ -flat, T say, which does not intersect $\text{Int}K$, and then T is called a tac plane of K at $\underline{a}$ (see also [2], p.6, under the name "Stützebene"). Some authors use the term support plane instead of tac plane.

A tac plane T of K , being an $(n-1)$ -flat, divides R^n into two closed half spaces, each bounded by T , which intersect only in T . It follows that a tac plane may be regarded as an $(n-1)$ -flat T which intersects K but so that K is a subset of one of the closed half spaces bounded by T . If the non-zero vector $\underline{u}$ is perpendicular to T , and is directed away from the closed half space bounded by T which contains K , then $\underline{u}$ is called an outer normal of the tac plane T of K . Whenever we use $\underline{w}$ or $-\underline{w}$ to denote an outer normal we will also assume that $|\underline{w}| = 1$. There are two tac planes of K perpendicular to any $\underline{w} \in R^n$ (see [2] p.4) such that one has outer normal $\underline{w}$ and the other has outer normal $-\underline{w}$. It follows that K is a subset of the closed set bounded by two such tac planes.

A tac plane of K is called regular if it has a single point in common with K .

The notions discussed here are clearly of a geometric nature and are not altered by affine transformations or embedding in a higher dimensional space. Further information on tac planes is given in [2].

3. The Tac Function of a Convex Body.

It is useful to have an analytic expression for convex bodies since many proofs may be simplified by using methods of analysis. One such expression for a convex body is the tac function.

The tac function H of an n -dimensional convex body K in R^n is a function $H : R^n \rightarrow R$ defined by

$$H(\underline{u}) = \sup_{\underline{x} \in K} (\underline{u} \cdot \underline{x}) .$$

The following are properties of the tac function.

- (1) $H(\underline{u}) \neq -H(-\underline{u})$ when $\underline{u} \neq \underline{0}$
- (2) $H(j\underline{u}) = jH(\underline{u})$ for all $j \geq 0$, so that H is positively homogenous.
- (3) $H(\underline{u} + \underline{v}) \leq H(\underline{u}) + H(\underline{v})$ so that H is a convex function.

These three properties are proved in [2], p.24. In

[2], p.24 and 26, it is shown that:

- (4) Any function $H : \mathbb{R}^n \rightarrow \mathbb{R}$ satisfying properties (1), (2) and (3) is the tac function of just one n -dimensional convex body K , defined by $\underline{x} \in K$ if and only if $\underline{x} \cdot \underline{u} \leq H(\underline{u})$ for all $\underline{u} \in \mathbb{R}^n$.
- (5) The tac plane of K which has unit outer normal $\underline{w}$ is given by $\{\underline{x} | \underline{w} \cdot \underline{x} = H(\underline{w})\}$ or more simply by $\underline{w} \cdot \underline{x} = |H(\underline{w})|$ (see [2], p.23). It follows that:
- (a) $H(\underline{w})$ is the distance from $\underline{o}$ to the tac plane of K with outer normal $\underline{w}$.
- (b) $H(\underline{w}) + H(-\underline{w})$ is the distance between the two tac planes of K perpendicular to $\underline{w}$; otherwise known as the width of K in the direction $\underline{w}$.
- (c) If T is the tac plane of K , $\underline{u} \cdot \underline{x} = H(\underline{u})$, then $T \cap K = \{\underline{x} | \underline{u} \cdot \underline{x} = H(\underline{u}) \text{ and } \underline{x} \in K\}$ and this set is non-empty.

A most important and perhaps surprising result is:

- (6) If T is the regular tac plane $\underline{u} \cdot \underline{x} = H(\underline{u})$ and $T \cap K = \{\underline{a}\}$, then the partial derivatives, $\frac{\partial H}{\partial u_i}(\underline{u})$ exist and are continuous, and

$$\frac{\partial H}{\partial u_i}(\underline{u}) = a_i \quad \text{for } i = 1, \dots, n.$$

This result is essentially given in [2], p.24, 26. It is easy to show that this differentiability property of H is unaltered by affine transformations of the space R^n .

Finally the following three results follow without difficulty,

- (7) $H(\underline{u}) > 0$ if $\underline{0} \in \text{Int}K$ and $\underline{u} \neq 0$.
- (8) K is symmetric if, and only if, $H(\underline{u}) = H(-\underline{u})$ for all $\underline{u} \in R^n$.
- (9) Let H_1, H_2 be tac functions of two n -dimensional convex bodies in R^n . Then the function

$h_1 H_1 + h_2 H_2$ where $h_1 \geq 0, h_2 \geq 0$, are real numbers not both zero, defined by

$$(h_1 H_1 + h_2 H_2)(\underline{u}) = h_1 H_1(\underline{u}) + h_2 H_2(\underline{u})$$

is a tac function of an n -dimensional convex body.

Similarly the function H_1^- defined by $H_1^-(\underline{u}) = H_1(-\underline{u})$

is a tac function of an n -dimensional convex body.

Lemma 1. Let H be the tac function of an n -dimensional convex body K in R^n . Then,

- (a) there is a positive constant j so that

$$|H(\underline{u})| \leq j|\underline{u}| \quad \text{for all } \underline{u} \in R^n,$$
- (b) H is absolutely continuous.

Proof

(a) $H(\underline{u}) = |\underline{u}|H(\underline{u}/|\underline{u}|)$ by property (2). $|H(\underline{u})|$ is bounded on $|\underline{u}| = 1$ by property (5) (a) and because K is bounded. Then,

$$j = \sup_{|\underline{u}|=1} |H(\underline{u})|$$

has the required property.

(b) In view of property (3) and part (a) of the present lemma,

$$\begin{aligned} & \sum_{i=1}^m |H(\underline{u}_i) - H(\underline{v}_i)| \\ & \leq \sum_{i=1}^m |H(\underline{u}_i - \underline{v}_i)| \\ & \leq j \sum_{i=1}^m |\underline{u}_i - \underline{v}_i|. \end{aligned}$$

It follows immediately that H is absolutely continuous.

The next result in Lemma 2 will be needed later. By "almost everywhere" we mean, "with the possible exception of a set of Lebesgue measure zero".

Lemma 2. Let $J : \mathbb{R}^n \rightarrow \mathbb{R}$ be a function which is continuous at $\underline{0}$ and absolutely continuous on any set which excludes $\underline{0}$. If the partial derivatives $\frac{\partial J}{\partial u_i}(\underline{u})$, exist and are zero for $i = 1, \dots, n$ almost everywhere, then J is a constant function on $\mathbb{R}^n$.

Proof

For $n = 1$, by a standard theorem of analysis (see for example [8], p.90), J is constant on any set which excludes $\underline{0}$. Then, by the continuity of J at $\underline{0}$, J is a constant function on R as required.

In the general case, for almost all $(u_2, \dots, u_n)$ we may define a function on R by

$$u_1 \mapsto J(u_1, u_2, \dots, u_n)$$

to which we may apply the one dimensional case. It then follows by the continuity of J that J is independent of u_1 . Similarly, J is independent of $u_2, \dots, u_n$ and so is a constant function.

4. Equivalent Convex Bodies.

Let K_1, K_2 be two n -dimensional convex bodies with tac functions H_1, H_2 . Define

$$h_1 K_1 + h_2 K_2$$

for $h_1, h_2 \geq 0$ and not both zero, to be the n -dimensional convex body with tac function $h_1 H_1 + h_2 H_2$ (see property (9) of section 3). Similarly define

$$-K_1$$

to be the n -dimensional convex body with tac function H_1^- . Other authors have used $K-K$ to mean $K + (-K)$ and we will use the same notation.

Let K be an n -dimensional convex body in R^n with the tac function H . The width of K in the direction $\underline{w}$ is defined as in the section 3, as $H(\underline{w}) + H(-\underline{w}) = (H+H^-)(\underline{w})$. Then, $H + H^-$ is known as the width function of K .

Two n -dimensional convex bodies K_1, K_2 in R^n will be called equivalent if for some positive constant j

$$(K_1 - K_1) = j(K_2 - K_2).$$

This will be written in symbols as $K_1 \sim K_2$, or more exactly $K_1 \overset{j}{\sim} K_2$, and it is clearly an equivalence relation. If K_1, K_2 have the tac functions H_1, H_2 , then it follows that

$$K_1 \overset{j}{\sim} K_2 \text{ if and only if } (H_1 + H_1^-) = j(H_2 + H_2^-).$$

Hence, the condition $K_1 \sim K_2$ is just that the width functions of K_1 and K_2 are proportional. Evidently equivalence is just a generalisation of K_1 and K_2 being two bodies of constant width. In fact in the sense described in [6], $K_1 \sim K_2$ means K_1 and K_2 have constant Minkowski breadth with respect to some Minkowski metric.

Another characterisation of the above equivalence is now proved in Theorem 1 for later use.

Theorem 1. Let K_1, K_2 be two n -dimensional convex bodies in R^n with tac functions H_1, H_2 . Let U_1 be a tac plane of K_1 at $\underline{a}_1$ with outer normal $\underline{u}$, and V_1 a tac plane of K_1 at $\underline{b}_1$ with outer normal $-\underline{u}$. Let U_2, V_2 be the parallel and similarly situated tac planes of K_2 at $\underline{a}_2, \underline{b}_2$ respectively (as in Diagram 1). Then $K_1 \sim K_2$ if, and only if, $\overline{\underline{a}_1 \underline{b}_1}$ is parallel to $\overline{\underline{a}_2 \underline{b}_2}$ for any choice of $\underline{u}$ for which U_1, V_1, U_2, V_2 are all regular (in this case $\underline{a}_1, \underline{b}_1, \underline{a}_2, \underline{b}_2$ are uniquely defined).

Proof.

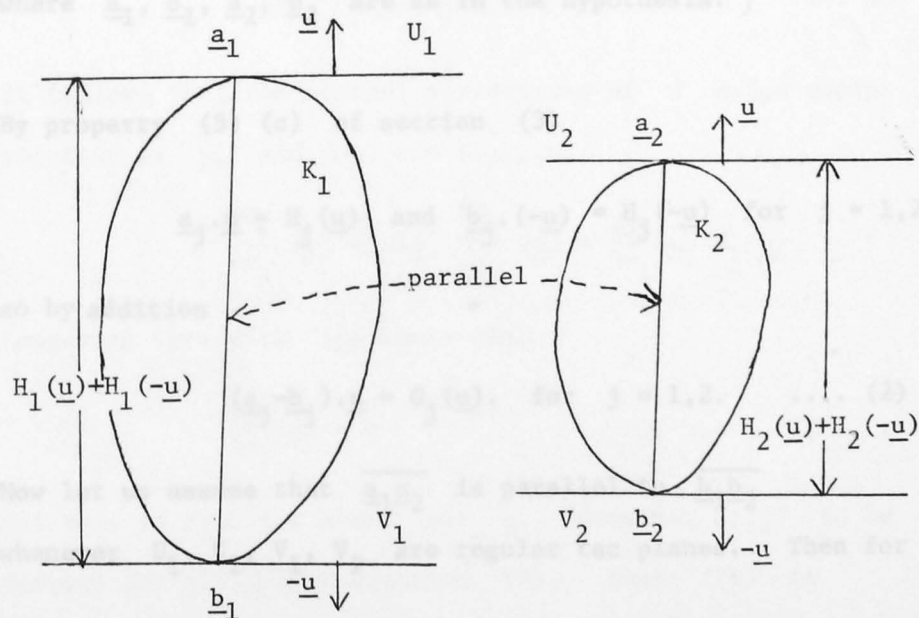


Diagram 1

For simplicity write $G_j = H_j + H_j^-$ for $j = 1, 2$. The tac planes U_1, U_2, V_1, V_2 must all be regular for almost all $\underline{u}$ (on this see [2], p.13 where a dual result is given). We will consider only those $\underline{u} \neq 0$ for which U_1, U_2, V_1, V_2 are all regular.

By property (6) of section 3, the partial derivatives of H_1, H_2 exist at $\underline{u}$ and $-\underline{u}$, and for $i = 1, \dots, n$

$$a_{1i} - b_{1i} = \frac{\partial H_1}{\partial u_i}(\underline{u}) - \frac{\partial H_1}{\partial u_i}(-\underline{u}) = \frac{\partial G_1}{\partial u_i}(\underline{u})$$

and similarly

$$a_{2i} - b_{2i} = \frac{\partial G_2}{\partial u_i}(\underline{u})$$

.... (1)

where $\underline{a}_1, \underline{b}_1, \underline{a}_2, \underline{b}_2$ are as in the hypothesis.

