Symplectic Geometry

Dr. Carl Ludwig Siegel

Professor of Mathematics

University of Göttingen

1964

ACADEMIC PRESS • New York and London

ACADEMIC PRESS INC.
111 FIFTH AVENUE
NEW YORK, NEW YORK 10003

United Kingdom Edition
Published by
ACADEMIC PRESS INC. (LONDON) LTD.
BERKELEY SQUARE HOUSE, LONDON W.1

Library of Congress Catalog Card Number: 64-20323

Reprinted from American Journal of Mathematics, Vol. LXV, No. 1, January, 1943

PRINTED IN THE UNITED STATES OF AMERICA

PREFACE

There still seems to be considerable interest in my paper on Symplectic Geometry which appeared 21 years ago in the *American Journal of Mathematics*. Since copies are no longer available, I am grateful to the editors of Academic Press for this new publication.

A page of "Errata" has been added which includes corrections for a few typographical errors and the revised value of a numerical constant.

I shall never forget the generous help from the Institute for Advanced Study in Princeton which enabled me to continue my scientific work during that critical time. This reprint is dedicated to the memory of my friends Oswald Veblen and Hermann Weyl.

Goettingen
January 1964

CARL LUDWIG SIEGEL

ERRATA

Page 4, line 7. The value of c_3 is incorrect. Recently, U. Christian computed $c_3 = 45/64$ which agrees with a general formula for c_n obtained some years ago by F. Hirzebruch. A corresponding correction should be made on page 25 and page 58.

Page 11, Formula (11). Read $r_n t\bar{t} < 1$ instead of > 1.

Page 25, Formula (56). Read $| \mathfrak{Y} |^{-n-1}$ instead of $| \mathfrak{Y} |^{n-1}$.

Page 25, line 15. Read $c_3 = 45/64$.

Page 26, Formula (59). Read $\mathfrak{C}$ instead of $\mathfrak{E}$.

Page 57, Formula (127). Read π^{-k} instead of π^{-1}.

Page 58. Correct values of c_3, χ_3 according to change on page 4.

Page 72, line 4. The last word is "properties".

SYMPLECTIC GEOMETRY.*

By Carl Ludwig Siegel.

I. INTRODUCTION.

1. Our present knowledge concerning functions of several complex variables $z_1, \cdots, z_m$ is much less far-reaching and complete than the classical theory in the case $m = 1$. If we want to proceed further, it seems reasonable to investigate, in the first place, a *special* class of analytic functions of m variables found by the following considerations:

Let R be the Riemann surface of an analytic function of a single variable. On account of the main theorem of uniformization, the universal covering surface U of R can be conformally mapped onto a simple domain E, which is either the unit-circle $|z| < 1$ or the finite z-plane or the complete z-plane. The conformal mappings of E onto itself form a group Ω of linear transformations, and the fundamental group of R is faithfully represented by a subgroup Δ of Ω, discontinuous in E. By the introduction of the uniformizing parameter z, the general theory of the analytic single-valued functions on R is reduced to the theory of the automorphic functions with the group Δ.

The group Ω is transitive, i. e., there exists for any two points z_1 and z_2 of E an element of Ω transforming z_1 into z_2. Moreover, there exists for every point z_1 of E an involution in Ω with the fixed point z_1, i. e., an element of Ω identical with its inverse and transforming z_1 into itself. Consequently E is a *symmetric* space, in the notation of Elie Cartan. The domain E is bounded, if we consider only the first case, the case of the unit-circle $|z| < 1$; it is well known, that this occurs if and only if U has at least two frontier points.

A generalization of the theory of automorphic functions to the case of an arbitrary number of variables requires the following three steps: 1) To determine all bounded simple domains E in the space of m complex variables, which are symmetric spaces with respect to a group Ω of analytic mappings. 2) To investigate the invariant geometric properties of E, to find the discontinuous subgroups Δ of Ω and to construct their fundamental domains. 3) To study the field of automorphic functions in E with the group Δ.

The first step has been made by Cartan; he obtained explicitly 6 different types of irreducible domains E, such that all other bounded simple symmetric

* **Received February 27, 1942.**

analytic spaces can be derived from them by analytic mappings and topological products.

We shall consider more closely the second step. We restrict our researches to one of the six possible types, which is the most important for applications to other branches of mathematics. In this case, the number m of complex dimensions is $\frac{1}{2}n(n+1)$, with integral $n \geq 1$, the m variables form the elements $z_{kl} = z_{lk}$ $(1 \leq k \leq l \leq n)$ of a symmetric complex matrix $\mathfrak{Z} = (z_{kl})$ with n rows and E consists of all points $\mathfrak{Z}$ for which the hermitian form $\sum_{k=1}^{n} (|u_k|^2 - \sum_{l=1}^{n} |z_{kl}u_l|^2)$ in the auxiliary variables $u_1, \cdots, u_n$ is positive definite.

The third step has already been carried out, in a former publication, for the special case of the modular group of degree n. It is possible to generalize most of those results, but we shall not do so in the present paper.

2. Notations, definitions, results. All German letters denote matrices with complex elements; small German letters denote columns. The upper indices p and q in $\mathfrak{A}^{(pq)}$ designate the number p of rows and the number q of columns of the matrix $\mathfrak{A}$; instead of $\mathfrak{A}^{(pp)}$ and $\mathfrak{a}^{(p1)}$ we write more simply $\mathfrak{A}^{(p)}$ and $\mathfrak{a}^{(p)}$. If $a_1, \cdots, a_p$ are the diagonal elements of $\mathfrak{A}^{(p)}$ and if all other elements are 0, we write $\mathfrak{A} = [a_1, \cdots, a_p]$ and call $\mathfrak{A}$ a *diagonal* matrix. The letter $\mathfrak{E}$ denotes a *unit* matrix, and 0 denotes also a *zero* matrix. If $\mathfrak{B}$ is any matrix, $\mathfrak{B}'$ is the *transposed* matrix and $\bar{\mathfrak{B}}$ the *conjugate complex* matrix. We use the abbreviations $\mathfrak{B}'\mathfrak{A}\mathfrak{B} = \mathfrak{A}[\mathfrak{B}]$, $\mathfrak{B}'\mathfrak{A}\bar{\mathfrak{B}} = \mathfrak{A}\{\mathfrak{B}\}$. The inequality $\mathfrak{A} > 0$ means that $\mathfrak{A} = \bar{\mathfrak{A}}'$ is the matrix of a positive definite hermitian form, i. e., $\mathfrak{A}\{\mathfrak{x}\} > 0$ for all $\mathfrak{x} \neq 0$; obviously $\mathfrak{A} > 0$ means in the case of a real $\mathfrak{A}$, that $\mathfrak{A} = \mathfrak{A}'$ is the matrix of a positive definite quadratic form, i. e., $\mathfrak{A}[\mathfrak{x}] > 0$ for all real $\mathfrak{x} \neq 0$. The *trace* $\sigma(\mathfrak{A})$ of a matrix $\mathfrak{A}^{(p)} = (a_{kl})$ is defined by $\sigma(\mathfrak{A}) = \sum_{k=1}^{p} a_{kk}$.

We denote by $\mathfrak{Z} = (z_{kl})$ a symmetric matrix with n rows and variable complex elements $z_{kl} = z_{lk}$ $(1 \leq k \leq l \leq n)$; $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$, where $\mathfrak{X} = \frac{1}{2}(\mathfrak{Z} + \bar{\mathfrak{Z}})$ and $\mathfrak{Y} = (1/2i)(\mathfrak{Z} - \bar{\mathfrak{Z}})$ are the real and imaginary part of $\mathfrak{Z}$. The condition $\mathfrak{E} - \mathfrak{Z}\bar{\mathfrak{Z}} > 0$ defines a bounded domain E which is obviously a generalization of the unit-circle. On the other hand, the domain H defined by the inequality $\mathfrak{Y} > 0$ is a generalization of the upper half-plane. It is well-known that the transformation $w = (az + b)/(cz + d)$ with real a, b, c, d and $ad - bc = 1$ is the most general analytic mapping of the upper half-plane onto itself. In order to generalize this theorem, we have to introduce the symplectic group. The *homogeneous symplectic* group Ω_0 consists of all real matrices

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A}^{(n)} & \mathfrak{B}^{(n)} \\ \mathfrak{C}^{(n)} & \mathfrak{D}^{(n)} \end{pmatrix}$$

satisfying the condition $\mathfrak{J}[\mathfrak{M}] = \mathfrak{J}$ with

$$\mathfrak{J} = \begin{pmatrix} 0 & \mathfrak{E}^{(n)} \\ -\mathfrak{E}^{(n)} & 0 \end{pmatrix}.$$

It is easily proved that the transformation

$$(1) \qquad \mathfrak{W} = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$$

maps the domain H onto itself. These transformations form the (inhomogeneous) *symplectic* group Ω obtained by identifying $\mathfrak{M}$ and $-\mathfrak{M}$.

THEOREM 1. *Every analytic mapping of H onto itself is symplectic.*

The next four theorems generalize known properties of the Poincaré model of non-euclidean geometry. For any two points $\mathfrak{Z}, \mathfrak{Z}_1$ of H we define

$$\mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1) = (\mathfrak{Z} - \mathfrak{Z}_1)(\mathfrak{Z} - \bar{\mathfrak{Z}}_1)^{-1}(\bar{\mathfrak{Z}} - \bar{\mathfrak{Z}}_1)(\bar{\mathfrak{Z}} - \mathfrak{Z}_1)^{-1}.$$

THEOREM 2. *There exists a symplectic transformation mapping a given pair $\mathfrak{Z}, \mathfrak{Z}_1$ of H into another given pair $\mathfrak{W}, \mathfrak{W}_1$ of H, if and only if the two matrices $\mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1)$ and $\mathfrak{R}(\mathfrak{W}, \mathfrak{W}_1)$ have the same characteristic roots.*

Let $d\mathfrak{Z} = (dz_{kl})$ denote the matrix of the differentials dz_{kl}. The quadratic differential form

$$(2) \qquad ds^2 = \sigma(\mathfrak{Y}^{-1} d\mathfrak{Z} \mathfrak{Y}^{-1} d\bar{\mathfrak{Z}})$$

is invariant under Ω and defines a Riemann metric in H.

THEOREM 3. *There exists exactly one geodesic arc connecting two arbitrary points $\mathfrak{Z}, \mathfrak{Z}_1$ of H; its length ρ is given by*

$$\rho^2 = \sigma\left(\log^2 \frac{1 + \mathfrak{R}^{\frac{1}{2}}}{1 - \mathfrak{R}^{\frac{1}{2}}}\right)$$

with $\mathfrak{R} = \mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1)$ and

$$\log^2 \frac{1 + \mathfrak{R}^{\frac{1}{2}}}{1 - \mathfrak{R}^{\frac{1}{2}}} = 4\mathfrak{R}\left(\sum_{k=0}^{\infty} \frac{\mathfrak{R}^k}{2k+1}\right)^2.$$

THEOREM 4. *All geodesics are symplectic images of the curves $\mathfrak{Z} = i[p_1^s, \cdots, p_n^s]$, where $p_1, \cdots, p_n$ are arbitrary positive constants satisfying $\sum_{k=1}^{n} \log^2 p_k = 1$.*

Let $\mathfrak{X} = (x_{kl})$, $\mathfrak{Y}^{-1} = (Y_{kl})$ and dv be the euclidean volume element in the space with the $n(n+1)$ rectangular cartesian coördinates x_{kl}, Y_{kl}

$(1 \leq k \leq l \leq n)$. It is easily shown that $2^{n(n-1)/2}dv$ is the volume element for the symplectic metric (2).

THEOREM 5. *The Euler characteristic of a closed manifold F with the metric* (2) *is*

$$\chi = c_n(-\pi)^{-n(n+1)/2} \int_F dv, \tag{3}$$

where c_n denotes a positive rational number depending only upon n; in particular $c_1 = \frac{1}{2}$, $c_2 = \frac{3}{8}$, $c_3 = \frac{45}{256}$.

The theorems 6 and 7 are concerned with the generalization of the Fuchsian groups and their fundamental domains. Let Δ be a subgroup of the symplectic group Ω. Two points $\mathfrak{Z}, \mathfrak{W}$ of H are called *equivalent* under Δ, if (1) holds for a matrix $\mathfrak{M}$ of Δ. The group Δ is *discontinuous,* if no set of equivalent points has a limit point in H. A domain F in H is a *fundamental domain* for Δ, if the images of F under Δ cover H without gaps and overlappings. A domain F is called a *star,* if there exists an inner point $\mathfrak{Z}_0$ of F such that for every point $\mathfrak{Z}$ of F the whole geodesic arc between $\mathfrak{Z}$ and $\mathfrak{Z}_0$ belongs to F.

THEOREM 6. *A fundamental domain F of a discontinuous group Δ may be chosen as a star bounded by analytic surfaces and such that every compact domain in H is covered by a finite number of images of F under Δ.*

A discontinuous group Δ is called of the *first kind,* if there exists a *normal* fundamental domain F having the following three properties: 1) Every compact domain in H is covered by a finite number of images of F; 2) only a finite number of images of F are neighbors of F; 3) the integral

$$V(\Delta) = \int_F dv$$

converges. The space H is called *compact relative to* Δ, if there exists for every infinite sequence of points $\mathfrak{Z}_k$ $(k = 1, 2, 3, \cdots)$ in H a compact sequence $\mathfrak{W}_k$ such that $\mathfrak{W}_k$ is equivalent to $\mathfrak{Z}_k$ under Δ.

THEOREM 7. *If H is compact relative to a discontinuous group Δ, then Δ is of the first kind and has a compact normal fundamental domain.*

Let us assume that a discontinuous group Δ has no fixed point in H, i. e., that no transformation of Δ except the identical one has a fixed point in H. Identifying equivalent frontier points of a fundamental domain F, we obtain a closed manifold, if H is compact relative to Δ. The Euler number of this manifold is then given by Theorem 5. If H is not compact relative to Δ, we obtain an open manifold. It is probable that Theorem 5 still holds good for this open manifold, provided Δ is of the first kind; it may easily be proved that this is true in the case $n = 1$.

The rest of the paper deals with two special classes of groups Δ defined by arithmetical properties. The simplest and most important example of a discontinuous subgroup of Ω is given by the *modular* group Γ of degree n consisting of all symplectic matrices $\mathfrak{M}^{(2n)}$ with rational integral elements.

THEOREM 8. *The modular group of degree n is a discontinuous group of the first kind.*

Let K be a totally real algebraic number-field of degree $h \geq 1$, $K(\sqrt{-r})$ a totally imaginary quadratic field over K and s a positive number in K such that all other conjugates of s are negative. Let $\mathfrak{G}^{(2n)}$ be a skew-symmetric matrix and $\mathfrak{H}^{(2n)}$ a hermitian matrix, both with elements from $K(\sqrt{-r})$ and non-singular. We assume that all conjugates of $\mathfrak{H}$ except $\mathfrak{H}$ and $\bar{\mathfrak{H}}$ are positive and that $\mathfrak{G}$ and $\mathfrak{H}$ are connected by the relation $\mathfrak{H}\bar{\mathfrak{G}}^{-1}\bar{\mathfrak{H}} = s\mathfrak{G}$. Let $\Lambda(\mathfrak{G}, \mathfrak{H})$ denote the group of matrices $\mathfrak{U}$ with integral elements of $K(\sqrt{-r})$ satisfying the two conditions $\mathfrak{G}[\mathfrak{U}] = \mathfrak{G}$ and $\mathfrak{H}\{\mathfrak{U}\} = \mathfrak{H}$. Then there exists a constant matrix $\mathfrak{C}$ such that $\mathfrak{C}^{-1}\mathfrak{U}\mathfrak{C} = \mathfrak{M}$ is symplectic, and $\mathfrak{C}^{-1}\Lambda(\mathfrak{G}, \mathfrak{H})\mathfrak{C} = \Lambda(\mathfrak{G}, \mathfrak{H})$ is a subgroup of Ω. The modular group Γ is a particular case of these groups $\Delta(\mathfrak{G}, \mathfrak{H})$, namely the case $h = 1$, $\mathfrak{G} = \mathfrak{J}$, $\mathfrak{H} = i\mathfrak{J}$, $r = 1$.

THEOREM 9. *The group $\Delta(\mathfrak{G}, \mathfrak{H})$ is discontinuous and of the first kind. In the case $h > 1$, the space H is compact relative to $\Delta(\mathfrak{G}, \mathfrak{H})$.*

For every ideal κ of $K(\sqrt{-r})$, we denote by $\Lambda_\kappa(\mathfrak{G}, \mathfrak{H})$ the congruence subgroup of $\Lambda(\mathfrak{G}, \mathfrak{H})$ defined by the condition $\mathfrak{U} \equiv \mathfrak{E} \pmod{\kappa}$, and by $\Delta_\kappa(\mathfrak{G}, \mathfrak{H}) = \mathfrak{C}^{-1}\Lambda_\kappa(\mathfrak{G}, \mathfrak{H})\mathfrak{C}$ the corresponding subgroup of $\Delta(\mathfrak{G}, \mathfrak{H})$.

THEOREM 10. *Let ρ be a prime ideal of $K(\sqrt{-r})$ and κ the least power of ρ such that p is not divisible by κ^{p-1}, where p denotes the rational prime number divisible by ρ. Then $\Delta_\kappa(\mathfrak{G}, \mathfrak{H})$ has no fixed point in H.*

On account of the theorems 5 and 10, the calculation of the integral $V(\Delta)$ for $\Delta = \Delta(\mathfrak{G}, \mathfrak{H})$ is important. Applying the Gauss-Dirichlet method from analytic number theory, we obtain in the case of the modular group of degree n a curious connection with Riemann's ζ-function. Using the abbreviation $\xi(t) = \pi^{-(t/2)}\Gamma(t/2)\zeta(t)$, so that $\xi(t) = \xi(1-t)$ is the functional equation of $\zeta(t)$, we have

THEOREM 11. *The symplectic volume of the fundamental domain of the modular group is*

$$V(\Gamma) = 2 \prod_{k=1}^{n} \xi(2k).$$

This formula may be written in a different way, suggested by the results of the analytic theory of quadratic forms. Consider a domain Q in the space of the real skew-symmetric matrices $\mathfrak{Q}^{(2n)} = (q_{kl})$, with the rectangular cartesian coördinates q_{kl} $(1 \leq k < l \leq 2n)$, and denote by L the corresponding part of the space of the real matrices $\mathfrak{L}^{(2n)}$ defined by the condition $\mathfrak{J}[\mathfrak{L}] = \mathfrak{Q}$, the coördinates in L being the $4n^2$ elements of $\mathfrak{L}$. Obviously L is invariant under any mapping $\mathfrak{L} \rightarrow \mathfrak{M}\mathfrak{L}$ with symplectic $\mathfrak{M}$. Let L_0 be a fundamental domain in L with respect to the homogeneous modular group, and let $v(L_0)$, $v(Q)$ be the euclidean volumes of L_0 and Q. We define

$$d_0(\Gamma) = \lim_{Q \to \mathfrak{J}} \frac{v(L_0)}{v(Q)}, \tag{4}$$

where Q runs over a sequence of domains tending to the single point $\mathfrak{J}$. On the other hand, let p be a rational prime number and E_p the number of modulo p incongruent integral solutions $\mathfrak{M}$ of the congruence $\mathfrak{J}[\mathfrak{M}] \equiv \mathfrak{J}$ $(\mathrm{mod}\ p)$. Since there are, modulo p, exactly $p^{n(2n-1)}$ integral skew-symmetric matrices $\mathfrak{Q}$ and p^{4n^2} integral matrices $\mathfrak{L}$, the expression

$$d_p(\Gamma) = p^{n(2n+1)} E_p^{-1}$$

may be considered as the p-adic analogue of $d_0(\Gamma)$. As a consequence of Theorem 11, we obtain

THEOREM 12. *Let p run over all prime numbers, then*

$$d_0(\Gamma) = \prod_p d_p(\Gamma).$$

It is possible to generalize this theorem for the case of an arbitrary group $\Delta(\mathfrak{G}, \mathfrak{H})$ instead of Γ.

Two subgroups Δ and Δ_1 of Ω are *conjugate*, if the relation $\Delta_1 = \mathfrak{F}^{-1}\Delta\mathfrak{F}$ holds for a symplectic matrix $\mathfrak{F}$. More generally, Δ and Δ_1 are called *commensurable*, if they contain conjugate subgroups of finite index. It is important, for the theory of automorphic functions, to know whether two given groups Δ and Δ_1 are commensurable or not. Let $\Delta = \Delta(\mathfrak{G}, \mathfrak{H})$, $\Delta_1 = \Delta(\mathfrak{G}_1, \mathfrak{H}_1)$ and let K_1, r_1, s_1 have the same meaning for $\mathfrak{G}_1, \mathfrak{H}_1$ that K, r, s have for $\mathfrak{G}, \mathfrak{H}$.

THEOREM 13. *The two groups $\Delta(\mathfrak{G}, \mathfrak{H})$ and $\Delta(\mathfrak{G}_1, \mathfrak{H}_1)$ are commensurable if, and only if, $K = K_1$ and the ternary quadratic forms $rsx^2 - ry^2 + sz^2$ and $r_1s_1x^2 - r_1y^2 + s_1z^2$ are equivalent in K.*

In the particular case $n = 2$, another class of discontinuous subgroups of Ω is given by the theory of *units* of quinary quadratic forms. Let K be again a totally real field of degree h. We consider a quadratic form $\mathfrak{T}[\mathfrak{x}]$ of 5 variables with coefficients from K and assume that $\mathfrak{T}[\mathfrak{x}]$ has the signature 2, 3, whereas all other conjugates of $\mathfrak{T}[\mathfrak{x}]$ are definite. Let $\Lambda(\mathfrak{T})$ be the group of all integral matrices $\mathfrak{U}$ in K satisfying $\mathfrak{T}[\mathfrak{U}] = \mathfrak{T}$, $|\mathfrak{U}| = 1$. On account of the spin representation of the orthogonal group, either $\Lambda(\mathfrak{T})$ itself or a subgroup of index 2 is then isomorphic to a certain subgroup $\Delta(\mathfrak{T})$ of Ω. Concerning these groups $\Delta(\mathfrak{T})$, there are analogues of the theorems 9, 10, 12, 13; in particular, analogous to Theorem 9, we have

THEOREM 14. *The group $\Delta(\mathfrak{T})$ is discontinuous and of the first kind. In the case $h > 1$, the space H is compact relative to $\Delta(\mathfrak{T})$.*

It would be interesting to seek discontinuous subgroups of Ω which are not commensurable with any of the groups $\Delta(\mathfrak{G}, \mathfrak{H})$ and $\Delta(\mathfrak{T})$. In the case $n = 1$, we may start with an arbitrary polygon satisfying certain conditions, and use the reflection method, but this simple geometric principle breaks down for $n > 1$.

---

3. Literature.

C. B. Allendoerfer, "The Euler number of a Riemann manifold," *American Journal of Mathematics* **62**, pp. 243-248 (1940).

E. Cartan, "Sur les domaines bornés homogènes de l'espace de n variables complexes," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität* **11**, pp. 116-162 (1936).

W. Fenchel, "On total curvatures of Riemannian manifolds: I," *The Journal of the London Mathematical Society* **15**, pp. 15-22 (1940).

R. Fricke and F. Klein, *Vorlesungen über die Theorie der automorphen Funktionen*, Vol. 1, B. G. Teubner, Leipzig (1897).

G. Fubini, "A remark on general Fuchsian groups," *Proceedings of the National Academy of Sciences* **26**, pp. 695-700 (1940).

———, "The distance in general Fuchsian geometries," *Proceedings of the National Academy of Sciences* **26**, pp. 700-708 (1940).

G. Giraud, "Sur une classe de groupes discontinus de transformations birationnelles quadratiques et sur les fonctions de trois variables indépendantes restant invariables par ces transformations," *Annales Scientifiques de l'Ecole Normale Supérieure* (3) **32**, pp. 237-403 (1915).

———, "Sur les groupes de transformations semblables arithmétiques de certaines formes quadratiques quinaires indéfinies et sur les fonctions de trois variables indépendantes invariantes par des groupes isomorphes aux précédents," *Annales Scientifiques de l'Ecole Normale Supérieure* (3) **33**, pp. 330-362 (1916).

P. Humbert, "Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini," *Commentarii Mathematici Helvetici* **12**, pp. 263-306 (1940).

H. Minkowski, "Diskontinutätsbereich für arithmetische Äquivalenz," *Journal für die reine und angewandte Mathematik* **129**, pp. 220-274 (1905).
C. L. Siegel, "Einführung in die Theorie der Modulfunktionen n-ten Grades," *Mathematische Annalen* **116**, pp. 617-657 (1939).
————, "Einheiten quadratischer Formen," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität* **13**, pp. 209-239 (1940).
M. Sugawara, "Über eine allgemeine Theorie der Fuchsschen Gruppen und Theta-Reihen," *Annals of Mathematics* (2) **41**, pp. 488-494 (1940).
————, "A generalization of Poincaré-space," *Proceedings of the Imperial Academy of Japan* **16**, pp. 373-377 (1940).
E. Witt, "Eine Identität zwischen Modulformen zweiten Grades," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität* **14**, pp. 323-337 (1941).

II. THE SYMPLECTIC GROUP.

4. The linear substitution $z = i\frac{1+z_0}{1-z_0}$ maps the unit-circle $z_0\bar{z}_0 < 1$ onto the upper half-plane $\frac{1}{2i}(z-\bar{z}) > 0$. We shall prove that there is an immediate generalization to the case $n > 1$.

Let $\mathfrak{Z}_0$ be a point of E, i. e., $\mathfrak{Z}_0 = \mathfrak{Z}'_0$, $\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0 > 0$. If $\mathfrak{x}$ is a solution of $(\mathfrak{E} - \mathfrak{Z}_0)\mathfrak{x} = 0$, then $\bar{\mathfrak{x}} = \bar{\mathfrak{Z}}_0\bar{\mathfrak{x}}$, $\mathfrak{x}' = \mathfrak{x}'\mathfrak{Z}_0$ and consequently $(\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0)\{\mathfrak{x}\} = \mathfrak{x}'\bar{\mathfrak{x}} - \mathfrak{x}'\mathfrak{Z}_0\bar{\mathfrak{Z}}_0\bar{\mathfrak{x}} = 0$, $\mathfrak{x} = 0$. This proves $|\mathfrak{E} - \mathfrak{Z}_0| \neq 0$ and the existence of the matrix

$$i(\mathfrak{E} + \mathfrak{Z}_0)(\mathfrak{E} - \mathfrak{Z}_0)^{-1} = \mathfrak{Z}. \tag{5}$$

Obviously $\mathfrak{Z} = \mathfrak{Z}'$ and

$$\begin{aligned}\frac{1}{2i}(\mathfrak{Z} - \bar{\mathfrak{Z}}) &= \tfrac{1}{2}(\mathfrak{E} - \mathfrak{Z}_0)^{-1}((\mathfrak{E} + \mathfrak{Z}_0)(\mathfrak{E} - \bar{\mathfrak{Z}}_0) + (\mathfrak{E} - \mathfrak{Z}_0)(\mathfrak{E} + \bar{\mathfrak{Z}}_0))(\mathfrak{E} - \bar{\mathfrak{Z}}_0)^{-1}\\ &= (\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0)\{(\mathfrak{E} - \mathfrak{Z}_0)^{-1}\} > 0;\end{aligned}$$

hence $\mathfrak{Z}$ is a point of H. On the other hand, let $\mathfrak{Z}$ be an arbitrary point of H, i. e., $\mathfrak{Z} = \mathfrak{Z}'$, $\frac{1}{2i}(\mathfrak{Z} - \bar{\mathfrak{Z}}) > 0$. If $\mathfrak{x}$ is a solution of $(\mathfrak{Z} + i\mathfrak{E})\mathfrak{x} = 0$, then $\bar{\mathfrak{Z}}\bar{\mathfrak{x}} = i\bar{\mathfrak{x}}$, $\mathfrak{x}'\mathfrak{Z} = -i\mathfrak{x}'$ and consequently $\frac{1}{2i}(\mathfrak{Z} - \bar{\mathfrak{Z}})\{\mathfrak{x}\} = \frac{1}{2i}(\mathfrak{x}'\mathfrak{Z}\bar{\mathfrak{x}} - \mathfrak{x}'\bar{\mathfrak{Z}}\bar{\mathfrak{x}}) = -\mathfrak{x}'\bar{\mathfrak{x}} \leq 0$, $\mathfrak{x} = 0$. This proves $|\mathfrak{Z} + i\mathfrak{E}| \neq 0$ and the existence of the matrix

$$(\mathfrak{Z} - i\mathfrak{E})(\mathfrak{Z} + i\mathfrak{E})^{-1} = \mathfrak{Z}_0. \tag{6}$$

H. Minkowski, "Diskontinutätsbereich für arithmetische Äquivalenz," *Journal für die reine und angewandte Mathematik* **129**, pp. 220-274 (1905).

C. L. Siegel, "Einführung in die Theorie der Modulfunktionen n-ten Grades," *Mathematische Annalen* **116**, pp. 617-657 (1939).

————, "Einheiten quadratischer Formen," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität* **13**, pp. 209-239 (1940).

M. Sugawara, "Über eine allgemeine Theorie der Fuchsschen Gruppen und Theta-Reihen," *Annals of Mathematics* (2) **41**, pp. 488-494 (1940).

————, "A generalization of Poincaré-space," *Proceedings of the Imperial Academy of Japan* **16**, pp. 373-377 (1940).

