Carl Ludwig Siegel

Lectures on the Geometry of Numbers

数的几何讲义

Springer

世界图书出版公司
www.wpcbj.com.cn

Carl Ludwig Siegel

Lectures on the Geometry of Numbers

Notes by B. Friedman

Rewritten by

Komaravolu Chandrasekharan

with the Assistance of Rudolf Suter

With 35 Figures

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong

图书在版编目（CIP）数据

数的几何讲义 = Lectures on the Geometry of Numbers：英文/（德）西格尔（Siegel，C. L.）著.—影印本.—北京：世界图书出版公司北京公司，2015.8
ISBN 978-7-5192-0024-4

Ⅰ.①数…　Ⅱ.①西…　Ⅲ.①几何—英文　Ⅳ.①O18

中国版本图书馆 CIP 数据核字（2015）第 207391 号

Lectures on the Geometry of Numbers
数的几何讲义

著　　者：Carl Ludwig Siegel
责任编辑：刘　慧　岳利青
装帧设计：任志远

出版发行：世界图书出版公司北京公司
地　　址：北京市东城区朝内大街 137 号
邮　　编：100010
电　　话：010-64038355（发行）　64015580（客服）　64033507（总编室）
网　　址：http://www.wpcbj.com.cn
邮　　箱：wpcbjst@vip.163.com
销　　售：新华书店
印　　刷：三河市国英印务有限公司
开　　本：711mm×1245 mm　1/24
印　　张：7.5
字　　数：145 千
版　　次：2016 年 1 月第 1 版　　2016 年 1 月第 1 次印刷
版权登记：01-2015-4928
ISBN 978-7-5192-0024-4　　　　**定价**：35.00 元

Siegel · Lectures on the Geometry of Numbers

Komaravolu Chandrasekharan
Mathematik, ETH Zürich
CH-8092 Zürich, Switzerland

Mathematics Subject Classification (1980):
01-XX, 11-XX, 12-XX, 15-XX, 20-XX, 32-XX, 51-XX, 52-XX

ISBN 3-540-50629-2 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-50629-2 Springer-Verlag New York Berlin Heidelberg

Library of Congress Cataloging-in-Publication Data.
Siegel, Carl Ludwig, 1896–1981
Lectures on the geometry of numbers / Carl Ludwig Siegel; notes by B. Friedman; rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter. p. cm.
Bibliography: p. Includes index.
ISBN 0-387-50629-2 (U.S. : alk. paper)
1. Geometry of numbers. I. Chandrasekharan, K. (Komaravolu), 1920– .
II. Suter, Rudolf, 1963– . III. Title. QA241.5.S54 1989 512'.5 – dc19 89-5946 CIP

Reprint from English language edition:
Lectures on the Geometry of Numbers
by Carl Ludwig Siegel

Preface

Carl Ludwig Siegel lectured on the *Geometry of Numbers* at New York University during 1945–46. There were hardly any books on the subject at that time other than Minkowski's original one. The freshness of his approach still lingers, and his presentation has its attractions for the aspiring young mathematician.

When he received a request, many years later, for permission to reissue the notes of those lectures, transcribed by the late B. Friedman, he declined. Those who know of Siegel's insistence on the expurgation of the first printing of his lecture notes on *Transcendental Numbers*, or of his insistence on the dissociation of his name from a projected English translation of his lecture notes on *Analytische Zahlentheorie* (Göttingen, 1963/64), which had therefore to be abandoned, need hardly be told that he had his own requirements.

We had occasion to discuss the matter further, and it was agreed that the notes should be published only after they had been checked, corrected, and rewritten, and he handed over his personal copy to me. I found that the task of revision required far more attention to detail than I had at first glance thought necessary. Other avocations prevented me from completing the work until the summer of 1987, when it happened that Rudolf Suter got actively interested in what I had been trying to carry out. His helpful and critical comments came to me as an unexpected stimulus, and the present version is the result. It is a pleasure for me to acknowledge Suter's assistance.

Admirers of Siegel's style can scarcely fail to notice his uncanny skill, and perspicuity in argument, with an occasional flash of wit, as they progress with the reading.