By property (5) (c) of section (3)

$$\underline{a}_j \cdot \underline{u} = H_j(\underline{u}) \quad \text{and} \quad \underline{b}_j \cdot (-\underline{u}) = H_j(-\underline{u}) \quad \text{for } j = 1, 2,$$

so by addition

$$(\underline{a}_j - \underline{b}_j) \cdot \underline{u} = G_j(\underline{u}) \quad \text{for } j = 1, 2. \quad \dots (2)$$

Now let us assume that $\overline{\underline{a}_1 \underline{a}_2}$ is parallel to $\overline{\underline{b}_1 \underline{b}_2}$

whenever U_1, U_2, V_1, V_2 are regular tac planes. Then for

the regular cases there is a $J : \mathbb{R}^n \rightarrow \mathbb{R}$ for which

$$(\underline{a}_1 - \underline{b}_1) = J(\underline{u}) (\underline{a}_2 - \underline{b}_2) \quad \dots (3)$$

or in components, for $i = 1, \dots, n$

$$(a_{1i} - b_{1i}) = J(\underline{u}) (a_{2i} - b_{2i}).$$

By equation (1) above this is equivalent to

$$\frac{\partial G_1}{\partial u_i}(\underline{u}) = J(\underline{u}) \frac{\partial G_2}{\partial u_i}(\underline{u}) \quad \text{for } i = 1, \dots, n. \quad \dots (4)$$

However, from (3), it follows that

$$(\underline{a}_1 - \underline{b}_1) \cdot \underline{u} = J(\underline{u}) (\underline{a}_2 - \underline{b}_2) \cdot \underline{u}$$

so by equation (2) we have

$$G_1(\underline{u}) = J(\underline{u}) G_2(\underline{u}). \quad \dots (5)$$

It follows that the partial derivatives of J exist except possibly at $\underline{0}$, and for $i = 1, \dots, n$,

$$\frac{\partial G_1}{\partial u_i}(\underline{u}) = J(\underline{u}) \frac{\partial G_2}{\partial u_i}(\underline{u}) + \frac{\partial J}{\partial u_i}(\underline{u}) G_2(\underline{u}).$$

Comparing this with (4) shows that

$$\frac{\partial J}{\partial u_i}(\underline{u}) = 0$$

and this is true for almost all $\underline{u}$. Consider $J(\underline{u})$ to be defined for all $\underline{u} \neq \underline{0}$ by equation (5). Then $J(\underline{u})$ is

absolutely continuous on any set excluding the origin since G_1 and G_2 are absolutely continuous everywhere, by Lemma 1, and $G_2(\underline{u}) = 0$ only if $\underline{u} = \underline{o}$. Hence by the proof of Lemma 2, we see that J is a constant function on any set excluding $\underline{o}$. Since $G_1(\underline{o}) = G_2(\underline{o}) = 0$, it follows from (5) that $K_1 \sim K_2$ as required.

If on the other hand we assume $K_1 \not\sim K_2$, then for some $j > 0$,

$$G_1 = jG_2.$$

In the case of regular tac planes, the partial derivatives exist at $\underline{u}$ and we have by differentiation for $i = 1, \dots, n$

$$\frac{\partial H_1}{\partial u_i}(\underline{u}) - \frac{\partial H_1}{\partial u_i}(-\underline{u}) = j \left[\frac{\partial H_2}{\partial u_i}(\underline{u}) - \frac{\partial H_2}{\partial u_i}(-\underline{u}) \right].$$

Now using property (6) of section 3 and combining the components of $\underline{a}_1, \underline{a}_2, \underline{b}_1$, and $\underline{b}_2$, this gives that

$$\underline{a}_1 - \underline{b}_1 = j(\underline{a}_2 - \underline{b}_2)$$

so that $\overline{\underline{a}_1 \underline{b}_1}$ is parallel to $\overline{\underline{a}_2 \underline{b}_2}$.

~~~~~

One further result on equivalent bodies, which is needed later, is now proved in Lemma 3.

Lemma 3. Let  $K_1, K_2$  be two 2-dimensional convex bodies with

$K_1 \not\sim K_2$ . If  $U_1, V_1$  are the two tac planes of  $K_1$

perpendicular to  $\underline{w}$ , then let  $h_1(\underline{w})$  be the total length of the two segments (either of which may be a single point) in which  $U_1$  and  $V_1$  meet  $\text{Fr}K_1$ . In particular define  $h_1(\underline{w}) = 0$  if both  $U_1$  and  $V_1$  are regular. If  $h_2(\underline{w})$  is defined similarly for  $K_2$ , then

$$h_1(\underline{w}) = j h_2(\underline{w}) \text{ for all } \underline{w}.$$

This is a consequence of Theorem 1 and a result in [2], p.31.

## CHAPTER 2.

Characterisations of the Ellipsoid5. Some previous Characterisations of the Ellipsoid.

Two important known characterisations of the ellipsoid are stated in this section. Here, an  $n$ -dimensional ellipsoid will mean a convex body of the type

$$\sum_{i=1}^n a_i x_i^2 \leq 1, \text{ where } a_i \in \mathbb{R}^+,$$

or an affine transformation of such a body. In the following work we will often assume that  $\underline{o}$  is in the interior of a convex body, but this is no loss of generality since the properties we are interested in are invariant under translations.

Theorem 2. Let  $K$  be an  $n$ -dimensional convex body in  $\mathbb{R}^n$  with  $\underline{o} \in \text{Int}K$ . If every hyperplane through  $\underline{o}$  intersects  $K$  in an ellipsoid, then  $K$  is an ellipsoid.

A proof can be found in [9].

A 1-flat  $T$  is called a tac line of a convex body  $K$  if  $T$  intersects  $K$  but not  $\text{Int}K$ . In  $\mathbb{R}^2$ ,  $T$  is just the ordinary tac plane of  $K$ , and in general  $T$  lies in a tac plane of  $K$ .



Theorem 3. Let  $K$  be an  $n$ -dimensional convex body in  $\mathbb{R}^n$  where  $n \geq 3$ . Let  $T(\underline{w})$  be the union of all the tac lines of  $K$  parallel to  $\underline{w}$  and let

$$C(\underline{w}) = T(\underline{w}) \cap K.$$

If  $C(\underline{w})$  lies in a hyperplane for every  $\underline{w}$ , then  $K$  is an ellipsoid.

This is a result of Blaschke. A proof is given in [3], p.93.

#### 6. A New Characterisation of the Ellipsoid.

In this section a new characterisation of the ellipsoid is established in Theorem 4. Further results on ellipsoids which are consequences of Theorem 4 are given in section 8.

Theorem 4. Let  $K$  be a three-dimensional convex body in  $\mathbb{R}^3$  with  $\underline{o} \in \text{Int}K$ , all of whose tac planes are regular. Let  $j$  be a constant with  $0 < j < 1$ . If  $(U_1 \cap K) \sim (U_2 \cap K)$  whenever  $U_1, U_2$  are any two parallel planes both on the same side of  $\underline{o}$  which both intersect  $\text{Int}K$  but not  $\text{Int}(jK)$ , then  $K$  is an ellipsoid.

#### Proof.

The proof is long and is given in a series of lemmas, for each of which the hypothesis of Theorem 4 is assumed to hold unless otherwise stated.



Lemma 4. If  $C(\underline{w})$  and  $T(\underline{w})$  are defined as in Theorem 3 of section 6, then

- (a) any plane  $U$  parallel to the vector  $\underline{w}$  which intersects  $\text{Int } K$  will intersect  $C(\underline{w})$  in two distinct points, and
- (b)  $C(\underline{w})$  is a simple closed curve in  $R^3$  in the sense described in [1] p.170. (see Diagram 2.)

Proof.

(a)  $T(\underline{w})$  is a convex cylinder since the projection of a convex body is still a convex body (see [2] p.45). However  $U$  is parallel to the generators of  $T(\underline{w})$  and  $U$  meets the interior of  $T(\underline{w})$ , therefore  $T(\underline{w}) \cap U$  consists of two distinct generators of  $T(\underline{w})$ . These two generators are tac lines of  $K$  by definition of  $T(\underline{w})$ , and so each has a single point in common with  $K$  because of the regularity of the tac planes of  $K$ . Hence  $C(\underline{w}) \cap U = T(\underline{w}) \cap K \cap U$  consists of exactly two points.

(b) Let  $Q$  be the line through  $\underline{o}$  parallel to the vector  $\underline{w}$ . From part (a) of this lemma it is clear that any half-plane bounded by  $Q$  intersects  $C(\underline{w})$  in one point, since  $\underline{o} \in \text{Int } K$ . Take one such half-plane, designate it  $V(0)$ , and let  $V(s)$  be the one of the half-planes making an angle  $s$  with  $V(0)$ , for  $0 \leq s \leq 2\pi$  (The direction of increasing  $s$  may be chosen arbitrarily.) Let  $\underline{a}(s)$  be the unique point of  $C(\underline{w})$  in  $V(s)$ . Now

$$C(\underline{w}) = \{\underline{a}(s) \mid 0 \leq s < 2\pi\}.$$

Also  $\underline{a}(s) \neq \underline{a}(t)$  if  $s \neq t$ , except that  $\underline{a}(0) = \underline{a}(2\pi)$ . It remains to show that  $\underline{a}(s)$  is a continuous function of  $s$ .  $C(\underline{w})$  is a closed set since  $C(\underline{w}) = T(\underline{w}) \cap K$ , where  $T(\underline{w})$  and  $K$  are closed. Consider a sequence  $\{\underline{a}(s_i)\}$  where  $s_i \rightarrow s$ . This sequence has a limit point in  $C(\underline{w})$  since  $C(\underline{w})$  is bounded and closed. However any such limit point must clearly lie in  $V(s)$  and so must be  $\underline{a}(s)$ . Hence  $\lim_{s_i \rightarrow s} \underline{a}(s_i)$  exists and it is  $\underline{a}(s)$ .

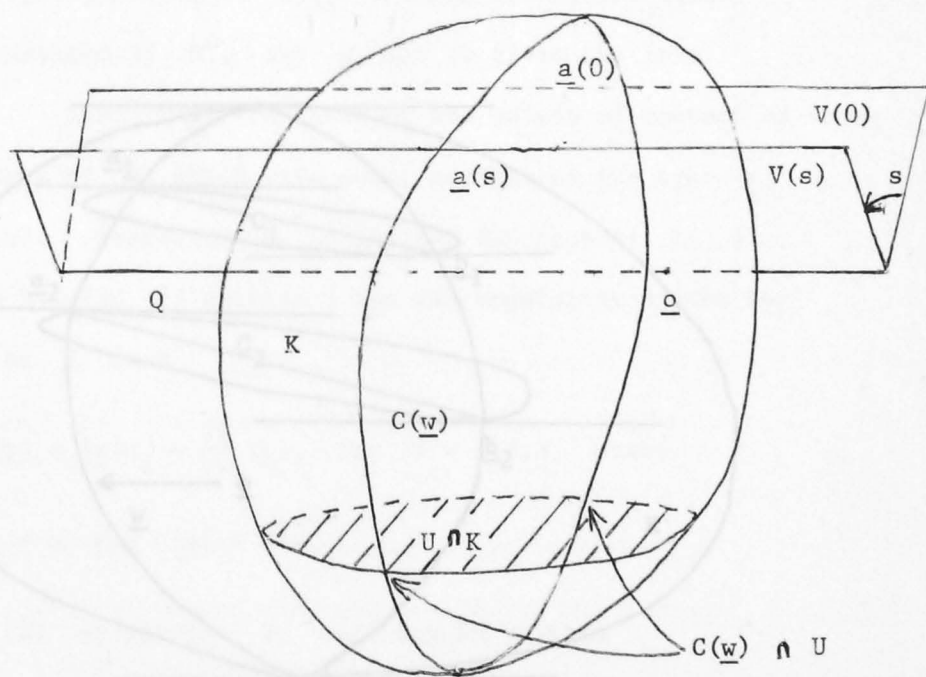


Diagram 2

Lemma 5. Let  $U_1, U_2$  be any two parallel planes both parallel to the vector  $\underline{w}$  which intersect  $\text{Int}K$  and satisfy

$$(U_1 \cap K) \sim (U_2 \cap K) .$$

If  $U_1$  intersects  $C(\underline{w})$  in  $\underline{a}_1, \underline{b}_1$  and  $U_2$  intersects  $C(\underline{w})$  in  $\underline{a}_2, \underline{b}_2$ , then  $\overline{\underline{a}_1 \underline{b}_1}$  is parallel to  $\overline{\underline{a}_2 \underline{b}_2}$ , (see Diagram 3).

Proof.

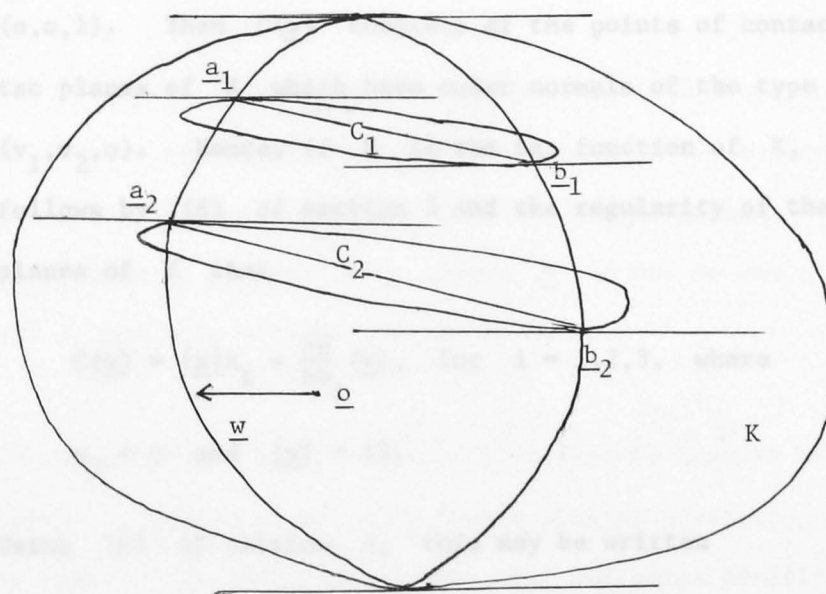


Diagram 3

Let  $C_i = U_i \cap K$  for  $i = 1, 2$ . Since  $\underline{a}_1, \underline{b}_1, \underline{a}_2, \underline{b}_2$  are in  $C(\underline{w})$ , there are tac lines of  $K$  parallel to the vector  $\underline{w}$  at each of these points. These four tac lines lie in  $U_1$  or  $U_2$  and so are also tac lines of  $C_1$  or  $C_2$  as the case may be. Since  $C_1 \sim C_2$  it follows that  $\overline{\underline{a}_1 \underline{b}_1}$  is parallel to  $\overline{\underline{a}_2 \underline{b}_2}$  by Theorem 1 of section 4.