E. Witt, "Eine Identität zwischen Modulformen zweiten Grades," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität* **14**, pp. 323-337 (1941).

II. THE SYMPLECTIC GROUP.

4. The linear substitution $z = i\dfrac{1+z_0}{1-z_0}$ maps the unit-circle $z_0\bar{z}_0 < 1$ onto the upper half-plane $\dfrac{1}{2i}(z-\bar{z}) > 0$. We shall prove that there is an immediate generalization to the case $n > 1$.

Let $\mathfrak{Z}_0$ be a point of E, i. e., $\mathfrak{Z}_0 = \mathfrak{Z}'_0$, $\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0 > 0$. If $\mathfrak{x}$ is a solution of $(\mathfrak{E} - \mathfrak{Z}_0)\mathfrak{x} = 0$, then $\bar{\mathfrak{x}} = \bar{\mathfrak{Z}}_0\bar{\mathfrak{x}}$, $\mathfrak{x}' = \mathfrak{x}'\mathfrak{Z}_0$ and consequently $(\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0)\{\mathfrak{x}\} = \mathfrak{x}'\bar{\mathfrak{x}} - \mathfrak{x}'\mathfrak{Z}_0\bar{\mathfrak{Z}}_0\bar{\mathfrak{x}} = 0$, $\mathfrak{x} = 0$. This proves $|\mathfrak{E} - \mathfrak{Z}_0| \neq 0$ and the existence of the matrix

$$i(\mathfrak{E} + \mathfrak{Z}_0)(\mathfrak{E} - \mathfrak{Z}_0)^{-1} = \mathfrak{Z}. \tag{5}$$

Obviously $\mathfrak{Z} = \mathfrak{Z}'$ and

$$\begin{aligned}\frac{1}{2i}(\mathfrak{Z} - \bar{\mathfrak{Z}}) &= \tfrac{1}{2}(\mathfrak{E} - \mathfrak{Z}_0)^{-1}((\mathfrak{E} + \mathfrak{Z}_0)(\mathfrak{E} - \bar{\mathfrak{Z}}_0) + (\mathfrak{E} - \mathfrak{Z}_0)(\mathfrak{E} + \bar{\mathfrak{Z}}_0))(\mathfrak{E} - \bar{\mathfrak{Z}}_0)^{-1} \\ &= (\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0)\{(\mathfrak{E} - \mathfrak{Z}_0)^{-1}\} > 0;\end{aligned}$$

hence $\mathfrak{Z}$ is a point of H. On the other hand, let $\mathfrak{Z}$ be an arbitrary point of H, i. e., $\mathfrak{Z} = \mathfrak{Z}'$, $\dfrac{1}{2i}(\mathfrak{Z} - \bar{\mathfrak{Z}}) > 0$. If $\mathfrak{x}$ is a solution of $(\mathfrak{Z} + i\mathfrak{E})\mathfrak{x} = 0$, then $\bar{\mathfrak{Z}}\bar{\mathfrak{x}} = i\bar{\mathfrak{x}}$, $\mathfrak{x}'\mathfrak{Z} = -i\mathfrak{x}'$ and consequently $\dfrac{1}{2i}(\mathfrak{Z} - \bar{\mathfrak{Z}})\{\mathfrak{x}\} = \dfrac{1}{2i}(\mathfrak{x}'\mathfrak{Z}\bar{\mathfrak{x}} - \mathfrak{x}'\bar{\mathfrak{Z}}\bar{\mathfrak{x}}) = -\mathfrak{x}'\bar{\mathfrak{x}} \leq 0$, $\mathfrak{x} = 0$. This proves $|\mathfrak{Z} + i\mathfrak{E}| \neq 0$ and the existence of the matrix

$$(\mathfrak{Z} - i\mathfrak{E})(\mathfrak{Z} + i\mathfrak{E})^{-1} = \mathfrak{Z}_0. \tag{6}$$

Obviously $\mathfrak{Z}_0 = \mathfrak{Z}'_0$ and

$$\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0 = (\mathfrak{Z} + i\mathfrak{E})^{-1}((\mathfrak{Z} + i\mathfrak{E})(\bar{\mathfrak{Z}} - i\mathfrak{E}) - (\mathfrak{Z} - i\mathfrak{E})(\bar{\mathfrak{Z}} + i\mathfrak{E}))(\bar{\mathfrak{Z}} - i\mathfrak{E})^{-1}$$
$$= \frac{2}{i}(\mathfrak{Z} - \bar{\mathfrak{Z}})\{(\mathfrak{Z} + i\mathfrak{E})^{-1}\} > 0;$$

hence $\mathfrak{Z}_0$ is a point of E. Moreover (6) follows from (5), and vice versa.

5. The homogeneous symplectic group Ω_0 consists of all matrices

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$$

with real elements satisfying $\mathfrak{M}'\mathfrak{J}\mathfrak{M} = \mathfrak{J}$. Since $\mathfrak{J}^{-1} = -\mathfrak{J}$, we have then also $\mathfrak{M}\mathfrak{J}\mathfrak{M}' = \mathfrak{J}$; hence $\mathfrak{M}'$ is symplectic and

$$(7) \qquad \mathfrak{A}\mathfrak{B}' = \mathfrak{B}\mathfrak{A}', \qquad \mathfrak{C}\mathfrak{D}' = \mathfrak{D}\mathfrak{C}', \qquad \mathfrak{A}\mathfrak{D}' - \mathfrak{B}\mathfrak{C}' = \mathfrak{E}.$$

Let $\mathfrak{Z}$ be a point of H, i. e.,

$$\mathfrak{J}\begin{bmatrix} \mathfrak{Z} \\ \mathfrak{E} \end{bmatrix} = 0, \qquad \frac{1}{2i}\mathfrak{J}\begin{Bmatrix} \mathfrak{Z} \\ \mathfrak{E} \end{Bmatrix} > 0.$$

The matrices $\mathfrak{A}\mathfrak{Z} + \mathfrak{B} = \mathfrak{P}$, $\mathfrak{C}\mathfrak{Z} + \mathfrak{D} = \mathfrak{Q}$ satisfy

$$\mathfrak{M}\begin{pmatrix} \mathfrak{Z} \\ \mathfrak{E} \end{pmatrix} = \begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}, \qquad \mathfrak{J}\begin{bmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{bmatrix} = 0, \qquad \frac{1}{2i}\mathfrak{J}\begin{Bmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{Bmatrix} > 0,$$

$$\mathfrak{P}'\mathfrak{Q} = \mathfrak{Q}'\mathfrak{P}, \qquad \frac{1}{2i}(\mathfrak{P}'\bar{\mathfrak{Q}} - \mathfrak{Q}'\bar{\mathfrak{P}}) > 0.$$

If $\mathfrak{x}$ is a solution of $\mathfrak{Q}\mathfrak{x} = 0$, then $\bar{\mathfrak{Q}}\bar{\mathfrak{x}} = 0$, $\mathfrak{x}'\mathfrak{Q}' = 0$, $\frac{1}{2i}(\mathfrak{P}'\bar{\mathfrak{Q}} - \mathfrak{Q}'\bar{\mathfrak{P}})\{\mathfrak{x}\} = 0$, whence $\mathfrak{x} = 0$, $|\mathfrak{Q}| \neq 0$. This proves the existence of

$$(\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1} = \mathfrak{P}\mathfrak{Q}^{-1} = \mathfrak{W},$$

with $\mathfrak{W} = \mathfrak{W}'$, $\frac{1}{2i}(\mathfrak{W} - \bar{\mathfrak{W}})\{\mathfrak{Q}\} > 0$, $\frac{1}{2i}(\mathfrak{W} - \bar{\mathfrak{W}}) > 0$. Consequently the fractional linear transformation

$$\mathfrak{W} = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1} = (\mathfrak{Z}\mathfrak{C}' + \mathfrak{D}')^{-1}(\mathfrak{Z}\mathfrak{A}' + \mathfrak{B}')$$

maps H into itself. Since $\mathfrak{Z}(-\mathfrak{C}'\mathfrak{W} + \mathfrak{A}') = \mathfrak{D}'\mathfrak{W} - \mathfrak{B}'$ and

$$(8) \qquad \mathfrak{M}^{-1} = \mathfrak{J}^{-1}\mathfrak{M}'\mathfrak{J} = \begin{pmatrix} \mathfrak{D}' & -\mathfrak{B}' \\ -\mathfrak{C}' & \mathfrak{A}' \end{pmatrix},$$

we obtain $|-\mathfrak{C}'\mathfrak{W} + \mathfrak{A}'| \neq 0$ and $\mathfrak{Z} = (\mathfrak{D}'\mathfrak{W} - \mathfrak{B}')(-\mathfrak{C}'\mathfrak{W} + \mathfrak{A}')^{-1}$; hence H is mapped onto itself.

It is easily seen that two symplectic matrices $\mathfrak{M}$ and $\mathfrak{M}_1$ define the same symplectic mapping $\mathfrak{W} = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$, if and only if $\mathfrak{M}_1 = \pm \mathfrak{M}$. Hence the inhomogeneous symplectic group Ω is the factor group of Ω_0 obtained by identifying $\mathfrak{M}$ and $-\mathfrak{M}$.

We have

$$\begin{pmatrix} i\mathfrak{C}' + \mathfrak{D}' & -i\mathfrak{A}' - \mathfrak{B}' \\ 0 & \mathfrak{E} \end{pmatrix} \mathfrak{M} \begin{pmatrix} \mathfrak{E} & i\mathfrak{E} \\ 0 & \mathfrak{E} \end{pmatrix} = \begin{pmatrix} \mathfrak{E} & 0 \\ \mathfrak{C} & i\mathfrak{C} + \mathfrak{D} \end{pmatrix}.$$

On the other hand $| i\mathfrak{C} + \mathfrak{D} | \neq 0$, since $i\mathfrak{E}$ is a point of H. This proves $| \mathfrak{M} | = 1$.

6. The fractional linear transformation (5) maps E onto H; its matrix is

$$\mathfrak{L} = \begin{pmatrix} i\mathfrak{E} & i\mathfrak{E} \\ -\mathfrak{E} & \mathfrak{E} \end{pmatrix}$$

and satisfies

$$\mathfrak{J}[\mathfrak{L}] = 2i\mathfrak{J}, \qquad \frac{1}{i}\mathfrak{J}\{\mathfrak{L}\} = 2\mathfrak{K}$$

with

$$\mathfrak{K} = \begin{pmatrix} -\mathfrak{E} & 0 \\ 0 & \mathfrak{E} \end{pmatrix}.$$

Let $\mathfrak{M}$ be an arbitrary symplectic matrix, i. e., $\mathfrak{J}[\mathfrak{M}] = \mathfrak{J}$, $\mathfrak{J}\{\mathfrak{M}\} = \mathfrak{J}$. Then

$$\mathfrak{L}^{-1}\mathfrak{M}\mathfrak{L} = \mathfrak{M}_0 = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_0 \\ \mathfrak{C}_0 & \mathfrak{D}_0 \end{pmatrix}$$

fulfills the conditions $\mathfrak{J}[\mathfrak{M}_0] = \mathfrak{J}$, $\mathfrak{K}\{\mathfrak{M}_0\} = \mathfrak{K}$, whence $\mathfrak{J}[\mathfrak{M}_0] = \mathfrak{J}$, $\mathfrak{F}\bar{\mathfrak{M}}_0 = \mathfrak{M}_0\mathfrak{F}$ with

$$\mathfrak{F} = \mathfrak{J}\mathfrak{K} = \begin{pmatrix} 0 & \mathfrak{E} \\ \mathfrak{E} & 0 \end{pmatrix},$$

or more explicitly

(9) $$\mathfrak{A}_0\mathfrak{B}'_0 = \mathfrak{B}_0\mathfrak{A}'_0, \quad \mathfrak{A}_0\bar{\mathfrak{A}}'_0 - \mathfrak{B}_0\bar{\mathfrak{B}}'_0 = \mathfrak{E}, \quad \mathfrak{C}_0 = \bar{\mathfrak{B}}_0, \quad \mathfrak{D}_0 = \bar{\mathfrak{A}}_0.$$

The corresponding transformation

(10) $$\mathfrak{W}_0 = (\mathfrak{A}_0\mathfrak{Z}_0 + \mathfrak{B}_0)(\bar{\mathfrak{B}}_0\mathfrak{Z}_0 + \bar{\mathfrak{A}}_0)^{-1}$$

maps E onto itself, and all these transformations form the group $\mathfrak{L}^{-1}\Omega\mathfrak{L} = \Omega_E$.

We shall prove that Ω_E is transitive. Let $\mathfrak{Z}_0$ be any point of E, i. e., $\mathfrak{Z}_0 = \mathfrak{Z}'_0$, $\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0 > 0$. It is sufficient to prove the existence of a transformation (10) mapping $\mathfrak{Z}_0$ into 0. We choose $\mathfrak{A}_0$ such that $\mathfrak{A}_0(\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0)\bar{\mathfrak{A}}' = \mathfrak{E}$ and define $\mathfrak{B}_0 = -\mathfrak{A}_0\mathfrak{Z}_0$; then (9) is satisfied and (10) has obviously the required property. Consequently Ω is also transitive.

A mapping of Ω_E has the fixed point 0, if and only if $\mathfrak{B}_0 = 0$; then $\mathfrak{A}_0$ is unitary, by (9). Consequently this mapping has the particular form

$$\mathfrak{W}_0 = \mathfrak{U}'\mathfrak{Z}_0\mathfrak{U},$$

where $\mathfrak{U}$ denotes an arbitrary unitary matrix, i. e., a matrix satisfying $\mathfrak{U}'\bar{\mathfrak{U}} = \mathfrak{E}$. Since (5) maps 0 into $i\mathfrak{E}$, the formula

$$\frac{\mathfrak{W} - i\mathfrak{E}}{\mathfrak{W} + i\mathfrak{E}} = \mathfrak{U}' \frac{\mathfrak{Z} - i\mathfrak{E}}{\mathfrak{Z} + i\mathfrak{E}} \mathfrak{U}$$

gives all symplectic transformations having $i\mathfrak{E}$ as a fixed point.

7. By the results of the preceding section, the proof of Theorem 1 is reduced to the proof of the following statement: *Let $\mathfrak{Z}_0 \to \mathfrak{W}_0$ be an analytic mapping of E onto itself with the fixed point* 0; *then $\mathfrak{W}_0 = \mathfrak{U}'\mathfrak{Z}_0\mathfrak{U}$ with unitary constant* $\mathfrak{U}$.

Let $\mathfrak{Z}_0 = (z_{kl})$ be an arbitrary point of E and denote by r_k $(k = 1, \cdots, n)$ the characteristic roots of the hermitian matrix $\mathfrak{Z}_0\bar{\mathfrak{Z}}_0$; then $r_k \geq 0$ and also $r_k < 1$, by $\mathfrak{E} - \mathfrak{Z}_0\bar{\mathfrak{Z}}_0 > 0$; we may assume $0 \leq r_1 \leq r_2 \leq \cdots \leq r_n < 1$. The matrix $\mathfrak{Z} = t\mathfrak{Z}_0$ is again a point of E, if the complex scalar factor t satisfies the condition $r_n t\bar{t} < 1$. Let $\mathfrak{W} = \mathfrak{W}(t)$ be the image of $\mathfrak{Z}$ under the analytic mapping $\mathfrak{Z}_0 \to \mathfrak{W}_0$. The elements of the matrix $\mathfrak{W}$ are analytic functions of the single complex variable t, for given $\mathfrak{Z}_0$; they are regular in the circle $r_n t\bar{t} < 1$ and a fortiori in the unit-circle $t\bar{t} \leq 1$. Consequently

$$\mathfrak{W} = \sum_{k=1}^{\infty} t^k \mathfrak{W}_k \qquad (r_n t\bar{t} > 1), \tag{11}$$

where the coefficients $\mathfrak{W}_k$ are matrices depending only upon $\mathfrak{Z}_0$. On the other hand, $\mathfrak{W}$ may be expressed as a power series in the variables tz_{kl}, converging for sufficiently small values of $t\bar{t}$. Since this expansion is unique, the matrix $t^k\mathfrak{W}_k$ is exactly the aggregate of the terms of order k in that power series. This proves, in particular, that the power series representation $\mathfrak{W}_0 = \sum_{k=1}^{\infty} \mathfrak{W}_k$ converges everywhere in E, if we do not split up the polynomials $\mathfrak{W}_k$ into their single terms.

Since $\mathfrak{Z}_0 \to \mathfrak{W}_0$ maps E onto itself, we have $\mathfrak{E} - \mathfrak{W}\bar{\mathfrak{W}} > 0$ for $t\bar{t} = 1$. Integrating over that circle we obtain

$$\frac{1}{2\pi i} \int_{t\bar{t}=1} (\mathfrak{E} - \mathfrak{W}\bar{\mathfrak{W}}) \frac{dt}{t} > 0,$$

whence by (11)

$$\mathfrak{E} - \sum_{k=1}^{\infty} \mathfrak{W}_k \bar{\mathfrak{W}}_k > 0 \tag{12}$$

and in particular

$$\mathfrak{E} - \mathfrak{W}_1 \bar{\mathfrak{W}}_1 > 0. \tag{13}$$

The $\frac{1}{2}n(n+1)$ elements w_{kl} $(1 \leq k \leq l \leq n)$ of $\mathfrak{W}_1 = (w_{kl})$ are linear functions of the independent variables z_{kl} $(1 \leq k \leq l \leq n)$; let D be their determinant. Since $\mathfrak{W}_1$ is the linear part of the power series for $\mathfrak{W}_0$, the functional determinant of the $\frac{1}{2}n(n+1)$ independent elements of $\mathfrak{W}_0$ with respect to the variables z_{kl} is also D, at the point $\mathfrak{Z}_0 = 0$. If we interchange $\mathfrak{W}_0$ and $\mathfrak{Z}_0$, the determinant D is replaced by D^{-1}. In order to prove Theorem 1, we may therefore assume $D\bar{D} \geq 1$.

Consider now the linear mapping $\mathfrak{Z}_0 \rightarrow \mathfrak{W}_1$, with the determinant D. By (13), the domain E is mapped onto a domain E_1 contained in E. Let $v(E)$ and $v(E_1)$ be the euclidean volumes of E and E_1, the real and imaginary parts of the z_{kl} being rectangular cartesian coördinates. Then $v(E_1) = D\bar{D}v(E) \geq v(E)$, whence $D\bar{D} = 1$, $E_1 = E$, and the boundary of E is mapped onto itself. We take $\mathfrak{Z}_0 = \mathfrak{U}'\mathfrak{P}\mathfrak{U}$ with unitary $\mathfrak{U}$ and $\mathfrak{P} = [p_1, \cdots, p_n]$; obviously $\mathfrak{Z}_0$ is a boundary point of E, if $-1 \leq p_k \leq 1$ $(k = 1, \cdots, n)$ and at least one $p_k = \pm 1$. On the other hand, the determinant $|\mathfrak{E} - \mathfrak{W}_1 \bar{\mathfrak{W}}_1|$ is a polynomial in $p_1, \cdots, p_n$, of total degree $2n$. Since $|\mathfrak{E} - \mathfrak{W}_1 \bar{\mathfrak{W}}_1|$ vanishes on the boundary of E, this polynomial is divisible by $\prod_{k=1}^{n} (1 - p_k^2)$, of total degree $2n$. Moreover the constant terms in both polynomials have the value 1; hence

$$|\mathfrak{E} - \mathfrak{W}_1 \bar{\mathfrak{W}}_1| = |\mathfrak{E} - \mathfrak{Z}_0 \bar{\mathfrak{Z}}_0| \tag{14}$$

for $\mathfrak{Z}_0 = \mathfrak{U}'\mathfrak{P}\mathfrak{U}$, where $\mathfrak{U}$ is an arbitrary unitary matrix and $\mathfrak{P}$ an arbitrary real diagonal matrix. We use now the following lemma, the proof of which will be given in Section **9**.

LEMMA 1. *Let $\mathfrak{Z}$ be a complex symmetric matrix and $\mathfrak{P}$ the diagonal matrix $[q_1^{\frac{1}{2}}, \cdots, q_n^{\frac{1}{2}}]$, where $q_1, \cdots, q_n$ denote the characteristic roots of $\mathfrak{Z}\bar{\mathfrak{Z}}$. There exists a unitary matrix $\mathfrak{U}$ such that $\mathfrak{Z} = \mathfrak{U}'\mathfrak{P}\mathfrak{U}$.*

On account of this lemma, the relationship (14) holds also identically in $\mathfrak{Z}_0 = (z_{kl})$. Since $\mathfrak{W}_1$ is linear in all z_{kl}, we obtain

$$|\lambda\mathfrak{E} - \mathfrak{W}_1 \bar{\mathfrak{W}}_1| = |\lambda\mathfrak{E} - \mathfrak{Z}_0 \bar{\mathfrak{Z}}_0|$$

identically in λ. This proves that $\mathfrak{Z}_0 \bar{\mathfrak{Z}}_0$ and $\mathfrak{W}_1 \bar{\mathfrak{W}}_1$ have the same characteristic roots. Applying again Lemma 1, we find

(15) $$\mathfrak{W}_1 = \mathfrak{U}'\mathfrak{Z}_0\mathfrak{U}$$
with unitary $\mathfrak{U}$.

By (12), the inequality $\mathfrak{E} - \mathfrak{W}_1\bar{\mathfrak{W}}_1 - \mathfrak{W}_k\bar{\mathfrak{W}}_k > 0$ holds for $k = 2, 3, \cdots$ and every $\mathfrak{Z}_0$ in E. Choose, in particular, $\mathfrak{Z}_0 = u \exp i\mathfrak{S}$ with real symmetric $\mathfrak{S}$ and $0 < u < 1$. Then, by (15),

$$(1 - u^2)\mathfrak{E} - \mathfrak{W}_k\bar{\mathfrak{W}}_k > 0 \qquad (k = 2, 3, \cdots);$$

hence $\mathfrak{W}_k$ tends to 0, if u tends to 1, and $\mathfrak{W}_k = 0$ for $\mathfrak{Z}_0 = \exp i\mathfrak{S}$ and arbitrary real symmetric $\mathfrak{S}$. But $\mathfrak{W}_k$ is analytic and consequently $\mathfrak{W}_k = 0$ also for $\mathfrak{Z}_0 = \exp i\mathfrak{S}$ with complex symmetric $\mathfrak{S}$. This proves that $\mathfrak{W}_k$ vanishes identically.

8. In order to complete the proof of Theorem 1, we have to prove that the unitary matrix $\mathfrak{U}$ in (15) can be chosen as a constant matrix. Let

(16) $$\mathfrak{W}_1 = \mathfrak{W}_1(\mathfrak{Z}_0) = \sum_{k \leq l} z_{kl}\mathfrak{A}_{kl}$$

with constant matrices $\mathfrak{A}_{kl}$ and define

(17) $$\mathfrak{W}_1^* = \mathfrak{W}_1^*(\mathfrak{Z}_0) = \sum_{k \leq l} z_{kl}\bar{\mathfrak{A}}_{kl};$$

whence $\bar{\mathfrak{W}}_1 = \mathfrak{W}_1^*(\bar{\mathfrak{Z}}_0)$. Now $\mathfrak{W}_1\bar{\mathfrak{W}}_1 = \mathfrak{E}$ for $\mathfrak{Z}_0\bar{\mathfrak{Z}}_0 = \mathfrak{E}$ and consequently

(18) $$\mathfrak{W}_1(\mathfrak{Z}_0)\mathfrak{W}_1^*(\mathfrak{Z}_0^{-1}) = \mathfrak{E}$$

for $\mathfrak{Z}_0 = \exp i\mathfrak{S}$ with arbitrary real symmetric $\mathfrak{S}$. Since $\mathfrak{W}_1$ and $\mathfrak{W}_1^*$ are analytic, we infer again that (18) is an identity in $\mathfrak{Z}_0$.

Putting $z_{kk} = z_k \neq 0$ $(k = 1, \cdots, n)$, $\mathfrak{Z}_1 = [z_1, \cdots, z_n]$, $\mathfrak{Z}_2 = \mathfrak{Z}_0 - \mathfrak{Z}_1$ and using the Taylor series in the neighborhood of $\mathfrak{Z}_2 = 0$, we find

$$\mathfrak{Z}_0^{-1} = \mathfrak{Z}_1^{-1}(\mathfrak{E} + \mathfrak{Z}_2\mathfrak{Z}_1^{-1})^{-1} = \mathfrak{Z}_1^{-1} - \mathfrak{Z}_1^{-1}\mathfrak{Z}_2\mathfrak{Z}_1^{-1} + \cdots$$
$$(\mathfrak{W}_1(\mathfrak{Z}_1) + \mathfrak{W}_1(\mathfrak{Z}_2))(\mathfrak{W}_1^*(\mathfrak{Z}_1^{-1}) - \mathfrak{W}_1^*(\mathfrak{Z}_1^{-1}\mathfrak{Z}_2\mathfrak{Z}_1^{-1}) + \cdots) = \mathfrak{E},$$

hence in particular

(19) $$\mathfrak{W}_1(\mathfrak{Z}_1)\mathfrak{W}_1^*(\mathfrak{Z}_1^{-1}) = \mathfrak{E},$$

(20) $$\mathfrak{W}_1(\mathfrak{Z}_2)\mathfrak{W}_1^*(\mathfrak{Z}_1^{-1}) = \mathfrak{W}_1(\mathfrak{Z}_1)\mathfrak{W}_1^*(\mathfrak{Z}_1^{-1}\mathfrak{Z}_2\mathfrak{Z}_1^{-1}).$$

It follows from (16), (17) and (19) that

$$\sum_{k, l=1}^{n} z_k z_l^{-1}\mathfrak{A}_k\bar{\mathfrak{A}}_l = \mathfrak{E}$$

with $\mathfrak{A}_k = \mathfrak{A}_{kk}$ $(k = 1, \cdots, n)$, whence

(21) $$\mathfrak{A}_k\bar{\mathfrak{A}}_l = 0 \qquad (k \neq l).$$

By (15), the matrix $\mathfrak{A}_k\bar{\mathfrak{A}}_k$ has the characteristic roots $1, 0, \cdots, 0$. Without loss of generality, we may replace $\mathfrak{W}_1$ by $\mathfrak{U}_1'\mathfrak{W}_1\mathfrak{U}_1$, for any constant unitary matrix $\mathfrak{U}_1$. On account of Lemma 1, we may therefore assume that $\mathfrak{A}_1 = [1, 0, \cdots, 0]$. Then, by (21), the matrices $\mathfrak{A}_2, \cdots, \mathfrak{A}_n$ have the form

$$\mathfrak{A}_k = \begin{pmatrix} 0 & 0 \\ 0 & \mathfrak{B}_k^{(n-1)} \end{pmatrix} \qquad (k = 2, \cdots, n).$$

By induction, applying again Lemma 1 and (21), we may assume

$$\mathfrak{A}_k = [e_{k1}, e_{k2}, \cdots, e_{kn}] \qquad (k = 1, \cdots, n)$$

with $e_{kl} = 0 (k \neq l)$ and $e_{kk} = 1$; hence

$$\mathfrak{W}_1(\mathfrak{Z}_1) = \mathfrak{Z}_1. \tag{22}$$

It follows from (20) and (22) that

$$\mathfrak{W}_1(\mathfrak{Z}_2) = \mathfrak{Z}_1\mathfrak{W}^*_1(\mathfrak{Z}_1^{-1}\mathfrak{Z}_2\mathfrak{Z}_1^{-1})\mathfrak{Z}_1,$$

whence

$$z_k z_l \mathfrak{A}_{kl} = \mathfrak{Z}_1 \bar{\mathfrak{A}}_{kl} \mathfrak{Z}_1 \qquad (k \neq l).$$

Consequently

$$\mathfrak{W}_1 = (a_{kl} z_{kl})$$

with real $a_{kl} = a_{lk}$ and $a_{kk} = 1$. Since the matrix $[\pm 1, \pm 1, \cdots, \pm 1]$ is unitary, we may, moreover, assume $a_{1l} \geq 0$ $(l = 2, \cdots, n)$.

The expression $|\mathfrak{W}_1| \, |\mathfrak{Z}_0|^{-1}$ is a rational function of the z_{kl} and has, by (15), the constant absolute value 1; hence it is identically constant. On the other hand, both determinants $|\mathfrak{W}_1|$ and $|\mathfrak{Z}_0|$ contain the term $z_1 z_2 \cdots z_n = z$ with the same coefficient 1. This proves $|\mathfrak{W}_1| = |\mathfrak{Z}_0|$. The term $(z_1 z_l)^{-1} z z_{1l}^2$ $(l = 2, \cdots, n)$ has in $|\mathfrak{W}_1|$ the coefficient $-a_{1l}^2$ and in $|\mathfrak{Z}_0|$ the coefficient -1, hence $a_{1l} = 1$. The term $(z_1 z_k z_l)^{-1} z z_{1k} z_{1l} z_{kl}$ $(1 < k < l)$ has then in $|\mathfrak{W}_1|$ the coefficient $2a_{kl}$ and in $|\mathfrak{Z}_0|$ the coefficient 2, hence $a_{kl} = 1$ and $\mathfrak{W}_1 = \mathfrak{Z}_0$.