E.T.H. Zürich

31 March 1988 K. Chandrasekharan

Table of Contents

Chapter I
Minkowski's Two Theorems

Chapter II

Linear Inequalities

Chapter III

Theory of Reduction

Chapter I

Minkowski's Two Theorems

Lectures I to IV

Lecture I

§ 1. Convex sets

Consider an n-dimensional real Euclidean space $\mathbb{R}^n$, $n \geq 1$. Assume that a rectangular coordinate system with origin at some point O is set up in $\mathbb{R}^n$, so that the coordinates of any point $P \in \mathbb{R}^n$ are $x_1, \ldots, x_n$. For simplicity we shall represent the point P by the vector $x = (x_1, \ldots, x_n)$. The origin O is then represented by the zero-vector $0 = (0, \ldots, 0)$.

A non-empty set $\mathcal{L}$ contained in $\mathbb{R}^n$ is called a linear manifold in $\mathbb{R}^n$, if whenever any two different points P and Q belong to $\mathcal{L}$, the infinite straight line passing through P and Q belongs to $\mathcal{L}$. Analytically the definition can be formulated as follows:

Let x be the vector associated with P, and y the vector associated with Q. Then $\mathcal{L}$ is a linear manifold, if whenever it contains P and Q, it contains every point represented by a vector of the form $\lambda x + \mu y$, where λ, μ are arbitrary real numbers, such that $\lambda + \mu = 1$.

Any linear manifold $\mathcal{L}$ has a dimension m, which is an integer not greater than n, and which can be found as follows.

Let P_0 be a point in $\mathcal{L}$. If $\mathcal{L}$ contains no other point, then $m = 0$. Otherwise let P_1 be another point in $\mathcal{L}$. Then all points on the line passing through P_0, P_1 belong to $\mathcal{L}$. If $\mathcal{L}$ contains no point besides those on the line through P_0 and P_1, then $m = 1$. Otherwise let P_2 be a point in $\mathcal{L}$ which is not on the line through P_0, P_1. Then all points of the plane determined by the points P_0, P_1, P_2 belong to $\mathcal{L}$. If $\mathcal{L}$ contains no point outside this plane, then $m = 2$. Otherwise let P_3 be a point in $\mathcal{L}$ outside the plane through P_0, P_1, P_2, and we can continue this procedure. Since the highest possible value of m is n, it is clear that this procedure terminates and gives a definite value of m. Note that $\mathcal{L}$ is completely determined by the m-dimensional tetrahedron, or m-simplex, $P_0 P_1 \ldots P_m$ obtained in the course of the proof. Analytically this means the following.

If $x^{(i)}$ is the vector representing the point P_i, then a point P belongs to $\mathcal{L}$ if and only if its vector can be written as $\lambda_0 x^{(0)} + \lambda_1 x^{(1)} + \ldots + \lambda_m x^{(m)}$, where $\lambda_0, \lambda_1, \ldots, \lambda_m$ are arbitrary real numbers, such that $\lambda_0 + \lambda_1 + \ldots + \lambda_m = 1$.

A non-empty set $\mathcal{K} \subset \mathbb{R}^n$ is called a *convex set* if whenever P and Q belong to $\mathcal{K}$, the *segment* joining P and Q belongs to $\mathcal{K}$. Analytically the definition can be formulated in this way: if P is represented by the vector x, and Q by the vector y, then $\mathcal{K}$ is a convex set if with P and Q it contains also every point with a vector of the form $\lambda x + \mu y$, where $\lambda \geq 0$, $\mu \geq 0$, and $\lambda + \mu = 1$.

Just as before, we can find a number m, such that $\mathcal{K}$ is contained in a linear manifold $\mathcal{L}_m$ of dimension m but not contained in any $\mathcal{L}_r$ for $r < m$.

Let P_0 be a point in $\mathcal{K}$. If $\mathcal{K}$ contains no other point, then $m = 0$. Otherwise let P_1 be another point in $\mathcal{K}$; then all points in the segment P_0P_1 belong to $\mathcal{K}$. If $\mathcal{K}$ is contained in the infinite straight line passing through P_0 and P_1, then $m = 1$, and so on. We can thus find an m-dimensional tetrahedron, or m-simplex, $P_0P_1 \ldots P_m$, all of whose points belong to $\mathcal{K}$.

If $x^{(i)}$ is the vector representing the vertex P_i of the simplex, then a point P belongs to $\mathcal{K}$, if its vector can be written as $\lambda_0 x^{(0)} + \lambda_1 x^{(1)} + \ldots + \lambda_m x^{(m)}$, where $\lambda_0 \geq 0, \lambda_1 \geq 0, \ldots, \lambda_m \geq 0$, and $\lambda_0 + \lambda_1 + \ldots + \lambda_m = 1$. $\mathcal{K}$ may contain other points than those above; for example, $\mathcal{K}$ may be a disc in $\mathbb{R}^2$, while the above points belong to an inscribed triangle $P_0P_1P_2$.