~~~~~

In order to simplify the following proofs we will now construct a new representation of $C(\underline{w})$. By an orthogonal linear transformation of R^n , any $\underline{w}$ may be given the form $(0, 0, 1)$. Then $C(\underline{w})$ consists of the points of contact of those tac planes of K which have outer normals of the type $(v_1, v_2, 0)$. Hence, if H is the tac function of K , it follows by (6) of section 3 and the regularity of the tac planes of K that

$$C(\underline{w}) = \{ \underline{x} \mid x_i = \frac{\partial H}{\partial v_i}(\underline{v}), \text{ for } i = 1, 2, 3, \text{ where}$$

$$v_3 = 0 \text{ and } |\underline{v}| = 1 \}.$$

Using (2) of section 3, this may be written

$$C(\underline{w}) = \{ \underline{f}(r) \mid \underline{f}_i(r) = \frac{\partial H}{\partial v_i}(\cos r, \sin r, 0),$$

$$\text{for } i = 1, 2, 3 \text{ and } 0 \leq r < 2\pi \},$$

in which case r is the angle which the tac plane of K at $\underline{f}(r)$ makes with the tac plane of K at $\underline{f}(0)$. The function $\underline{f}$ is continuous by property (6) of section 3. $\underline{f}$ is one-to-one except when $\underline{f}(r)$ is one of at most countably many points of $C(\underline{w})$ where there is more than one tac plane of K . This one-to-one property is a consequence of a result in [2], p.15. $C(\underline{w})$ will now be considered exclusively in terms of the function $\underline{f}$.

If $I \subseteq (0, 2\pi)$, then $\underline{f}(I)$ will denote

$$\{\underline{f}(r) \mid r \in I\}.$$

The function $\underline{f}$ induces the ordering of $(0, 2\pi)$ in $C(\underline{w})$ so that we may speak of neighbourhoods on $C(\underline{w})$ so long as the point $\underline{f}(0)$ is excluded from the neighbourhood. It is no loss of generality to assume $\underline{f}$ is one-to-one at $r = 0$ and this will be assumed to be so.

Chords of $C(\underline{w})$ are of special significance because of Lemma 5, and so we now give them a special notation.

By Lemma 4 and the properties of $\underline{f}$, any plane parallel to the vector $\underline{w}$, which is also perpendicular to the vector $(\cos r, \sin r, 0)$ for some r with $0 \leq r < 2\pi$, will cut $C(\underline{w})$ not at all, or in one of the points $\underline{f}(r)$, $\underline{f}(r \pm \pi)$

where $0 \leq r \pm \pi < 2\pi$, or in two points $\underline{f}(s), \underline{f}(t)$ say. In the last case $\overline{\underline{f}(s)\underline{f}(t)}$ is called an $\underline{r}$ -chord. There is clearly a unique $\underline{r}$ -chord through each point of $C(\underline{w})$ other than $\underline{f}(r)$ and $\underline{f}(r \pm \pi)$.

Lemma 6. (a) Let $\overline{\underline{f}(s)\underline{f}(t)}$ be an $\underline{r}$ -chord, where $0 < r \leq \pi$, and $s < t$.

Then either $s < r < t$ or $s < r + \pi < t$ but not both.

(b) If $\underline{r}$ is defined as a function of s and t in the cases

$\underline{f}(s) \neq \underline{f}(t)$, by $\overline{\underline{f}(s)\underline{f}(t)}$ being an $\underline{r}$ -chord with $s < r < t$,

then it is a continuous function. If s is fixed then $\underline{r}$ is

a monotonic increasing function of t .

(c) If $\underline{f}(t)$ is defined as a function of r and s by

$\overline{\underline{f}(s)\underline{f}(t)}$ being an $\underline{r}$ -chord, then it is also a continuous function.

Proof.

(a) Let T_1 and T_2 be the tac planes of K perpendicular to $(\cos r, \sin r, 0)$, through $\underline{f}(r)$ and $\underline{f}(r+\pi)$ and let U be the parallel plane through the $\underline{r}$ -chord $\overline{\underline{f}(s)\underline{f}(t)}$. Then U separates T_1 and T_2 and it divides $C(\underline{w})$ into

$$P_1 = \{\underline{f}(x) \mid s \leq x \leq t\}, \text{ and}$$

$$P_2 = \{\underline{f}(x) \mid 0 \leq x \leq s \text{ or } t \leq x < 2\pi\}$$

(with $\underline{f}(s)$ and $\underline{f}(t)$ common). Hence, just one of $\underline{f}(r), \underline{f}(r+\pi)$ lies in P_1 and it is distinct from $\underline{f}(s)$ and $\underline{f}(t)$. The result follows.

(b) The chord $\overline{\underline{f}(s)\underline{f}(t)}$ varies continuously with s and t , since $\underline{f}$ is a continuous function, and therefore so does the plane U defined in the proof of part (a). However U makes an angle $\underline{r}$ with some fixed plane, U_1 , parallel to $\underline{w}$. Hence the function $\underline{r}$ must vary

continuously with s and t , provided there is not a jump discontinuity from r to $r \pm \pi$. However from the proof of part (a) this can only happen at s or $t = 0$, in which case there is a discontinuity in s or t .

If s is fixed and t decreases monotonically, then the plane U must rotate monotonically and in the direction of decreasing r (for otherwise r would not stay in the interval (s, t)). Hence, r is a monotonic increasing function of t .

(c) The plane U through $\underline{f}(s)$ making an angle r with U_1 must vary continuously with r and s . Hence $\underline{f}(t)$, the second point of intersection of U with $C(\underline{w})$, varies continuously with r and s .

Lemma 7. Let $0 < r < 2\pi$. There exists an open neighbourhood (p, q) of r , designated $N(r)$, satisfying the following:

- (a) $\underline{f}(p) \neq \underline{f}(q)$, and $\underline{f}(r)$ is in the interior of the interval $\{\underline{f}(x) \mid p < x < q\} = \underline{f}(N(r))$ on $C(\underline{w})$,
- (b) if s_1 and $s_2 \in N(r)$, and if $\overline{\underline{f}(s_1)\underline{f}(t_1)}$ and $\overline{\underline{f}(s_2)\underline{f}(t_2)}$ are both r -chords, then they are parallel (see Diagram 4).

Proof.

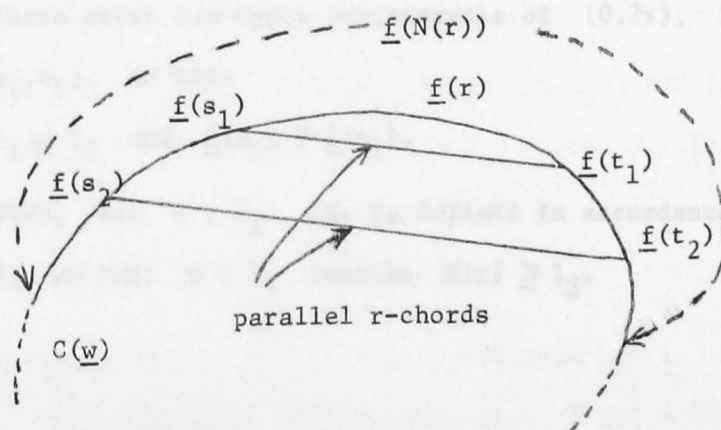


Diagram 4

Let the tac plane T of jK with outer normal $(\cos r, \sin r, 0)$ intersect $C(\underline{w})$ in $\underline{f}(p)$ and $\underline{f}(q)$, with $p < q$. Since $j < 1$, it follows that $\underline{f}(p)$, $\underline{f}(q)$, and $\underline{f}(r)$ are all distinct.

If $p < r < q$, and $s_1, s_2 \in (p, q)$, then let $\underline{f}(t_1)$ and $\underline{f}(t_2)$ be the respective second points of intersection, with $C(\underline{w})$ of the planes U_1 and U_2 parallel to T through $\underline{f}(s_1)$ and $\underline{f}(s_2)$. U_1 and U_2 must lie between T and $\underline{f}(r)$, so they cannot intersect jK . Lemma 5 and the hypothesis of Theorem 4 show that $\overline{\underline{f}(s_1)\underline{f}(t_1)}$ and $\overline{\underline{f}(s_2)\underline{f}(t_2)}$ are parallel r -chords. Hence the result follows with $N(r) = (p, q)$.

If $0 < r < p$ or $q < r < 2\pi$, then choose p' and q' as follows: if T_1 is the tac plane of K at $\underline{f}(r)$ parallel to T , then $\underline{f}(0) \notin T_1$ since T_1 is regular and $\underline{f}(0) \neq \underline{f}(r)$. Hence there is a plane U parallel to T separating $\underline{f}(0)$ and $\underline{f}(r)$. If U intersects $C(\underline{w})$ in $\underline{f}(p')$ and $\underline{f}(q')$ with $p' < q'$, then, as in the proof of Lemma 6(a), $p' < r < q'$. The result now follows as above with $N(r) = (p', q')$.

~~~~~

Lemma 8. There exist non-empty subintervals of  $(0, 2\pi)$ ,  $I_1 = (s, t)$  and  $I_2 = (s_1, t_1)$ , so that

(a)  $I_1 \subseteq I_2$  and  $\underline{f}(s_1) \neq \underline{f}(t_1)$ ,

(b)  $N(r)$ , for  $r \in I_1$ , can be defined in accordance with

Lemma 7, so that  $r \in I_1$  implies  $N(r) \supseteq I_2$ .

Proof.

Let an  $N(r)$  be chosen for each  $r \in (0, 2\pi)$  as in Lemma 7. For each  $r \in (0, 2\pi)$ , if  $N(r) = (p, q)$ , then define

$$D(r) = \min (|\underline{f}(r) - \underline{f}(p)|, |\underline{f}(r) - \underline{f}(q)|). \quad \dots (1)$$

By Lemma 7(a),  $D$  is a strictly positive function. Hence,

$$(0, 2\pi) = \bigcup_{m=1}^{\infty} S_m, \text{ where } S_m = \{r | D(r) > \frac{1}{m}\}.$$

The Baire Category Theorem (see [5], p.31) shows that there is an  $m$  for which the closure of  $S_m$  has an interior point. Hence, for this  $m$ , there exists an open interval  $I$  and a set  $J$  dense in  $I$ , where

$$J = \{r | D(r) > \frac{1}{m} \text{ and } r \in I\}. \quad \dots (2)$$

If  $I = (s', t')$  and  $\underline{f}(s') \neq \underline{f}(t')$ , then let  $I_1 = I_2 = (s, t)$ , where  $(s, t)$  is a subinterval of  $(s', t')$  satisfying,  $\underline{f}(s) \neq \underline{f}(t)$  and

$$\max. |\underline{f}(x) - \underline{f}(y)| < \frac{1}{m}, \text{ whenever } x \text{ and } y \in (s, t).$$

On the other hand, if  $\underline{f}(s') = \underline{f}(t')$ , then take  $I_1 = I = (s', t')$ , and define  $I_2 = (s_1, t_1)$  with  $s_1 < s'$  and  $t_1 > t'$  by

$$\begin{aligned} |\underline{f}(s_1) - \underline{f}(s')| &= |\underline{f}(t_1) - \underline{f}(s')| = \frac{1}{m}, \text{ and} \\ |\underline{f}(x) - \underline{f}(s')| &< \frac{1}{m} \text{ whenever } s_1 < x < t_1. \end{aligned}$$

In both cases, (a) is satisfied since  $\underline{f}(s_1) \neq \underline{f}(t_1)$ , and it follows on considering (1) and (2) that if  $J_1 = J \cap I_1$ , then  $J_1$  is dense in  $I_1$  and

$$r \in J_1 \text{ implies } N(r) \supseteq I_2. \quad \dots (3)$$

To establish (b) we show that  $J_1$  can be replaced by  $I_1$  in (3).

Let  $r \in I_1$ . If  $N(r) \not\supseteq I_2$  then we show that  $N'(r) = N(r) \cup I_2$  still satisfies Lemma 7. We must show that if  $\overline{\underline{f}(s_1)\underline{f}(t_1)}$  and  $\overline{\underline{f}(s_2)\underline{f}(t_2)}$

are  $r$ -chords with  $s_1$  and  $s_2 \in I_2$ , then they are parallel. Since  $J_1$  is dense in  $I_1$ , there is a sequence  $\{r_i\}$  with  $r_i \in J_1$ , so that  $r_i \rightarrow r$  as  $i \rightarrow \infty$ . If, for each  $i$ ,  $\overline{f(s_1)f(t_{1i})}$  and  $\overline{f(s_2)f(t_{2i})}$  are  $r_i$  chords, then they are parallel since  $N(r_i) \supseteq I_2$ . By Lemma 6(c),  $\overline{f(t_{1i})} \rightarrow \overline{f(t_1)}$  and  $\overline{f(t_{2i})} \rightarrow \overline{f(t_2)}$  as  $i \rightarrow \infty$ , so it is clear that  $\overline{f(s_1)f(t_1)}$  and  $\overline{f(s_2)f(t_2)}$  are also parallel. Now (b) follows with the original  $N(r)$  replaced by  $N'(r)$  for each  $r \in I_1$ .

~~~~~

Lemma 9. There exists an interval $(a_1, a_2) \subseteq (0, 2\pi)$, with $\underline{f}(a_1) \neq \underline{f}(a_2)$, on which $C(\underline{w})$ is a plane curve.

Proof.