9. It remains to prove Lemma 1. There exists a unitary matrix $\mathfrak{U}_1$ such that

$$\mathfrak{Z}\bar{\mathfrak{Z}} = \mathfrak{P}^2\{\mathfrak{U}_1\}.$$

Then the matrix $\mathfrak{Z}[\mathfrak{U}_1^{-1}] = \mathfrak{F}$ is symmetric and $\mathfrak{F}\bar{\mathfrak{F}} = \mathfrak{P}^2$. Let $\mathfrak{F}_1$ and $\mathfrak{F}_2$ be the real and imaginary parts of $\mathfrak{F} = \mathfrak{F}_1 + i\mathfrak{F}_2$. Since $\mathfrak{P}$ is real, we obtain $\mathfrak{F}_1\mathfrak{F}_2 = \mathfrak{F}_2\mathfrak{F}_1$; consequently the two real symmetric matrices $\mathfrak{F}_1$ and $\mathfrak{F}_2$ are permutable. This proves the existence of a real orthogonal matrix $\mathfrak{O}$ such that $\mathfrak{F}_1[\mathfrak{O}]$ and $\mathfrak{F}_2[\mathfrak{O}]$ are both diagonal matrices. Hence $\mathfrak{F}[\mathfrak{O}] = \mathfrak{R}$ is also a diagonal matrix $[r_1, \cdots, r_n]$ and $\mathfrak{R}\bar{\mathfrak{R}} = \mathfrak{P}^2[\mathfrak{O}]$. The numbers $r_k\bar{r}_k$ $(k = 1, \cdots, n)$ are therefore a permutation of $q_1, \cdots, q_n$, and we may obviously assume $r_k\bar{r}_k = q_k$.

The diagonal matrix $\mathfrak{U}_2 = [s_1, \cdots, s_n]$ with $s_k = r_k^{1/2} q_k^{-(1/4)}$ $(k = 1, \cdots, n)$ is unitary and $\mathfrak{P}[\mathfrak{U}_2] = \mathfrak{R}$. Defining $\mathfrak{U} = \mathfrak{U}_2\mathfrak{O}'\mathfrak{U}_1$, we have $\mathfrak{P}[\mathfrak{U}] = \mathfrak{R}[\mathfrak{O}'\mathfrak{U}_1] = \mathfrak{Y}[\mathfrak{U}_1] = \mathfrak{Z}$; q. e. d.

10. Consider the symplectic mappings in the case $n = 1$, i. e.,

$$w = \frac{az + b}{cz + d} \tag{23}$$

with real a, b, c, d and $ad - bc = 1$. It is well-known that there exists a transformation (23) mapping two given points z, z_1 of the upper half-plane into two other given points w, w_1 of the upper half-plane, if and only if $R(z, z_1) = R(w, w_1)$, where $R(z, z_1)$ denotes the cross-ratio $\dfrac{z - z_1}{z - \bar{z}_1}\,\dfrac{\bar{z} - \bar{z}_1}{\bar{z} - z_1}$. Theorem 2 is the generalization to the case of an arbitrary n.

Let $\mathfrak{Z}, \mathfrak{Z}_1$ be two points of H and $\mathfrak{W}, \mathfrak{W}_1$ their images under the symplectic mapping $\mathfrak{W} = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ with the matrix $\mathfrak{M}$. We have

$$\mathfrak{Z}_1 - \mathfrak{Z} = (\mathfrak{Z}_1\mathfrak{E})\mathfrak{J}\binom{\mathfrak{Z}}{\mathfrak{E}} = (\mathfrak{Z}_1\mathfrak{E})\mathfrak{M}'\mathfrak{J}\mathfrak{M}\binom{\mathfrak{Z}}{\mathfrak{E}} \tag{24}$$
$$= (\mathfrak{C}\mathfrak{Z}_1 + \mathfrak{D})'(\mathfrak{W}_1 - \mathfrak{W})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D}),$$

$$\bar{\mathfrak{Z}}_1 - \mathfrak{Z} = (\mathfrak{C}\bar{\mathfrak{Z}}_1 + \mathfrak{D})'(\bar{\mathfrak{W}}_1 - \mathfrak{W})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D}). \tag{25}$$

Now $(\mathfrak{Z} - \bar{\mathfrak{Z}}_1)^{-1}$ exists, since $\mathfrak{Z} - \bar{\mathfrak{Z}}_1$ is a point of H; consequently

$$(\mathfrak{Z} - \mathfrak{Z}_1)(\mathfrak{Z} - \bar{\mathfrak{Z}}_1)^{-1}$$
$$= (\mathfrak{Z}_1\mathfrak{C}' + \mathfrak{D}')(\mathfrak{W} - \mathfrak{W}_1)(\mathfrak{W} - \bar{\mathfrak{W}}_1)^{-1}(\bar{\mathfrak{Z}}_1\mathfrak{C}' + \mathfrak{D}')^{-1}.$$

Introducing the cross-ratio

$$\mathfrak{R} = \mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1) = (\mathfrak{Z} - \mathfrak{Z}_1)(\mathfrak{Z} - \bar{\mathfrak{Z}}_1)^{-1}(\bar{\mathfrak{Z}} - \bar{\mathfrak{Z}}_1)(\bar{\mathfrak{Z}} - \mathfrak{Z}_1)^{-1}$$

and putting $\mathfrak{R}^* = \mathfrak{R}(\mathfrak{W}, \mathfrak{W}_1)$, $\mathfrak{Q} = (\mathfrak{C}\mathfrak{Z}_1 + \mathfrak{D})'$, we find

$$\mathfrak{R} = \mathfrak{Q}\mathfrak{R}^*\mathfrak{Q}^{-1}. \tag{26}$$

Hence the matrices $\mathfrak{R}$ and $\mathfrak{R}^*$ have the same characteristic roots.

Choose in particular $\mathfrak{Z}_1 = i\mathfrak{E}$, $\mathfrak{Z} = i\mathfrak{T}$ with $\mathfrak{T} = [t_1, \cdots, t_n]$ and $1 \leq t_1 \leq t_2 \leq \cdots \leq t_n$. Then $\mathfrak{R} = [r_1, \cdots, r_n]$ with

$$r_k = \left(\frac{t_k - 1}{t_k + 1}\right)^2 \qquad (k = 1, \cdots n),$$

whence $0 \leq r_1 \leq r_2 \leq \cdots \leq r_n < 1$ and

$$t_k = \frac{1 + r_k^{\frac{1}{2}}}{1 - r_k^{\frac{1}{2}}}. \tag{27}$$

In this case, the diagonal matrix $\mathfrak{T}$ is uniquely determined by the characteristic roots $r_1, \cdots, r_n$ of $\mathfrak{R}$. In order to complete the proof of Theorem 2, we have only to prove

LEMMA 2. *Let $\mathfrak{Z}, \mathfrak{Z}_1$ be two arbitrary points of H. There exists a symplectic transformation mapping $\mathfrak{Z}, \mathfrak{Z}_1$ into $i\mathfrak{T}, i\mathfrak{E}$ with $\mathfrak{T} = [t_1, \cdots, t_n]$ and $1 \leq t_1 \leq t_2 \leq \cdots \leq t_n$.*

Since Ω is transitive, we may already assume $\mathfrak{Z}_1 = i\mathfrak{E}$. If $\mathfrak{T} = [t_1, \cdots, t_n]$ with $1 \leq t_1 \leq t_2 \leq \cdots \leq t_n$, then $(\mathfrak{T} - \mathfrak{E})(\mathfrak{T} + \mathfrak{E})^{-1} = \mathfrak{P} = [p_1, \cdots, p_n]$ with $p_k = (t_k - 1)(t_k + 1)^{-1}$ $(k = 1, \cdots, n)$, $0 \leq p_1 \leq p_2 \leq \cdots \leq p_n < 1$, and vice versa. By (5), (6) and the results of Section **6**, we have only to prove that there exists for every point $\mathfrak{Z}$ of E a unitary matrix $\mathfrak{U}_1$ satisfying $\mathfrak{U}'_1\mathfrak{Z}\mathfrak{U}_1 = \mathfrak{P} = [p_1, \cdots, p_n]$ with $0 \leq p_1 \leq p_2 \leq \cdots \leq p_n < 1$. This follows from Lemma 1: We choose $\mathfrak{U}_1 = \mathfrak{U}^{-1}$ and $p_k = q_k^{\frac{1}{2}}$; since $q_1, \cdots, q_n$ are the characteristic roots of the hermitian matrix $\mathfrak{Z}\bar{\mathfrak{Z}}$ and $\mathfrak{E} - \mathfrak{Z}\bar{\mathfrak{Z}} > 0$, we may assume $0 \leq q_1 \leq q_2 \leq \cdots \leq q_n < 1$, and $p_1, \cdots, p_n$ have the required property.

On account of the symplectic invariance of the characteristic roots $r_1, \cdots, r_n$ of $\mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1)$, the diagonal elements t_k of $\mathfrak{T}$ are given by (27). This proves that those characteristic roots are always real numbers of the interval $0 \leq r < 1$.

III. THE SYMPLECTIC METRIC.

11. We consider the cross-ratio

$$\mathfrak{R} = (\mathfrak{Z} - \mathfrak{Z}_1)(\mathfrak{Z} - \bar{\mathfrak{Z}}_1)^{-1}(\bar{\mathfrak{Z}} - \bar{\mathfrak{Z}}_1)(\bar{\mathfrak{Z}} - \mathfrak{Z}_1)^{-1}$$

as a function of $\mathfrak{Z}_1$, for any given $\mathfrak{Z}$ in H. Since the two factors $\mathfrak{Z} - \mathfrak{Z}_1$ and $\bar{\mathfrak{Z}} - \bar{\mathfrak{Z}}_1$ vanish for $\mathfrak{Z}_1 = \mathfrak{Z}$, the second differential of $\mathfrak{R}$, at the point $\mathfrak{Z}_1 = \mathfrak{Z}$, has the value

$$d^2\mathfrak{R} = 2d\mathfrak{Z}(\mathfrak{Z} - \bar{\mathfrak{Z}})^{-1}d\bar{\mathfrak{Z}}(\bar{\mathfrak{Z}} - \mathfrak{Z})^{-1} = \tfrac{1}{2}d\mathfrak{Z}\mathfrak{Y}^{-1}d\bar{\mathfrak{Z}}\mathfrak{Y}^{-1},$$

where $\mathfrak{Y}$ denotes the imaginary part of $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$. On the other hand, by (26), the trace $\sigma(\mathfrak{R})$ of $\mathfrak{R} = \mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1)$ is invariant under any cogredient whence $0 \leq r_1 \leq r_2 \leq \cdots \leq r_n < 1$ and

$$t_k = \frac{1 + r_k^{\frac{1}{2}}}{1 - r_k^{\frac{1}{2}}}. \tag{27}$$

In this case, the diagonal matrix $\mathfrak{T}$ is uniquely determined by the characteristic roots $r_1, \cdots, r_n$ of $\mathfrak{R}$. In order to complete the proof of Theorem 2, we have only to prove

LEMMA 2. *Let $\mathfrak{Z}, \mathfrak{Z}_1$ be two arbitrary points of H. There exists a symplectic transformation mapping $\mathfrak{Z}, \mathfrak{Z}_1$ into $i\mathfrak{T}, i\mathfrak{E}$ with $\mathfrak{T} = [t_1, \cdots, t_n]$ and $1 \leq t_1 \leq t_2 \leq \cdots \leq t_n$.*

Since Ω is transitive, we may already assume $\mathfrak{Z}_1 = i\mathfrak{E}$. If $\mathfrak{T} = [t_1, \cdots, t_n]$ with $1 \leq t_1 \leq t_2 \leq \cdots \leq t_n$, then $(\mathfrak{T} - \mathfrak{E})(\mathfrak{T} + \mathfrak{E})^{-1} = \mathfrak{P} = [p_1, \cdots, p_n]$ with $p_k = (t_k - 1)(t_k + 1)^{-1}$ $(k = 1, \cdots, n)$, $0 \leq p_1 \leq p_2 \leq \cdots \leq p_n < 1$, and vice versa. By (5), (6) and the results of Section **6**, we have only to prove that there exists for every point $\mathfrak{Z}$ of E a unitary matrix $\mathfrak{U}_1$ satisfying $\mathfrak{U}'_1\mathfrak{Z}\mathfrak{U}_1 = \mathfrak{P} = [p_1, \cdots, p_n]$ with $0 \leq p_1 \leq p_2 \leq \cdots \leq p_n < 1$. This follows from Lemma 1: We choose $\mathfrak{U}_1 = \mathfrak{U}^{-1}$ and $p_k = q_k^{\frac{1}{2}}$; since $q_1, \cdots, q_n$ are the characteristic roots of the hermitian matrix $\mathfrak{Z}\bar{\mathfrak{Z}}$ and $\mathfrak{E} - \mathfrak{Z}\bar{\mathfrak{Z}} > 0$, we may assume $0 \leq q_1 \leq q_2 \leq \cdots \leq q_n < 1$, and $p_1, \cdots, p_n$ have the required property.

On account of the symplectic invariance of the characteristic roots $r_1, \cdots, r_n$ of $\mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1)$, the diagonal elements t_k of $\mathfrak{T}$ are given by (27). This proves that those characteristic roots are always real numbers of the interval $0 \leq r < 1$.

III. THE SYMPLECTIC METRIC.

11. We consider the cross-ratio

$$\mathfrak{R} = (\mathfrak{Z} - \mathfrak{Z}_1)(\mathfrak{Z} - \bar{\mathfrak{Z}}_1)^{-1}(\bar{\mathfrak{Z}} - \bar{\mathfrak{Z}}_1)(\bar{\mathfrak{Z}} - \mathfrak{Z}_1)^{-1}$$

as a function of $\mathfrak{Z}_1$, for any given $\mathfrak{Z}$ in H. Since the two factors $\mathfrak{Z} - \mathfrak{Z}_1$ and $\bar{\mathfrak{Z}} - \bar{\mathfrak{Z}}_1$ vanish for $\mathfrak{Z}_1 = \mathfrak{Z}$, the second differential of $\mathfrak{R}$, at the point $\mathfrak{Z}_1 = \mathfrak{Z}$, has the value

$$d^2\mathfrak{R} = 2d\mathfrak{Z}(\mathfrak{Z} - \bar{\mathfrak{Z}})^{-1}d\bar{\mathfrak{Z}}(\bar{\mathfrak{Z}} - \mathfrak{Z})^{-1} = \tfrac{1}{2}d\mathfrak{Z}\mathfrak{Y}^{-1}d\bar{\mathfrak{Z}}\mathfrak{Y}^{-1},$$

where $\mathfrak{Y}$ denotes the imaginary part of $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$. On the other hand, by (26), the trace $\sigma(\mathfrak{R})$ of $\mathfrak{R} = \mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1)$ is invariant under any cogredient symplectic transformation of the points $\mathfrak{Z}, \mathfrak{Z}_1$. Moreover $d^2\sigma(\mathfrak{R}) = \sigma(d^2\mathfrak{R})$, and consequently the hermitian differential form

(28) $$ds^2 = \sigma(\mathfrak{Y}^{-1}d\mathfrak{Z}\mathfrak{Y}^{-1}d\bar{\mathfrak{Z}})$$

is invariant under Ω. Introducing $\mathfrak{X} = (x_{kl})$ and $\mathfrak{Y} = (y_{kl})$, we obtain

(29) $$ds^2 = \sigma(\mathfrak{Y}^{-1}d\mathfrak{X}\mathfrak{Y}^{-1}d\mathfrak{X} + \mathfrak{Y}^{-1}d\mathfrak{Y}\mathfrak{Y}^{-1}d\mathfrak{Y})$$

and in particular, for $\mathfrak{Z} = i\mathfrak{E}$,

$$ds^2 = \sum_{k=1}^{n} (dx_{kk}^2 + dy_{kk}^2) + 2\sum_{k<l} (dx_{kl}^2 + dy_{kl}^2).$$

Since Ω is transitive in H, the quadratic differential form ds^2 is obviously positive definite everywhere in H.

Let us determine the most general quadratic differential invariant Q of the symplectic group. On account of the transitivity of Ω, we have only to find Q at the point $\mathfrak{Z} = i\mathfrak{E}$ of H or, if we use the variable $\mathfrak{Z}_0 = (\mathfrak{Z} - i\mathfrak{E})(\mathfrak{Z} + i\mathfrak{E})^{-1}$ already defined in (6), at the point $\mathfrak{Z}_0 = 0$ of E. Then Q becomes a quadratic form of the elements of $\mathfrak{S} = d\mathfrak{Z}_0$ and $\bar{\mathfrak{S}} = d\bar{\mathfrak{Z}}_0$ which is, by the result of Section **6**, invariant under all transformations $\mathfrak{S} \rightarrow \mathfrak{U}'\mathfrak{S}\mathfrak{U}$ with unitary $\mathfrak{U}$. By Lemma 1, there exists for any complex symmetric $\mathfrak{S}$ a unitary matrix $\mathfrak{U}$, such that $\mathfrak{U}'\mathfrak{S}\mathfrak{U} = \mathfrak{P} = [p_1, \cdots, p_n]$ with real p_k $(k = 1, \cdots, n)$, where the p_k^2 are the characteristic roots of $\mathfrak{S}\bar{\mathfrak{S}}$. This proves that Q is a quadratic function of $p_1, \cdots, p_n$ alone. Let $k_1, \cdots, k_n$ be a permutation of the numbers $1, \cdots, n$ and ϵ_l $(l = 1, \cdots, n)$ a fourth root of unity; then the matrix $\mathfrak{U}_0$ of the substitution $s_{k_l} \rightarrow \epsilon_l s_l$ $(l = 1, \cdots, n)$ is unitary and $\mathfrak{U}'_0\mathfrak{P}\mathfrak{U}_0 = [q_1, \cdots, q_n]$ with $q_l = \epsilon_l^2 p_{k_l} = \pm p_{k_l}$ $(l = 1, \cdots, n)$. Hence Q is a symmetric polynomial in $p_1^2, \cdots, p_n^2$,

$$Q = \lambda \sum_{k=1}^{n} p_k^2 = \lambda\sigma(\mathfrak{S}\bar{\mathfrak{S}})$$

with constant λ. Consequently any quadratic differential invariant of the symplectic group is a constant multiple of ds^2.

12. We are now interested in the properties of the geodesics for the symplectic metric (28). In order to find the shortest arc connecting two arbitrarily given points $\mathfrak{Z}_1$ and $\mathfrak{Z}_2$ of H, we have, by Lemma 2, only to investigate the special case $\mathfrak{Z}_1 = i\mathfrak{E}$, $\mathfrak{Z}_2 = i\mathfrak{T} = i[t_1, \cdots, t_n]$, $1 \leq t_1 \leq t_2 \leq \cdots \leq t_n$; moreover, we may obviously assume $\mathfrak{Z}_1 \neq \mathfrak{Z}_2$, i. e., $t_n > 1$. Let now $\mathfrak{Z} = \mathfrak{Z}(u)$ be any curve connecting these two points in H and having a piecewise continuous tangent, $\mathfrak{Z}(0) = i\mathfrak{E}$, $\mathfrak{Z}(1) = i\mathfrak{T}$. We may put

$$\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Q}[\mathfrak{D}],$$

where $\mathfrak{Q} = [q_1, \cdots, q_n]$ with $q_k > 0$ $(k = 1, \cdots, n)$ and $\mathfrak{D}$ denotes a real orthogonal matrix; moreover $\mathfrak{X}$, $\mathfrak{Q}$, $\mathfrak{D}$ have again piecewise continuous derivatives; $\mathfrak{Q} = \mathfrak{E}$, $\mathfrak{D} = \mathfrak{E}$, $\mathfrak{X} = 0$ for $u = 0$; $\mathfrak{Q} = \mathfrak{T}$, $\mathfrak{D} = \mathfrak{E}$, $\mathfrak{X} = 0$ for $u = 1$. This arc has the length

$$s = \int_0^1 \sigma^{\frac{1}{2}}(\mathfrak{Y}^{-1}\dot{\mathfrak{Z}}\mathfrak{Y}^{-1}\dot{\bar{\mathfrak{Z}}})\,du,$$

where the dot denotes differentiation with respect to u.

By (29), we have $s \geq s_1$, where s_1 denotes the length of the curve

$$\mathfrak{Z} = i\mathfrak{Q}[\mathfrak{D}] \tag{30}$$

also connecting $\mathfrak{Z}_1$ and $\mathfrak{Z}_2$, and $s > s_1$, if both curves do not coincide.

We use the abbreviation $\dot{\mathfrak{D}}\mathfrak{D}' = \mathfrak{F} = (f_{kl})$. Since $\mathfrak{D}\mathfrak{D}' = \mathfrak{E}$, we have $\dot{\mathfrak{D}}\mathfrak{D}' = -\mathfrak{D}\dot{\mathfrak{D}}'$, and consequently $\mathfrak{F}$ is skew-symmetric. Differentiating the equation $\mathfrak{D}\mathfrak{Y}\mathfrak{D}' = \mathfrak{Q}$, we obtain

$$\mathfrak{D}\dot{\mathfrak{Y}}\mathfrak{D}' = \dot{\mathfrak{Q}} - \mathfrak{F}\mathfrak{Q} + \mathfrak{Q}\mathfrak{F}$$

$$\begin{aligned}
\mathfrak{D}\mathfrak{Y}^{-1}\dot{\mathfrak{Y}}\mathfrak{Y}^{-1}\dot{\mathfrak{Y}}\mathfrak{D}' &= \mathfrak{Q}^{-1}(\dot{\mathfrak{Q}} - \mathfrak{F}\mathfrak{Q} + \mathfrak{Q}\mathfrak{F})\mathfrak{Q}^{-1}(\dot{\mathfrak{Q}} - \mathfrak{F}\mathfrak{Q} + \mathfrak{Q}\mathfrak{F}) \\
&= \mathfrak{F}^2 + \mathfrak{Q}^{-1}\mathfrak{F}^2\mathfrak{Q} + \mathfrak{Q}^{-1}\dot{\mathfrak{Q}}\mathfrak{Q}^{-1}\dot{\mathfrak{Q}} - \mathfrak{Q}^{-1}\mathfrak{F}\mathfrak{Q}\mathfrak{F} - \mathfrak{F}\mathfrak{Q}^{-1}\mathfrak{F}\mathfrak{Q} \\
&\quad - \mathfrak{Q}^{-1}\dot{\mathfrak{Q}}\mathfrak{Q}^{-1}\mathfrak{F}\mathfrak{Q} - \mathfrak{Q}^{-1}\mathfrak{F}\dot{\mathfrak{Q}} + \mathfrak{Q}^{-1}\dot{\mathfrak{Q}}\mathfrak{F} + \mathfrak{F}\mathfrak{Q}^{-1}\dot{\mathfrak{Q}}
\end{aligned}$$

$$\begin{aligned}
\sigma(\mathfrak{Y}^{-1}\dot{\mathfrak{Y}}\mathfrak{Y}^{-1}\dot{\mathfrak{Y}}) &= 2\sigma(\mathfrak{F}^2) - 2\sigma(\mathfrak{F}\mathfrak{Q}\mathfrak{F}\mathfrak{Q}^{-1}) + \sigma(\mathfrak{Q}^{-1}\dot{\mathfrak{Q}}\mathfrak{Q}^{-1}\dot{\mathfrak{Q}}) \\
&= \sum_{k,l=1}^{n} f_{kl}^2 \frac{(q_k - q_l)^2}{q_k q_l} + \sum_{k=1}^{n} \left(\frac{\dot{q}_k}{q_k}\right)^2. \qquad (31)
\end{aligned}$$

On the other hand, the formula

$$\sum_{k=1}^{n} Q_k^2 = (c_1 Q_1 + \cdots + c_n Q_n)^2 + \tfrac{1}{2} \sum_{k,l=1}^{n} (c_k Q_l - c_l Q_k)^2 \tag{32}$$

holds for $c_1^2 + c_2^2 + \cdots + c_n^2 = 1$ and in particular with

$$Q_k = \frac{\dot{q}_k}{q_k}, \qquad c_k = \rho^{-1} \log t_k \qquad (k = 1, \cdots, n),$$

where

$$\rho = \left(\sum_{k=1}^{n} \log^2 t_k\right)^{\frac{1}{2}} > 0. \tag{33}$$

By (31) and (32),

$$s_1 \geq \int_0^1 (c_1 Q_1 + \cdots + c_n Q_n)\,du = \sum_{k=1}^{n} c_k \log t_k = \rho,$$

with the sign of inequality, if not all the three conditions

$$f_{kl}(q_k - q_l) = 0 \qquad (k, l = 1, \cdots, n), \tag{34}$$

$$c_k Q_l - c_l Q_k = 0 \qquad (k, l = 1, \cdots, n), \tag{35}$$

$$\sum_{k=1}^{n} c_k Q_k \geq 0 \tag{36}$$

are fulfilled. By (35),

$$\log t_n \log q_k = \log t_k \log q_n \qquad (k = 1, \cdots, n),$$

whence

$$q_k = t_k^{\gamma} \qquad (k = 1, \cdots, n) \tag{37}$$

with $\gamma = \gamma(u)$, $\gamma(0) = 0$, $\gamma(1) = 1$. By (36), the function $\gamma(u)$ is monotone. By (34) and (37),

$$f_{kl}(t_k - t_l) = 0 \qquad (k, l = 1, \cdots, n)$$
$$\mathfrak{D}\dot{\mathfrak{D}}'\mathfrak{T} + \mathfrak{T}\dot{\mathfrak{D}}\mathfrak{D}' = 0$$
$$(\mathfrak{D}'\mathfrak{T}\mathfrak{D})^{\cdot} = \dot{\mathfrak{D}}'\mathfrak{T}\mathfrak{D} + \mathfrak{D}'\mathfrak{T}\dot{\mathfrak{D}} = 0$$
$$\mathfrak{D}'\mathfrak{T}\mathfrak{D} = \mathfrak{T};$$

consequently $\mathfrak{T}\mathfrak{D} = \mathfrak{D}\mathfrak{T}$ and, by (37), also $\mathfrak{Q}\mathfrak{D} = \mathfrak{D}\mathfrak{Q}$. This proves, by (30), that the minimum ρ of s is attained, if and only if $\mathfrak{Z} = i[t_1^{\gamma}, \cdots, t_n^{\gamma}]$, where $\gamma(u)$ is a monotone function with $\gamma(0) = 0$, $\gamma(1) = 1$. We may replace $\gamma(u)$ by u and obtain the curve $\mathfrak{Z} = i[t_1^{u}, \cdots, t_n^{u}]$ as the unique solution. Introducing the length of arc $\tau = \rho u$, we have $\mathfrak{Z} = i[e^{c_1\tau}, \cdots, e^{c_n\tau}]$ with $c_k = \rho^{-1} \log t_k$ $(k = 1, \cdots, n)$ and $c_1^2 + \cdots + c_n^2 = 1$.

13. Let $\mathfrak{Z}$ and $\mathfrak{Z}_1$ be again two arbitrary points of H. By (33) and the results of Section **10**, the symplectic distance $\rho = \rho(\mathfrak{Z}, \mathfrak{Z}_1)$ is given by

$$\rho^2 = \sum_{k=1}^{n} \log^2 \frac{1 + r_k^{\frac{1}{2}}}{1 - r_k^{\frac{1}{2}}}, \tag{38}$$

where $r_1, \cdots, r_n$ denote the characteristic roots of the cross-ratio $\mathfrak{R} = \mathfrak{R}(\mathfrak{Z}, \mathfrak{Z}_1)$. Since

$$\log^2 \frac{1 + r^{\frac{1}{2}}}{1 - r^{\frac{1}{2}}} = 4r \left(\sum_{k=0}^{\infty} \frac{r^k}{2k+1} \right)^2 \qquad (0 \leq r < 1)$$

and

$$\sum_{k=1}^{n} r_k^{\,l} = \sigma(\mathfrak{R}^l) \qquad (l = 1, 2, \cdots),$$

we may write

$$\rho^2 = \sigma \left(\log^2 \frac{1 + \mathfrak{R}^{\frac{1}{2}}}{1 - \mathfrak{R}^{\frac{1}{2}}} \right)$$

with

$$\log^2 \frac{1+\mathfrak{N}^{\frac{1}{2}}}{1-\mathfrak{N}^{\frac{1}{2}}} = 4\mathfrak{N}\left(\sum_{k=0}^{\infty} \frac{\mathfrak{N}^k}{2k+1}\right)^2.$$

By the results of this and the preceding section, Theorem 3 and Theorem 4 are completely proved.