In general we shall deal with the case in which $m = n$. Before further developing the properties of convex sets, we introduce some terms from set topology.

A point P is an *interior point* of a set $\mathcal{M}$ contained in $\mathbb{R}^n$, if there exists an n-dimensional ball, with centre at P, all of whose points lie in $\mathcal{M}$.

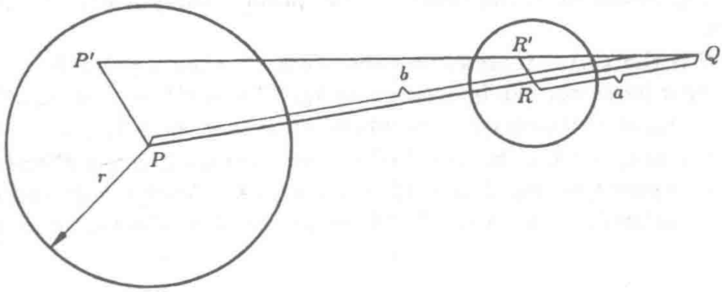
An *open set* is a set containing only interior points. The *interior* of a set $\mathcal{M}$, written Int $\mathcal{M}$, or $\mathcal{M}^\circ$, is the set of all its interior points.

It is easy to show that if $\mathcal{K}$ is an n-dimensional convex set in $\mathbb{R}^n$, then it must contain interior points, since the centre of gravity of an n-dimensional tetrahedron is an interior point of the tetrahedron, and we know that such a tetrahedron is contained in $\mathcal{K}$.

Theorem 1. *If $\mathcal{K}$ is an n-dimensional convex set in $\mathbb{R}^n$, then* Int $\mathcal{K}$ *is a convex set.*

Let P be any point in Int $\mathcal{K}$, $Q \in \mathcal{K}$, $Q \neq P$, and R a point in the segment PQ, $R \neq Q$. Then $R \in \mathcal{K}$, since $\mathcal{K}$ is convex. We shall prove that $R \in$ Int $\mathcal{K}$.

Let $|PQ|$ denote the length of PQ. Suppose $|PQ| = b$, and $|RQ| = a$. Since $P \in$ Int $\mathcal{K}$, there is an n-dimensional ball with radius $r > 0$ and centre P, all of whose points lie in $\mathcal{K}$. By choosing r small enough, we may further suppose that $b > r$. Construct an n-dimensional ball of radius $\frac{ra}{b}$, with R as centre, and choose a point R' in the interior of the ball. Since $b > r > 0$, we have $a > \frac{ra}{b}$,



and therefore $R' \neq Q$. Construct the point P' on the ray emanating from Q and passing through R', so that $\frac{|QR'|}{|QP'|} = \frac{a}{b}$. Then P' belongs to the interior of the ball of radius r around P. Therefore P' will be a point in $\mathcal{K}$, and since Q is also in $\mathcal{K}$, we have $R' \in \mathcal{K}$. Since R' was an arbitrary point in a ball around R, we have proved that R is an interior point of $\mathcal{K}$.

§ 2. Convex bodies

We introduce some definitions for well-known ideas.

Definition. A *convex body* is a bounded, convex, open set in $\mathbb{R}^n$.

The interior of an n-dimensional ball, defined by

$$x_1^2 + x_2^2 + \ldots + x_n^2 < a^2 , \quad a \neq 0 ,$$

provides an example.

A *frontier point* P [cf. Lecture XIV, §1] of a convex body $\mathcal{B}$ is a point *not* belonging to $\mathcal{B}$, such that there exist points of $\mathcal{B}$ arbitrarily close to P.

The *surface* $\partial\mathcal{B}$ of a convex body $\mathcal{B}$ is the set of all its frontier points.

Let $\overline{\mathcal{B}} = \mathcal{B} \cup \partial\mathcal{B}$. Then $\overline{\mathcal{B}}$, called the *closure* of $\mathcal{B}$, is a closed set; that is, it contains all its limit points.

Theorem 2. *If $\mathcal{B}$ is a convex body, then* Int $\overline{\mathcal{B}} = \mathcal{B}$.