Let $I_1 = (s, t)$, $I_2 = (s_1, t_1)$ and N be defined as in Lemma 8. We choose an $r \in I_1$ and an r -chord $\overline{f(a_1)f(b_1)}$ with

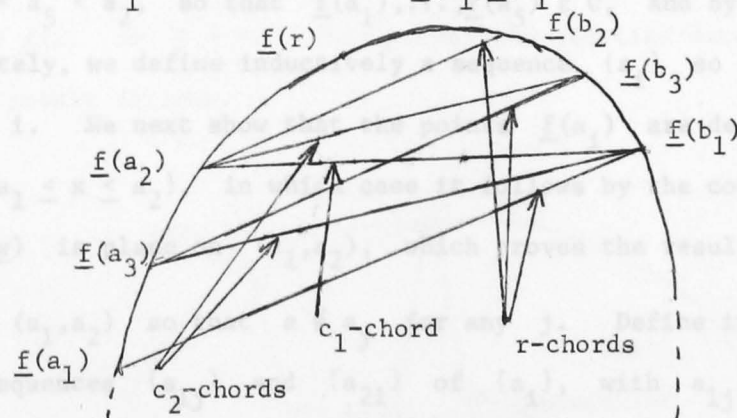


Diagram 5

$a_1 \in I_2$. For convenience assume $a_1 < r$. If $a_1 < x < r$ and $\overline{f(b_1)f(x)}$ is a c -chord, then, by Lemma 6(b), we have $c \rightarrow r$ as $x \rightarrow a_1$. Hence there is an a_2 , with $\underline{f}(a_2) \neq \underline{f}(r)$ and $\underline{f}(a_2) \neq \underline{f}(a_1)$, so that $c \in I_1$ whenever $a_1 < a < a_2$ (since $r \in I_1$, and I_1 is open). We now show that there exists an r -chord $\overline{f(a_3)f(b_3)}$ with $a_1 < a_3 < a_2$,

so that $\overline{f(a_3)f(b_1)}$ is parallel to $\overline{f(a_2)f(b_3)}$ (see Diagram 5).

Let $\overline{f(a_2)f(b_1)}$ be a c_1 -chord.

Consider a_3 as a variable increasing from a_1 to a_2 . Then $\overline{f(a_3)f(b_1)}$ changes continuously and monotonically from an r -chord to a c_1 -chord (by Lemma 6(b)) and similarly $\overline{f(a_2)f(b_3)}$ from a c_1 -chord to an r -chord. Hence there is a $c_2 \in (r, c_1)$, so that both are c_2 -chords. Since $a_1 < a_3 < a_2$, we have $c_2 \in I_1$ and consequently the two c_2 -chords are parallel. Assume a_3 is now fixed with this property.

It follows that $\underline{f(a_1)}, \underline{f(a_2)}$, and $\underline{f(a_3)}$ all lie in the plane U through $\underline{f(a_1)}$ parallel to the r -chords and c_2 -chords in question. By repeating this process we find a_4 and a_5 with $a_1 < a_4 < a_3$, and $a_3 < a_5 < a_2$, so that $\underline{f(a_1)}, \dots, \underline{f(a_5)} \in U$, and by repeating it indefinitely, we define inductively a sequence $\{a_i\}$ so that $\underline{f(a_i)} \in U$ for all i . We next show that the points $\underline{f(a_i)}$ are dense in $\{\underline{f(x)} \mid a_1 \leq x \leq a_2\}$, in which case it follows by the continuity of $\underline{f}$, that $C(\underline{w})$ is plane on (a_1, a_2) , which proves the result.

Let $a \in (a_1, a_2)$ so that $a \neq a_j$ for any j . Define inductively the subsequences $\{a_{1j}\}$ and $\{a_{2j}\}$ of $\{a_i\}$, with $a_{1j} < a_{2j}$, as follows: $a_{11} = a_1$ and $a_{21} = a_2$; if a_{1j} and a_{2j} are defined (with $a \in (a_{1j}, a_{2j})$), then let $a_k \in (a_{1j}, a_{2j})$ be the one of the a_i which is defined in the j 'th subdivision of the process used to define the a_i ; now define $(a_{1,j+1}, a_{2,j+1})$ to be whichever of (a_{1j}, a_k) or (a_k, a_{2j}) contains a . If, for each j , $\overline{f(a_{2j})f(b_{1j})}$ (see Diag. 6) is a c_j -chord, then we next show that $c_j \rightarrow r$ as $r \rightarrow \infty$.

Let $T(t)$ intersect $C(w)$ in the two points $\underline{f}(s), \underline{f}(s')$, so that $\overline{\underline{f}(s)\underline{f}(s')}$ is a t -chord. It is clear that the two points $\underline{f}(s), \underline{f}(s')$ of $C(w)$ vary continuously with t , where t is taken modulo 2π . It follows from this continuity property that we can choose t with $t \in (p, q)$ with $\underline{f}(t) \neq \underline{f}(p)$ or $\underline{f}(q)$, so that s and s' satisfy either (i) $s' \notin [p, q]$ and $s \in [p, q]$, or if (i) is impossible, then (ii) $s' \notin [p, q]$ and $s \notin [p, q]$.

In case (i), $\underline{f}(s') \neq \underline{f}(p)$ or $\underline{f}(q)$ because of the maximality of (p, q) and the fact that $\underline{f}$ is one-to-one at o . By Lemma 5 and the hypothesis of Theorem 4, all of the t -chords $\overline{\underline{f}(r)\underline{f}(r')}$ for $t < r < s$, are parallel to each other, since they are cut-off from $C(w)$ by parallel planes which do not intersect $\text{Int}(jK)$. However, for r sufficiently close to t , both r and $r' \in (p, q)$ and yet $\underline{f}(r) \neq \underline{f}(r')$. Hence all of the t -chords $\overline{\underline{f}(r)\underline{f}(r')}$ for $t < r < s$ are parallel to the plane in which $\underline{f}((p, q))$ lies. Yet these t -chords have the one end $\underline{f}(r)$ in $\underline{f}([p, q])$, so that $\underline{f}(r')$ for $t < r < s$ also lies in the plane of $\underline{f}([p, q])$. This contradicts the maximality of (p, q) , so that $p = 0$.

In case (ii), if $\overline{\underline{f}(q)\underline{f}(q')}$ is the t -chord through $\underline{f}(q)$, then by choosing t sufficiently close to p with

$\underline{f}(t) \neq \underline{f}(p)$, we can ensure that $q' \notin [p, q]$. The case (ii) then reduces to case (i) with q taking the place of s .

then K is an ellipsoid.

Hence, in both cases (i) and (ii) we find $p = o$. Similarly, $q = 2\pi$, so that $C(\underline{w})$ is a plane curve as required.

In the case $n = 3$ this is just Theorem 4. The proof uses

induction on n . Assume that the result is true for dimension

Theorem 4 now follows immediately from Lemma 10 and Theorem 3 of section 6.

7. Further Results on Ellipsoids.

The result in section 6, namely Theorem 4, will now be generalised in a number of ways which may be of interest. Corollary 4 will be used later in the proofs of the major theorems on reduction theory in section 10.

The generalisation of Theorem 4 from R^3 to R^n is without difficulty and is now proved in Corollary 1.

Corollary 1. Let K be an n -dimensional convex body in R^n , for $n \geq 3$, all of whose tac planes are regular, with $\underline{o} \in \text{Int}K$. Let j be a constant with $0 < j < 1$. If

$$(U_1 \cap K) \sim (U_2 \cap K)$$

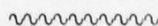
whenever U_1, U_2 are any two parallel hyperplanes both on the same side of $\underline{o}$ intersecting $\text{Int}K$ but not $\text{Int}(jK)$, then K is an ellipsoid.

Proof.

In the case $n = 3$ this is just Theorem 4. The proof uses induction on n . Assume that the result is true for dimension $(n-1)$ and that K is an n -dimensional convex body in R^n which satisfies the hypothesis.

Consider any hyperplane U in R^n which contains $\underline{o}$. U may be identified with R^{n-1} in a well-known way, and then $U \cap K$ is an $(n-1)$ -dimensional convex body in R^{n-1} where the new origin is the same point $\underline{o}$. Then it is easy to show that any hyperplane in R^{n-1} is the intersection of a hyperplane of R^n with U . It follows easily that the hypothesis of this Corollary 1 applies to $U \cap K$ in R^{n-1} , so that $U \cap K$ is an ellipsoid.

The above proof applies to any hyperplane U of R^{n-1} containing $\underline{o}$, so by Theorem 2 of section 5, K is an ellipsoid. Hence Corollary 1 follows for all $n \geq 3$ by the induction principle.



Corollary 1, and so Theorem 4, still remains true when the condition that the tac planes be regular is deleted, as we shall now show.

Corollary 2. Let K be an n -dimensional convex body in $\mathbb{R}^n$ for $n \geq 3$ with $\underline{o} \in \text{Int } K$. Let j be a constant with $0 < j < 1$. If

$$(U_1 \cap K) \sim (U_2 \cap K)$$

whenever U_1 and U_2 are any two parallel hyperplanes both on the same side of $\underline{o}$ intersecting $\text{Int } K$ but not $\text{Int}(jK)$, then every tac plane of K is regular.

Proof.

We will establish Corollary 2 for $n = 3$. The result for $n > 3$ then follows by a simple induction proof using the fact that, if an n -dimensional convex body satisfies the hypothesis, then so does the $(n-1)$ -dimensional intersection of K with a hyperplane through $\underline{o}$.

Let T be a tac plane of K and let U_1 and U_2 be planes parallel to T on the same side of $\underline{o}$ as T as described in the hypothesis. If $T \cap K$ is a segment, then the ratio of the minimum width to the maximum width of $U_2 \cap K$ must approach zero as U_2 approaches T . Hence we can find a U_2 not intersecting jK

so that $(U_1 \cap K)$ cannot be equivalent to $(U_2 \cap K)$. Hence $T \cap K$ must be a two-dimensional convex body, or in other words a plane face of K , or a single point.

Let T, T' be a pair of distinct parallel tac planes of K , so that if $D = T \cap K$ and $D' = T' \cap K$, then D is a plane face of K , as in Diagram 8. D' may be a single point.

Let $\overline{a_1 a_2}$ be any chord of D . The argument is now divided into two cases: (i) every tac plane of K parallel to $\overline{a_1 a_2}$ intersects either D or D' ; (ii) there is a tac plane U of K parallel to $\overline{a_1 a_2}$ which does not intersect D or D' .

In case (i) we can clearly find a tac plane U parallel to $\overline{a_1 a_2}$ which intersects both D and D' . Then $U \cap K$ must contain a segment which does not lie in D or D' . Then by the first part of this proof $U \cap K$ contains a plane face of K parallel to $\overline{a_1 a_2}$.

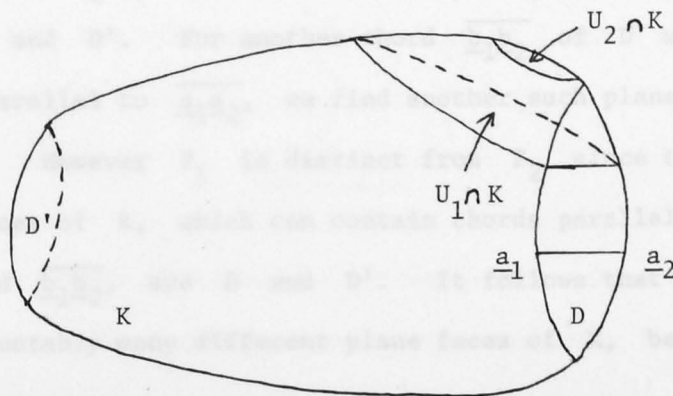


Diagram 8

In case (ii) let U_1 be the tac plane of jK with the same outer normal as U . By a simple continuity argument we can show that U may be chosen still distinct from D and D' but so that U_1 intersects $\text{Int}D$. (D is here considered as a two-dimensional convex body.) In this case there is another hyperplane, U_2 say, between U_1 and U distinct from U which does not intersect D or D' . It is then clear that U_1 and U_2 satisfy the hypothesis of this corollary so that $(U_1 \cap K) \sim (U_2 \cap K)$. However, $\text{Fr}(U_1 \cap K)$ contains a segment parallel to $\overline{a_1 a_2}$ since U_1 intersects $\text{Int}D$. Hence, by Lemma 3 of section 4, $\text{Fr}(U_2 \cap K)$ also contains such a straight segment which does not lie in D or D' , and by the first part of this proof, this segment must lie in a plane face of K distinct from D and D' .

In both cases (i) and (ii), we deduce that there is a plane face, F_1 say, of K parallel to $\overline{a_1 a_2}$ and distinct from D and D' . For another chord $\overline{b_1 b_2}$ of D which is not parallel to $\overline{a_1 a_2}$, we find another such plane face, F_2 say. However F_1 is distinct from F_2 since the only plane faces of K , which can contain chords parallel to both $\overline{a_1 a_2}$ and $\overline{b_1 b_2}$, are D and D' . It follows that there are uncountably many different plane faces of K , because

there are uncountably many, mutually non-parallel chords of D . However K cannot have uncountably many different plane faces, and so K cannot have a non-regular tac plane.

By taking $j = 0$ in Corollary 2 and Corollary 3, we obtain the simple result of Corollary 3.

Corollary 3. Let K be an n -dimensional convex body for $n \geq 3$ with $\underline{0} \in \text{Int}K$. If

$$(U_1 \cap K) \sim (U_2 \cap K)$$

whenever U_1 and U_2 are any two parallel hyperplanes intersecting $\text{Int}K$, then K is an ellipsoid.

Proof.

Since the hypothesis of this corollary is the same as that of Corollaries 2 and 3 with $j = 0$, it is clear that K must satisfy the hypotheses of Corollaries 2 and 3 with any $j > 0$.

Corollary 3 generalises many previously-known characterisations of the ellipsoid. For instance, by specialising "equivalence",

we find the result in R^3 : if K is a three-dimensional convex body whose cross-section by any plane is a body of constant width, then K is an ellipsoid. Similarly, if K is a three-dimensional convex body and any two parallel cross-sections of K are homothetic, then K is an ellipsoid. These two results are mentioned in [2], p.142.

Another possible generalisation of Theorem 4 would be to relax the conditions on j . Namely, we would consider a convex body K satisfying the following condition, which will be referred to as condition (*).

K is an n -dimensional convex body for $n \geq 3$ with $\underline{o} \in \text{Int}K$.