14. In order to calculate the differential equation of the geodesics and the tensor of curvature, we determine the first variation δs. We consider any curve $\mathfrak{Z} = \mathfrak{Z}(s)$ $(0 \leq s \leq s_0)$, where the parameter s denotes the length of arc. Then $\sigma(\mathfrak{Y}^{-1}\dot{\mathfrak{Z}}\mathfrak{Y}^{-1}\dot{\bar{\mathfrak{Z}}}) = 1$ and

$$\delta s = \tfrac{1}{2}\int_0^{s_0} \delta\sigma(\mathfrak{Y}^{-1}\dot{\mathfrak{Z}}\mathfrak{Y}^{-1}\dot{\bar{\mathfrak{Z}}})\, ds.$$

Using the abbreviations $\dot{\mathfrak{Z}}\mathfrak{Y}^{-1}\dot{\bar{\mathfrak{Z}}} = \mathfrak{B}$, $\mathfrak{Y}^{-1}\dot{\mathfrak{Z}}\mathfrak{Y}^{-1} = \mathfrak{W}$ and denoting by R the real part, we find

$$\delta\sigma(\mathfrak{Y}^{-1}\dot{\mathfrak{Z}}\mathfrak{Y}^{-1}\dot{\bar{\mathfrak{Z}}}) = 2R\sigma(\mathfrak{B}\delta\mathfrak{Y}^{-1} + (\mathfrak{W}\delta\bar{\mathfrak{Z}})^{\cdot} - \dot{\mathfrak{W}}\delta\bar{\mathfrak{Z}})$$

$$\delta\mathfrak{Y}^{-1} = \frac{i}{2}\,\mathfrak{Y}^{-1}(\delta\mathfrak{Z} - \delta\bar{\mathfrak{Z}})\mathfrak{Y}^{-1}$$

$$\dot{\mathfrak{W}} = \mathfrak{Y}^{-1}\ddot{\mathfrak{Z}}\mathfrak{Y}^{-1} + i\mathfrak{Y}^{-1}\dot{\mathfrak{Z}}\mathfrak{Y}^{-1}\dot{\mathfrak{Z}}\mathfrak{Y}^{-1} - \frac{i}{2}\,\mathfrak{Y}^{-1}(\mathfrak{B} + \bar{\mathfrak{B}})\mathfrak{Y}^{-1},$$

whence

$$\delta s = -R\int_0^{s_0} \sigma(\mathfrak{Y}^{-1}(\ddot{\mathfrak{Z}} + i\dot{\mathfrak{Z}}\mathfrak{Y}^{-1}\dot{\mathfrak{Z}})\mathfrak{Y}^{-1}\delta\bar{\mathfrak{Z}})\, ds.$$

Consequently

(39) $$\ddot{\mathfrak{Z}} = -i\dot{\mathfrak{Z}}\mathfrak{Y}^{-1}\dot{\mathfrak{Z}}$$

is the differential equation of the geodesic lines.

It is easy to perform the integration without using Section **12.** On account of the symplectic invariance of the geodesics and the transitivity of Ω, it is sufficient to integrate (39) for the initial point $\mathfrak{Z} = i\mathfrak{E}$ and an arbitrary direction $\dot{\mathfrak{Z}} = \mathfrak{K}$ through this point; obviously $\sigma(\mathfrak{K}\bar{\mathfrak{K}}) = 1$. By Section **6**, the mapping

(40) $$\frac{\mathfrak{Z} - i\mathfrak{E}}{\mathfrak{Z} + i\mathfrak{E}} \to \mathfrak{U}'\,\frac{\mathfrak{Z} - i\mathfrak{E}}{\mathfrak{Z} + i\mathfrak{E}}\,\mathfrak{U}$$

is symplectic for arbitrary unitary $\mathfrak{U}$. Under this mapping, the direction $\mathfrak{K}$ through $i\mathfrak{E}$ is replaced by $\mathfrak{U}'\mathfrak{K}\mathfrak{U}$. By Lemma 1, we can determine $\mathfrak{U}$ such that $\mathfrak{U}'\mathfrak{K}\mathfrak{U} = i\mathfrak{G} = i[g_1, \cdots, g_n]$ with $0 \leq g_1 \leq \cdots \leq g_n$; since $\sigma(\mathfrak{K}\bar{\mathfrak{K}}) = 1$, we have $g_1^2 + \cdots + g_n^2 = 1$. It is now sufficient to integrate (39) for the initial conditions $\mathfrak{Z} = i\mathfrak{E}$, $\dot{\mathfrak{Z}} = i\mathfrak{G}$. Obviously the solution is $\mathfrak{Z} = i \exp s\mathfrak{G}$. Consequently the most general geodesic line is

$$(\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1} = i[e^{g_1 s}, \cdots, e^{g_n s}],$$

where the left-hand side is an arbitrary symplectic transformation of $\mathfrak{Z}$ and $g_1, \cdots, g_n$ are arbitrary real numbers with $0 \leq g_1 \leq \cdots \leq g_n$, $g_1^2 + \cdots + g_n^2 = 1$.

15. We shall now establish directly, without using Section **12**, that there exists exactly one geodesic through two arbitrarily given points $\mathfrak{Z}_1$ and $\mathfrak{Z}_2 \neq \mathfrak{Z}_1$ of H. We may again assume $\mathfrak{Z}_1 = i\mathfrak{E}$, $\mathfrak{Z}_2 = i\mathfrak{T} = i[t_1, \cdots, t_n]$, $1 \leq t_1 \leq \cdots \leq t_n$,

$$\rho = \Big(\sum_{k=1}^{n} \log^2 t_k\Big)^{\frac{1}{2}} > 0.$$

Defining $g_k = \rho^{-1} \log t_k$ $(k = 1, \cdots, n)$, we obtain the geodesic line

(41) $$\mathfrak{Z} = i \exp s\mathfrak{G}.$$

Since (40) is the most general symplectic mapping with the fixed point $i\mathfrak{E}$, any geodesic through this point has an equation

(42) $$\frac{\mathfrak{Z} - i\mathfrak{E}}{\mathfrak{Z} + i\mathfrak{E}} = \mathfrak{U}' \, \frac{\exp s\mathfrak{H} - \mathfrak{E}}{\exp s\mathfrak{H} + \mathfrak{E}} \, \mathfrak{U}$$

with unitary $\mathfrak{U}$ and $\mathfrak{H} = [h_1, \cdots, h_n]$, $0 \leq h_1 \leq \cdots \leq h_n$, $h_1^2 + \cdots + h_n^2 = 1$. If this curve goes also through the point $\mathfrak{Z} = i\mathfrak{T}$ of (41), we obtain

$$\mathfrak{U}\left(\frac{\mathfrak{E} - \mathfrak{T}}{\mathfrak{E} + \mathfrak{T}}\right)^2 = \left(\frac{\mathfrak{E} - \exp s_0\mathfrak{H}}{\mathfrak{E} + \exp s_0\mathfrak{H}}\right)^2 \mathfrak{U}$$

for a certain $s_0 > 0$, whence $\mathfrak{T} = \exp s_0\mathfrak{H}$, $s_0\mathfrak{H} = \rho\mathfrak{G}$, $s_0 = \rho$, $\mathfrak{H} = \mathfrak{G}$. Moreover $\mathfrak{U}$ and $(\exp s_0\mathfrak{H} - \mathfrak{E})(\exp s_0\mathfrak{H} + \mathfrak{E})^{-1}$ are permutable, hence also $\mathfrak{U}$ and $(\exp s\mathfrak{H} - \mathfrak{E})(\exp s\mathfrak{H} + \mathfrak{E})^{-1}$. Putting $s = \rho$ in (42), we find $\mathfrak{U}'\mathfrak{U} = \mathfrak{E}$, and consequently the geodesics (41) and (42) coincide.

This result proves again, by a general theorem from the calculus of variations, that there exists exactly one shortest arc between two arbitrarily given points of H.

16. By the minimum property of the geodesic arc, the symplectic distance $\rho(\mathfrak{Z}_1, \mathfrak{Z}_2)$ satisfies the triangle inequality

$$\rho(\mathfrak{Z}_1, \mathfrak{Z}_3) \leq \rho(\mathfrak{Z}_1, \mathfrak{Z}_2) + \rho(\mathfrak{Z}_2, \mathfrak{Z}_3)$$

for three arbitrary points $\mathfrak{Z}_1, \mathfrak{Z}_2, \mathfrak{Z}_3$ of H, and the sign of equality is true, if and only if $\mathfrak{Z}_2$ is a point on the uniquely determined geodesic arc between $\mathfrak{Z}_1$

and $\mathfrak{Z}_3$. Obviously $\rho(\mathfrak{Z}, \mathfrak{Z}_1)$ is a continuous function of $\mathfrak{Z}$. If G is any compact point set in H, then $\rho(\mathfrak{Z}, \mathfrak{Z}_1) \leq c$ for all $\mathfrak{Z}$ in G, where c is a positive constant depending only upon $\mathfrak{Z}_1$ and G. Let us prove that also the converse statement is true: If c is an arbitrary positive constant and $\mathfrak{Z}_1$ any given point of H, then the inequality $\rho(\mathfrak{Z}, \mathfrak{Z}_1) \leq c$ defines a compact set G of points $\mathfrak{Z}$ in H. It is sufficient to prove this in the special case $\mathfrak{Z}_1 = i\mathfrak{E}$. By the definition of the cross-ratio,

$$\mathfrak{R}(\mathfrak{Z}, i\mathfrak{E}) = \mathfrak{Z}_0\bar{\mathfrak{Z}}_0,$$

where $\mathfrak{Z}_0 = (\mathfrak{Z} - i\mathfrak{E})(\mathfrak{Z} + i\mathfrak{E})^{-1}$ is the image of $\mathfrak{Z}$ under the transformation (6) mapping H onto E. We infer from (38) that the characteristic roots r_k of the hermitian matrix $\mathfrak{Z}_0\bar{\mathfrak{Z}}_0$ satisfy an inequality

$$0 \leq r_k \leq \vartheta < 1 \qquad (k = 1, \cdots, n)$$

for all $\mathfrak{Z}$ with $\rho(\mathfrak{Z}, \mathfrak{Z}_1) \leq c$, where ϑ depends only upon c. Since an arbitrary symmetric matrix $\mathfrak{Z}_0$ is a point of E, if the characteristic roots of $\mathfrak{Z}_0\bar{\mathfrak{Z}}_0$ are < 1, all limit points of the images $\mathfrak{Z}_0$ of the points $\mathfrak{Z}$ in G belong to E again, and consequently G is compact.

17. Let

$$ds^2 = \sum_{k,l=1}^{m} g_{kl}dx_k dx_l \tag{43}$$

be a Riemann metric in an m-dimensional space and let

$$\ddot{x}_k = -\sum_{p,q=1}^{m} \{pq, k\}\dot{x}_p\dot{x}_q \qquad (k = 1, \cdots, m)$$

be the differential equations of the geodesics, so that $\{pq, k\}$ denotes the Christoffel symbol of the second kind. The Riemann tensor of curvature R is obtained in the following way: Define two covariant differentials $\delta_1 u_k$ and $\delta_2 u_k$ by

$$\delta_r u_k = -\sum_{p,q} \{pq, k\} u_p \delta_r x_q \qquad (r = 1, 2); \tag{44}$$

then

$$R = \sum_{k,l} g_{kl} v_k (\delta_1\delta_2 - \delta_2\delta_1) u_l = \sum_{k,l,p,q} R_{klpq} u_k v_l \delta_1 x_p \delta_2 x_q, \tag{45}$$

where u_k, v_l, $\delta_1 x_p$, $\delta_2 x_q$ are the components of 4 covariant vectors.

In the case of the symplectic metric (28), the differential equations of the geodesics are given by (39). Instead of (44), we may write now

$$2i\delta_r\mathfrak{U} = \mathfrak{U}\mathfrak{Y}^{-1}\delta_r\mathfrak{Z} + \delta_r\mathfrak{Z}\mathfrak{Y}^{-1}\mathfrak{U} \qquad (r = 1, 2)$$

with complex symmetric $\mathfrak{U} = (u_{kl})$, and we obtain

$$-4\delta_1\delta_2\mathfrak{U} = (\mathfrak{U}\mathfrak{Y}^{-1}\delta_1\bar{\mathfrak{Z}} + \delta_1\mathfrak{Z}\mathfrak{Y}^{-1}\mathfrak{U})\mathfrak{Y}^{-1}\delta_2\mathfrak{Z} + \delta_2\mathfrak{Z}\mathfrak{Y}^{-1}(\mathfrak{U}\mathfrak{Y}^{-1}\delta_1\mathfrak{Z} + \delta_1\bar{\mathfrak{Z}}\mathfrak{Y}^{-1}\mathfrak{U})$$

$$(46) \qquad 4(\delta_1\delta_2 - \delta_2\delta_1)\mathfrak{U} = \mathfrak{F}\mathfrak{Y}^{-1}\mathfrak{U} + \mathfrak{U}\mathfrak{Y}^{-1}\mathfrak{F}',$$

where

$$(47) \qquad \mathfrak{F} = \delta_1\mathfrak{Z}\mathfrak{Y}^{-1}\delta_2\bar{\mathfrak{Z}} - \delta_2\mathfrak{Z}\mathfrak{Y}^{-1}\delta_1\bar{\mathfrak{Z}}.$$

Introducing

$$(48) \qquad \mathfrak{G} = \mathfrak{U}\mathfrak{Y}^{-1}\bar{\mathfrak{V}} - \mathfrak{V}\mathfrak{Y}^{-1}\bar{\mathfrak{U}}$$

with complex symmetric $\mathfrak{V} = (v_{kl})$, we find, by (28), (45) and (46),

$$(49) \qquad \begin{aligned} 4R &= \sigma(\mathfrak{Y}^{-1}\mathfrak{V}\mathfrak{F}\mathfrak{Y}^{-1}\bar{\mathfrak{U}} + \mathfrak{Y}^{-1}\mathfrak{F}\mathfrak{Y}^{-1}\mathfrak{U}\mathfrak{Y}^{-1}\bar{\mathfrak{V}}) \\ &= \sigma(\mathfrak{Y}^{-1}\mathfrak{F}\mathfrak{Y}^{-1}\mathfrak{G}) = -\sigma(\mathfrak{Y}^{-1}\mathfrak{F}\mathfrak{Y}^{-1}\bar{\mathfrak{G}}'). \end{aligned}$$

In order to determine the Gaussian curvature, we have to take two arbitrary different directions $\delta_1\mathfrak{Z}$ and $\delta_2\mathfrak{Z}$ at the point $\mathfrak{Z}$ and to choose $\mathfrak{U} = \delta_1\mathfrak{Z}$, $\mathfrak{V} = \delta_2\mathfrak{Z}$. Then

$$R = -\tfrac{1}{4}\sigma(\mathfrak{Y}^{-1}\mathfrak{F}\mathfrak{Y}^{-1}\bar{\mathfrak{F}}') \leq 0,$$

where the sign of equality is true only for $\mathfrak{F} = 0$. Consequently the curvature is negative for $\delta_1\mathfrak{Z}\mathfrak{Y}^{-1}\delta_2\bar{\mathfrak{Z}} \neq \delta_2\mathfrak{Z}\mathfrak{Y}^{-1}\delta_1\bar{\mathfrak{Z}}$, and 0 otherwise.

It may easily be seen, that the contracted tensor of curvature is $\frac{n+1}{2}\,ds^2$; hence we have an Einstein metric with cosmological term.

18. Allendoerfer and Fenchel proved independently the following generalization of the Gauss-Bonnet formula concerning the curvatura integra of a closed two-dimensional surface. Let F be a closed manifold with the Riemann metric (43) and an even number m of dimensions. For every permutation $k_1, \cdots, k_m$ of the numbers $1, \cdots, m$ we define $\epsilon_{k_1 \ldots k_m} = 1$, if the permutation is even, and $= -1$, if the permutation is odd. Let g be the determinant $|g_{kl}|$ and

$$(50) \quad K = (2^{m/2}gm\,!)^{-1}\Sigma R_{k_1k_2l_1l_2}R_{k_3k_4l_3l_4}\cdots R_{k_{m-1}k_ml_{m-1}l_m}\epsilon_{k_1k_2\ldots k_{m-1}k_m}\epsilon_{l_1l_2\ldots l_{m-1}l_m},$$

where the summation is extended over all permutations $k_1, \cdots, k_m$ and $l_1, \cdots, l_m$ of $1, \cdots, m$; moreover let $d\omega$ be the volume element in the given metric. Then the Euler characteristic of F has the value

$$(51) \qquad \chi = \pi^{-(m+1)/2}\Gamma\left(\frac{m+1}{2}\right)\int_F K\,d\omega.$$

For practical purposes, the sum on the right-hand side of (50) may be calculated in the following manner: Determine the single terms of the polynomial

$$R^{m/2} = (\Sigma R_{klpq} u_k v_l u^*_p v^*_q)^{m/2}$$

and replace every product $u_{k_1} v_{k_2} \cdots u_{k_{m-1}} v_{k_m} u^*_{l_1} v^*_{l_2} \cdots u^*_{l_{m-1}} v^*_{l_m}$ by $\epsilon_{k_1 \ldots k_m} \epsilon_{l_1 \ldots l_m}$.

In the case of the symplectic metric, the transitive group Ω of isometric mappings exists, and consequently the invariant K is constant in the whole space H. In order to find this constant value, we may assume $\mathfrak{Z} = i\mathfrak{E}$. Writing $\mathfrak{U}^*, \mathfrak{V}^*$ instead of $\delta_1\mathfrak{Z}, \delta_2\mathfrak{Z}$, we obtain, by (47), (48) and (49),

$$R = \tfrac{1}{4}\sigma(\mathfrak{Q}\mathfrak{Q}^*)$$

with

$$\mathfrak{Q} = \mathfrak{U}\bar{\mathfrak{V}} - \mathfrak{V}\bar{\mathfrak{U}}, \qquad \mathfrak{Q}^* = \mathfrak{U}^*\bar{\mathfrak{V}}^* - \mathfrak{V}^*\bar{\mathfrak{U}}^*,$$

where $\mathfrak{U}, \mathfrak{V}, \mathfrak{U}^*, \mathfrak{V}^*$ are indeterminate symmetric complex matrices. Hence

(52) $$R^\nu = 2^{-2\nu} \sum q_{k_1 l_1} \cdots q_{k_\nu l_\nu} q^*_{k_1 l_1} \cdots q^*_{k_\nu l_\nu} \qquad (\nu = 1, 2, \cdots)$$

with

$$q_{kl} = \sum_{r=1}^{n} (u_{kr}\bar{v}_{rl} - v_{kr}\bar{u}_{rl}), \qquad q^*_{kl} = \sum_{r=1}^{n} (u^*_{kr}\bar{v}^*_{rl} - v^*_{kr}\bar{u}^*_{rl}),$$

where $k_1, l_1, \cdots, k_\nu, l_\nu$ run independently from 1 to n. We choose

$$\nu = \frac{m}{2} = \frac{n(n+1)}{2}.$$

Let us denote the ν elements u_{kl} $(1 \leq k \leq l \leq n)$ of $\mathfrak{U} = (u_{kl})$ in lexicographic order by $u_1, \cdots u_\nu$, their conjugates by $u_{\nu+1}, \cdots, u_m$, and introduce the corresponding notation for the elements of $\mathfrak{V}, \mathfrak{U}^*, \mathfrak{V}^*$. Replacing every term $u_{g_1} v_{g_2} \cdots u_{g_{m-1}} v_{g_m}$ in $q_{k_1 l_1} \cdots q_{k_\nu l_\nu}$ by $\epsilon_{g_1 \ldots g_m}$, we get the expression $2^\nu \eta_{k_1 l_1 \ldots k_\nu l_\nu}$ with

(53) $$\eta_{k_1 l_1 \ldots k_\nu l_\nu} = \Sigma \epsilon_{g_1 \ldots g_m},$$

where $g_1, \cdots, g_m$ run over all permutations of $1, \cdots, m$ such that the m conditions

$$u_{k_h r_h} = u_{g_{2h-1}}, \qquad \bar{v}_{l_h r_h} = v_{g_{2h}} \qquad (h = 1, \cdots, \nu)$$

have a solution $r_1, \cdots, r_\nu$. By (52), the sum of the right-hand side of (50) has, for $\mathfrak{Z} = i\mathfrak{E}$, the positive integral value

(54) $$a_n = \Sigma \eta^2_{k_1 l_1 \ldots k_\nu l_\nu}.$$

Moreover g is the determinant of the quadratic form $\sigma(\mathfrak{Y}^{-1} d\mathfrak{Z} \mathfrak{Y}^{-1} d\bar{\mathfrak{Z}})$ of the variables dz_{kl} and $d\bar{z}_{kl}$ $(1 \leq k \leq l \leq n)$; hence

$$g = (-1)^\nu 2^{-2n},$$

for $\mathfrak{Z} = i\mathfrak{E}$, and consequently

$$K = (-1)^{\nu} 2^{2n-\nu} \frac{a_n}{(2\nu)!}. \tag{55}$$

On the other hand,

$$d\omega = 2^{\nu-n} |\mathfrak{Y}|^{n-1} \prod_{k \leq l} (dx_{kl} dy_{kl}) = 2^{\nu-n} \prod_{k \leq l} (dx_{kl} dY_{kl}) \tag{56}$$

with $(Y_{kl}) = \mathfrak{Y}^{-1}$. Since

$$\pi^{-\nu-\frac{1}{2}} \Gamma(\nu + \tfrac{1}{2}) \frac{2^{2n-\nu}}{(2\nu)!} 2^{\nu-n} = (2^{n^2} \pi^{\nu} \nu!)^{-1},$$

we obtain, by (51), (55) and (56),

$$\chi = c_n (-\pi)^{-n(n+1)/2} \int_F dv,$$

where the positive rational number

$$c_n = \frac{a_n}{2^{n^2}[(n^2+n)/2]!}$$

is defined in (53), (54) and

$$dv = \prod_{k \leq l} (dx_{kl} dY_{kl}) \tag{57}$$

denotes the euclidean volume element in the space of $\mathfrak{X}, \mathfrak{Y}^{-1}$.

We find by direct calculation $a_1 = 1$, $a_2 = 6 \cdot 3!$, $a_3 = 90 \cdot 6!$ and therefore $c_1 = \frac{1}{2}$, $c_2 = \frac{3}{8}$, $c_3 = \frac{45}{256}$, but a simple explicit formula for a_n and c_n in the case of an arbitrary n is not known.

The proof of Theorem 5 is now accomplished.

IV. DISCONTINUOUS GROUPS.

19. A group of mappings of H onto itself is called discontinuous (in H), if for every $\mathfrak{Z}$ of H the set of images of $\mathfrak{Z}$ has no limit point in H. Since H can be covered by a countable number of compact domains, the number of elements of a discontinuous group is either finite or countably infinite. We shall assume, moreover, that the mappings are analytic. Then, by Theorem 1, they form a subgroup Δ of the symplectic group.

On the other hand, let us consider the definition of a *discrete* group. A group of matrices $\mathfrak{M}$ with real (or complex) elements is called discrete, if every infinite sequence of different $\mathfrak{M}$ diverges. It is obvious that a discontinuous group of symplectic matrices is discrete. Let us now prove the confor $\mathfrak{Z} = i\mathfrak{E}$, and consequently

$$K = (-1)^{\nu} 2^{2n-\nu} \frac{a_n}{(2\nu)!} \,. \tag{55}$$

On the other hand,

$$d\omega = 2^{\nu-n} \,|\, \mathfrak{Y} \,|^{n-1} \prod_{k \leq l} (dx_{kl} dy_{kl}) = 2^{\nu-n} \prod_{k \leq l} (dx_{kl} dY_{kl}) \tag{56}$$

with $(Y_{kl}) = \mathfrak{Y}^{-1}$. Since

$$\pi^{-\nu-\frac{1}{2}} \Gamma(\nu + \tfrac{1}{2}) \frac{2^{2n-\nu}}{(2\nu)!} 2^{\nu-n} = (2^{n^2} \pi^{\nu} \nu!)^{-1},$$

we obtain, by (51), (55) and (56),

$$\chi = c_n (-\pi)^{-n(n+1)/2} \int_F dv,$$

where the positive rational number

$$c_n = \frac{a_n}{2^{n^2} [(n^2 + n)/2]!}$$

is defined in (53), (54) and

$$dv = \prod_{k \leq l} (dx_{kl} dY_{kl}) \tag{57}$$

denotes the euclidean volume element in the space of $\mathfrak{X}, \mathfrak{Y}^{-1}$.

We find by direct calculation $a_1 = 1$, $a_2 = 6 \cdot 3!$, $a_3 = 90 \cdot 6!$ and therefore $c_1 = \frac{1}{2}$, $c_2 = \frac{3}{8}$, $c_3 = \frac{45}{256}$, but a simple explicit formula for a_n and c_n in the case of an arbitrary n is not known.

The proof of Theorem 5 is now accomplished.

IV. DISCONTINUOUS GROUPS.

19. A group of mappings of H onto itself is called discontinuous (in H), if for every $\mathfrak{Z}$ of H the set of images of $\mathfrak{Z}$ has no limit point in H. Since H can be covered by a countable number of compact domains, the number of elements of a discontinuous group is either finite or countably infinite. We shall assume, moreover, that the mappings are analytic. Then, by Theorem 1, they form a subgroup Δ of the symplectic group.

On the other hand, let us consider the definition of a *discrete* group. A group of matrices $\mathfrak{M}$ with real (or complex) elements is called discrete, if every infinite sequence of different $\mathfrak{M}$ diverges. It is obvious that a discontinuous group of symplectic matrices is discrete. Let us now prove the converse of this statement. If Δ is a non-discontinuous group of symplectic mappings

$$\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}, \tag{58}$$

we can find a point $\mathfrak{Z}$ of H and an infinite sequence of different matrices

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$$

in Δ, such that the corresponding sequence (58) tends to a limit $\mathfrak{Z}^*_1$ in H. Denoting by $\mathfrak{Y}, \mathfrak{Y}^*, \mathfrak{Y}^*_1$ the imaginary parts of $\mathfrak{Z}, \mathfrak{Z}^*, \mathfrak{Z}^*_1$, we have, by (25),

$$\mathfrak{Y}^* = \mathfrak{Y}\{(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}\}. \tag{59}$$

Now $\mathfrak{Y}^*$ is bounded, $\mathfrak{Y}$ is fixed and $\mathfrak{Y} > 0$. By (59), the sequence of matrices $(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ is bounded; moreover, the square of the absolute value of the determinant $|\mathfrak{C}\mathfrak{Z} + \mathfrak{D}|$ tends to the limit $|\mathfrak{Y}|\,|\mathfrak{Y}^*_1|^{-1}$; hence also $\mathfrak{C}\mathfrak{Z} + \mathfrak{D}$ is bounded. Since $\mathfrak{C}$ is the imaginary part of $(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})\mathfrak{Y}^{-1}$ and $\mathfrak{D} = (\mathfrak{C}\mathfrak{Z} + \mathfrak{D}) - \mathfrak{C}\mathfrak{Z}$, the matrices $\mathfrak{C}, \mathfrak{D}$ are bounded. It follows from $\mathfrak{A}\mathfrak{Z} + \mathfrak{B} = \mathfrak{Z}^*(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})$ that also $\mathfrak{A}$ and $\mathfrak{B}$ are bounded. Consequently there exists a converging subsequence of matrices $\mathfrak{M}$, and Δ is non-discrete.

20. For any point set P in H, we define the diameter $\delta(P)$ as the least upper bound of the distance $\rho(\mathfrak{Z}, \mathfrak{Z}^*)$, where $\mathfrak{Z}$ and $\mathfrak{Z}^*$ run independently over all points of P. The diameter is finite, if P is compact. The distance $\rho(P, P^*)$ of two point sets P, P^* in H is defined as the greatest lower bound of the distance $\rho(\mathfrak{Z}, \mathfrak{Z}^*)$, $\mathfrak{Z}$ running over P and $\mathfrak{Z}^*$ over P^*. By the triangle inequality,

$$\delta(P + P^*) \leq \rho(P, P^*) + \delta(P) + \delta(P^*). \tag{60}$$

Let $D_1, D_2, \cdots$ be the elements of the discontinuous group Δ and let D_1 be the identity. We denote by $D_k(P) = P_k$ the image of the set P under D_k $(k = 1, 2, \cdots)$. We assume now that P and another point set Q in H are compact. We shall prove that the distance $\rho(Q, P_k)$ tends to infinity with k. Let us first consider the case of two points $Q = \mathfrak{Z}$, $P = \mathfrak{Z}_1$. By Section **16**, the condition $\rho(\mathfrak{Z}, \mathfrak{Z}^*) \leq c$ defines, for arbitrarily given $c > 0$ and variable $\mathfrak{Z}^*$, a compact point set in H; hence the inequality $\rho(\mathfrak{Z}, \mathfrak{Z}_k) \leq c$ holds only for a finite number of indices k so that $\rho(\mathfrak{Z}, \mathfrak{Z}_k) \to \infty$ for $k \to \infty$. Consider now the general case for P and Q. By (60),

$$\rho(Q, P_k) \geq \delta(Q + P_k) - \delta(Q) - \delta(P_k).$$

Choosing a point $\mathfrak{Z}$ in Q and a point $\mathfrak{Z}_1$ in P, we have $\delta(Q + P_k) \geq \rho(\mathfrak{Z}, \mathfrak{Z}_k) \to \infty$ and $\delta(P_k) = \delta(P)$, whence $\rho(Q, P_k) \to \infty$.

A point $\mathfrak{Z}$ of H is called a fixed point of Δ, if $D_k(\mathfrak{Z}) = \mathfrak{Z}$ for at least one index $k > 1$. Let P be an arbitrary compact domain in H, e. g., the domain $\rho(\mathfrak{Z}, i\mathfrak{E}) \leq 1$. Since $\rho(P, P_k) \to \infty$ for $k \to \infty$, there exists only a finite number of values k, such that the equation $D_k(\mathfrak{Z}) = \mathfrak{Z}$ has a solution $\mathfrak{Z}$ in P. But this equation, for any $k > 1$, defines an algebraic manifold in H, and consequently we may construct a point of P which is not contained in any of those manifolds; in other words, we may certainly construct a point $\mathfrak{Z}_1$ of H which is not a fixed point. The images $\mathfrak{Z}_k = D_k(\mathfrak{Z}_1)$ of $\mathfrak{Z}_1$ are then all different one from another.

21. We denote by F the set of all points $\mathfrak{Z}$ satisfying all the inequalities

$$\rho(\mathfrak{Z}, \mathfrak{Z}_1) \leq \rho(\mathfrak{Z}, \mathfrak{Z}_k) \qquad (k = 2, 3, \cdots). \tag{61}$$

It follows from this definition that F is closed, with respect to H; but F is not necessarily compact. Let $G = H - F$ be the complement of G in H and let B be the frontier of F and $F_0 = F - B$ the set of inner points of F.