This theorem is not true for an arbitrary set $\mathcal{B}$. Suppose, for instance in $\mathbb{R}^2$, that $\mathcal{B}$ is the interior of the unit disc excluding the origin. Then $\overline{\mathcal{B}}$ is the closed unit disc, while Int $\overline{\mathcal{B}}$ is the complete interior of the unit disc. Of course the reason for the failure of the theorem is that the original set $\mathcal{B}$ is not convex. [If $\mathbb{Q}$ denotes the set of rational numbers in $\mathbb{R}^1$, and we define $\mathcal{U} = [0,1] \cap \mathbb{Q}$, then Int $\overline{\mathcal{U}} = (0,1)$, and it is not true that $\mathcal{U} \subset$ Int $\overline{\mathcal{U}}$, nor is it true that $\mathcal{U} \supset$ Int $\overline{\mathcal{U}}$.]

To prove Theorem 2, we shall first prove that $\mathcal{B} \subset$ Int $\overline{\mathcal{B}}$, and then that Int $\overline{\mathcal{B}} \subset \mathcal{B}$. Let $P \in \mathcal{B}$. Since $\mathcal{B}$ is open, there exists a ball with centre at P, which lies completely in $\mathcal{B}$. This ball belongs also to $\overline{\mathcal{B}}$, since $\overline{\mathcal{B}} \supset \mathcal{B}$. Therefore P is an interior point of $\overline{\mathcal{B}}$. Hence $\mathcal{B} \subset$ Int $\overline{\mathcal{B}}$. Conversely let $P \in$ Int $\overline{\mathcal{B}}$. Then there exists a ball, with centre at P, all of whose points lie in $\overline{\mathcal{B}}$. Inscribe in the ball an n-dimensional tetrahedron containing P in its interior. All the vertices of the tetrahedron belong to $\overline{\mathcal{B}}$, and therefore either to $\mathcal{B}$ or to $\partial\mathcal{B}$. If any vertex belongs to $\partial\mathcal{B}$, we can find points of $\mathcal{B}$ arbitrarily close to it, so that we can construct a new tetrahedron containing P in its interior, whose vertices all belong to $\mathcal{B}$. Since $\mathcal{B}$ is convex, P must belong to $\mathcal{B}$. Hence Int $\overline{\mathcal{B}} \subset \mathcal{B}$.

Theorem 3. *The closure of a convex body is convex.*

Let $\mathcal{B}$ be a convex body, with $P \in \overline{\mathcal{B}}, Q \in \overline{\mathcal{B}}$. We can then find two sequences of points $P_j \in \mathcal{B}, Q_j \in \mathcal{B}$ converging respectively to P and to Q. The segments P_jQ_j lie completely in $\mathcal{B}$ and tend to the segment PQ. Therefore the points of PQ are limit points of sequences of points in $\mathcal{B}$, and so belong to $\overline{\mathcal{B}}$. This proves that $\overline{\mathcal{B}}$ is convex.

§ 3. Gauge function of a convex body

One of the many important ideas introduced by Minkowski into the study of convex bodies was that of gauge function. Roughly, the gauge function is the equation of a convex body. Minkowski showed that the gauge function could be defined in a purely geometric way and that it must have certain properties analogous to those possessed by the distance of a point from the origin. He also showed that conversely given any function possessing these properties, there exists a convex body with the given function as its gauge function.

Before giving the definition of gauge function, we shall investigate some further properties of the surface $\partial\mathcal{B}$ of a convex body $\mathcal{B}$. Let O be a point in $\mathcal{B}$. Consider any ray starting from O and going to infinity in an arbitrary direction. We shall prove that this ray intersects $\partial\mathcal{B}$ in exactly one point. The ray must intersect $\partial\mathcal{B}$ in at least one point, because $\mathcal{B}$ is bounded; and all points Q far enough away do not belong to $\mathcal{B}$. The distances $|OQ|$ of all points Q of the ray which do not belong to $\mathcal{B}$, have a greatest lower bound λ, say. Then the point P on the ray such that $|OP| = \lambda$ belongs to $\partial\mathcal{B}$. For if we choose any point P' between P and O, then by the construction of P, P' belongs to $\mathcal{B}$. This shows that there exist points of $\mathcal{B}$ arbitrarily close to P, but that P is not a point of $\mathcal{B}$, since there is no ball with centre at P, which is completely contained in $\mathcal{B}$. Hence $P \in \partial\mathcal{B}$.