There is for each $\underline{w}$ a $j(\underline{w})$ with $0 \leq j(\underline{w}) < 1$. Let

$T(\underline{w})$ be the tac plane of K with outer normal $\underline{w}$.

Then

$$(U_1 \cap K) \sim (U_2 \cap K)$$

for each $\underline{w}$, whenever U_1 and U_2 are any two hyperplanes both being parallel to and on the same side of $\underline{o}$ as $T(\underline{w})$ and intersecting $\text{Int}K$, but not $\text{Int}(j(\underline{w})K)$.

When (*) holds, rather surprisingly, K need not be an ellipsoid, as will be shown in the example below. Lemma 9 still holds when K satisfies condition (*). In view of

Lemma 9 and Theorem 3, it seems quite probable that if K satisfies (*), then K must be composed of pieces of ellipsoids and possibly pieces of other second order surfaces. I have not been able to prove this result.

Example. Let K be the union of a half-ellipsoid K_1 and a hemisphere K_2 , where K_1 and K_2 are the set of points $\underline{x}$ of R^3 satisfying

$$K_1 : \frac{1}{4}x_1^2 + x_2^2 + x_3^2 \leq 1 \text{ and } x_1 \geq 0,$$

$$K_2 : x_1^2 + x_2^2 + x_3^2 \leq 1 \text{ and } x_1 \leq 0.$$

C is the circular disc:

$$x_1 = 0 \text{ and } x_2^2 + x_3^2 \leq 1.$$

K is clearly a three-dimensional convex body.

Let U be a tac plane of K at $\underline{a}$, which has outer normal $\underline{w}$ with $w_1 \neq 0$, so that $\underline{a} \notin C$. Ellipsoids have the property that any two parallel cross-sections are similar. Hence, if U_1 and U_2 are any two planes parallel to, and on the same side of $\underline{0}$ as U and which do not cross C , then $(U_1 \cap K) \sim (U_2 \cap K)$.

Let U be a tac plane of K at $\underline{a}$, which has outer normal $\underline{w}$ with $w_1 = 0$, so that $\underline{a} \in C$. If U_1 is a plane parallel

to U which intersects K , then $U_1 \cap K_1$ and $U_1 \cap K_2$ are a half ellipse and a half-disc with a common diameter. If U_2 is another plane parallel to U_1 , then it follows that $(U_1 \cap K)$ is similar to $(U_2 \cap K)$ and so $(U_1 \cap K) \sim (U_2 \cap K)$.

It is clear therefore that K satisfies (*) for some appropriate $j(\underline{w})$. However K does not satisfy the hypothesis of Theorem 4 since as $w_1 \rightarrow 0$, with $w_1 \neq 0$ we must have $j(\underline{w}) \rightarrow 1$, to ensure that the hyperplanes U_1 and U_2 defined above do not intersect C .

In the next Corollary we prove a result which is specifically intended to be used in the proofs of Theorems 9 and 10 of section 10. The hypothesis of this Corollary is in some ways weaker and other ways stronger than condition (*).

Corollary 4. Let K be a three-dimensional convex body in R^3 which satisfies (*) not in its entirety, but only for each $\underline{w}$ which is the outer normal of a regular tac plane of K . Assume in addition that: no tac plane of K intersects K in just a segment; for each $\underline{w}$ which is an outer normal of a regular tac plane,

$$(U_1 \cap K) \sim (U_0 \cap K)$$

whenever U_0 and U_1 are two planes both perpendicular to $\underline{w}$,

so that $\underline{o} \in U_0$, and U_1 is as described in (*). Then every tac plane of K is regular.

Proof.

The proof is in many ways similar to the proof of the three-dimensional case of Corollary 2 and many details are referred to that proof.

By hypothesis a tac plane can intersect K in a single point or a plane face but not a segment. As in Corollary 2, let D and D' be the intersections of two parallel tac planes with K , where D is a plane face and D' may be a single point. Let $\overline{a_1 a_2}$ be any chord of D , then there are two cases: (i) every tac plane of K parallel to $\overline{a_1 a_2}$ intersects D or D' ; (ii) there is a tac plane, U , of K parallel to $\overline{a_1 a_2}$ which does not intersect D or D' .

In case (i) we deduce, exactly as in Corollary 2, that there is a plane face of K parallel to $\overline{a_1 a_2}$ and distinct from the planes of D and D' .

In case (ii), let U_0 be the hyperplane through $\underline{o}$ parallel to U . A simple continuity argument shows that U may be chosen so that it does not intersect D or D' but U_0 intersects $\text{Int } D$, or $\text{Int } D'$ if $\text{Int } D'$ exists (D and D' are considered

as two-dimensional convex bodies). Assume that U has been chosen so that U_0 intersects $\text{Int } D$. If U is not regular we can immediately reach the conclusion of case (i), so assume U is regular. It follows that we can choose a plane U_1 parallel to U and sufficiently close to U that U_1 does not intersect

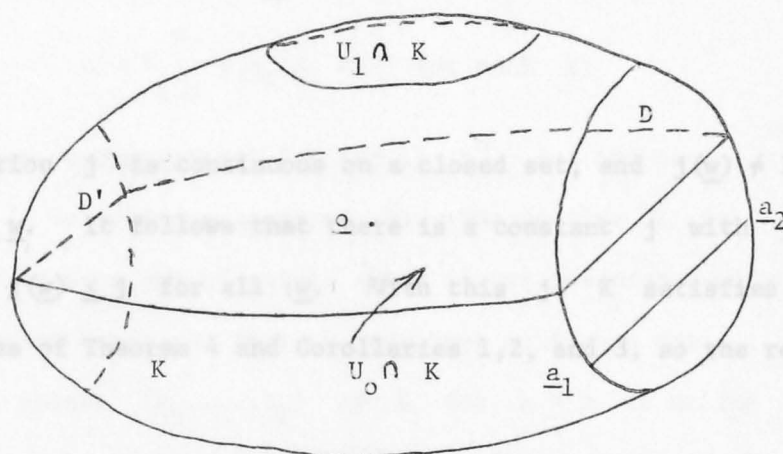


Diagram 9

D , D' , or $\text{Int}(j(\underline{w})K)$, where $\underline{w}$ is the outer normal of U .

Then by hypothesis,

$$(U_1 \cap K) \sim (U_0 \cap K).$$

By Lemma 3, page 12, it follows that $\text{Fr}(U_1 \cap K)$ contains a straight segment parallel to $\overline{a_1 a_2}$, since $\text{Fr}(U_0 \cap K)$ contains such a segment. Hence there is a plane face of K , distinct from D or D' and parallel to $\overline{a_1 a_2}$, containing this segment in $\text{Fr}(U_1 \cap K)$.

Now from the conclusions of cases (i) and (ii), it follows exactly as in Corollary 2, that every tac plane of K is regular.

We prove one more almost trivial Corollary.

Corollary 5. Let K satisfy condition (*) and let $j(\underline{w})$ be a continuous function of $\underline{w}$. Then K is an ellipsoid.

Proof.

The function j is continuous on a closed set, and $j(\underline{w}) \neq 1$ for any $\underline{w}$. It follows that there is a constant j with $j < 1$ so that $j(\underline{w}) \leq j$ for all $\underline{w}$. With this j , K satisfies the hypotheses of Theorem 4 and Corollaries 1, 2, and 3, so the result follows.

If L and M are two n -dimensional lattices with respective bases $(\underline{a}_1, \dots, \underline{a}_n)$ and $(\underline{b}_1, \dots, \underline{b}_n)$, then there is a linear transformation from L to M of the form

$$\underline{b}_i = \sum_{j=1}^n t_{ij} \underline{a}_j, \text{ for } i = 1, \dots, n,$$

where the coefficients $t_{ij} \in \mathbb{R}$. In this case, $L = M$ if, and only if, the transformation is unimodular, or in other words the t_{ij} are integers and the determinant of the t_{ij} is ± 1 . Proofs of these results are in [4], p. 9ff.

CHAPTER 3

Two Finiteness Theorems for theReduction Theory8 Lattices.

If $\underline{a}_1, \dots, \underline{a}_n$ are n -linearly independent points in $\mathbb{R}^n$ then the set of points

$$L = \left\{ \sum_{i=1}^n p_i \underline{a}_i \mid p_i \in \mathbb{I} \text{ for each } i \right\}$$

is called an n -dimensional lattice in $\mathbb{R}^n$, and the set $\{\underline{a}_1, \dots, \underline{a}_n\}$ is called a basis of L . The lattice L is understood to be a set of points which is not associated with any particular basis, so that L can have more than one basis. A subset $\{\underline{b}_1, \dots, \underline{b}_k\}$ of L for $k \leq n$ is called primitive in L if it can be extended to form a basis of L .

If L and M are two n -dimensional lattices with respective bases $\{\underline{a}_1, \dots, \underline{a}_n\}$ and $\{\underline{b}_1, \dots, \underline{b}_n\}$, then there is a linear transformation from L to M of the form

$$\underline{b}_i = \sum_{j=1}^n f_{ij} \underline{a}_j, \text{ for } i = 1, \dots, n,$$

where the coefficients $f_{ij} \in \mathbb{R}$. In this case, $L = M$ if, and only if, the transformation is unimodular, or in other words the f_{ij} are integers and the determinant of the f_{ij} is ± 1 . Proofs of these results are in [4], p.9ff.

In Lemma 11 we give a useful result on primitive sets. A proof may be found in [4], p.14, or [11], p.271, 272. The abbreviation, g.c.d. $(p_j, \dots, p_n)$, will mean the greatest common divisor of $p_j, \dots, p_n$.

Lemma 11. Let $\{a_1, \dots, a_n\}$ be a basis of a lattice L .

A necessary and sufficient condition that

$$\{a_1, \dots, a_{j-1}, (p_1 a_1 + \dots + p_n a_n)\}$$

be primitive in L when $1 \leq j \leq n$ is that not all of the integers p_1 are zero and g.c.d. $(p_j, \dots, p_n) = 1$. (When $j = 1$, it is understood that the set in question is