Obviously, the set G consists of all points $\mathfrak{Z}$ satisfying the inequality $\rho(\mathfrak{Z}, \mathfrak{Z}_1) > \rho(\mathfrak{Z}, \mathfrak{Z}_k)$ for at least one value of k; hence all the points $\mathfrak{Z}_2, \mathfrak{Z}_3, \cdots$ belong to G.

Let us now consider a point $\mathfrak{Z}$ which fulfills all conditions

$$\rho(\mathfrak{Z}, \mathfrak{Z}_1) < \rho(\mathfrak{Z}, \mathfrak{Z}_k) \qquad (k = 2, 3, \cdots); \tag{62}$$

the point $\mathfrak{Z} = \mathfrak{Z}_1$ is an example. The differences $\rho(\mathfrak{Z}, \mathfrak{Z}_k) - \rho(\mathfrak{Z}, \mathfrak{Z}_1)$ $(k = 2, 3, \cdots)$ are all positive and tend to infinity with k and, consequently, they have a positive minimum μ. The points $\mathfrak{Z}^*$ of the geodesic sphere $\rho(\mathfrak{Z}, \mathfrak{Z}^*) < \frac{1}{2}\mu$ form a neighborhood of $\mathfrak{Z}$. It follows from

$$\rho(\mathfrak{Z}^*, \mathfrak{Z}_k) - \rho(\mathfrak{Z}^*, \mathfrak{Z}_1) > \rho(\mathfrak{Z}, \mathfrak{Z}_k) - \tfrac{1}{2}\mu - \rho(\mathfrak{Z}, \mathfrak{Z}_1) - \tfrac{1}{2}\mu \geq 0 \qquad (k = 2, 3, \cdots),$$

that all these points belong to F. Consequently $\mathfrak{Z}$ is a point of F_0.

Consider next the case where all conditions (61) are fulfilled, with the sign of equality for at least one index $k = l > 1$. Then $\mathfrak{Z} \neq \mathfrak{Z}_l$. Let $\mathfrak{Z}^*$ be an arbitrary point on the geodesic arc joining $\mathfrak{Z}$ and $\mathfrak{Z}_l$, different from $\mathfrak{Z}$. Since $\rho(\mathfrak{Z}, \mathfrak{Z}_1) = \rho(\mathfrak{Z}, \mathfrak{Z}_l)$ and $\mathfrak{Z}_1 \neq \mathfrak{Z}_l$, the point $\mathfrak{Z}^*$ does not lie at the same time on the geodesic arc between $\mathfrak{Z}$ and $\mathfrak{Z}_1$ so that

$$\rho(\mathfrak{Z}, \mathfrak{Z}_1) < \rho(\mathfrak{Z}, \mathfrak{Z}^*) + \rho(\mathfrak{Z}^*, \mathfrak{Z}_1).$$

On the other hand,

$$\rho(\mathfrak{Z}, \mathfrak{Z}_l) = \rho(\mathfrak{Z}, \mathfrak{Z}^*) + \rho(\mathfrak{Z}^*, \mathfrak{Z}_l),$$

and the inequality $\rho(\mathfrak{Z}^*, \mathfrak{Z}_1) > \rho(\mathfrak{Z}^*, \mathfrak{Z}_l)$ is proved. Consequently, the whole geodesic arc between $\mathfrak{Z}$ and $\mathfrak{Z}_l$ belongs to G, except the point $\mathfrak{Z}$ itself, which is a point of F. This proves that $\mathfrak{Z}$ is a point of B. Therefore F_0 consists of all $\mathfrak{Z}$ satisfying (62) and B consists of all $\mathfrak{Z}$ satisfying (61) with at least one sign of equality.

Let again $\mathfrak{Z}$ be a point of B, and choose a point $\mathfrak{Z}^* \neq \mathfrak{Z}$ on the geodesic arc joining $\mathfrak{Z}$ and $\mathfrak{Z}_1$; then

$$\rho(\mathfrak{Z}, \mathfrak{Z}_1) = \rho(\mathfrak{Z}, \mathfrak{Z}^*) + \rho(\mathfrak{Z}^*, \mathfrak{Z}_1).$$

Moreover

$$\rho(\mathfrak{Z}, \mathfrak{Z}_1) \leq \rho(\mathfrak{Z}, \mathfrak{Z}_k) \leq \rho(\mathfrak{Z}, \mathfrak{Z}^*) + \rho(\mathfrak{Z}^*, \mathfrak{Z}_k) \qquad (k = 2, 3, \cdots),$$

where the sign of equality cannot be true in both places. Hence $\rho(\mathfrak{Z}^*, \mathfrak{Z}_1) < \rho(\mathfrak{Z}^*, \mathfrak{Z}_k)$, i. e., $\mathfrak{Z}^*$ is a point of F_0. This proves that any geodesic ray through $\mathfrak{Z}_1$ either lies completely in F or intersects B in exactly one point. The domain F is a star formed by geodesic arcs through $\mathfrak{Z}_1$.

The boundary B of F consists of parts of the analytic surfaces $\rho(\mathfrak{Z}, \mathfrak{Z}_1) = \rho(\mathfrak{Z}, \mathfrak{Z}_k)$ for certain values of $k > 1$. It is not generally true that the number of these values is finite. However, if we consider a compact domain P in H, the distance $\rho(P, \mathfrak{Z}_k)$ tends to infinity with k; consequently only a finite number of these bounding surfaces enter into P.

Let $\mathfrak{Z}$ be an arbitrary point of H. Since $\rho(\mathfrak{Z}, \mathfrak{Z}_k) \rightarrow \infty$, there exists a positive integer r, such that

$$(63) \qquad \rho(\mathfrak{Z}, \mathfrak{Z}_r) \leq \rho(\mathfrak{Z}, \mathfrak{Z}_k) \qquad (k = 1, 2, \cdots).$$

Then the point $\mathfrak{Z}^* = D_r^{-1}(\mathfrak{Z})$ satisfies the conditions (61). Consequently $\mathfrak{Z}$ is equivalent to a point of F. On the other hand, a point $\mathfrak{Z}$ cannot satisfy both conditions (62) and (63), for any $r > 1$ and all k. It follows that no point of F_0 is equivalent to any point of F, except to itself under the identical mapping D_1.

Our results contain the proof of Theorem 6.

22. If the fundamental domain F is compact, then the boundary B consists of a finite number of surfaces $\rho(\mathfrak{Z}, \mathfrak{Z}_1) = \rho(\mathfrak{Z}, \mathfrak{Z}_k)$. Now F depends upon the initial point $\mathfrak{Z}_1$; we write more explicitly $F = F(\mathfrak{Z}_1)$. We shall prove that $F(\mathfrak{Z}^*_1)$ is compact, for an arbitrary initial point $\mathfrak{Z}^*_1$, if $F(\mathfrak{Z}_1)$ is compact.

The space H is called compact relative to Δ, if there exists for every infinite sequence of points $\mathfrak{Z}^{(k)}$, $(k = 1, 2, \cdots)$, in H at least one compact sequence of images $\mathfrak{Z}_{l_k}{}^{(k)}$ under Δ. Obviously this condition is satisfied, if and only if there exists a compact domain G in H, such that every point $\mathfrak{Z}$

of H has at least one image $\mathfrak{Z}_k$ in G. By the minimum property of F, this domain is then also compact, and vice versa. Hence our assertion is proved.

In the classical case $n = 1$, the fundamental polygon F is compact, if and only if all vertices are elliptic; it is well-known that the uniformization of any field of algebraic functions of genus $p > 1$ leads to a discontinuous group with the required property. From the algebraic point of view, the most important discontinuous groups Δ, in the case $n = 1$, are, more generally, those having a fundamental polygon with a finite number of elliptic or parabolic vertices. They constitute the Fuchsian groups of the first kind, and the corresponding automorphic functions form algebraic function fields of a single variable.

For arbitrary n, we say that a discontinuous group Δ is of the first kind, if there exists a fundamental domain F with the following three properties: 1) Every compact domain in H is covered by a finite number of images of F; 2) only a finite number of images of F are neighbors of F; 3) the integral

$$V(\Delta) = \int_F dv \tag{64}$$

converges. In the special case $n = 1$, it is easily seen that this definition is tantamount to the ordinary definition of Fuchsian groups of the first kind.

It is now clear that Δ is certainly of the first kind, if H is compact relative to Δ; hence Theorem 7 is proved.

Let

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$$

be any symplectic matrix. Under the automorphism $\mathfrak{Z} \to (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ of H, a subgroup Δ of Ω is replaced by $\mathfrak{M}\Delta\mathfrak{M}^{-1}$, i. e., by a conjugate subgroup, and a fundamental domain of Δ is mapped onto a fundamental domain of $\mathfrak{M}\Delta\mathfrak{M}^{-1}$. Obviously all conjugate subgroups $\mathfrak{M}\Delta\mathfrak{M}^{-1}$ will be of the first kind, if Δ itself is of the first kind.

23. Let us now assume that Δ has no fixed point in H. Then the images $\mathfrak{Z}_k (k = 1, 2, \cdots)$ of an arbitrary point $\mathfrak{Z}_1$ of H are all different from each other, and the minimum of the distances $\rho(\mathfrak{Z}_k, \mathfrak{Z}_1)$ $(k = 2, 3, \cdots)$ is a positive number $\delta = \delta(\mathfrak{Z}_1)$. The images of the geodesic sphere $\rho(\mathfrak{Z}, \mathfrak{Z}_1) < \frac{1}{2}\delta$ with the center $\mathfrak{Z}_1$ do not overlap.

Identifying equivalent points of H, we obtain a set H_Δ. We may obviously introduce the symplectic metric into H_Δ, defining a neighborhood of $\mathfrak{Z}_1$ by $\rho(\mathfrak{Z}, \mathfrak{Z}_1) < \frac{1}{2}\delta$. Starting from a fundamental domain F of Δ, we obtain a model of H_Δ, if we identify equivalent points on the boundary of F. Assume now that H is compact relative to Δ. Then F may be considered as a closed manifold with the symplectic metric. By Theorem 5, this manifold has the Euler number

$$\chi = c_n(-\pi)^{-n(n+1)/2}V(\Delta), \tag{65}$$

where $V(\Delta)$ denotes the symplectic volume (6) of F.

Probably the formula (65) is true for all groups Δ of the first kind, provided Δ has no fixed point in H. This is easily proved in the case $n=1$. The general proof of our suggestion would require a careful investigation of the geodesics of infinite length in the fundamental domain.

V. HERMITIAN FORMS.

24. In the case $n=1$, we know three different methods of constructing discontinuous groups of the first kind, namely an analytic, a geometric and an arithmetic method. The analytic method starts with a Riemann surface of finite genus and applies the theory of uniformization. The geometric method uses the principle of reflection for a circular polygon with a finite number of elliptic and parabolic vertices, the angles at the elliptic vertices being aliquot parts of π. The arithmetic method depends upon the theory of units of indefinite binary hermitian forms, in an imaginary quadratic ring over a totally real algebraic number field of finite degree. It is not known to what extent the analytic and the geometric method may be generalized; however, we shall show in the following sections, that there is a generalization of the arithmetic method to the case of an arbitrary n.

LEMMA 3. *Let $\mathfrak{H}^{(2n)}$ be a hermitian and $\mathfrak{S}^{(2n)}$ a non-singular skew-symmetric matrix with complex elements. If*

$$\mathfrak{H}\bar{\mathfrak{S}}^{-1}\bar{\mathfrak{H}} = \mathfrak{S}, \tag{66}$$

then there exists a matrix $\mathfrak{C}$ such that $\mathfrak{H}\{\mathfrak{C}\} = i\mathfrak{J}$ and $\mathfrak{S}[\mathfrak{C}] = \mathfrak{J}$.

Putting $\mathfrak{S}^{-1}\mathfrak{H} = \mathfrak{F}$, we have $\mathfrak{F}\bar{\mathfrak{F}} = \mathfrak{E}$, by (66), whence

$$(\mathfrak{F} + i\lambda\mathfrak{E})(\bar{\mathfrak{F}} + i\bar{\lambda}\mathfrak{E}) + (\mathfrak{F} - i\lambda\mathfrak{E})(\bar{\mathfrak{F}} - i\bar{\lambda}\mathfrak{E}) = 0$$

for any scalar λ of absolute value 1. Choosing this λ such that $|\mathfrak{F} + i\lambda\mathfrak{E}| \neq 0$, we obtain

$$\frac{\mathfrak{F} - i\lambda\mathfrak{E}}{\mathfrak{F} + i\lambda\mathfrak{E}} = i\mathfrak{T}$$

model of H_Δ, if we identify equivalent points on the boundary of F. Assume now that H is compact relative to Δ. Then F may be considered as a closed manifold with the symplectic metric. By Theorem 5, this manifold has the Euler number

$$\chi = c_n(-\pi)^{-n(n+1)/2}V(\Delta), \tag{65}$$

where $V(\Delta)$ denotes the symplectic volume (6) of F.

Probably the formula (65) is true for all groups Δ of the first kind, provided Δ has no fixed point in H. This is easily proved in the case $n=1$. The general proof of our suggestion would require a careful investigation of the geodesics of infinite length in the fundamental domain.

V. HERMITIAN FORMS.

24. In the case $n=1$, we know three different methods of constructing discontinuous groups of the first kind, namely an analytic, a geometric and an arithmetic method. The analytic method starts with a Riemann surface of finite genus and applies the theory of uniformization. The geometric method uses the principle of reflection for a circular polygon with a finite number of elliptic and parabolic vertices, the angles at the elliptic vertices being aliquot parts of π. The arithmetic method depends upon the theory of units of indefinite binary hermitian forms, in an imaginary quadratic ring over a totally real algebraic number field of finite degree. It is not known to what extent the analytic and the geometric method may be generalized; however, we shall show in the following sections, that there is a generalization of the arithmetic method to the case of an arbitrary n.

LEMMA 3. *Let $\mathfrak{H}^{(2n)}$ be a hermitian and $\mathfrak{S}^{(2n)}$ a non-singular skew-symmetric matrix with complex elements. If*

$$\mathfrak{H}\bar{\mathfrak{S}}^{-1}\bar{\mathfrak{H}} = \mathfrak{S}, \tag{66}$$

then there exists a matrix $\mathfrak{C}$ such that $\mathfrak{H}\{\mathfrak{C}\} = i\mathfrak{J}$ and $\mathfrak{S}[\mathfrak{C}] = \mathfrak{J}$.

Putting $\mathfrak{S}^{-1}\mathfrak{H} = \mathfrak{F}$, we have $\mathfrak{F}\bar{\mathfrak{F}} = \mathfrak{E}$, by (66), whence

$$(\mathfrak{F} + i\lambda\mathfrak{E})(\bar{\mathfrak{F}} + i\bar{\lambda}\mathfrak{E}) + (\mathfrak{F} - i\lambda\mathfrak{E})(\bar{\mathfrak{F}} - i\bar{\lambda}\mathfrak{E}) = 0$$

for any scalar λ of absolute value 1. Choosing this λ such that $|\mathfrak{F} + i\lambda\mathfrak{E}| \neq 0$, we obtain

$$\frac{\mathfrak{F} - i\lambda\mathfrak{E}}{\mathfrak{F} + i\lambda\mathfrak{E}} = i\mathfrak{T}$$

with real $\mathfrak{X}$; consequently $\mathfrak{E} - i\mathfrak{X} = 2i\lambda(\mathfrak{F} + i\lambda\mathfrak{E})^{-1}$, $|\mathfrak{E} - i\mathfrak{X}| \neq 0$,

$$\mathfrak{F} = i\lambda \frac{\mathfrak{E} + i\mathfrak{X}}{\mathfrak{E} - i\mathfrak{X}}.$$

Let $\mathfrak{C}_1 = \lambda^{\frac{1}{2}}(\mathfrak{E} + i\mathfrak{X})$, $\mathfrak{H}_1 = \mathfrak{H}\{\mathfrak{C}_1\}$, $\mathfrak{G}_1 = \mathfrak{G}[\mathfrak{C}_1]$; then

$$\mathfrak{G}_1^{-1}\mathfrak{H}_1 = \mathfrak{C}_1^{-1}\mathfrak{F}\bar{\mathfrak{C}}_1 = i\mathfrak{E}; \; \bar{\mathfrak{H}}_1 = \mathfrak{H}'_1 = i\mathfrak{G}'_1 = -i\mathfrak{G}_1 = -\mathfrak{H}_1;$$

hence $\mathfrak{H}_1$ is pure imaginary and $\mathfrak{G}_1 = -i\mathfrak{H}_1$ real. There exists a real matrix $\mathfrak{C}_2$ satisfying $\mathfrak{G}_1[\mathfrak{C}_2] = \mathfrak{J}$, and $\mathfrak{C} = \mathfrak{C}_1\mathfrak{C}_2$ has the required property.

25. Let K be a totally real algebraic number field of finite degree h and let $K^{(1)}, \cdots, K^{(h)}$ be its conjugate fields, $K = K^{(1)}$. If r is any positive number of K, then the field $K_0 = K(\sqrt{-r})$, of degree $2h$, is imaginary. We consider a hermitian matrix $\mathfrak{H} = \mathfrak{H}^{(2n)}$ and a non-singular skew-symmetric matrix $\mathfrak{G}$, both with elements in K_0, and we assume that the relationship

$$\mathfrak{H}\bar{\mathfrak{G}}^{-1}\bar{\mathfrak{H}} = s\mathfrak{G} \tag{67}$$

holds with a positive scalar factor s. Obviously s is then a number of K.

The matrices $\mathfrak{U}$ with integral elements in K_0, satisfying the two conditions

$$\mathfrak{G}[\mathfrak{U}] = \mathfrak{G}, \qquad \mathfrak{H}\{\mathfrak{U}\} = \mathfrak{H},$$

constitute a multiplicative group $\Lambda = \Lambda(\mathfrak{G}, \mathfrak{H})$. Applying Lemma 3 with $s^{-\frac{1}{2}}\mathfrak{H}$ instead of $\mathfrak{H}$, we obtain a complex matrix $\mathfrak{C}$, such that $\mathfrak{G}[\mathfrak{C}] = \mathfrak{J}$ and $\mathfrak{H}\{\mathfrak{C}\} = is^{\frac{1}{2}}\mathfrak{J}$. Consequently the elements $\mathfrak{C}^{-1}\mathfrak{U}\mathfrak{C} = \mathfrak{M}$ of the group $\mathfrak{C}^{-1}\Lambda\mathfrak{C} = \Delta_0 = \Delta_0(\mathfrak{G}, \mathfrak{H})$ satisfy $\mathfrak{J}[\mathfrak{M}] = \mathfrak{J}$ and $\mathfrak{J}\{\mathfrak{M}\} = \mathfrak{J}$, whence $\mathfrak{J}[\mathfrak{M}] = \mathfrak{J}$ and $\bar{\mathfrak{M}} = \mathfrak{M}$. This proves that Δ_0 is a subgroup of the homogeneous symplectic group Ω_0. Identifying $\mathfrak{U}$ and $-\mathfrak{U}$, i. e., $\mathfrak{M}$ and $-\mathfrak{M}$, we obtain a subgroup $\Delta = \Delta(\mathfrak{G}, \mathfrak{H})$ of Ω.

The matrix $\mathfrak{C}$ is not uniquely determined. If also $\mathfrak{H}\{\mathfrak{C}^*\} = is^{\frac{1}{2}}\mathfrak{J}$ and $\mathfrak{G}[\mathfrak{C}^*] = \mathfrak{J}$, then $\mathfrak{C}^{-1}\mathfrak{C}^* = \mathfrak{B}$ is symplectic, and vice versa. Using $\mathfrak{C}^*$ instead of $\mathfrak{C}$, we have to replace Δ by $\mathfrak{B}^{-1}\Delta\mathfrak{B}$; hence the class of conjugate subgroups $\mathfrak{B}^{-1}\Delta\mathfrak{B}$ in Ω is uniquely determined by $\mathfrak{G}$ and $\mathfrak{H}$.

Obviously $\Lambda(\mathfrak{G}, a\mathfrak{H}) = \Lambda(\mathfrak{G}, \mathfrak{H})$ for any number $a \neq 0$ of K. Therefore we may assume r and s to be integers. Henceforth we shall, moreover, assume that r is totally positive and that all conjugates of $\mathfrak{H}$ except $\mathfrak{H}$ and $\bar{\mathfrak{H}}$ are positive. Let r_l and the pair $\mathfrak{H}_l, \bar{\mathfrak{H}}_l$ be the image of r and the pair $\mathfrak{H}, \bar{\mathfrak{H}}$ under the isomorphism $K \to K^{(l)}$ $(l = 1, \cdots, h)$. For any element $\mathfrak{U}$ of Λ, we have $\mathfrak{H}_l\{\mathfrak{U}_l\} = \mathfrak{H}_l$, where $\mathfrak{U}_l, \bar{\mathfrak{U}}_l$ $(l = 1, \cdots, h)$ denote the $2h$ conjugates of $\mathfrak{U} = \mathfrak{U}_1$. Since $\mathfrak{H}_l$ is positive for $l > 1$, the matrices $\mathfrak{U}_2, \cdots, \mathfrak{U}_h$ are bounded. If also $\mathfrak{U}$ itself is bounded, then all conjugates of $\mathfrak{U}$ are bounded.

On the other hand, there exists only a finite number of integers in K_0 with bounded conjugates. Consequently Λ and Δ_0 are discrete groups and, by Section **19**, the group $\Delta(\mathfrak{G}, \mathfrak{H})$ is discontinuous.

It follows from (67) that $\mathfrak{H} = -s\bar{\mathfrak{H}}^{-1}\{\mathfrak{G}\}$. Since s is positive, $\mathfrak{H} = \mathfrak{H}_1$ is necessarily the matrix of an indefinite hermitian form. Since $\mathfrak{H}_l$ is positive for $l > 1$, the conjugates $s_2, \cdots, s_h$ of the positive number $s = s_1$ are all negative.

The most important example of a group $\Delta(\mathfrak{G}, \mathfrak{H})$ is provided by $\mathfrak{G} = \mathfrak{J}$, $\mathfrak{H} = i\mathfrak{J}$, $r = 1$, $h = 1$. Then we may choose $\mathfrak{C} = \mathfrak{E}$, and $\Delta_0(\mathfrak{G}, \mathfrak{H})$ consists of all symplectic matrices $\mathfrak{M}$ with rational integral elements. We call this group the homogeneous modular group of degree n and denote it by Γ_0. Identifying the elements $\mathfrak{M}$ and $-\mathfrak{M}$ of Γ_0, we obtain the (inhomogeneous) modular group Γ.

26. Two subgroups Δ and Δ^* of Ω are called commensurable, if there exist a subgroup Δ_1 of finite index in Δ and a subgroup Δ^*_1 of finite index in Δ^*, such that Δ_1 and Δ^*_1 are conjugate subgroups of Ω. If Δ is a discontinuous group of the first kind, then the same holds for Δ^*, and we obtain $jV(\Delta) = j^*V(\Delta^*)$, where j and j^* denote the indices of the subgroups Δ_1 and Δ^*_1; consequently the quotient $V(\Delta)/V(\Delta^*)$ is a rational number.

It is easily seen that the property of commensurability is symmetric and transitive; therefore we may speak of a class of commensurable groups. We have now the problem of deciding whether two groups $\Delta(\mathfrak{G}, \mathfrak{H})$ and $\Delta(\mathfrak{G}^*, \mathfrak{H}^*)$ are commensurable or not. The complete answer is given by Theorem 13. In this section we solve only a particular case of the problem: We assume that $\mathfrak{G}^*$ and $\mathfrak{H}^*$ are also matrices of the field K_0 and that they fulfill the condition

$$\mathfrak{H}^*\bar{\mathfrak{G}}^{*-1}\bar{\mathfrak{H}}^* = s\mathfrak{G}^*$$

with the same factor s as in (67).

LEMMA 4. *Let $c_1, \cdots, c_{2n}$ be $2n$ numbers of K_0, not all 0. There exists a matrix $\mathfrak{C}_1^{(2n)} = (c_{kl})$ in K_0, such that $c_{k1} = c_k$ $(k = 1, \cdots, 2n)$ and $\mathfrak{J}[\mathfrak{C}_1] = \mathfrak{J}$. If, moreover, $c_1 \neq 0$, we may choose $c_{1l} = 0$ $(l = 2, \cdots, 2n)$.*

Put $\mathfrak{c}'_1 = (c_1 \cdots c_n)$ and $\mathfrak{c}'_2 = (c_{n+1} \cdots c_{2n})$. If $\mathfrak{c}_1 = 0$, we choose in K_0 a non-singular matrix $\mathfrak{Q}^{(n)}$ with the first row $\mathfrak{c}'_2$ and define

$$\mathfrak{C}_1 = \begin{pmatrix} 0 & -\mathfrak{Q}^{-1} \\ \mathfrak{Q}' & 0 \end{pmatrix}.$$

If $\mathfrak{c}_1 \neq 0$, we choose in K_0 a non-singular matrix $\mathfrak{P}^{(n)}$ with the first row $\mathfrak{c}'_1$ and a symmetric matrix $\mathfrak{S}$ with the first column $\mathfrak{P}\mathfrak{c}_2$; then

$$\mathfrak{C}_1 = \begin{pmatrix} \mathfrak{P}' & 0 \\ \mathfrak{P}^{-1}\mathfrak{S} & \mathfrak{P}^{-1} \end{pmatrix}$$

has the required property. In the case $c_1 \neq 0$, we may obviously choose $(c_1 0 \cdots 0)$ as the first row of $\mathfrak{P}'$.

LEMMA 5. *There exists a matrix $\mathfrak{C}_0$ in K_0 such that $\mathfrak{G}[\mathfrak{C}_0] = \mathfrak{G}^*$ and $\mathfrak{H}\{\mathfrak{C}_0\} = \mathfrak{H}^*$.*

The equation $\mathfrak{G}[\mathfrak{X}] = \mathfrak{J}$ has a solution $\mathfrak{X}$ in K_0; hence we may assume, without loss of generality, that $\mathfrak{G} = \mathfrak{G}^* = \mathfrak{J}$. Moreover it is sufficient to prove the lemma for the special case

$$\mathfrak{H}^* = \begin{pmatrix} \mathfrak{E} & 0 \\ 0 & -s\mathfrak{E} \end{pmatrix}.$$

Since none of the conjugates of $-\mathfrak{H}$ is positive, it follows from Hasse's generalization of A. Meyer's theorem, that the diophantine equation $\mathfrak{H}\{\mathfrak{x}\} = 1$ has a solution $\mathfrak{x}$ in K_0. Applying Lemma 4 with $(c_1 \cdots c_{2n}) = \mathfrak{x}'$, we construct a matrix $\mathfrak{C}_1$ in K_0 which has the first column $\mathfrak{x}$ and satisfies $\mathfrak{J}[\mathfrak{C}_1] = \mathfrak{J}$. Then $\mathfrak{H}\{\mathfrak{C}_1\}$ has the first diagonal element 1. On the other hand, the condition (67) means now

$$\mathfrak{H}\mathfrak{J}\bar{\mathfrak{H}} = -s\mathfrak{J}. \tag{68}$$

For the proof of Lemma 5, we may therefore replace $\mathfrak{H}\{\mathfrak{C}_1\}$ again by $\mathfrak{H}$.

By Lemma 4, there exists a matrix $\mathfrak{C}_2$ in K_0 with the following three properties: $\mathfrak{C}_2$ and $\mathfrak{H}$ have the same first column; $\mathfrak{C}_2$ has the first row $(1\,0 \cdots 0)$; $\mathfrak{J}[\mathfrak{C}_2] = \mathfrak{J}$. Put $\mathfrak{C}_2^{-1} = \mathfrak{C}'_3$; then also $\mathfrak{J}[\mathfrak{C}_3] = \mathfrak{J}$, and the two matrices $\mathfrak{C}'_3\mathfrak{H}$ and $\bar{\mathfrak{C}}_3$ have both the first column $(1\,0 \cdots 0)'$. Writing again $\mathfrak{H}$ instead of $\mathfrak{H}\{\mathfrak{C}_3\}$, we obtain the decomposition

$$\mathfrak{H} = \begin{pmatrix} \mathfrak{H}_1 & \mathfrak{H}_{12} \\ \bar{\mathfrak{H}}'_{12} & \mathfrak{H}_2 \end{pmatrix},$$

$$\mathfrak{H}_1^{(n)} = \begin{pmatrix} 1 & 0 \\ 0 & \mathfrak{F}_1 \end{pmatrix}, \qquad \mathfrak{H}_{12} = \begin{pmatrix} 0 & 0 \\ \mathfrak{a} & \mathfrak{F}_{12} \end{pmatrix}, \qquad \mathfrak{H}_2 = \begin{pmatrix} t & \mathfrak{c}' \\ \mathfrak{b} & \mathfrak{F}_2 \end{pmatrix}.$$

By (68),

$$\mathfrak{H}_1\mathfrak{H}'_{12} = \mathfrak{H}_{12}\mathfrak{H}'_1, \qquad \bar{\mathfrak{H}}'_{12}\mathfrak{H}'_2 = \mathfrak{H}_2\bar{\mathfrak{H}}_{12},$$
$$\mathfrak{H}_1\mathfrak{H}'_2 - \mathfrak{H}_{12}\bar{\mathfrak{H}}_{12} = -s\mathfrak{E}, \qquad \mathfrak{H}'_1\mathfrak{H}_2 - \bar{\mathfrak{H}}_{12}\mathfrak{H}_{12} = -s\mathfrak{E},$$

whence $\mathfrak{a} = 0$, $t = -s$, $\mathfrak{b} = 0$, $\mathfrak{c} = 0$. This contains, in particular, the proof of the lemma for $n = 1$. If $n > 1$, the hermitian matrix

$$\mathfrak{F} = \begin{pmatrix} \mathfrak{F}_1 & \mathfrak{F}_{12} \\ \bar{\mathfrak{F}}'_{12} & \mathfrak{F}_2 \end{pmatrix}$$

fulfills the same conditions as $\mathfrak{H}$, with $n-1$ instead of n; and we may apply induction with respect to n. Hence the lemma is proved.