If the ray starting from O intersects $\partial\mathcal{B}$ in (at least) two different points, first in P and then in Q, we reach a contradiction. For Theorem 3 implies that $\overline{\mathcal{B}}$ is convex since $\mathcal{B}$ is, and the proof of Theorem 1 shows that P must be an interior point of $\overline{\mathcal{B}}$ and so belong to $\mathcal{B}$. Since $\mathcal{B}$ is open, P cannot belong both to $\mathcal{B}$ and to $\partial\mathcal{B}$.

Given a convex body $\mathcal{B} \subset \mathbb{R}^n$ containing the origin O, we define a function $f : \mathbb{R}^n \to [0, \infty)$, as follows. If $x \in \partial\mathcal{B}$, (and x denotes also the vector representing the point x), then

$$(1) \qquad f(x) = 1 \, .$$

For any other vector $x \neq 0$, construct the ray through O and the point (whose vector is) x. Suppose this ray intersects the surface $\partial\mathcal{B}$ in a point y. Then there exists a $\lambda > 0$, such that $x = \lambda y$, and we define

$$(2) \qquad f(x) = \lambda \, .$$

We complete the definition of f by setting

$$(3) \qquad f(0) = 0 \, .$$

The function f so defined is the *gauge function* of the convex body $\mathcal{B}$.

We now prove that f is a positive-homogeneous (since $\lambda > 0$) function of degree one.

Theorem 4. *If f is the gauge function of a convex body $\mathcal{B} \subset \mathbb{R}^n$ containing the origin O, $x \in \mathbb{R}^n$, and $\mu > 0$, then $f(\mu x) = \mu f(x)$.*

This is trivial for $x = 0$ because of (3). If $x \neq 0$, there exists a point $y \in \partial\mathcal{B}$, such that $x = \lambda y$, $\lambda > 0$. Because of (1) and (2), we then have

$$f(\mu x) = f(\mu\lambda y) = \mu\lambda = \mu f(x) .$$

We note the trivial

Theorem 5. *If f is the gauge function of a convex body $\mathcal{B} \subset \mathbb{R}^n$ containing the origin O, $x \in \mathbb{R}^n$, then $f(x) > 0$ for $x \neq 0$, while $f(0) = 0$.*

Note that the properties of the gauge function f, as expressed in Theorems 4 and 5, are also properties of the distance function $|\ |$, which assigns to a vector $x \in \mathbb{R}^n$ (representing the point X) the distance of X from the origin, that is $|x| = |OX| = (x_1^2 + \ldots + x_n^2)^{1/2}$, where $x = (x_1, \ldots, x_n)$. The distance function is the gauge function of the n-dimensional unit ball; it has, however, a third very important property, namely it satisfies the triangle inequality. We shall show that an arbitrary gauge function also has this property.

Theorem 6. *If f is the gauge function of a convex body $\mathcal{B} \subset \mathbb{R}^n$ containing the origin O, and $x, y \in \mathbb{R}^n$, then*

$$f(x + y) \leq f(x) + f(y) .$$

[This, together with the property expressed in Theorem 4, is referred to, later on, as the *convexity property* of the gauge function f.]

By Definitions (1), (2) and (3), $f(x) \leq 1$ for all $x \in \overline{\mathcal{B}}$, and conversely, $f(x) \leq 1$ implies that $x \in \overline{\mathcal{B}}$. Let $x', y' \in \overline{\mathcal{B}}$. Then by Theorem 3 and the definition of a convex set, we have $\lambda x' + \mu y' \in \overline{\mathcal{B}}$, for $\lambda > 0$, $\mu > 0$, and $\lambda + \mu = 1$, so that

$$f(\lambda x' + \mu y') \leq 1 . \tag{4}$$

The theorem is trivial if either $x = 0$, or $y = 0$. Assume that $x \neq 0$, $y \neq 0$, and define

$$x^* = \frac{1}{f(x)} \cdot x , \quad y^* = \frac{1}{f(y)} \cdot y .$$

By Theorem 4, we have $f(x^*) = f(y^*) = 1$, therefore $x^* \in \overline{\mathcal{B}}$, $y^* \in \overline{\mathcal{B}}$. Let

$$\lambda = \frac{f(x)}{f(x) + f(y)} , \quad \mu = \frac{f(y)}{f(x) + f(y)} ;$$

then we have, from (4), $f(\lambda x^* + \mu y^*) \leq 1$, or using Theorem 4,

$$f\left(\frac{1}{f(x) + f(y)}(x + y)\right) = \frac{f(x + y)}{f(x) + f(y)} \leq 1 ,$$

so that we have finally $f(x + y) \leq f(x) + f(y)$.