$$\{(p_1 a_1 + \dots + p_n a_n)\}.)$$

~~~~~

## 9 The Theory of Reduction.

The theory of reduction of symmetric convex bodies is concerned with the relation of a fixed symmetric convex body  $K$  with an arbitrary lattice  $L$ . More exactly, the theory is concerned with special bases of  $L$ , called  $K$ -reduced bases, which are, in a sense to be made precise below, the closest bases of  $L$  to  $\underline{0}$ . The definitions here follow those of Weyl in [10](a), p.279.

Let  $K$  be an  $n$ -dimensional symmetric convex body in  $\mathbb{R}^n$  and  $L$  an  $n$ -dimensional lattice in  $\mathbb{R}^n$ . Define a basis  $\{\underline{a}_1, \dots, \underline{a}_n\}$  of  $L$  and the positive numbers  $g_1, \dots, g_n$  inductively as follows:

- (i)  $\underline{a}_1 \in \text{Fr}(g_1 K)$  and no point of  $L$  lies in  $\text{Int}(g_1 K)$ ;
- (ii) let  $\underline{a}_1, \dots, \underline{a}_{j-1}$ , and  $g_1, \dots, g_{j-1}$  for  $j \leq n$  be defined. Define  $\underline{a}_j$  and  $g_j$  so that  $\{\underline{a}_1, \dots, \underline{a}_j\}$  is primitive in  $L$  and  $\underline{a}_j \in \text{Fr}(g_j K)$ , but if also  $\{\underline{a}_1, \dots, \underline{a}_{j-1}, \underline{b}\}$  is primitive in  $L$ , then  $\underline{b} \notin \text{Int}(g_j K)$ .

In this case,  $\{\underline{a}_1, \dots, \underline{a}_n\}$  is called a K-reduced basis of  $L$ . We will often speak of a K-reduced basis without mentioning the lattice  $L$ , but this is permissible since a basis determines a unique lattice. Neither the K-reduced basis nor the  $g_i$  are uniquely determined but it is easy to show, using Lemma 11 and some simple properties of  $K$  and  $L$ , that a K-reduced basis of  $L$  exists for each lattice  $L$ .

The definition of a K-reduced basis may be expressed very neatly in terms of the so-called distance function of  $K$ .

The distance function is a homogeneous (of degree one) function  $F$  defined on  $\mathbb{R}^n$  by

$$K = \{\underline{x} \mid F(\underline{x}) \leq 1\}.$$

The properties of this function are discussed in detail in [4] chpt. III, and also in [2] p.21. In particular  $F$  has the following properties.  $F$  is absolutely continuous;

$$\text{Int}K = \{\underline{x} \mid F(\underline{x}) < 1\}; \quad \text{Fr}K = \{\underline{x} \mid F(\underline{x}) = 1\};$$

$$gK = \{\underline{x} \mid F(\underline{x}) \leq g\}; \quad F \text{ is } \underline{\text{homogeneous}} \text{ so that}$$

$$F(t\underline{x}) = tF(\underline{x}) \text{ if } t > 0; \quad F \text{ is } \underline{\text{convex}} \text{ so that}$$

$$F(\underline{x} + \underline{y}) \leq F(\underline{x}) + F(\underline{y}); \quad K \text{ is symmetric if and only if}$$

$$F(\underline{x}) = F(-\underline{x}) \text{ for all } \underline{x} \in \mathbb{R}^n.$$

Let  $K$  have the distance function  $F$ , and let  $L$  have the basis  $\{\underline{a}_1, \dots, \underline{a}_n\}$ . Then it follows from the properties

of  $F$  that  $\{\underline{a}_1, \dots, \underline{a}_n\}$  is a  $K$ -reduced basis of  $L$  if

$$(i)' \quad F(\underline{a}_1) = \min_{\underline{a} \in L} F(\underline{a}), \quad \underline{a} \neq \underline{0} \quad (ii)' \quad \text{for each } j \text{ with}$$

$1 < j \leq n$ ,  $F(\underline{a}_j) \leq F(\underline{b})$  whenever  $\{\underline{a}_1, \dots, \underline{a}_{j-1}, \underline{b}\}$  is primitive in  $L$ .

Finally, by Lemma 11 we can write this definition in an even simpler form. The basis  $\{\underline{a}_1, \dots, \underline{a}_n\}$  of  $L$  is a

$K$ -reduced basis of  $L$  if, for each  $j$  with  $1 \leq j \leq n$ , we

have  $F(\underline{a}_j) \leq F(p_1 \underline{a}_1 + \dots + p_n \underline{a}_n)$  whenever  $\text{g.c.d.}(p_1, \dots, p_n) = 1$ .

It is useful now to relate the reduction theory of a convex body  $K$  to the Minkowski reduction theory for quadratic forms. The Minkowski reduction theory of quadratic forms is a special case in which the convex body  $K$  is a sphere (or more generally

an ellipsoid). In this case, many results on the minimum values of quadratic forms at integral points have been obtained. The connection with quadratic forms may be seen briefly as follows.

Let  $K$  be the unit sphere  $\sum_{i=1}^n x_i^2 \leq 1$  in  $R^n$ , so that the distance function  $F$  is given by  $F(\underline{x}) = \left( \sum_{i=1}^n x_i^2 \right)^{1/2}$ . The value of  $F$ , at a point  $\sum_{i=1}^n y_i \underline{a}_i$  of a lattice  $L$  with basis  $\{\underline{a}_1, \dots, \underline{a}_n\}$ , is  $F\left(\sum_{i=1}^n y_i \underline{a}_i\right)$  for integers  $y_1, \dots, y_n$ . If we write

$$G(\underline{y}) = F\left(\sum_{i=1}^n y_i \underline{a}_i\right),$$

then  $G(\underline{y})$  is clearly the square root of a positive definite, quadratic form in the  $n$ -variables,  $y_1, \dots, y_n$ . It is easy to show (see [11], p.272, 273) that any positive definite, quadratic form of  $n$ -variables may be obtained in this way from some lattice  $L$  in  $R^n$  by choosing  $\underline{a}_1, \dots, \underline{a}_n$  appropriately. A form which corresponds in this way to a  $K$ -reduced basis is called a reduced form (that is, reduced in the Minkowski sense), and two forms which correspond to different bases of the same lattice are called equivalent.

It now follows that any property of a  $K$ -reduced basis of a lattice corresponds to a property of the corresponding reduced, positive definite, quadratic form and vice versa.

In this way we see a connection with the values of positive definite, quadratic forms at integral points. The theory concerning reduction of quadratic forms is very extensive and goes much further than is indicated here. Van der Waerden in [11] gives a good account of the present state of the theory of reduction of positive definite, quadratic forms.

It is interesting to reconsider the  $K$ -reduced basis. An  $n$ -dimensional Minkowski space is  $R^n$  with a metric  $D$  given by  $D(\underline{x}, \underline{y}) = F(\underline{x} - \underline{y})$  where  $F$  is the distance function of a symmetric  $n$ -dimensional convex body. In particular,  $F(\underline{x}) = D(\underline{x}, \underline{o})$ . A  $K$ -reduced basis of a lattice is therefore defined in the Minkowski space in terms of the distances,  $D(\underline{x}, \underline{o})$ , of lattice points from  $\underline{o}$ . In the case when  $K$  is the sphere we are in ordinary Euclidean space and when  $K$  is not a sphere we have generalised the definition of reduced basis to a Minkowski space.

Theorem 5. Let  $K$  be a symmetric  $n$ -dimensional ellipsoid in  $R^n$  with distance function  $F$ . There exists a finite set  $P \subseteq R^n$ , so that if  $\underline{a}_1, \dots, \underline{a}_n$  are linearly independent points which satisfy for  $j = 1, \dots, n$ ,

$$F(\underline{a}_j) \leq F(\underline{a}_1 + \dots + \underline{a}_j)$$



# 10. The Two Finiteness Theorems.

Some results concerning reduced quadratic forms or in other words, concerning  $K$ -reduced bases when  $K$  is the sphere, are known to hold when  $K$  is any symmetric convex body (see [10] (a), (b), (c).). However two important finiteness theorems discovered by Minkowski for quadratic forms have not apparently been investigated in the general situation, except in  $R^2$ . In this section we investigate these finiteness theorems.

The first of the finiteness theorems states that all reduced positive definite quadratic forms are determined by a finite number of inequalities of a certain type. The second theorem states that there are only finitely many different unimodular transformations which transform a reduced quadratic form again into a reduced quadratic form. Weyl in [10] (a), (b), discusses these results under the names first and second finiteness theorems, and he simplifies parts of Minkowski's proof. Van der Waerden gives complete proofs in [11]. For reference we state these two results in their geometric formulation in Theorems 5 and 6.

Theorem 5. Let  $K$  be a symmetric  $n$ -dimensional ellipsoid in  $R^n$  with distance function  $F$ . There exists a finite set  $P \subseteq I^n$ , so that if  $\underline{a}_1, \dots, \underline{a}_n$  are linearly independent points which satisfy for  $j = 1, \dots, n$ ,

$$F(\underline{a}_j) \leq F(p_1 \underline{a}_1 + \dots + p_n \underline{a}_n)$$

whenever  $p \in P$  and  $\text{g.c.d. } (p_1, \dots, p_n) = 1$ , then  $\{\underline{a}_1, \dots, \underline{a}_n\}$  is a  $K$ -reduced basis.

~~~~~

Theorem 6. 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 unimodular transformations which transform a K -reduced basis again into a K -reduced basis.

~~~~~

Minkowski in [7], p.193, has shown that Theorem 5 also holds in  $R^2$  for all symmetric convex bodies. For completeness we reproduce Minkowski's result in Theorem 7.

Theorem 7. Let  $K$  be a symmetric two-dimensional convex body in  $R$  with distance function  $F$ . If  $\underline{a}_1$  and  $\underline{a}_2$  are linearly independent, then  $\{\underline{a}_1, \underline{a}_2\}$  is a  $K$ -reduced basis if and only if

$$F(\underline{a}_1 + \underline{a}_2) \geq F(\underline{a}_2)$$

$$F(\underline{a}_1 - \underline{a}_2) \geq F(\underline{a}_2)$$

$$F(\underline{a}_2) \geq F(\underline{a}_1).$$

Proof.

Any  $K$ -reduced basis  $\{\underline{a}_1, \underline{a}_2\}$  must satisfy the three conditions by definition.

By symmetry  $F(\underline{x}) = F(-\underline{x})$  for all  $\underline{x} \in \mathbb{R}^n$ , so we can assume in the following that  $p_2 \geq 0$ . Assume that the conditions of the hypothesis hold for the linearly independent pair  $\underline{a}_1$  and  $\underline{a}_2$ . Then using the convexity, homogeneity and symmetry of  $F$ , together with the three conditions of the hypothesis, we have when  $p_1 > 0$  and  $p_2 > 0$ ;

$$\begin{aligned} \text{for } p_1 > p_2, F(p_1 \underline{a}_1 + p_2 \underline{a}_2) &\geq p_1 F(\underline{a}_1 + \underline{a}_2) - (p_1 - p_2) F(\underline{a}_2) \\ &\geq p_2 F(\underline{a}_2); \end{aligned}$$

$$\text{for } p_1 = p_2, F(p_1 \underline{a}_1 + p_2 \underline{a}_2) = p_2 F(\underline{a}_1 + \underline{a}_2) \geq F(\underline{a}_2);$$

$$\begin{aligned} \text{for } p_1 < p_2, F(p_1 \underline{a}_1 + p_2 \underline{a}_2) &\geq p_2 F(\underline{a}_1 + \underline{a}_2) - (p_2 - p_1) F(\underline{a}_1) \\ &\geq p_1 F(\underline{a}_1). \end{aligned}$$

We have from the above inequalities, using the symmetry of  $K$ , that

$$F(p_1 \underline{a}_1 + p_2 \underline{a}_2) \geq F(\underline{a}_1) \quad \text{and}$$

$$F(p_1 \underline{a}_1 + \underline{a}_2) \geq F(\underline{a}_2)$$

for all non-zero integers,  $p_1$  and  $p_2$ . Hence, by the definition,  $\{\underline{a}_1, \underline{a}_2\}$  is a  $K$ -reduced basis.

~~~~~

Theorem 6 surprisingly does not hold in $\mathbb{R}^2$ for all convex bodies, but only for those bodies which have no straight pieces on their frontier, as we now show in Theorem 8.

Theorem 8. Let K be a symmetric two-dimensional convex body in R^2 with distance function F . There are finitely many unimodular transformations which transform a K -reduced basis again into a K -reduced basis if, and only if, every tac plane of K is regular.

Proof.

Let every tac plane of K be regular and $\{\underline{a}_1, \underline{a}_2\}$ be a K -reduced basis of a lattice L . As in the proof of Theorem 7, we obtain when $p_1 > 0$ and $p_2 > 0$:

$$\begin{aligned} \text{for } p_1 > p_2, F(\pm p_1 \underline{a}_1 + p_2 \underline{a}_2) &\geq p_1 F(\pm \underline{a}_1 + \underline{a}_2) - (p_1 - p_2) F(\underline{a}_2) \\ &\geq p_2 F(\underline{a}_2); \quad \dots (1) \end{aligned}$$

$$\text{for } p_1 = p_2, F(\pm p_1 \underline{a}_1 + p_2 \underline{a}_2) \geq F(\pm \underline{a}_1 + \underline{a}_2); \quad \dots (2)$$

$$\begin{aligned} \text{for } p_1 < p_2, F(\pm p_1 \underline{a}_1 + p_2 \underline{a}_2) &\geq p_2 F(\pm \underline{a}_1 + \underline{a}_2) - (p_2 - p_1) F(\underline{a}_1) \\ &\geq p_1 F(\underline{a}_1). \quad \dots (3) \end{aligned}$$

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

$$\begin{aligned} F(\pm p_1 \underline{a}_1 + p_2 \underline{a}_2) &\geq p_2 F(\underline{a}_2) - p_1 F(\underline{a}_1) \\ &\geq (p_2 - p_1) F(\underline{a}_2) \quad \dots (4) \end{aligned}$$

From (1), it follows that $F(\pm p_1 \underline{a}_1 + p_2 \underline{a}_2) > F(\underline{a}_2)$ unless both $p_2 = 1$ and $F(\pm \underline{a}_1 + \underline{a}_2) = F(\underline{a}_2)$. From (2), we find that $F(\pm p_1 \underline{a}_1 + p_2 \underline{a}_2) > F(\underline{a}_2)$ unless $p_1 = p_2 = 1$.

From (3), $F(\pm p_1 \underline{a}_1 + p_2 \underline{a}_2) > F(\underline{a}_1)$ unless $p_1 = 1$, and when $p_1 = 1$, by (4), $F(\pm \underline{a}_1 + p_2 \underline{a}_2) > F(\underline{a}_2)$ unless $p_2 \leq 2$. It follows from these results and the definition of K-reduced basis that the only possible candidates for a K-reduced basis of L are

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

$$\pm p_1 \underline{a}_1 \pm \underline{a}_2, \text{ where } p_1 \geq 2.$$

In the last case we also found that $F(\underline{a}_2) = F(\pm \underline{a}_1 + \underline{a}_2)$, and since we also have $F(\underline{a}_2) = F(\pm p_1 \underline{a}_1 \pm \underline{a}_2)$ (for appropriate choice of signs), there are three linearly dependent points on $\text{Fr}K$. This means that K has a non-regular tac plane, 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

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

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

Now let us assume that K has a non-regular tac plane so there is a segment $\overline{ab}$ in $\text{Fr}K$. Choose a sequence of lattices L_m with respective bases $\{\underline{a}_1^m, \underline{a}_2^m\}$ as follows:

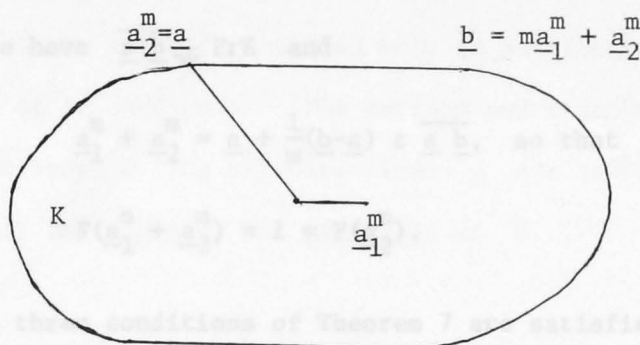


Diagram 10

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

We now show using Theorem 7 that $\{\underline{a}_1^m, \underline{a}_2^m\}$ is a K -reduced basis for all m sufficiently large. We have first of all

$$F(\underline{a}) \geq \frac{1}{m}F(\underline{b} - \underline{a})$$

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

$$F(\underline{a}_2^m) \geq F(\underline{a}_1^m).$$

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

$$\begin{aligned} F(\underline{a}_1^m - \underline{a}_2^m) &= F\left(\left(\frac{m+1}{m}\right)\underline{a} - \frac{1}{m}\underline{b}\right) \\ &\geq \left(\frac{m+1}{m}\right)F(\underline{a}) - \frac{1}{m}F(\underline{b}). \end{aligned}$$

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

$$F(\underline{a}_1^m - \underline{a}_2^m) \geq F(\underline{a}_2^m).$$

Finally, we have $\overline{a \ b} \subseteq \text{FrK}$ and

$$\underline{a}_1^m + \underline{a}_2^m = \underline{a} + \frac{1}{m}(\underline{b} - \underline{a}) \in \overline{a \ b}, \text{ so that}$$

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

Hence, the three conditions of Theorem 7 are satisfied and

$\{\underline{a}_1^m, \underline{a}_2^m\}$ is a K -reduced basis of L_m when $m \geq m_0$.