Let $\mathfrak{C}_0$ be the matrix of Lemma 5 and choose a positive rational integer q, such that the two matrices $q\mathfrak{C}_0$ and $q\mathfrak{C}_0^{-1}$ have integral elements. Since the integers of K_0 belong to a finite number of classes of residues modulo q^2, the elements $\mathfrak{U}$ of $\Lambda(\mathfrak{S},\mathfrak{H})$ satisfying $\mathfrak{U}\equiv\mathfrak{E} \pmod{q^2}$ form a subgroup Λ_1 of finite index. Consider now the subgroup Λ_2 consisting of all $\mathfrak{U}$ with integral $\mathfrak{C}_0^{-1}\mathfrak{U}\mathfrak{C}_0=\mathfrak{U}^*$. Obviously Λ_1 is contained in Λ_2; consequently Λ_2 is a fortiori of finite index in $\Lambda(\mathfrak{S},\mathfrak{H})$. On the other hand, $\mathfrak{U}^*$ is an element of $\Lambda(\mathfrak{S}^*,\mathfrak{H}^*)$ with the characteristic property that $\mathfrak{C}_0\mathfrak{U}^*\mathfrak{C}_0^{-1}=\mathfrak{U}$ is integral; hence the group $\Lambda^*_2=\mathfrak{C}_0^{-1}\Lambda_2\mathfrak{C}_0$ is of finite index in $\Lambda(\mathfrak{S}^*,\mathfrak{H}^*)$. If $\mathfrak{C}$ is the matrix of Section **25**, we have $\Delta_0(\mathfrak{S},\mathfrak{H})=\mathfrak{C}^{-1}\Lambda(\mathfrak{S},\mathfrak{H})\mathfrak{C}$, and we may define $\Delta_0(\mathfrak{S}^*,\mathfrak{H}^*)=\mathfrak{C}_4^{-1}\Lambda(\mathfrak{S}^*,\mathfrak{H}^*)\mathfrak{C}_4$ with $\mathfrak{C}_4=\mathfrak{C}_0^{-1}\mathfrak{C}$. Then $\mathfrak{C}^{-1}\Lambda_2\mathfrak{C}=\mathfrak{C}_4^{-1}\Lambda^*_2\mathfrak{C}_4$ is a common subgroup of $\Delta_0(\mathfrak{S},\mathfrak{H})$ and $\Delta_0(\mathfrak{S}^*,\mathfrak{H}^*)$, of finite indices. This proves that $\Delta(\mathfrak{S},\mathfrak{H})$ and $\Delta(\mathfrak{S}^*,\mathfrak{H}^*)$ are commensurable.

27. The two conditions $\mathfrak{S}[\mathfrak{U}]=\mathfrak{S}$ and $\mathfrak{H}\{\mathfrak{U}\}=\mathfrak{H}$ for the elements $\mathfrak{U}$ of $\Lambda(\mathfrak{S},\mathfrak{H})$ may be written $\mathfrak{F}\bar{\mathfrak{U}}=\mathfrak{U}\mathfrak{F}$ and $\mathfrak{U}\mathfrak{S}^{-1}\mathfrak{U}'\mathfrak{S}=\mathfrak{E}$, with $\mathfrak{F}=\mathfrak{S}^{-1}\mathfrak{H}$. Let us consider the set R of all matrices $\mathfrak{W}$ in K_0 which satisfy the condition

$$\mathfrak{F}\bar{\mathfrak{W}}=\mathfrak{W}\mathfrak{F}. \tag{69}$$

Obviously R is a ring. By (67), the matrix

$$\tilde{\mathfrak{W}}=\mathfrak{S}^{-1}\mathfrak{W}'\mathfrak{S} \tag{70}$$

is again a solution of (69), and consequently (70) defines an anti-automorphism of R. The elements $\mathfrak{U}$ of $\Lambda(\mathfrak{S},\mathfrak{H})$ are the integral elements $\mathfrak{W}=\mathfrak{U}$ of R with the property

$$\mathfrak{U}\tilde{\mathfrak{U}}=\mathfrak{E}. \tag{71}$$

By Lemma 5,

$$\mathfrak{S}[\mathfrak{C}_0]=\mathfrak{T},\quad \mathfrak{H}\{\mathfrak{C}_0\}=\begin{pmatrix}\mathfrak{E} & 0\\ 0 & -s\mathfrak{E}\end{pmatrix}=\mathfrak{H}^*,\quad \mathfrak{C}_0^{-1}\mathfrak{F}\mathfrak{C}_0=\begin{pmatrix}0 & s\mathfrak{E}\\ \mathfrak{E} & 0\end{pmatrix}=\mathfrak{F}^*,$$

where $\mathfrak{C}_0$ is a matrix in K_0. The elements $\mathfrak{W}^*=\mathfrak{C}_0^{-1}\mathfrak{W}\mathfrak{C}_0$ of the ring $R^*=\mathfrak{C}_0^{-1}R\mathfrak{C}_0$ satisfy $\mathfrak{F}^*\bar{\mathfrak{W}}^*=\mathfrak{W}^*\mathfrak{F}^*$, whence

$$\mathfrak{W}^*=\begin{pmatrix}\mathfrak{P} & s\bar{\mathfrak{Q}}\\ \mathfrak{Q} & \bar{\mathfrak{P}}\end{pmatrix}$$

with arbitrary matrices $\mathfrak{P}^{(n)},\mathfrak{Q}^{(n)}$ in K_0. Defining

$$2^{1/2}s^{1/4}\mathfrak{L}=\begin{pmatrix}is^{1/2}\mathfrak{E} & s^{1/2}\mathfrak{E}\\ -\mathfrak{E} & -i\mathfrak{E}\end{pmatrix},\qquad \mathfrak{C}_0\mathfrak{L}=\mathfrak{C},$$

we obtain

(72) $$\mathfrak{G}[\mathfrak{C}] = \mathfrak{J}, \qquad \mathfrak{H}\{\mathfrak{C}\} = is^{\frac{1}{2}}\mathfrak{J},$$

(73) $$\mathfrak{C}^{-1}\mathfrak{B}\mathfrak{C} = \mathfrak{L}^{-1}\mathfrak{B}^{*}\mathfrak{L} = \begin{pmatrix} \mathfrak{A}_0 + \sqrt{rs}\mathfrak{A}_1 & \sqrt{r}\mathfrak{A}_2 + \sqrt{s}\mathfrak{A}_3 \\ -\sqrt{r}\mathfrak{A}_2 + \sqrt{s}\mathfrak{A}_3 & \mathfrak{A}_0 - \sqrt{rs}\mathfrak{A}_1 \end{pmatrix} = \mathfrak{M}$$

with

$$\mathfrak{A}_0 = \tfrac{1}{2}(\mathfrak{P} + \bar{\mathfrak{P}}), \quad \mathfrak{A}_1 = \frac{1}{2\sqrt{-r}}(\mathfrak{Q} - \bar{\mathfrak{Q}}),$$
$$\mathfrak{A}_2 = \frac{1}{2\sqrt{-r}}(\mathfrak{P} - \bar{\mathfrak{P}}), \quad \mathfrak{A}_3 = -\tfrac{1}{2}(\mathfrak{Q} + \bar{\mathfrak{Q}});$$

consequently $\mathfrak{A}_0, \mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3$ are arbitrary matrices in K.

Consider now the generalized quaternion algebra A over K consisting of the elements $\alpha = a_0\epsilon_0 + a_1\epsilon_1 + a_2\epsilon_2 + a_3\epsilon_3$ with arbitrary a_0, a_1, a_2, a_3 in K, where ϵ_0 is the unit and $\epsilon_1^2 = rs\epsilon_0$, $\epsilon_2^2 = -r\epsilon_0$, $\epsilon_1\epsilon_2 = -\epsilon_2\epsilon_1 = s\epsilon_3$. We denote by $\hat{\alpha} = a_0\epsilon_0 - a_1\epsilon_1 - a_2\epsilon_2 - a_3\epsilon_3$ the conjugate quaternion. There exists the well-known representation of A, of degree 2, defined by

(74) $$\epsilon_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \epsilon_1 = \sqrt{rs}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\epsilon_2 = \sqrt{r}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \epsilon_3 = \sqrt{s}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then obviously

(75) $$\mathfrak{M} = \sum_{k=0}^{3} \mathfrak{A}_k \times \epsilon_k,$$

where $\mathfrak{A}_k \times \epsilon_k$ denotes the Kronecker product of the matrices $\mathfrak{A}_k$ and ϵ_k; and consequently $\mathfrak{C}^{-1}R\mathfrak{C}$ is the ring of all matrices $M = (\alpha_{kl})$ of n rows and columns with arbitrary elements α_{kl} of A.

By (70) and (73), the condition (71) may be expressed in the form

(76) $$\mathfrak{M}\tilde{\mathfrak{M}} = \mathfrak{E}$$

with

$$\tilde{\mathfrak{M}} = \mathfrak{C}^{-1}\tilde{\mathfrak{B}}\mathfrak{C} = \mathfrak{J}^{-1}\mathfrak{M}'\mathfrak{J} = \mathfrak{A}'_0 \times \epsilon_0 - \sum_{k=1}^{3} \mathfrak{A}'_k \times \epsilon_k;$$

hence $\tilde{\mathfrak{M}}$, written as a quaternion matrix, is the transpose $(\hat{\alpha}_{lk})$ of the conjugate $(\hat{\alpha}_{kl})$ of M. By (72) and Section **25**, the group $\Delta_0(\mathfrak{G}, \mathfrak{H})$ consists of all matrices $\mathfrak{M}$ of the form (75), such that (76) is satisfied and $\mathfrak{C}\mathfrak{M}\mathfrak{C}^{-1}$ is integral. On the other hand, the solutions of (76) with integral $\mathfrak{A}_k$ $(k = 0, \cdots, 3)$ in K constitute also a subgroup $\Delta_0(r, s)$ of the homogeneous symplectic group Ω_0. It follows from the argument at the end of Section **26**, that the two groups $\Delta_0(\mathfrak{G}, \mathfrak{H})$ and $\Delta_0(r, s)$ are commensurable. The problem of the commensurability of two groups $\Delta(\mathfrak{G}, \mathfrak{H})$ and $\Delta(\mathfrak{G}_1, \mathfrak{H}_1)$ is therefore reduced to the corresponding problem for $\Delta_0(r, s)$ and $\Delta_0(r_1, s_1)$. The solution will be given in Chapter IX.

VI. THE FUNDAMENTAL DOMAIN OF THE MODULAR GROUP.

28. We shall construct a fundamental F for any group $\Delta(\mathfrak{G}, \mathfrak{H})$ and, in particular, for the modular group Γ. The application of the general method of Chapter IV would lead to a rather complicated shape of the frontier of F, and it would then be difficult to prove that $\Delta(\mathfrak{G}, \mathfrak{H})$ is a group of the first kind. Therefore we shall use another procedure applying the special arithmetic properties of these groups.

LEMMA 6. *The equation*

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{Y}^{-1} & 0 \\ 0 & \mathfrak{Y} \end{pmatrix} \begin{bmatrix} \mathfrak{E} & -\mathfrak{X} \\ 0 & \mathfrak{E} \end{bmatrix} \tag{77}$$

defines a mapping of the space H of the matrices $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$ onto the space S of the symplectic positive symmetric matrices $\mathfrak{S}$. Any symplectic transformation $\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ with the matrix $\mathfrak{M}$ induces in S the transformation $\mathfrak{S}^* = \mathfrak{S}[\mathfrak{M}^{-1}]$.

Let

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1 & \mathfrak{S}_{12} \\ \mathfrak{S}'_{12} & \mathfrak{S}_2 \end{pmatrix}$$

be an arbitrary point of S. Since $\mathfrak{S} > 0$, the inequality $\mathfrak{S}_1 > 0$ holds, whence $\mathfrak{S}_1^{-1} = \mathfrak{Y} > 0$. Moreover $\mathfrak{S}_1\mathfrak{S}'_{12} = \mathfrak{S}_{12}\mathfrak{S}_1$ and $\mathfrak{S}_1\mathfrak{S}_2 - \mathfrak{S}_{12}^2 = \mathfrak{E}$, whence $-\mathfrak{S}_1^{-1}\mathfrak{S}_{12} = \mathfrak{X} = \mathfrak{X}'$, $\mathfrak{S}_{12} = -\mathfrak{Y}^{-1}\mathfrak{X}$ and $\mathfrak{S}_2 = \mathfrak{Y} + \mathfrak{Y}^{-1}[\mathfrak{X}]$. This proves the first assertion of the lemma.

The relationship (77) can be written

$$\mathfrak{S}[\mathfrak{w}] = \mathfrak{Y}^{-1}[\mathfrak{u} - \mathfrak{X}\mathfrak{v}] + \mathfrak{Y}[\mathfrak{v}] = \mathfrak{Y}^{-1}\{\mathfrak{u} - \mathfrak{Z}\mathfrak{v}\} \tag{78}$$

with an arbitrary real column

$$\mathfrak{w}^{(2n)} = \begin{pmatrix} \mathfrak{u}^{(n)} \\ \mathfrak{v}^{(n)} \end{pmatrix}.$$

For the symplectic transformation $\mathfrak{Z}^* = \mathfrak{X}^* + i\mathfrak{Y}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ we obtain, by (59),

$$\mathfrak{Y}^{*-1} = \mathfrak{Y}^{-1}\{\mathfrak{Z}\mathfrak{C}' + \mathfrak{D}'\}$$

$$\mathfrak{Y}^{*-1}\{\mathfrak{u} - \mathfrak{Z}^*\mathfrak{v}\} = \mathfrak{Y}^{-1}\{(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})'\mathfrak{u} - (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})'\mathfrak{v}\} = \mathfrak{Y}^{-1}\{\mathfrak{u}^* - \mathfrak{Z}\mathfrak{v}^*\},$$

of the commensurability of two groups $\Delta(\mathfrak{G},\mathfrak{H})$ and $\Delta(\mathfrak{G}_1,\mathfrak{H}_1)$ is therefore reduced to the corresponding problem for $\Delta_0(r,s)$ and $\Delta_0(r_1,s_1)$. The solution will be given in Chapter IX.

VI. THE FUNDAMENTAL DOMAIN OF THE MODULAR GROUP.

28. We shall construct a fundamental F for any group $\Delta(\mathfrak{G},\mathfrak{H})$ and, in particular, for the modular group Γ. The application of the general method of Chapter IV would lead to a rather complicated shape of the frontier of F, and it would then be difficult to prove that $\Delta(\mathfrak{G},\mathfrak{H})$ is a group of the first kind. Therefore we shall use another procedure applying the special arithmetic properties of these groups.

LEMMA 6. *The equation*

$$\mathfrak{S}=\begin{pmatrix}\mathfrak{Y}^{-1} & 0\\ 0 & \mathfrak{Y}\end{pmatrix}\begin{bmatrix}\mathfrak{E} & -\mathfrak{X}\\ 0 & \mathfrak{E}\end{bmatrix} \tag{77}$$

defines a mapping of the space H of the matrices $\mathfrak{Z}=\mathfrak{X}+i\mathfrak{Y}$ onto the space S of the symplectic positive symmetric matrices $\mathfrak{S}$. Any symplectic transformation $\mathfrak{Z}^*=(\mathfrak{A}\mathfrak{Z}+\mathfrak{B})(\mathfrak{C}\mathfrak{Z}+\mathfrak{D})^{-1}$ with the matrix $\mathfrak{M}$ induces in S the transformation $\mathfrak{S}^*=\mathfrak{S}[\mathfrak{M}^{-1}]$.

Let

$$\mathfrak{S}=\begin{pmatrix}\mathfrak{S}_1 & \mathfrak{S}_{12}\\ \mathfrak{S}'_{12} & \mathfrak{S}_2\end{pmatrix}$$

be an arbitrary point of S. Since $\mathfrak{S}>0$, the inequality $\mathfrak{S}_1>0$ holds, whence $\mathfrak{S}_1^{-1}=\mathfrak{Y}>0$. Moreover $\mathfrak{S}_1\mathfrak{S}'_{12}=\mathfrak{S}_{12}\mathfrak{S}_1$ and $\mathfrak{S}_1\mathfrak{S}_2-\mathfrak{S}_{12}^2=\mathfrak{E}$, whence $-\mathfrak{S}_1^{-1}\mathfrak{S}_{12}=\mathfrak{X}=\mathfrak{X}'$, $\mathfrak{S}_{12}=-\mathfrak{Y}^{-1}\mathfrak{X}$ and $\mathfrak{S}_2=\mathfrak{Y}+\mathfrak{Y}^{-1}[\mathfrak{X}]$. This proves the first assertion of the lemma.

The relationship (77) can be written

$$\mathfrak{S}[\mathfrak{w}]=\mathfrak{Y}^{-1}[\mathfrak{u}-\mathfrak{X}\mathfrak{v}]+\mathfrak{Y}[\mathfrak{v}]=\mathfrak{Y}^{-1}\{\mathfrak{u}-\mathfrak{Z}\mathfrak{v}\} \tag{78}$$

with an arbitrary real column

$$\mathfrak{w}^{(2n)}=\begin{pmatrix}\mathfrak{u}^{(n)}\\ \mathfrak{v}^{(n)}\end{pmatrix}.$$

For the symplectic transformation $\mathfrak{Z}^*=\mathfrak{X}^*+i\mathfrak{Y}^*=(\mathfrak{A}\mathfrak{Z}+\mathfrak{B})(\mathfrak{C}\mathfrak{Z}+\mathfrak{D})^{-1}$ we obtain, by (59),

$$\mathfrak{Y}^{*-1}=\mathfrak{Y}^{-1}\{\mathfrak{Z}\mathfrak{C}'+\mathfrak{D}'\}$$

$$\mathfrak{Y}^{*-1}\{\mathfrak{u}-\mathfrak{Z}^*\mathfrak{v}\}=\mathfrak{Y}^{-1}\{(\mathfrak{C}\mathfrak{Z}+\mathfrak{D})'\mathfrak{u}-(\mathfrak{A}\mathfrak{Z}+\mathfrak{B})'\mathfrak{v}\}=\mathfrak{Y}^{-1}\{\mathfrak{u}^*-\mathfrak{Z}\mathfrak{v}^*\},$$

where $\mathfrak{u}^* = \mathfrak{D}'\mathfrak{u} - \mathfrak{B}'\mathfrak{v}$ and $\mathfrak{v}^* = -\mathfrak{C}'\mathfrak{u} + \mathfrak{A}'\mathfrak{v}$. Now the second part of the lemma follows from (8) and (78).

29. Let P be the space of all positive symmetric matrices $\mathfrak{T}^{(m)}$ with real elements. Any $\mathfrak{T}$ in P may be uniquely expressed as $\mathfrak{T} = \mathfrak{P}[\mathfrak{Q}]$, where $\mathfrak{P} = [p_1, \cdots, p_m]$ is a diagonal matrix with $p_k > 0$ $(k = 1, \cdots, m)$ and $\mathfrak{Q} = (q_{kl})$ is a triangular matrix with $q_{kl} = 0$ for $k > l$ and $q_{kk} = 1$. If t is any positive number, the inequalities

$$(79) \qquad 0 < p_k \leq t p_{k+1}, \qquad -t \leq q_{kl} \leq t \qquad (1 \leq k < l \leq m)$$

define a compact domain $Q(t)$ in P, and any given compact set in P is contained in $Q(t)$ for sufficiently large values of t.

Let U denote the group of all different transformations $\mathfrak{T} \rightarrow \mathfrak{T}[\mathfrak{U}]$, where $\mathfrak{U}$ runs over the unimodular matrices, i. e., the matrices with rational integral elements and determinant ± 1. On account of Minkowski's theory of reduction, there exists in P a fundamental domain R with respect to U, defined by a finite number of inequalities

$$(80) \qquad L_r(\mathfrak{T}) \geq 0 \qquad (r = 1, 2, \cdots, g),$$

where $L_r(\mathfrak{T})$ denotes a certain homogeneous linear function of the elements of $\mathfrak{T}$ with rational coefficients. A point $\mathfrak{T}$ lies on the frontier of R if, and only if, the conditions (80) are fulfilled with at least one sign of equality. The images of R under U cover the whole space P without gaps and overlappings. Only a finite number of images enter into any compact part of P, and only a finite number of images are neighbors of R.

Most of the results of the theory of reduction are simple consequences of the following two known lemmata.

LEMMA 7. *There exists a positive number τ_1 depending only upon m, such that R is contained in $Q(\tau_1)$.*

LEMMA 8. *Let $\mathfrak{T}_1, \mathfrak{T}_2$ be two points of $Q(t)$ and let $\mathfrak{T}_2 = \mathfrak{T}_1[\mathfrak{F}]$, where $\mathfrak{F}$ is a matrix with rational integral elements f_{kl}. Then*

$$-\tau \leq f_{kl} \leq \tau \qquad (k, l = 1, \cdots, m),$$

where τ is a positive number depending only upon t, m and the determinant $|\mathfrak{F}|$.

Let $t_1, \cdots, t_m$ be the diagonal elements of a point $\mathfrak{T} = \mathfrak{P}[\mathfrak{Q}]$ of R. Then

$$t_l = \sum_{k=1}^{m} p_k q_{kl}^2 = p_l \left(1 + \sum_{k=1}^{l-1} \frac{p_k}{p_l} q_{kl}^2\right) \qquad (l = 1, \cdots, m)$$

and $p_1 p_2 \cdots p_m = |\mathfrak{T}|$. By (79) and Lemma 7, the inequality

$$\prod_{k=1}^{m} t_k < \tau_2 |\mathfrak{T}| \tag{81}$$

follows, where τ_2 depends only upon m.

30. The general method for constructing a fundamental domain with respect to any discontinuous group Δ uses the minimum of the distance $\rho(\mathfrak{Z}^*, \mathfrak{Z}_1)$, where $\mathfrak{Z}_1$ is given and $\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ runs over all the images of $\mathfrak{Z}$ under Δ.

Let us now choose in particular $\mathfrak{Z}_1 = i\lambda\mathfrak{E}$, with a positive scalar factor λ; we shall investigate the asymptotic behavior of the distance $\rho(\mathfrak{Z}, \mathfrak{Z}_1)$ for $\lambda \to \infty$. By (38), we have

$$\rho^2(\mathfrak{Z}, \mathfrak{Z}_1) = \sum_{k=1}^{n} \log^2 \frac{1 + r_k^{\frac{1}{2}}}{1 - r_k^{\frac{1}{2}}},$$

where $r_1, \cdots, r_n$ denote the characteristic roots of the cross-ratio

$$\mathfrak{R} = (\mathfrak{Z} - \mathfrak{Z}_1)(\mathfrak{Z} - \bar{\mathfrak{Z}}_1)^{-1}(\bar{\mathfrak{Z}} - \bar{\mathfrak{Z}}_1)(\bar{\mathfrak{Z}} - \mathfrak{Z}_1)^{-1} = \mathfrak{E} + 2i\lambda^{-1}(\mathfrak{Z} - \bar{\mathfrak{Z}}) + \cdots.$$

If $s_1, \cdots, s_n$ are the characteristic roots of the imaginary part $\mathfrak{Y}$ of $\mathfrak{Z}$, we obtain

$$r_k = 1 - 4 s_k \lambda^{-1} + \cdots \qquad (k = 1, \cdots, n),$$

whence

$$\rho^2(\mathfrak{Z}, i\lambda\mathfrak{E}) = \sum_{k=1}^{n} \log^2 (s_k^{-1}\lambda) + \omega(\lambda),$$

where $\omega(\lambda)$ is a power series in λ^{-1} without constant term. Consequently

$$\lim_{\lambda \to \infty} (\rho(\mathfrak{Z}, i\lambda\mathfrak{E}) - n^{\frac{1}{2}} \log \lambda) = n^{-\frac{1}{2}} \log |\mathfrak{Y}|^{-1}.$$

This suggests a consideration of the minimum of $|\mathfrak{Y}^*|^{-1}$.

Denoting by the sign abs $\mathfrak{K}$ the absolute value of the determinant of a matrix $\mathfrak{K}$, we have, by (59),

$$|\mathfrak{Y}^*|^{-1} = |\mathfrak{Y}|^{-1} \operatorname{abs} (\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^2.$$

In order to obtain the minimum of $|\mathfrak{Y}^*|^{-1}$, we have therefore to determine the minimum of abs $(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})$. The existence of this minimum is by no means trivial; we shall prove it now in the case of the modular group Γ.

Let

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}, \qquad \mathfrak{M}_0 = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_0 \\ \mathfrak{C}_0 & \mathfrak{D}_0 \end{pmatrix}$$

be two elements of the homogeneous modular group Γ_0 and let

$$\mathfrak{M}_0\mathfrak{M}^{-1} = \mathfrak{M}_1 = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{C}_1 & \mathfrak{D}_1 \end{pmatrix}.$$

We assume that the equation

$$\text{abs}\,(\mathfrak{C}\mathfrak{Z} + \mathfrak{D}) = \text{abs}\,(\mathfrak{C}_0\mathfrak{Z} + \mathfrak{D}_0) \tag{82}$$

holds identically for all $\mathfrak{Z}$ in H. Introducing $(\mathfrak{D}'\mathfrak{Z} - \mathfrak{B}')(-\mathfrak{C}'\mathfrak{Z} + \mathfrak{A}')^{-1}$ instead of $\mathfrak{Z}$, we obtain the necessary and sufficient condition

$$\text{abs}\,(\mathfrak{C}_1\mathfrak{Z} + \mathfrak{D}_1) = 1. \tag{83}$$

Since $|\,\mathfrak{C}_1\mathfrak{Z} + \mathfrak{D}_1\,|$ is an analytic function of the elements z_{kl} of $\mathfrak{Z}$, we infer that $|\,\mathfrak{C}_1\mathfrak{Z} + \mathfrak{D}_1\,| = c$, identically, for all complex symmetric matrices $\mathfrak{Z}$, with a constant c of absolute value 1. Putting $\mathfrak{Z} = 0$, we find $|\,\mathfrak{D}_1\,| = c$. On the other hand, the elements of $\mathfrak{D}_1$ are rational integers; consequently $\mathfrak{D}_1$ is a unimodular matrix $\mathfrak{U}$ and $c = \pm 1$. Calculating the linear terms in the identity $|\,\mathfrak{D}_1^{-1}\mathfrak{C}_1\mathfrak{Z} + \mathfrak{E}\,| = 1$, we obtain $\sigma(\mathfrak{D}_1^{-1}\mathfrak{C}_1\mathfrak{Z}) = 0$. But the matrix $\mathfrak{D}_1^{-1}\mathfrak{C}_1$ is symmetric and therefore $\mathfrak{C}_1 = 0$.

Let now $\mathfrak{M}_1$ be any modular matrix with $\mathfrak{C}_1 = 0$. The general form is

$$\mathfrak{M}_1 = \begin{pmatrix} \mathfrak{U}'^{-1} & \mathfrak{B}\mathfrak{U} \\ 0 & \mathfrak{U} \end{pmatrix} \tag{84}$$

with unimodular $\mathfrak{U}$ and integral symmetric $\mathfrak{B}$. Obviously (79) is satisfied, and $\mathfrak{M}_0 = \mathfrak{M}_1\mathfrak{M}$, with an arbitrary modular matrix $\mathfrak{M}$, gives the general solution of (82). Then

$$\mathfrak{C}_0 = \mathfrak{U}\mathfrak{C}, \qquad \mathfrak{D}_0 = \mathfrak{U}\mathfrak{D}. \tag{85}$$

It is also easily seen that $\mathfrak{M}_1 = \mathfrak{M}_0\mathfrak{M}^{-1}$ has always the form (84), if the second matrix rows $(\mathfrak{C}\mathfrak{D})$ and $(\mathfrak{C}_0\mathfrak{D}_0)$ of two modular matrices $\mathfrak{M}$ and $\mathfrak{M}_0$ are connected by (85), with unimodular $\mathfrak{U}$. The two pairs $\mathfrak{C}, \mathfrak{D}$ and $\mathfrak{C}_0, \mathfrak{D}_0$ are called *associate.*

Denoting by $\mathfrak{Y}^*$ and $\mathfrak{Y}^*_0$ the imaginary parts of

$$\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1} \quad \text{and} \quad \mathfrak{Z}^*_0 = (\mathfrak{A}_0\mathfrak{Z} + \mathfrak{B}_0)(\mathfrak{C}_0\mathfrak{Z} + \mathfrak{D}_0)^{-1},$$

we obtain, by (59),

$$\mathfrak{Y}^{-1}\{\mathfrak{Z}\mathfrak{C}'_0 + \mathfrak{D}'_0\} = \mathfrak{Y}^{*-1}[\mathfrak{U}'] = \mathfrak{Y}^{*}{}_0^{-1}. \tag{86}$$

Let $\mathfrak{Z}$ be a given point of H. For any modular matrix $\mathfrak{M}$, we choose a unimodular matrix $\mathfrak{U}$, such that $\mathfrak{Y}^{*-1}[\mathfrak{U}'] = \mathfrak{Y}^{*}{}_0^{-1}$ lies in the Minkowski domain R of Section **29.** We shall now prove that abs $(\mathfrak{C}_0\mathfrak{Z} + \mathfrak{D}_0)$ tends to infinity, if $(\mathfrak{C}_0\mathfrak{D}_0)$ runs over all second matrix rows of modular matrices with the required property of $\mathfrak{Y}^*_0$.

Let $y_1, \cdots, y_n$ denote the diagonal elements of $\mathfrak{Y}^*{}_0{}^{-1}$ and $\mathfrak{c}_l, \mathfrak{d}_l$ the l-th columns of $\mathfrak{C}'_0, \mathfrak{D}'_0$ $(l = 1, \cdots, n)$. By (86),

$$\text{(87)} \qquad \begin{aligned} \mathfrak{Y}^*{}_0{}^{-1} &= \mathfrak{Y}^{-1}[\mathfrak{X}\mathfrak{C}'_0 + \mathfrak{D}'_0] + \mathfrak{Y}[\mathfrak{C}'_0]; \\ y_l &= \mathfrak{Y}^{-1}[\mathfrak{X}\mathfrak{c}_l + \mathfrak{d}_l] + \mathfrak{Y}[\mathfrak{c}_l] \end{aligned} \qquad (l = 1, \cdots, n).$$

Consider all solutions $\mathfrak{C}_0, \mathfrak{D}_0$ of the inequality abs $(\mathfrak{C}_0\mathfrak{Z} + \mathfrak{D}_0)^2 < a$, where a is an arbitrary positive constant. By (81) and (86),

$$\prod_{l=1}^{n} y_l < \tau_2 a \mid \mathfrak{Y} \mid^{-1};$$

by (87),

$$\text{(88)} \qquad \mathfrak{Y}[\mathfrak{c}_l] \leq y_l, \qquad \mathfrak{Y}^{-1}[\mathfrak{X}\mathfrak{c}_l + \mathfrak{d}_l] \leq y_l \qquad (l = 1, \cdots, n),$$

and $\mathfrak{Y}^{-1}[\mathfrak{d}_l] = y_l$ in the case $\mathfrak{c}_l = 0$. Since $\mid \mathfrak{C}_0\mathfrak{Z} + \mathfrak{D}_0 \mid \neq 0$, the columns $\mathfrak{c}_l, \mathfrak{d}_l$ are not both 0; hence $y_l > y$, where y is a positive number depending only upon $\mathfrak{Y}$, and

$$y_l < \tau_2 a y^{1-n} \mid \mathfrak{Y} \mid^{-1}.$$

By (88), we obtain only a finite number of pairs $\mathfrak{C}_0, \mathfrak{D}_0$.

On account of (82), the existence of a modular transformation $\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ with the minimum value of abs $(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})$ is established for any $\mathfrak{Z}$ in H. We determine again $\mathfrak{U}$ by the condition that $\mathfrak{Y}^{*-1}[\mathfrak{U}']$ is a point of R and define $\mathfrak{Z}^*{}_0 = (\mathfrak{A}_0\mathfrak{Z} + \mathfrak{B}_0)(\mathfrak{C}_0\mathfrak{Z} + \mathfrak{D}_0)^{-1} = \mathfrak{Z}^*[\mathfrak{U}^{-1}] + \mathfrak{B}$, by (84), where $\mathfrak{B}$ is an arbitrary symmetric matrix with rational integral elements. We may choose $\mathfrak{B}$ such that all elements of the real part of $\mathfrak{Z}^*{}_0$ lie in the interval $-\frac{1}{2} \leq x \leq \frac{1}{2}$.

31. Let F be the set of all points $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$ of H satisfying the following three conditions:

$$\text{(89)} \qquad \text{abs}\,(\mathfrak{C}\mathfrak{Z} + \mathfrak{D}) \geq 1$$

for all modular transformations $\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$;

$$\text{(90)} \qquad L_r(\mathfrak{Y}^{-1}) \geq 0 \qquad (r = 1, \cdots, g);$$

$$\text{(91)} \qquad x_{kl} \geq -\tfrac{1}{2}, \qquad -x_{kl} \geq -\tfrac{1}{2} \qquad (1 \leq k \leq l \leq n)$$

for the elements x_{kl} of $\mathfrak{X}$. In (89), we shall omit the trivial case $\mathfrak{C} = 0$, since the corresponding condition abs $(\mathfrak{D}) \geq 1$ holds identically for all $\mathfrak{Z}$. By the result of the preceding section, the images of F under Γ cover the whole space H.

We write $\mathfrak{Y}^{-1} = \mathfrak{P}[\mathfrak{Q}]$ with $\mathfrak{P} = [p_1, \cdots, p_n]$, $\mathfrak{Q} = (q_{kl})$, $q_{kl} = 0$ $(1 \leq l < k \leq n)$, $q_{kk} = 1$ $(k = 1, \cdots, n)$ and define $\mathfrak{W}^{(n)} = (w_{kl})$ with $w_{kl} = 0$ $(k + l \neq n + 1)$, $w_{kl} = 1$ $(k + l = n + 1)$,

$$\mathfrak{P}_1=\begin{pmatrix}\mathfrak{P} & 0\\ 0 & \mathfrak{P}^{-1}[\mathfrak{W}]\end{pmatrix},\qquad \mathfrak{Q}_1=\begin{pmatrix}\mathfrak{Q} & -\mathfrak{Q}\mathfrak{X}\\ 0 & \mathfrak{W}\mathfrak{Q}'^{-1}\mathfrak{W}\end{pmatrix},\qquad \mathfrak{W}_1=\begin{pmatrix}\mathfrak{E} & 0\\ 0 & \mathfrak{W}\end{pmatrix}.$$

By (77),

(92) $$\mathfrak{S}[\mathfrak{W}_1]=\mathfrak{P}_1[\mathfrak{Q}_1].$$

By Lemma 7 and (91), the absolute values of the elements of the triangular matrix $\mathfrak{Q}_1$ are less than a number depending only upon n. Denoting the diagonal elements of $\mathfrak{P}_1$ by $d_1, \cdots, d_{2n}$, we have

$$d_k d_{k+1}^{-1}=p_k p_{k+1}^{-1}\ (1\leq k<n),\ =p_n^2\ (k=n),\ =p_{2n-k}p_{2n-k+1}^{-1}\ (n<k<2n).$$

By Lemma 7,

(93) $$0<d_k\leq\tau_1 d_{k+1}\qquad (k\neq n),$$

where τ_1 depends only upon $m=2n$.

We apply (89) for the particular modular transformation with

$$\mathfrak{A}=\begin{pmatrix}\mathfrak{E}^{(n-1)} & 0\\ 0 & 0\end{pmatrix},\quad \mathfrak{B}=\begin{pmatrix}0 & 0\\ 0 & -1\end{pmatrix},\quad \mathfrak{C}=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix},\quad \mathfrak{D}=\begin{pmatrix}\mathfrak{E}^{(n-1)} & 0\\ 0 & 0\end{pmatrix}.$$

Denoting by x_n+iy_n the last diagonal element of $\mathfrak{Z}$, we obtain the inequality $x_n^2+y_n^2\geq 1$. By (91), we have moreover $x_n^2\leq\frac{1}{4}$, whence $y_n^2\geq\frac{3}{4}$. But $\mathfrak{Y}=\mathfrak{P}^{-1}[\mathfrak{Q}'^{-1}]$, and consequently $y_n=p_n^{-1}$,

(94) $$0<d_n\leq(4/3)\,d_{n+1}.$$

By (92), (93) and (94), $\mathfrak{S}[\mathfrak{W}_1]$ is contained in a domain $Q(\tau_3)$ of the space P of positive symmetric matrices with $2n$ rows, where τ_3 depends only upon n.

Consider now any modular transformation $\mathfrak{Z}^*=(\mathfrak{A}\mathfrak{Z}+\mathfrak{B})(\mathfrak{C}\mathfrak{Z}+\mathfrak{D})^{-1}$ different from identity, i. e.,

$$\mathfrak{M}=\begin{pmatrix}\mathfrak{A} & \mathfrak{B}\\ \mathfrak{C} & \mathfrak{D}\end{pmatrix}\neq\pm\mathfrak{E},$$

and assume that $\mathfrak{Z}$ and $\mathfrak{Z}^*$ both are points of F. By Lemma 6, $\mathfrak{S}=\mathfrak{S}^*[\mathfrak{M}]$,

$$\mathfrak{S}[\mathfrak{W}_1]=\mathfrak{S}^*[\mathfrak{W}_1][\mathfrak{W}_1\mathfrak{M}\mathfrak{W}_1].$$

Applying Lemma 8 with

$$\mathfrak{T}_1=\mathfrak{S}^*[\mathfrak{W}_1],\quad \mathfrak{T}_2=\mathfrak{S}[\mathfrak{W}_1],\quad \mathfrak{F}=\mathfrak{W}_1\mathfrak{M}\mathfrak{W}_1,\quad |\mathfrak{F}|=1,$$

we conclude that $\mathfrak{M}$ belongs to a finite set of modular matrices $\mathfrak{M}_1,\cdots,\mathfrak{M}_h$, independent of $\mathfrak{Z}$ and $\mathfrak{Z}^*$.

On account of the minimum property of $|\mathfrak{Y}|^{-1}$, we have $|\mathfrak{Y}|=|\mathfrak{Y}^*|$, whence abs $(\mathfrak{C}\mathfrak{Z}+\mathfrak{D})=1$. If $\mathfrak{C}\neq 0$, then the sign of equality is true in one of the conditions (89). If $\mathfrak{C}=0$, then $\mathfrak{M}$ has the form (84),

$$\mathfrak{M}=\begin{pmatrix}\mathfrak{U}'^{-1} & \mathfrak{B}\mathfrak{U}\\ 0 & \mathfrak{U}\end{pmatrix}$$

and $\mathfrak{Y}^{*-1}=\mathfrak{Y}^{-1}[\mathfrak{U}']$. In the case $\mathfrak{U}\neq\pm\mathfrak{E}$, the sign of equality is true in one of the conditions (90). In the case $\mathfrak{U}=\pm\mathfrak{E}$, we have $\mathfrak{Z}^*=\mathfrak{Z}+\mathfrak{B}$, $\mathfrak{X}^*=\mathfrak{X}+\mathfrak{B}$ with integral symmetric $\mathfrak{B}\neq 0$, and then the sign of equality holds in one of the conditions (91).

We have proved the following statement: If two points $\mathfrak{Z}$ and $\mathfrak{Z}^*$ of F are equivalent under a modular transformation with the matrix $\mathfrak{M}\neq\pm\mathfrak{E}$, then $\mathfrak{M}$ is one of the matrices

$$\mathfrak{M}_s=\begin{pmatrix}\mathfrak{A}_s & \mathfrak{B}_s\\ \mathfrak{C}_s & \mathfrak{D}_s\end{pmatrix}\qquad (s=1,\cdots,h)$$

and the conditions

(95) $$\text{abs}\,(\mathfrak{C}_s\mathfrak{Z}+\mathfrak{D}_s)\geq 1\qquad (s=1,\cdots,h),$$

(96) $$L_r(\mathfrak{Y}^{-1})\geq 0\qquad (r=1,\cdots,g),$$

(97) $$x_{kl}\geq -\tfrac{1}{2},\qquad -x_{kl}\geq -\tfrac{1}{2}\qquad (1\leq k\leq l\leq n)$$

are fulfilled with at least one sign of equality.

32. Since (95) is contained in (89), every point $\mathfrak{Z}$ of F satisfies (95), (96) and (97). We prove, now, that the converse is true, namely, that all the inequalities (89) follow from (95), (96) and (97). We shall demonstrate at the same time, that then the stronger inequalities abs $(\mathfrak{C}\mathfrak{Z}+\mathfrak{D})>1$ hold, if $\mathfrak{C},\mathfrak{D}$ is not associate with one of the pairs $\mathfrak{C}_s,\mathfrak{D}_s$ $(s=1,\cdots,h)$.

LEMMA 9. *Let $\mathfrak{Z}=\mathfrak{X}+i\mathfrak{Y}$ be a point of H and $\mathfrak{Z}_\lambda=\mathfrak{X}+i\lambda\mathfrak{Y}$, with an arbitrary scalar factor λ. If $(\mathfrak{C}\mathfrak{D})$ is the second matrix row of any symplectic matrix and $\mathfrak{C}\neq 0$, then the inequality* abs $(\mathfrak{C}\mathfrak{Z}_\lambda+\mathfrak{D})>$ abs $(\mathfrak{C}\mathfrak{Z}_\mu+\mathfrak{D})$ *holds for $\lambda>\mu>0$.*

The determinant $|\mathfrak{C}\mathfrak{Z}^\lambda+\mathfrak{D}|=\phi(\lambda)$ is a polynomial in λ. For any λ with positive real part, $\mathfrak{Z}_\lambda$ is a point of H and consequently $\phi(\lambda)\neq 0$. Moreover $\overline{\phi(\lambda)}=\phi(-\bar{\lambda})$; hence all zeros of $\phi(\lambda)$ are pure imaginary. This proves that for real λ the expression abs $(\mathfrak{C}\mathfrak{Z}_\lambda+\mathfrak{D})^2$ is a polynomial in λ^2 with real non-negative coefficients. It remains only to prove that this polynomial is not identically constant.

Assume now that

$$\text{abs}\,(\mathfrak{C}\mathfrak{Z}^\lambda+\mathfrak{D})=\text{abs}\,(\mathfrak{C}\mathfrak{Z}_0+\mathfrak{D})=\text{abs}\,(\mathfrak{C}\mathfrak{X}+\mathfrak{D}),$$

identically in λ. Then abs $(\mathfrak{C}\mathfrak{X} + \mathfrak{D}) \neq 0$ and

$$\text{abs}\,(\mathfrak{Y}^{-1} + i\lambda(\mathfrak{C}\mathfrak{X} + \mathfrak{D})^{-1}\mathfrak{C}) = |\,\mathfrak{Y}\,|^{-1}. \tag{98}$$

Since $(\mathfrak{C}\mathfrak{X} + \mathfrak{D})^{-1}\mathfrak{C}$ is a real symmetric matrix and $\mathfrak{Y}^{-1} > 0$, there exists a real matrix $\mathfrak{K}^{(n)}$ and a diagonal matrix $\mathfrak{R} = [r_1, \cdots, r_n]$, such that

$$\mathfrak{Y}^{-1}[\mathfrak{K}] = \mathfrak{E}, \qquad ((\mathfrak{C}\mathfrak{X} + \mathfrak{D})^{-1}\mathfrak{C})[\mathfrak{K}] = \mathfrak{R}. \tag{99}$$

By (98) and (99),

$$\prod_{k=1}^{n} (1 + r_k^2\lambda^2) = 1$$

for all real values of λ, and consequently $\mathfrak{R} = 0$, $\mathfrak{C} = 0$, which is a contradiction. This completes the proof of the lemma.

We denote again by $(\mathfrak{C}\mathfrak{D})$ the second matrix rows of the modular matrices. Let $\mathfrak{Z}$ be a point of H satisfying all conditions (95), (96) and (97), and assume that the inequality abs $(\mathfrak{C}\mathfrak{Z} + \mathfrak{D}) \leq 1$ holds for at least one pair $\mathfrak{C}, \mathfrak{D}$, where $\mathfrak{C} \neq 0$ and $\mathfrak{C}, \mathfrak{D}$ is not associate with one of the pairs $\mathfrak{C}_s, \mathfrak{D}_s$ $(s = 1, \cdots, h)$. By the result of Section **30**, only a finite number of non-associate pairs $\mathfrak{C}, \mathfrak{D}$ fulfill that inequality. By Lemma 9, there exists a number $\lambda \geq 1$, such that abs $(\mathfrak{C}\mathfrak{Z}_\lambda + \mathfrak{D}) \geq 1$ for all $\mathfrak{C}, \mathfrak{D}$ and abs $(\mathfrak{C}\mathfrak{Z}_\lambda + \mathfrak{D}) = 1$ for $\mathfrak{C} = \mathfrak{C}_0$, $\mathfrak{D} = \mathfrak{D}_0$, where $\mathfrak{C}_0 \neq 0$ and $\mathfrak{C}_0, \mathfrak{D}_0$ is not associate with one of the pairs $\mathfrak{C}_s, \mathfrak{D}_s$. Since $\mathfrak{Z}_\lambda$ has the real part $\mathfrak{X}$ and $L_r(\lambda^{-1}\mathfrak{Y}^{-1}) = \lambda^{-1}L_r(\mathfrak{Y}^{-1})$, all conditions (89), (90) and (91) are satisfied for $\mathfrak{Z}_\lambda$ instead of $\mathfrak{Z}$; hence $\mathfrak{Z}_\lambda$ is a point of F. On the other hand, the expression abs $(\mathfrak{C}\mathfrak{Z}_\lambda + \mathfrak{D})$ attains its minimum 1 for $\mathfrak{C} = \mathfrak{C}_0$, $\mathfrak{D} = \mathfrak{D}_0$, and consequently there exists a modular transformation $\mathfrak{Z}^*_\lambda = (\mathfrak{A}\mathfrak{Z}_\lambda + \mathfrak{B})(\mathfrak{C}\mathfrak{Z}_\lambda + \mathfrak{D})^{-1}$, such that $\mathfrak{C}, \mathfrak{D}$ is associate with $\mathfrak{C}_0, \mathfrak{D}_0$ and $\mathfrak{Z}^*_\lambda$ is a point of F. By Section **31**, $\mathfrak{C} = \mathfrak{C}_s$, $\mathfrak{D} = \mathfrak{D}_s$, and this is a contradiction. Consequently abs $(\mathfrak{C}\mathfrak{Z} + \mathfrak{D}) \geq 1$ for all $\mathfrak{C}, \mathfrak{D}$ and abs $(\mathfrak{C}\mathfrak{Z} + \mathfrak{D}) > 1$, if $\mathfrak{C} \neq 0$ and $\mathfrak{C}, \mathfrak{D}$ is not associate with one of the pairs $\mathfrak{C}_s, \mathfrak{D}_s$.

33. By the result of the preceding section, F may be defined by the inequalities (95), (96) and (97), in finite number. Obviously F is closed relative to H. It follows from Lemma 9 and the linearity of the conditions (96) and (97), that $\mathfrak{Z}$ is a frontier point of F, if, and only if, (95), (96) and (97) are fulfilled with at least one sign of equality.

Let $F_{\mathfrak{M}}$ be the image of F under the modular transformation $\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ with the matrix $\mathfrak{M} \neq \pm\,\mathfrak{E}$. If F and $F_{\mathfrak{M}}$ have a point $\mathfrak{Z}^*$ in common, then, by Section **31**, $\mathfrak{M}$ is one of the matrices $\mathfrak{M}_1, \cdots, \mathfrak{M}_h$, and $\mathfrak{Z}^*$ is a frontier point of F. Consequently the images $F_{\mathfrak{M}}$ cover H without overlappings, and F has only a finite number of neighbors.

Consider any compact domain G in H, and let G_1 be the corresponding domain in the space S of the matrices $\mathfrak{S}$ defined in Lemma 6. There exists a number t depending only upon G, such that G_1 is contained in the domain $Q(t)$ of Section **29**. We may choose $t \geq \tau_3$, where τ_3 was defined in Section **31**. Let $\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ be a common point of $F_{\mathfrak{M}}$ and G. Then $\mathfrak{Z}$ is a point of F and the relationship $\mathfrak{S}^* = \mathfrak{S}[\mathfrak{M}^{-1}]$ holds for the corresponding points $\mathfrak{S}^*$ and $\mathfrak{S}$ of S, by Lemma 6. It follows from the result of Section **31**, that the point $\mathfrak{S}[\mathfrak{W}_1] = \mathfrak{S}^*[\mathfrak{M}\mathfrak{W}_1]$ lies in $Q(t)$. But also $\mathfrak{S}^*$ itself is a point of $Q(t)$, and consequently, by Lemma 8, the matrix $\mathfrak{M}$ belongs to a finite set. This proves that only a finite number of images $F_{\mathfrak{M}}$ enter into the compact domain G.

For the particular value $\mathfrak{Z} = i\mathfrak{E}$, we have $|\mathfrak{C}\mathfrak{Z} + \mathfrak{D}| = c + id$, with rational integers c, d not both 0. Consequently (89) is satisfied. Also (91) holds, since $\mathfrak{X} = 0$. Moreover $\mathfrak{Y}^{-1} = \mathfrak{E}$ is a point of the Minkowski domain R. Consequently $\mathfrak{Z} = i\mathfrak{E}$ is a point of F. By Lemma 9, the whole curve $\mathfrak{Z} = i\lambda\mathfrak{E}$ $(\lambda \geq 1)$ belongs to F. Since λ may be arbitrarily large, the fundamental domain F is not compact. Let G be any compact domain in H and consider the finite set of modular matrices $\mathfrak{M}$, such that $F_{\mathfrak{M}}$ enters into G. The set of images of G under the inverse mappings with the matrices $\mathfrak{M}^{-1}$ constitutes again a compact domain G_0. For sufficiently large values of λ, the point $i\lambda\mathfrak{E}$ of F does not lie in G_0; hence no image of this point lies in G. This proves that the space H is not compact relative to the modular group Γ.

By the results of Section **31**, the matrices $\mathfrak{X}$ and $\mathfrak{Y}^{-1}$ are bounded for all $\mathfrak{Z}$ in F. On account of (57), the integral $V(\Gamma)$ converges.

Theorem 8 is now completely proved.

VII. THE FUNDAMENTAL DOMAIN OF THE GROUP $\Delta(\mathfrak{G}, \mathfrak{H})$.

34. Let K_0 be an algebraic number field, of finite degree g over the field of rational numbers. Let g_1 of the conjugate fields be real and $2g_2$ imaginary, $g = g_1 + 2g_2$. We denote the real conjugate fields by $K_0^{(\alpha)}$ $(\alpha = 1, \cdots, g_1)$ and the pairs of conjugate complex conjugate fields by $K_0^{(\alpha)}$ and $K_0^{(\alpha+g_2)}$ $(\alpha = g_1 + 1, \cdots, g_1 + g_2)$. We consider g_1 positive symmetric matrices $\mathfrak{T}_\alpha$ $(\alpha = 1, \cdots, g_1)$ with real elements and g_2 positive hermitian matrices $\mathfrak{T}_\alpha$ $(\alpha = g_1 + 1, \cdots, g_1 + g_2)$ with complex elements, all of m rows. We denote the systems of $g_1 + g_2$ matrices $\mathfrak{T}_\alpha$ $(\alpha = 1, \cdots, g_1 + g_2)$ more shortly by $\mathfrak{T}$; they form the points of a space P of $\frac{1}{2}g_1 m(m+1) + g_2 m^2$ dimensions.

We have a unique decomposition $\mathfrak{T}_\alpha = \mathfrak{P}_\alpha\{\mathfrak{Q}_\alpha\}$ with a diagonal matrix

Consider any compact domain G in H, and let G_1 be the corresponding domain in the space S of the matrices $\mathfrak{S}$ defined in Lemma 6. There exists a number t depending only upon G, such that G_1 is contained in the domain $Q(t)$ of Section **29**. We may choose $t \geq \tau_3$, where τ_3 was defined in Section **31.** Let $\mathfrak{Z}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ be a common point of $F_{\mathfrak{M}}$ and G. Then $\mathfrak{Z}$ is a point of F and the relationship $\mathfrak{S}^* = \mathfrak{S}[\mathfrak{M}^{-1}]$ holds for the corresponding points $\mathfrak{S}^*$ and $\mathfrak{S}$ of S, by Lemma 6. It follows from the result of Section **31**, that the point $\mathfrak{S}[\mathfrak{W}_1] = \mathfrak{S}^*[\mathfrak{M}\mathfrak{W}_1]$ lies in $Q(t)$. But also $\mathfrak{S}^*$ itself is a point of $Q(t)$, and consequently, by Lemma 8, the matrix $\mathfrak{M}$ belongs to a finite set. This proves that only a finite number of images $F_{\mathfrak{M}}$ enter into the compact domain G.

For the particular value $\mathfrak{Z} = i\mathfrak{E}$, we have $|\mathfrak{C}\mathfrak{Z} + \mathfrak{D}| = c + id$, with rational integers c, d not both 0. Consequently (89) is satisfied. Also (91) holds, since $\mathfrak{X} = 0$. Moreover $\mathfrak{Y}^{-1} = \mathfrak{E}$ is a point of the Minkowski domain R. Consequently $\mathfrak{Z} = i\mathfrak{E}$ is a point of F. By Lemma 9, the whole curve $\mathfrak{Z} = i\lambda\mathfrak{E}$ $(\lambda \geq 1)$ belongs to F. Since λ may be arbitrarily large, the fundamental domain F is not compact. Let G be any compact domain in H and consider the finite set of modular matrices $\mathfrak{M}$, such that $F_{\mathfrak{M}}$ enters into G. The set of images of G under the inverse mappings with the matrices $\mathfrak{M}^{-1}$ constitutes again a compact domain G_0. For sufficiently large values of λ, the point $i\lambda\mathfrak{E}$ of F does not lie in G_0; hence no image of this point lies in G. This proves that the space H is not compact relative to the modular group Γ.

By the results of Section **31**, the matrices $\mathfrak{X}$ and $\mathfrak{Y}^{-1}$ are bounded for all $\mathfrak{Z}$ in F. On account of (57), the integral $V(\Gamma)$ converges.

Theorem 8 is now completely proved.

VII. THE FUNDAMENTAL DOMAIN OF THE GROUP $\Delta(\mathfrak{G}, \mathfrak{H})$.

34. Let K_0 be an algebraic number field, of finite degree g over the field of rational numbers. Let g_1 of the conjugate fields be real and $2g_2$ imaginary, $g = g_1 + 2g_2$. We denote the real conjugate fields by $K_0^{(\alpha)}$ $(\alpha = 1, \cdots, g_1)$ and the pairs of conjugate complex conjugate fields by $K_0^{(\alpha)}$ and $K_0^{(\alpha+g_2)}$ $(\alpha = g_1 + 1, \cdots, g_1 + g_2)$. We consider g_1 positive symmetric matrices $\mathfrak{T}_\alpha$ $(\alpha = 1, \cdots, g_1)$ with real elements and g_2 positive hermitian matrices $\mathfrak{T}_\alpha$ $(\alpha = g_1 + 1, \cdots, g_1 + g_2)$ with complex elements, all of m rows. We denote the systems of $g_1 + g_2$ matrices $\mathfrak{T}_\alpha$ $(\alpha = 1, \cdots, g_1 + g_2)$ more shortly by $\mathfrak{T}$; they form the points of a space P of $\frac{1}{2}g_1 m(m+1) + g_2 m^2$ dimensions.

We have a unique decomposition $\mathfrak{T}_\alpha = \mathfrak{P}_\alpha\{\mathfrak{Q}_\alpha\}$ with a diagonal matrix

$\mathfrak{P}_\alpha = [p_1{}^{(\alpha)}, \cdots, p_m{}^{(\alpha)}]$, $p_k{}^{(\alpha)} > 0$ $(k = 1, \cdots, m)$, and a triangular matrix $\mathfrak{Q}_\alpha = (q_{kl}^{(\alpha)})$, $q_{kl}^{(\alpha)} = 0$ $(k > l)$, $q_{kk}^{(\alpha)} = 1$, where $\mathfrak{Q}_\alpha$ is real for $\alpha = 1, \cdots, g_1$. If t is any positive number > 1, the inequalities

$$0 < p_k{}^{(\alpha)} \leq t p_{k+1}^{(\alpha)} \quad (k < m), \qquad p_k{}^{(\alpha)} \leq t p_k{}^{(\beta)} \quad (k \leq m)$$
$$\operatorname{abs} q_{kl}^{(\alpha)} \leq t \qquad (k < l)$$

with $\alpha, \beta = 1, \cdots, g_1 + g_2$ define a compact domain $Q(t)$ in P.

A matrix $\mathfrak{U}$ with integral elements in K_0 is called unimodular if the determinant $|\mathfrak{U}|$ is an algebraic unit. The unimodular matrices $\mathfrak{U}^{(m)}$ constitute the unimodular group $\mathfrak{U}$ in K_0, of degree m. The center C of U consists of the matrices $\mathfrak{U} = u\mathfrak{E}$, where u is any root of unity in K_0. We denote by U_0 the factor group U/C. Let $\mathfrak{U}_\alpha$ be the conjugate of $\mathfrak{U}$ in $K_0{}^{(\alpha)}$. The transformation $\mathfrak{T}_\alpha \to \mathfrak{T}_\alpha\{\mathfrak{U}_\alpha\}$ $(\alpha = 1, \cdots, g_1 + g_2)$, or more shortly $\mathfrak{T} \to \mathfrak{T}\{\mathfrak{U}\}$, maps the space P onto itself. This mapping is the identical one, if and only if $\mathfrak{U}$ is an element of C; consequently the transformations $\mathfrak{T} \to \mathfrak{T}\{\mathfrak{U}\}$ give a faithful representation of U_0.