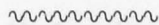
Similarly, $\{\underline{a}_1^m, \underline{b}\}$ is a K -reduced basis of L_m when $m \geq m_0$.

The transformation from the basis $\{\underline{a}_1^m, \underline{a}_2^m\}$ to the basis

$\{\underline{a}_1^m, \underline{b}\}$ has the matrix

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

Infinitely many of these transformations are different for $m \geq m_0$. Hence when FrK contains a segment, there are infinitely many unimodular transformations which transform a K -reduced basis into a K -reduced basis.



For $n > 2$, the generalisations of Theorems 5 and 6 have not apparently been investigated for general convex bodies. In fact, as we show in Theorems 9 and 10, the position for $n > 2$ is quite different from when $n = 2$, and neither of the finiteness theorems holds for a convex body other than an ellipsoid.

In Theorem 9 the width of a convex body in a direction $\underline{u}$ is defined as in section 4. The maximum and minimum width of a convex body K for all directions $\underline{u}$ are called respectively the diameter and thickness of K .

Theorem 9. For $n \geq 3$ let K be an n -dimensional, symmetric (about $\underline{o}$), convex body which has the distance function F . Let there be a finite set $P \subseteq I^n$, so that if $\underline{a}_1, \dots, \underline{a}_n$ are linearly independent points satisfying, for $j = 1, \dots, n$,

$$F(\underline{a}_j) \leq F(p_1 \underline{a}_1 + \dots + p_n \underline{a}_n) \quad \dots (A)$$

whenever $\underline{p} \in P$ and $\text{g.c.d.}(p_1, \dots, p_n) = 1$, then $\{\underline{a}_1, \dots, \underline{a}_n\}$ is a K -reduced basis. Then K is an ellipsoid.

Proof.

We first prove the theorem for $n = 3$. 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 characterise 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 U and U_0 be two parallel planes where U is a fixed regular tac plane of K with outer normal $\underline{w}$ and $\underline{o} \in U_0$.

Let $D_0 = U_0 \cap K$. Let $h > 0$ be so that: if U' is the tac plane of hK with outer normal $\underline{w}$, then the diameter of $U' \cap K$ is equal to $\frac{1}{4}$ of the thickness of D_0 . This condition in fact defines h uniquely with $h < 1$, since the diameter of $U' \cap K$ must decrease monotonically and continuously to zero as the distance between U' and U decreases to zero. Now define

$$j(\underline{w}) = \max(h, \frac{2}{3}), \text{ so } j(\underline{w}) < 1.$$

It is not hard to show that j is a continuous function of $\underline{w}$ (for those $\underline{w}$ for which it exists).

Let U_1 be any plane parallel to U not intersecting $\text{Int}(j(\underline{w})K)$, and let $D_1 = U_1 \cap K$. Let V_1 and V_2 be two distinct parallel tac planes of D_0 (in U_0) at the points $\underline{b}_1$ and $\underline{b}_2$. Let W_1 and W_2 be distinct tac planes of D_1 (in U_1) at $\underline{c}_1$ and $\underline{c}_2$, which are both parallel to V_1 and V_2 and similarly situated with respect to D_1 and D_0 . (See Diagram 11.)

If $\overline{\underline{b}_1 \underline{b}_2}$ is parallel to $\overline{\underline{c}_1 \underline{c}_2}$ for every choice of V_1, V_2, W_1 and W_2 when all four are regular tac planes, then $D_0 \sim D_1$ by Theorem 1. It is this result we will eventually obtain.

Assume for some choice of V_1, V_2, W_1 and W_2 , all regular, we have $\overline{\underline{b}_1 \underline{b}_2}$ is not parallel to $\overline{\underline{c}_1 \underline{c}_2}$. We now choose a sequence of lattices L_m with respective bases $\{a_1^m, a_2^m, a_3^m\}$.

Notice that $\underline{b}_1 = -\underline{b}_2$, and any result concerning the plane U_1 also applies to the plane $(-1)U_1$, by the symmetry of K .

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

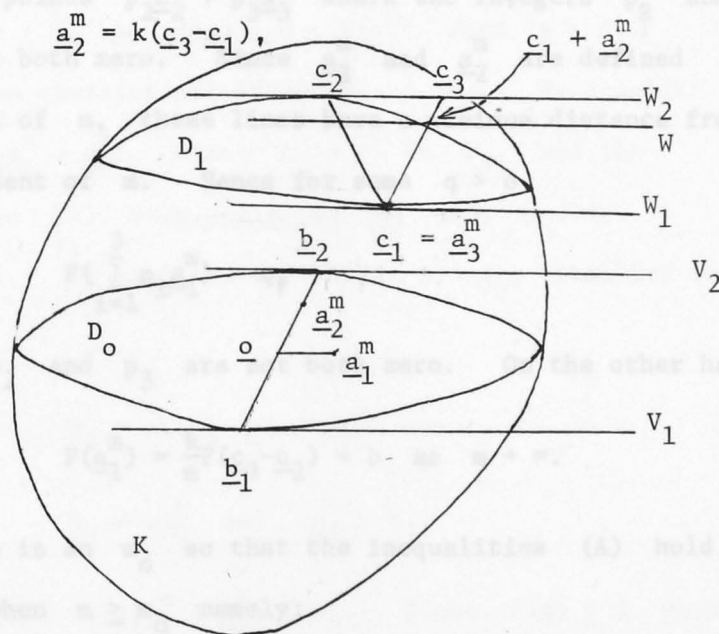


Diagram 11

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

(i) $\frac{1}{2} < k < 1$; (ii) $\underline{c}_1 + \underline{a}_2^m \notin K$. Condition (ii)

may be satisfied by choosing k sufficiently close to 1,

since $\underline{c}_3 \notin K$ and $\underline{c}_1 + \underline{a}_2^m = k\underline{c}_3 + \underline{c}_1(1-k) \rightarrow \underline{c}_3$ as $k \rightarrow 1$.

Define $\underline{a}_3^m = \underline{c}_1$ (again independent of m) and

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

We will now show that all but a finite number of the inequalities

(A) of the hypothesis are satisfied by the linearly independent points $\underline{a}_1^m, \underline{a}_2^m$ and $\underline{a}_3^m$ when m is large.

First consider $\underline{a}_1^m$. Every point of L_m , which is not a multiple of $\underline{a}_1^m$ lies on a line parallel to V_1 , through one of the points $p_2 \underline{a}_2^m + p_3 \underline{a}_3^m$ where the integers p_2 and p_3 are not both zero. Since $\underline{a}_3^m$ and $\underline{a}_2^m$ are defined independent of m , these lines have a minimum distance from $\underline{0}$ independent of m . Hence for some $q > 0$

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

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

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

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

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

for all $\underline{p} \in I^3$, whenever $m \geq m_0$.

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

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

By our assumption on the widths of D_0 and D_1 ,

$$|c_3 - c_1| \leq \frac{1}{4}|b_2 - b_1| = \frac{1}{2}|b_2|.$$

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

$$F(\underline{a}_2^m) \leq \frac{1}{2}.$$

It follows that we need only investigate points $\sum_{i=1}^3 p_i \underline{a}_i^m$ in $\frac{1}{2}K$. However U_1 does not intersect $\text{Int}(j(\underline{w})K)$

where $j(\underline{w}) \geq \frac{2}{3}$, so $F(\underline{a}) > \frac{1}{2} \geq F(\underline{a}_2^m)$ when $\underline{a} \in D_1$.

Hence we can restrict our attention to D_0 . We consider

points $(p_1 \underline{a}_1^m + \underline{a}_2^m)$, since $p_3 = 0$ in U_0 , and the

inequalities (A) only apply to $\underline{a}_2^m$ when g.c.d.

$(p_2, p_3) = 1$. We know, by the choice of $\underline{c}_3$, that for some

$q > 0$

$$\underline{b}_2 = qk(\underline{c}_3 - \underline{c}_1) = q\underline{a}_2^m, \text{ so}$$

$$\underline{b}_2 = q\underline{a}_2^m \text{ and } q\underline{a}_2^m \in V_2.$$

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

$\underline{a} \in V_2$,

$$F(q(p_1 \underline{a}_1^m + \underline{a}_2^m)) \geq 1 \text{ and so}$$

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

We have shown that the inequalities (A) hold for $\underline{a}_2^m$ and for

all m , namely: whenever g.c.d. $(p_2, p_3) = 1$,

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

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

$$\underline{a}_3^m + p_2 \underline{a}_2^m = \underline{c}_1 + p_2 k (\underline{c}_3 - \underline{c}_1) \quad \text{where } p_2 \in I.$$

When $p_2 = 0$, this line is W_1 through $\underline{c}_1$; when $p_2 = 1$, it is W through $\underline{a}_2^m + \underline{a}_3^m$ and when $p_2 = 1/k$ (not an integer), it is W_2 through $\underline{c}_3$. Since by the construction of k $1/k < 2$, the only such line which intersects $\text{Int}D_1$ is W . Therefore we need consider only points of $(D_1 \cap W) = (W \cap K)$.

Since $\underline{a}_2^m + \underline{a}_3^m \notin K$, let $\underline{c}_4$ be the nearest point of $(W \cap K)$ to $\underline{a}_2^m + \underline{a}_3^m$. The distance between successive lattice points on W is $|\underline{a}_1^m|$, so the number of lattice points between $\underline{a}_2^m + \underline{a}_3^m$ and $\underline{c}_4$ is at least

$$\frac{|\underline{c}_4, \underline{a}_2^m + \underline{a}_3^m|}{|\underline{a}_1^m|} = \frac{m |\underline{c}_4, \underline{a}_2^m + \underline{a}_3^m|}{k |\underline{c}_3 - \underline{c}_2|} = mt, \quad \text{say.}$$

t is independent of m since $\underline{a}_2^m$ and $\underline{a}_3^m$ are independent of m and $t > 0$. Hence, all lattice points of L_m in $W \cap D_1$ must be of the form

$$p_1 \underline{a}_1^m + \underline{a}_2^m + \underline{a}_3^m, \quad \text{where } |p_1| \geq mt.$$

We have shown therefore that

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

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

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

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

whenever $p \in I^3$ and $\text{g.c.d.}(p_j, \dots, p_n) = 1$, except when $p_2 = p_3 = 1$ and $|p_1| \geq mt$. By choosing m large enough, say $m \geq m_1 \geq m_0$, we can ensure that none of the p , for which the above inequalities fail, lie in the finite set P of the hypothesis. Hence for $m \geq m_1$, the basis $\{\underline{a}_1^m, \underline{a}_2^m, \underline{a}_3^m\}$ satisfies all of the finite set of the inequalities (A). However $\{\underline{a}_1^m, \underline{a}_2^m, \underline{a}_3^m\}$ is not K -reduced for $m \geq m_1$, since the point

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

lies in $\text{Int}K$, so that

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

Hence we have a contradiction of the initial assumption that

$\overline{\underline{b}_1 \underline{b}_2}$ is not parallel to $\overline{\underline{c}_1 \underline{c}_2}$. As previously indicated, this leads us to $D_0 \sim D_1$.

We have shown, for each initial choice of the tac plane U , that $D_0 \sim D_1$ whenever U_1 does not intersect $\text{Int}(j(\underline{w})K)$. In order to apply Corollary 4 (page 38), we next show that no tac plane intersects K in just a segment.

Assume that a tac plane T with outer normal $\underline{w}$ intersects K in just a segment $\overline{d_1 d_2}$ ($d_1 \neq d_2$). Let U_i , $i = 2, 3, \dots$ be planes parallel to D at a perpendicular distance of $1/i$ from T . We next define points and planes related to each U_i in the same way as we defined points and planes related to U_1 at the beginning of this proof. Let U_0 be the plane parallel to T with $\underline{o} \in U_0$, $D_0 = U_0 \cap K$, and, V_1 and V_2 be parallel tac planes of D_0 (in U_0). For each i , let $D_i = U_i \cap K$, and let W_{1i} and W_{2i} be tac planes 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 $\overline{d_1 d_2}$, then clearly $d_i \rightarrow 0$ as $i \rightarrow \infty$. Hence if we choose V_1 sufficiently close in direction to $\overline{d_1 d_2}$, yet not parallel to $\overline{d_1 d_2}$, then we can find an i_0 so that $d_i \leq \frac{1}{4}d$ if $i > i_0$. 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 tac planes of D_i are not regular. Let $\{c_{-1i}\} = W_{1i} \cap D_i$, $\{c_{-2i}\} = W_{2i} \cap D_i$, $\{b_{-1}\} = V_1 \cap D_0$, and $\{b_{-2}\} = V_2 \cap D_0$. Finally in addition to the above conditions, we can clearly assume that $\overline{b_{-1} b_{-2}}$ is not parallel to

$\overline{d_1 d_2}$. V_1 and V_2 are now fixed.

Note that $U_i \cap \text{Int}(\frac{2}{3}K)$ is empty for $i > i_0$. Each D_i , with $i > i_0$, now satisfies conditions by which we can show (with $j(\underline{w}) = \frac{2}{3}$) that $\overline{c_{1i} c_{2i}}$ is parallel to $\overline{b_1 b_2}$, in exactly the same way as we previously showed that the chord $\overline{c_1 c_2}$ of D_1 (in the previous notation) is parallel to $\overline{b_1 b_2}$ in D_0 . (Even though $j(\underline{w})$ here does not satisfy the complete condition satisfied by $j(\underline{w})$ (page 59) in the previous proof, the condition $d_i < \frac{1}{4}d_1$ is sufficient to follow through the proof for the particular choice of V_1 and V_2 .)

The sequence $\{c_{1i}\}$ clearly has a limit point $\underline{d}$ where $\underline{d} \in T \cap K = \overline{d_1 d_2}$ and we show that $\underline{d} = \underline{d_1}$ or $\underline{d_2}$. Project all of the sets in question from $\underline{o}$ onto T , and denote the projected sets by an asterisk. Then clearly $D_1^* \supseteq D_2^* \supseteq \dots \supseteq \overline{d_1 d_2}$, and $c_{1i}^* \rightarrow \underline{d}$ as $i \rightarrow \infty$. Now W_{1i}^* cannot intersect the interior of the segment $\overline{d_1 d_2}$ since $D_i^* \supseteq \overline{d_1 d_2}$, and consequently $\underline{d} = \underline{d_1}$ or $\underline{d_2}$, say $\underline{d} = \underline{d_1}$. Similarly $c_{2i} \rightarrow \underline{d_2}$ as $i \rightarrow \infty$. Hence the direction of $\overline{c_{1i} c_{2i}}$ approaches that of $\overline{d_1 d_2}$ as $i \rightarrow \infty$, yet $\overline{c_{1i} c_{2i}}$ is parallel to $\overline{b_1 b_2}$ for $i > i_0$ and $\overline{b_1 b_2}$ is not parallel to $\overline{d_1 d_2}$. This is a contradiction. Hence $T \cap K$ is not just a segment.

Now we can apply Corollary 4 to show all tac planes of K are regular. Then $j(\underline{w})$, as defined on page 59 is continuous for all $\underline{w}$, and $j(\underline{w}) < 1$, so by Corollary 5 (page 41), K is an ellipsoid. This completes the three-dimensional case.

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 $\underline{o}$, and let $J = K \cap U$. Clearly U can be identified with $\mathbb{R}^{n-1}$ so that J is an $(n-1)$ -dimensional convex body. Let

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

We now show that J satisfies the hypothesis of this theorem with P replaced by P'

Let $\underline{a}_1, \dots, \underline{a}_{n-1}$ be linearly independent points in U satisfying for $j = 1, \dots, n-1$,

$$F(\underline{a}_j) \leq F(p_1 \underline{a}_1 + \dots + p_{n-1} \underline{a}_{n-1}) \quad \dots (1)$$

whenever $(p_1, \dots, p_{n-1}) \in P'$ and $\text{g.c.d.}(p_1, \dots, p_{n-1}) = 1$.

We must show that $\underline{a}_1, \dots, \underline{a}_{n-1}$ is a J -reduced basis.

Choose a hyperplane V in $\mathbb{R}^n$, parallel to U , which does not intersect the set $F(\underline{x}) \leq F(\underline{a}_1)$ for $\underline{x} \in \mathbb{R}^n$, and $i = 1, \dots, n-1$.

Define $\underline{a}_n \in V$ by

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

By the construction of V , none of the planes parallel to V ,

through points $p \underline{a}_n$, for $p \in I$, can intersect the sets

$F(\underline{x}) \leq F(\underline{a}_1)$ for $i = 1, \dots, n-1$. Hence, for $j = 1, \dots, n$,

$$F(\underline{a}_j) \leq F(p_1 \underline{a}_1 + \dots + p_n \underline{a}_n) \quad \dots (2)$$

for all $(p_1, \dots, p_n) \in \mathbb{Z}^n$ with $p_n \neq 0$. From equations (1) and (2) we find, for $j = 1, \dots, n$,

$$F(\underline{a}_j) \leq F(p_1 \underline{a}_1 + \dots + p_n \underline{a}_n)$$

for all $\underline{p} \in P$, with $\text{g.c.d.}(p_1, \dots, p_n) = 1$. Since K satisfies the hypothesis of this theorem, it follows that $\{\underline{a}_1, \dots, \underline{a}_n\}$ is a K -reduced basis. Hence we have, in particular, by the definition of a K -reduced basis, for $j = 1, \dots, n-1$,

$$F(\underline{a}_j) \leq F(p_1 \underline{a}_1 + \dots + p_{n-1} \underline{a}_{n-1})$$

whenever $\text{g.c.d.}(p_1, \dots, p_{n-1}) = 1$. This shows that $\{\underline{a}_1, \dots, \underline{a}_{n-1}\}$ is a J -reduced basis.

We have now shown that J satisfies the hypothesis of this theorem, and so by the induction argument, J is an ellipsoid. This result is true for each choice of the hyperplane U through $\underline{o}$, so by Theorem 2 of section 5, K is an ellipsoid. Hence the theorem follows for all n by the induction principle.

~~~~~

Theorem 10. For  $n \geq 3$  let  $K$  be an  $n$ -dimensional, symmetric (about  $\underline{o}$ ), convex body in  $\mathbb{R}^n$ . If all  $K$ -reduced bases of all  $n$ -dimensional lattices in  $\mathbb{R}^n$  are considered, then let there be only finitely many, unimodular transformations which transform a  $K$ -reduced basis again into a  $K$ -reduced basis. Then  $K$  is an ellipsoid.

Proof.

The proof of this theorem is very similar to the proof of Theorem 9, and many of the details of this proof are referred to Theorem 9. We first consider the case where  $n = 3$ .

Let  $U$  be a regular tac plane of  $K$  and let  $U_0, j(\underline{w}), U_1, D_0, D_1, W_1, W_2, V_1, V_2, \underline{b}_1, \underline{b}_2, \underline{c}_1, \underline{c}_2$  and  $\underline{c}_3$  be defined as in Theorem 9 (see Diagram 12). We assume that, as in Theorem 9, for some choice of  $V_1, V_2, W_1$  and  $W_2$ , all regular, we have  $\underline{c}_2 \neq \underline{c}_3$ . We now define a sequence of lattices  $L_m$  with respective bases  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{a}_3^m\}$ .

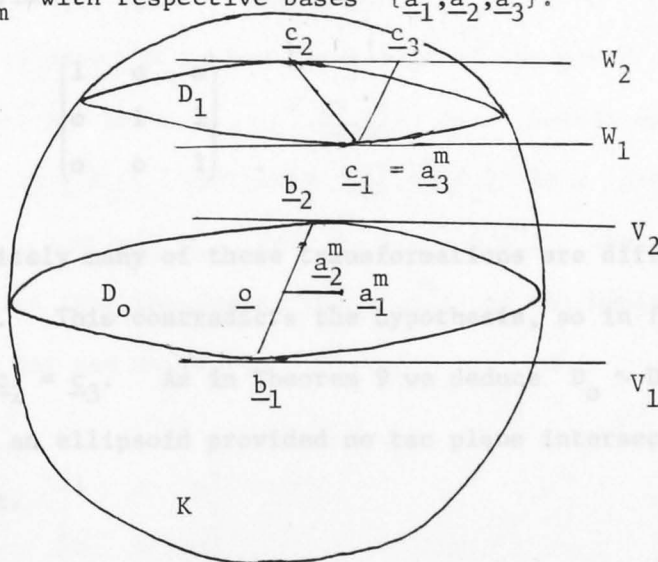


Diagram 12

Define

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

The only difference between the situation here and that of Theorem 9 is that the line  $W$  defined in Theorem 9 has now become  $W_2$ . Hence we can show, as in Theorem 9 (but without

the exceptional points on the line  $W$ ), that for  $m \geq m_0$  and for  $j = 1, 2, 3$ ,

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

whenever  $\text{g.c.d.}(p_1, \dots, p_3) = 1$ . Hence  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{a}_3^m\}$  is a  $K$ -reduced basis of  $L_m$  when  $m \geq m_0$ . However,  $\underline{c}_2 \in L_m$ , since  $\underline{c}_2 = m \underline{a}_1^m + \underline{a}_2^m + \underline{a}_3^m$ , and  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{c}_2\}$  is a basis of  $L_m$  by Lemma 11. Yet  $F(\underline{c}_2) = F(\underline{a}_3^m) = 1$ , so  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{c}_2\}$  is also a  $K$ -reduced basis of  $L_m$ , for  $m \geq m_0$ . The transformation from the basis  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{a}_3^m\}$  to the basis  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{c}_2\}$  has the matrix

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

Hence infinitely many of these transformations are different for  $m \geq m_0$ . This contradicts the hypothesis, so in fact we must have  $\underline{c}_2 = \underline{c}_3$ . As in Theorem 9 we deduce  $D_0 \sim D_1$ , and that  $K$  is an ellipsoid provided no tac plane intersects  $K$  in a segment.

Assume therefore that the tac plane  $U$  of  $K$  intersects  $K$  in a segment  $\overline{\underline{d}_1 \underline{d}_2}$ . We define  $U_0, D_0, V_1, V_2, \underline{b}_1$  and  $\underline{b}_2$  with  $V_1$  and  $V_2$  regular, as in the first part of this proof (see Diagram 13). We define a sequence of lattices  $L_m$  with respective bases  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{a}_3^m\}$ .



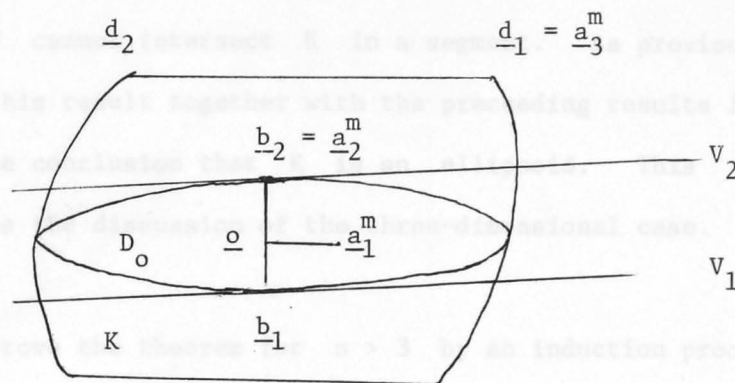


Diagram 13

Define

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

It is easy to show, as in the first part of the proof of this theorem, that for some  $m_0$ ,  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{a}_3^m\}$  is a  $K$ -reduced basis of  $L_m$  for  $m \geq m_0$ . Similarly  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{d}_2\}$  is a  $K$ -reduced basis of  $L_m$  for  $m \geq m_0$ , and  $\underline{d}_2 = m\underline{a}_1^m + \underline{a}_3^m$ . The transformation from the basis  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{a}_3^m\}$  to the basis  $\{\underline{a}_1^m, \underline{a}_2^m, \underline{d}_2\}$  has the matrix

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

Infinitely many of these transformations are different for  $m \geq m_0$ . This contradicts the hypothesis.

Hence  $U$  cannot intersect  $K$  in a segment. As previously noted, this result together with the preceeding 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  $\underline{o}$  and let  $J = U \cap K$ . We now show that the  $(n-1)$ -dimensional convex body  $J$  satisfies the hypothesis of this theorem.

Let  $\{\underline{a}_1, \dots, \underline{a}_{n-1}\}$  and  $\{\underline{b}_1, \dots, \underline{b}_{n-1}\}$  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 does not intersect the sets  $F(\underline{x}) \leq F(\underline{a}_{n-1})$  and  $F(\underline{x}) \leq F(\underline{b}_{n-1})$  for  $\underline{x} \in R^n$ , and define  $\underline{a}_n$  by

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

Then, as in the previous proof of Theorem 9,  $\{\underline{a}_1, \dots, \underline{a}_n\}$  and  $\{\underline{b}_1, \dots, \underline{b}_{n-1}, \underline{a}_n\}$  are both  $K$ -reduced bases. The transformation from the first basis to the second has the matrix

$$\begin{pmatrix} f_{11} & \dots & f_{1,n-1} & 0 \\ \vdots & & \vdots & \vdots \\ f_{n-1,1} & \dots & f_{n,n} & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

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 argument. It follows from Theorem 2 of section 5 that  $K$  is an ellipsoid, and so the theorem is proved for all  $n$  by the induction principle.

- [10] Artin, E. 1941: "The reduction for arithmetical equivalence". Trans. Amer. Math. Soc., 48, 126-154, 1940.  
 (a): "The theory of reduction for arithmetical equivalence." Trans. Amer. Math. Soc., 51, 203-231, 1942.  
 (b): "On geometry of numbers." Proc. Lond. Math. Soc., 41, 280-289, 1942.
- [11] van der Waerden, S.J. "Die Reduktionstheorie der positiven quadratischen Formen". Acta Math., 26, 263-309, 1936.

### References

- [1] Apostol, T.M. Mathematical Analysis. A Modern Approach to Advanced Calculus. Addison-Wesley, U.S.A., 1957.
- [2] Bonnesen, T. and Fenchel W. Theorie der konvexen Körper. Reprint by Chelsea, New York, 1948.
- [3] Busemann, H. Geometry of Geodesics. Academic Press, New York, 1955.
- [4] Cassels, J.W.S. An Introduction to the Geometry of Numbers. Springer-Verlag, Berlin, 1959.
- [5] Edwards, R.E. Functional Analysis: Theory and Applications. Holt, Rinehart and Winston, U.S.A., 1965.
- [6] Hammer, P.C. "Convex curves of constant Minkowski breadth". Proc. Sympos. Pure Math. VII, Convexity, 291-304. Amer. Math. Soc, 1963.
- [7] Minkowski, H. Geometrie der Zahlen. Reprint by Chelsea, New York, 1953.
- [8] Royden, H.L. Real Analysis. Macmillan, New York, 1963.
- [9] Süss, W. "Kennzeichnende Eigenschaften der Kugel als Folgerung eines Brouwerschen Fixpunktsatzes". Comm. Math. Helv., 20, 61-64, 1947.
- [10] Weyl, H. (a): "The theory of reduction for arithmetical equivalence". Trans. Amer. Math. Soc., 48, 126-164, 1940.  
 (b): "The theory of reduction for arithmetical equivalence. II". Trans. Amer. Math. Soc. 51, 203-231, 1942.  
 (c): "On geometry of numbers" Proc. Lond. Math. Soc., 47, 268-289, 1942.
- [11] van der Waerden, B.L. "Die Reduktionstheorie der positiven quadratischen Formen". Acta Math., 96, 265-309, 1956.