Minkowski's theory of reduction of positive quadratic forms is concerned with the case $g = 1$, the field of rational numbers. The generalization to the case of an arbitrary field K_0 is due to P. Humbert. He obtained the following results:

There exists in P a fundamental domain R with respect to U_0, which is the union of a finite number of convex pyramids. The faces of these pyramids have equations of the form

$$\sum_{\alpha=1}^{g_1+g_2} (\mathfrak{a}'_\alpha \mathfrak{T}_\alpha \bar{\mathfrak{b}}_\alpha + \bar{\mathfrak{a}}'_\alpha \bar{\mathfrak{T}}_\alpha \mathfrak{b}_\alpha) = 0, \tag{100}$$

where $\mathfrak{a}_\alpha$ and $\mathfrak{b}_\alpha$ are the conjugates of two columns $\mathfrak{a} \neq 0$ and $\mathfrak{b} \neq 0$ in K_0; moreover $\mathfrak{a} \neq \lambda\mathfrak{b}$ for every pure imaginary scalar factor λ. Any compact domain in P is covered by a finite number of images $R_{\mathfrak{U}}$ of R, and R has only a finite number of neighbors $R_{\mathfrak{U}}$.

LEMMA 10. *There exists a finite set L of matrices $\mathfrak{L}$ with integral elements in K_0 and a positive number τ_4 depending only upon K_0 and m, such that for every $\mathfrak{T}$ in R the point $\mathfrak{T}\{\mathfrak{L}\}$ belongs to $Q(\tau_4)$, with at least one $\mathfrak{L}$ of the set L.*

LEMMA 11. *Let $\mathfrak{T}$ and $\mathfrak{T}\{\mathfrak{F}\}$ be two points of $Q(t)$, where $\mathfrak{F}$ is an integral matrix in K_0, and let ν be the norm of $|\mathfrak{F}|$. Then $\mathfrak{F}$ belongs to a finite set of matrices depending only upon K_0, m, t and ν.*

These statements are generalizations of the lemmata 7 and 8.

35. We assume now that $K_0 = K(\sqrt{-r})$, where K is a totally real algebraic number field of degree h and r a totally positive number of K; then $g_1 = 0$, $g_2 = h$. Let $K^{(\alpha)}$ $(\alpha = 1, \cdots, h)$ be the conjugates of $K = K^{(1)}$, r_α the conjugate of r in $K^{(\alpha)}$ and $K_0{}^{(\alpha)} = K^{(\alpha)}(\sqrt{-r_\alpha})$. In the notation of Chapter V, $\mathfrak{H}$ is a hermitian matrix and $\mathfrak{G}$ is a skew-symmetric matrix, both in K_0, satisfying the condition (67). Let $\mathfrak{H}_\alpha, \mathfrak{G}_\alpha$ be the conjugates of $\mathfrak{H}, \mathfrak{G}$ in $K_0{}^{(\alpha)}$ and s_α the conjugate of s in $K^{(\alpha)}$. We assumed moreover $s > 0$, $\mathfrak{H}_\alpha > 0$ for $\alpha = 2, \cdots, h$; then $s_\alpha < 0$ $(\alpha = 2, \cdots, h)$. The group $\Lambda = \Lambda(\mathfrak{G}, \mathfrak{H})$ consists of all unimodular matrices $\mathfrak{W}$ in K_0 which satisfy $\mathfrak{G}[\mathfrak{W}] = \mathfrak{G}$ and $\mathfrak{H}\{\mathfrak{W}\} = \mathfrak{H}$. We have $\Delta_0 = \mathfrak{C}^{-1}\Lambda\mathfrak{C}$, where $\mathfrak{C}$ is a complex matrix with $\mathfrak{G}[\mathfrak{C}] = \mathfrak{J}$ and $\mathfrak{H}\{\mathfrak{C}\} = is^{\frac{1}{2}}\mathfrak{J}$. Identifying $\mathfrak{W}$ and $-\mathfrak{W}$, we obtain the factor group $\Delta = \Delta(\mathfrak{G}, \mathfrak{H})$ of Δ_0. Obviously this group is not changed, if we replace $\mathfrak{G}, \mathfrak{H}$ by $a\mathfrak{G}, b\mathfrak{H}$ with arbitrary positive rational numbers a, b; consequently we may assume that $\mathfrak{G}$ and $\mathfrak{H}$ have integral elements.

The matrix $\mathfrak{S}$ of (77) is the general solution of $\mathfrak{S}' = \bar{\mathfrak{S}} > 0$, $\mathfrak{J}[\mathfrak{S}] = \mathfrak{J}$, $\mathfrak{J}\{\mathfrak{S}\} = \mathfrak{J}$. Consequently

(101) $$\mathfrak{T}_1 = \mathfrak{S}\{\mathfrak{C}^{-1}\}$$

is the general solution of

(102) $$\mathfrak{T}'_1 = \bar{\mathfrak{T}}_1 > 0, \quad \mathfrak{T}_1\mathfrak{G}^{-1}\bar{\mathfrak{T}}_1 = -\bar{\mathfrak{G}}, \quad \mathfrak{T}_1\mathfrak{H}^{-1}\mathfrak{T}_1 = s^{-1}\mathfrak{H}.$$

We define

(103) $$\mathfrak{T}_\alpha = (-s_\alpha)^{-\frac{1}{2}}\mathfrak{H}_\alpha \qquad (\alpha = 2, \cdots, h);$$

then, by (67) and (102),

(104) $$\mathfrak{T}'_\alpha = \bar{\mathfrak{T}}_\alpha > 0, \quad \mathfrak{T}_\alpha = \bar{\mathfrak{T}}_\alpha^{-1}\{\mathfrak{G}_\alpha\}, \quad \mathfrak{T}_\alpha = |\, s_\alpha\,|^{-1}\mathfrak{T}_\alpha^{-1}\{\mathfrak{H}'_\alpha\} \qquad (\alpha = 1, \cdots, h),$$

where $|\, s_\alpha \,|$ denotes the absolute value of s_α. The matrices $\mathfrak{T}_2, \cdots, \mathfrak{T}_h$ are fixed, whereas $\mathfrak{T}_1$ depends upon the variable point $\mathfrak{Z}$ of H, by (77). The space H is mapped onto a surface T, of $n(n+1)$ dimensions, in the space R. If $\mathfrak{W}$ is any element of the group Λ, then the transformation $\mathfrak{T}_\alpha \rightarrow \mathfrak{T}_\alpha\{\mathfrak{W}_\alpha{}^{-1}\}$ $(\alpha = 1, \cdots, h)$ maps T onto itself, and this mapping is the identical one, if and only if $\mathfrak{W} = \pm\,\mathfrak{E}$; on the other hand, by Lemma 6, the corresponding mapping in H is a symplectic transformation of $\mathfrak{Z}$, with the matrix $\mathfrak{M} = \mathfrak{C}^{-1}\mathfrak{W}\mathfrak{C}$ of the group Δ.

For any point $\mathfrak{T}$ of T, there exists a unimodular matrix $\mathfrak{U} = \mathfrak{U}_{\mathfrak{Z}}$ in K_0, such that $\mathfrak{T}\{\mathfrak{U}\}$ is a point of the domain R. By Lemma 10, we may choose a matrix $\mathfrak{L}$ of the finite set L, such that $\hat{\mathfrak{T}} = \mathfrak{T}\{\mathfrak{U}\mathfrak{L}\}$ belongs to $Q(\tau_4)$. Putting $\hat{\mathfrak{G}} = \mathfrak{G}[\mathfrak{U}\mathfrak{L}]$, $\hat{\mathfrak{H}} = \mathfrak{H}\{\mathfrak{U}\mathfrak{L}\}$ we obtain, by (104),

$$(105) \qquad \hat{\mathfrak{T}} = \bar{\hat{\mathfrak{T}}}^{-1}\{\hat{\mathfrak{G}}\}, \qquad \hat{\mathfrak{T}} = |s|^{-1}\hat{\mathfrak{T}}^{-1}\{\hat{\mathfrak{H}}'\};$$

we omit here and in the following formulae the index α which runs always from 1 to h.

Let $\mathfrak{V}$ denote the matrix of the linear transformation $x_k \to x_{2n-k+1}$ $(k = 1, \cdots, 2n)$. If $\hat{\mathfrak{T}} = \mathfrak{P}\{\mathfrak{Q}\}$ is the decomposition defined in Section **34**, then $\bar{\hat{\mathfrak{T}}}^{-1}\{\mathfrak{V}\} = \mathfrak{P}^{-1}\{\mathfrak{V}\}\{\mathfrak{V}\bar{\mathfrak{Q}}'^{-1}\mathfrak{V}\}$, and consequently the points $|s|^{-1}\hat{\mathfrak{T}}^{-1}\{\mathfrak{V}\}$ and $\hat{\mathfrak{T}}^{-1}\{\mathfrak{V}\}$ belong to a domain $Q(\tau_5)$, where τ_5 depends only upon K_0, n and s. Moreover

$$|\mathfrak{V}\hat{\mathfrak{H}}'| = (-1)^n |\mathfrak{H}| \operatorname{abs}(\mathfrak{U}\mathfrak{L})^2, \qquad |\mathfrak{V}\hat{\mathfrak{G}}| = (-1)^n |\mathfrak{G}| \; |\mathfrak{U}\mathfrak{L}|^2;$$

hence the norms of $|\mathfrak{V}\hat{\mathfrak{H}}'|$ and $|\mathfrak{V}\hat{\mathfrak{G}}|$ belong to a finite set. It follows now from Lemma 11 and (105), that also the matrices $\hat{\mathfrak{G}}$ and $\hat{\mathfrak{H}}$ belong to a finite set, independent of $\mathfrak{Z}$, and the same holds good for $\mathfrak{G}[\mathfrak{U}] = \hat{\mathfrak{G}}[\mathfrak{L}^{-1}]$ and $\mathfrak{H}\{\mathfrak{U}\} = \hat{\mathfrak{H}}\{\mathfrak{L}^{-1}\}$.

Choose now a complete system of points $\mathfrak{Z}_0$ in H, such that the pairs $\mathfrak{G}[\mathfrak{U}_0]$, $\mathfrak{H}\{\mathfrak{U}_0\}$ with $\mathfrak{U}_0 = \mathfrak{U}_{\mathfrak{Z}_0}$ are all different, and let V be the finite set of the unimodular matrices $\mathfrak{U}_0$. We denote by $G(\mathfrak{U}_0)$ the closed set of all points $\mathfrak{Z}$ of H, such that the corresponding point $\mathfrak{T}$ of T lies in $R_{\mathfrak{U}_0^{-1}}$, and by G the union of these $G(\mathfrak{U}_0)$, as $\mathfrak{U}_0$ runs over the elements of the set V.

Let $\mathfrak{Z}$ be again an arbitrary point of H and $\mathfrak{U} = \mathfrak{U}_{\mathfrak{Z}}$. Then there exists a uniquely determined $\mathfrak{U}_0$ in V, such that $\mathfrak{G}[\mathfrak{U}_0] = \mathfrak{G}[\mathfrak{U}]$ and $\mathfrak{H}\{\mathfrak{U}_0\} = \mathfrak{H}\{\mathfrak{U}\}$; thus $\mathfrak{U}_0\mathfrak{U}^{-1} = \mathfrak{W}$ is an element of the group Λ. Since $\mathfrak{T}\{\mathfrak{U}\}$ lies in R, the point $\mathfrak{T}\{\mathfrak{W}^{-1}\} = \mathfrak{T}\{\mathfrak{U}\mathfrak{U}_0^{-1}\}$ is contained in $R_{\mathfrak{U}_0^{-1}}$; hence $\mathfrak{Z}$ is mapped by the element $\mathfrak{M} = \mathfrak{C}^{-1}\mathfrak{W}\mathfrak{C}$ of Δ into a point of $G(\mathfrak{U}_0)$. This proves that any $\mathfrak{Z}$ in H is under Δ equivalent to at least one point of G; we call this point a *reduced image* of $\mathfrak{Z}$.

36. Let us assume that there exists in H a compact domain B, such that $\mathfrak{T}\{\mathfrak{U}_{\mathfrak{Z}}\}$ is a boundary point of R, relative to P, for all $\mathfrak{Z}$ in B. By Section **34**, the unimodular matrix $\mathfrak{U}_{\mathfrak{Z}}$ belongs then to a finite set, and we infer from (77), (100), (101), (103), that the expression $\mathfrak{p}'\mathfrak{S}\bar{\mathfrak{q}} + \bar{\mathfrak{p}}'\mathfrak{S}\mathfrak{q}$ has a constant value in H, where $\mathfrak{p} = \mathfrak{C}^{-1}\mathfrak{a}$ and $\mathfrak{q} = \mathfrak{C}^{-1}\mathfrak{b}$ with two columns $\mathfrak{a} \neq 0$ and $\mathfrak{b} \neq 0$ in K_0; moreover $\mathfrak{a} \neq \lambda\mathfrak{b}$ for every pure imaginary scalar factor λ. Replacing $\mathfrak{Y}$ by $\mathfrak{E} + \mathfrak{Y}$, we have the Taylor series

$$\mathfrak{S} = \mathfrak{E} + \mathfrak{S}_1 + \mathfrak{S}_2 + \cdots, \qquad \mathfrak{S}_1 = \begin{pmatrix} -\mathfrak{Y} & -\mathfrak{X} \\ -\mathfrak{X} & \mathfrak{Y} \end{pmatrix}, \qquad \mathfrak{S}_2 = \begin{pmatrix} \mathfrak{Y}^2 & \mathfrak{Y}\mathfrak{X} \\ \mathfrak{X}\mathfrak{Y} & \mathfrak{X}^2 \end{pmatrix},$$

in the neighborhood of $\mathfrak{Y} = 0$. It follows that the real part of $\mathfrak{p}'\mathfrak{S}_2\bar{\mathfrak{q}}$ vanishes identically in the real symmetric matrices $\mathfrak{X}$ and $\mathfrak{Y}$. Since $\mathfrak{a} = \mathfrak{C}\mathfrak{p}$, $\mathfrak{b} = \mathfrak{C}\mathfrak{q}$

and $\mathfrak{a} \neq \lambda \mathfrak{b}$, for all pure imaginary values of λ, we find easily $\mathfrak{a} = \omega \mathfrak{C} \mathfrak{r}$, $\mathfrak{b} = i\omega \mathfrak{C} \mathfrak{s}$ with real $\mathfrak{r}, \mathfrak{s}$ and complex scalar $\omega \neq 0$.

On the other hand $\mathfrak{S}[\mathfrak{C}] = \mathfrak{J}$, $\mathfrak{H}\{\mathfrak{C}\} = \sqrt{-s}\mathfrak{J}$, whence $\bar{\mathfrak{C}} = \sqrt{-s}\mathfrak{H}^{-1}\mathfrak{S}\mathfrak{C}$. We obtain, therefore,

$$\bar{\omega}\sqrt{-s}\mathfrak{H}^{-1}\mathfrak{S}\mathfrak{a} = \omega\bar{\mathfrak{a}}.$$

But $\mathfrak{S}, \mathfrak{H}$ and $\mathfrak{a} \neq 0$ are in $K_0 = K(\sqrt{-r})$, hence

$$\begin{gathered} \bar{\omega}\sqrt{-s} = \omega(\xi + \eta\sqrt{-r}) ; \\ s = \xi^2 + r\eta^2, \end{gathered} \tag{106}$$

where ξ, η are numbers in K. Since $r_\alpha > 0$, $s_\alpha < 0$ $(\alpha = 2, \cdots, h)$, the relationship (106) is only possible for $h = 1$; then K is the field of rational numbers.

It will be proved in Chapter IX, that $\Delta(\mathfrak{S}, \mathfrak{H})$ is commensurable with the modular group Γ, if and only if the diophantine equation (106) has a rational solution ξ, η. In this case, however, the construction and the properties of a fundamental domain for Δ follow in a simple way from the results of Chapter VI. Therefore we exclude this case for the rest of the present chapter.

For every point $\mathfrak{Z}_0$ of H, there exists now a unimodular matrix $\mathfrak{U}$ and a sequence of points $\mathfrak{Z}$ tending to $\mathfrak{Z}_0$, such that the corresponding points $\mathfrak{T}$ of T are inner points of $R_{\mathfrak{U}^{-1}}$, relative to P.

37. We denote by $F(\mathfrak{U}_0)$ the closure of the set of inner points of $G(\mathfrak{U}_0)$, relative to H. If $\mathfrak{Z}_0$ is a point of $G(\mathfrak{U}_0)$ which does not belong to $F(\mathfrak{U}_0)$, then we use the result of the last section to construct a sequence of points $\mathfrak{Z}$ tending to $\mathfrak{Z}_0$, such that they have as reduced images inner points of $G(\mathfrak{U})$, where $\mathfrak{U}$ is a certain matrix of the set V. Consequently $\mathfrak{Z}_0$ has a reduced image in $F(\mathfrak{U})$, and any point of H is equivalent under Δ to at least one point in one of the domains $F(\mathfrak{U}_0)$.

Let $\mathfrak{Z}^*$ be the image of $\mathfrak{Z}$ under the transformation $\mathfrak{M} = \mathfrak{C}^{-1}\mathfrak{W}\mathfrak{C}$ of Δ and let $\mathfrak{T}^*, \mathfrak{T}$ be the corresponding points in T. We assume now the existence of an inner point $\mathfrak{Z}$ of $F(\mathfrak{U}_0)$, such that $\mathfrak{Z}^*$ is a point of $F(\mathfrak{U}^*_0)$, where $\mathfrak{U}^*_0$ is also one of the matrices of the set V. By Section **36**, this holds then even under the further condition that $\mathfrak{T}\{\mathfrak{U}_0\}$ be an inner point of R, relative to P. But $\mathfrak{T}^*\{\mathfrak{U}^*_0\} = \mathfrak{T}\{\mathfrak{U}_0\}\{\mathfrak{U}_0^{-1}\mathfrak{W}^{-1}\mathfrak{U}^*_0\}$ is again a point of R, and consequently $\mathfrak{U}^*_0 = \pm\mathfrak{W}\mathfrak{U}_0$, $\mathfrak{S}[\mathfrak{U}^*_0] = \mathfrak{S}[\mathfrak{U}_0]$, $\mathfrak{H}\{\mathfrak{U}^*_0\} = \mathfrak{H}\{\mathfrak{U}_0\}$. Now it follows from the definition of V, that $\mathfrak{U}^*_0 = \mathfrak{U}_0$, $\mathfrak{W} = \pm\mathfrak{E}$. This proves that $F(\mathfrak{U}_0)$ and $F(\mathfrak{U}^*_0)$ do not overlap, if $\mathfrak{U}_0 \neq \mathfrak{U}^*_0$, and that the sum of the domains $F(\mathfrak{U}_0)$ is a fundamental domain F of Δ.

Obviously every $F(\mathfrak{U}_0)$ is bounded by a finite number of algebraic surfaces, and F has the same property. It follows immediately from Section **34**, that any compact domain in H is covered by a finite number of images $F_{\mathfrak{M}}$ of F under Δ and that F has only a finite number of neighbors $F_{\mathfrak{M}}$.

38. Let $\mathfrak{Z}$ be a point of $F(\mathfrak{U}_0)$ and $\mathfrak{S}$ the corresponding point of S. By (101) and (105),

$$\mathfrak{P} = s^{-1}\mathfrak{P}^{-1}\{\hat{\mathfrak{H}}'\{\bar{\mathfrak{Q}}^{-1}\}\}, \tag{107}$$

where

$$\begin{cases} \hat{\mathfrak{H}} = \mathfrak{H}\{\mathfrak{U}_0\mathfrak{L}\}, & \mathfrak{P}\{\mathfrak{Q}\} = \mathfrak{T}_1\{\mathfrak{U}_0\mathfrak{L}\} = \mathfrak{S}\{\mathfrak{C}^{-1}\mathfrak{U}_0\mathfrak{L}\} \\ \mathfrak{P} = [p_1, \cdots, p_{2n}], & 0 < p_k \leq \tau_4 p_{k+1} \qquad (k = 1, \cdots, 2n-1) \\ \mathfrak{Q} = (q_{kl}), \quad q_{kl} = 0 \ (k > l), & q_{kk} = 1, \quad \text{abs}\, q_{kl} \leq \tau_4 \quad (k < l). \end{cases} \tag{108}$$

Let d be the first diagonal element of $\hat{\mathfrak{H}}$. Then

$$p_1^2 \geq s^{-1}d^2 \tag{109}$$

and

$$\prod_{k=1}^{2n} p_k = (-s)^{-n} \mid \hat{\mathfrak{H}} \mid, \tag{110}$$

by (107).

We assume now $h > 1$, i. e., K is not the field of rational numbers. Then the conjugates of $\hat{\mathfrak{H}}$ in $K^{(\alpha)}(\sqrt{-r_\alpha})$ $(\alpha = 2, \cdots, h)$ are positive, and consequently $d \neq 0$. On the other hand, $\mathfrak{U}_0$ and $\mathfrak{L}$ belong to a finite set. It follows from (108), (109), (110), that $\mathfrak{S}$ is bounded for all $\mathfrak{Z}$ in the fundamental domain F. By (77), the matrices $\mathfrak{Y}^{-1}$, $\mathfrak{Y} + \mathfrak{Y}^{-1}[\mathfrak{X}]$, $\mathfrak{Y}^{-1}\mathfrak{X}$ are bounded, hence also $\mathfrak{Y}$, $\mid \mathfrak{Y} \mid^{-1}$, $\mathfrak{X}$. This proves that F is compact.

In the remaining case $h = 1$, F is not necessarily compact, and the proof of the convergence of the volume integral $V(\Delta)$ requires more detailed estimates. This proof may be given by the same method which leads to the analogous result in the theory of units of indefinite quadratic forms; we omit it here.

It is also not difficult to prove that the space H is compact relative to $\Delta(\mathfrak{G}, \mathfrak{H})$, in the case $h = 1$, if and only if $n = 1$ and Δ is not commensurable with the elliptic modular group, and then also F is compact.

39. The congruence subgroup $\Lambda_\kappa(\mathfrak{G}, \mathfrak{H})$ of $\Lambda(\mathfrak{G}, \mathfrak{H})$ consists of all elements of Λ satisfying $\mathfrak{W} \equiv \mathfrak{E} \pmod{\kappa}$, where κ is a given ideal in K_0. Let ρ be a prime ideal of K_0 and p the rational prime number which is divisible by ρ; let κ be a power of ρ, such that p is not divisible by κ^{p-1}. If the transformation with the matrix $\mathfrak{C}^{-1}\mathfrak{W}\mathfrak{C} \neq \pm \mathfrak{E}$ has a fixed point in H, then $\mathfrak{W}$ is of finite order, since Δ is discontinuous in H.

We shall prove that $\Lambda_\kappa(\mathfrak{G}, \mathfrak{H})$ contains no element of finite order except $\mathfrak{E}$. Otherwise we may assume

$$\mathfrak{W}^q = \mathfrak{E}, \quad \mathfrak{W} = \mathfrak{E} + \mathfrak{R}, \quad \mathfrak{R} \equiv 0 \pmod{\rho^a}, \quad \mathfrak{R} \not\equiv 0 \pmod{\rho^{a+1}},$$

where q is a rational prime number and ρ^a divisible by κ. Then

$$\sum_{l=1}^{q} \binom{q}{l} \mathfrak{R}^l = 0; \quad \mathfrak{R} \equiv -q^{-1}\mathfrak{R}^q \pmod{\rho^{2a}}.$$

Since

$$q^{-1}\mathfrak{R}^q \equiv 0 \pmod{\rho^{a+1}},$$

we arrive at a contradiction.

The proofs of Theorems 9 and 10 are finished.

VIII. THE VOLUME OF THE FUNDAMENTAL DOMAIN OF THE MODULAR GROUP.

40. In the interval $0 \leq x \leq 1$, we consider an arbitrary monotone function $f(x)$, such that

$$(111) \qquad f(1) = 0, \qquad \int_0^1 f(x)x^{n-1}dx = 1;$$

an example is $f(x) = n(n+1)(1-x)$. For $x \geq 1$, we put $f(x) = 0$. Let $\mathfrak{Z}$ be a point of H and $\mathfrak{S}$ the positive symmetric matrix defined in (77). For any $\epsilon > 0$, we define

$$(112) \qquad \phi(\epsilon, \mathfrak{Z}) = \epsilon^{2n} \sum_{\mathfrak{w} \neq 0} f(\mathfrak{S}[\epsilon\mathfrak{w}]),$$

where $\mathfrak{w}$ runs over all lattice points $\neq 0$; this is a finite sum.

LEMMA 12. *If ϵ tends to 0 through positive values and $\mathfrak{Z}$ is fixed, then*

$$\lim \phi(\epsilon, \mathfrak{Z}) = \frac{\pi^n}{(n-1)!}.$$

On account of the definition of the integral, we have

$$\lim_{\epsilon \to 0} \phi(\epsilon, \mathfrak{Z}) = \int_{\mathfrak{S}[\mathfrak{q}] \leq 1} f(\mathfrak{S}[\mathfrak{q}])\,d\mathfrak{q},$$

where $d\mathfrak{q}$ denotes the euclidean volume element in the space of the real vectors $\mathfrak{q}$ of $2n$ dimensions. Since the volume of the ellipsoid $\mathfrak{S}[\mathfrak{q}] \leq x$ is

$$J(x) = \frac{\pi^n}{n!} x^n \qquad (x \geq 0),$$

We shall prove that $\Lambda_\kappa(\mathfrak{G}, \mathfrak{H})$ contains no element of finite order except $\mathfrak{E}$. Otherwise we may assume

$$\mathfrak{W}^q = \mathfrak{E}, \quad \mathfrak{W} = \mathfrak{E} + \mathfrak{R}, \quad \mathfrak{R} \equiv 0 \ (\mathrm{mod}\ \rho^a), \quad \mathfrak{R} \not\equiv 0 \ (\mathrm{mod}\ \rho^{a+1}),$$

where q is a rational prime number and ρ^a divisible by κ. Then

$$\sum_{l=1}^{q} \binom{q}{l} \mathfrak{R}^l = 0; \quad \mathfrak{R} \equiv -q^{-1}\mathfrak{R}^q \ (\mathrm{mod}\ \rho^{2a}).$$

Since

$$q^{-1}\mathfrak{R}^q \equiv 0 \ (\mathrm{mod}\ \rho^{a+1}),$$

we arrive at a contradiction.

The proofs of Theorems 9 and 10 are finished.

VIII. THE VOLUME OF THE FUNDAMENTAL DOMAIN OF THE MODULAR GROUP.

40. In the interval $0 \leq x \leq 1$, we consider an arbitrary monotone function $f(x)$, such that

$$(111) \qquad f(1) = 0, \qquad \int_0^1 f(x) x^{n-1} dx = 1;$$

an example is $f(x) = n(n+1)(1-x)$. For $x \geq 1$, we put $f(x) = 0$. Let $\mathfrak{Z}$ be a point of H and $\mathfrak{S}$ the positive symmetric matrix defined in (77). For any $\epsilon > 0$, we define

$$(112) \qquad \phi(\epsilon, \mathfrak{Z}) = \epsilon^{2n} \sum_{\mathfrak{w} \neq 0} f(\mathfrak{S}[\epsilon \mathfrak{w}]),$$

where $\mathfrak{w}$ runs over all lattice points $\neq 0$; this is a finite sum.

LEMMA 12. *If ϵ tends to 0 through positive values and $\mathfrak{Z}$ is fixed, then*

$$\lim \phi(\epsilon, \mathfrak{Z}) = \frac{\pi^n}{(n-1)!}.$$

On account of the definition of the integral, we have

$$\lim_{\epsilon \to 0} \phi(\epsilon, \mathfrak{Z}) = \int_{\mathfrak{S}[\mathfrak{q}] \leq 1} f(\mathfrak{S}[\mathfrak{q}]) d\mathfrak{q},$$

where $d\mathfrak{q}$ denotes the euclidean volume element in the space of the real vectors $\mathfrak{q}$ of $2n$ dimensions. Since the volume of the ellipsoid $\mathfrak{S}[\mathfrak{q}] \leq x$ is

$$J(x) = \frac{\pi^n}{n!} x^n \qquad (x \geq 0),$$

we obtain

$$\int\limits_{\mathfrak{S}[\mathfrak{q}]\leq 1} f(\mathfrak{S}[\mathfrak{q}])\,d\mathfrak{q} = \int_0^1 f(x)\,\frac{dJ(x)}{dx}\,dx = \frac{\pi^n}{(n-1)!}\int_0^1 f(x)x^{n-1}dx = \frac{\pi^n}{(n-1)!}\,.$$

41. Let F be the fundamental domain of the modular group, in the space H of $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$, and denote by dv the euclidean volume element in the space of $\mathfrak{X}$ and $\mathfrak{Y}^{-1}$, of $n(n+1)$ dimensions.

LEMMA 13. *There exists an integrable positive function* $g(\mathfrak{Z})$ *of the elements of* $\mathfrak{Z}$, *independent of* ϵ, *such that*

(113) $$\phi(\epsilon, \mathfrak{Z}) \leq g(\mathfrak{Z}) \qquad (0 < \epsilon \leq 1)$$

and the integral

$$\gamma = \int\limits_F g(\mathfrak{Z})\,dv$$

converges.

We denote by $h(\rho, \mathfrak{Z})$ the number of lattice points $\mathfrak{w}$ satisfying $\mathfrak{S}[\mathfrak{w}] \leq \rho$, where ρ is an arbitrary positive number. By (78),

$$\mathfrak{S}[\mathfrak{w}] = \mathfrak{Y}^{-1}[\mathfrak{u} - \mathfrak{X}\mathfrak{v}] + \mathfrak{Y}[\mathfrak{v}], \qquad \mathfrak{w} = \begin{pmatrix}\mathfrak{u}\\ \mathfrak{v}\end{pmatrix},$$

and consequently $h(\rho, \mathfrak{Z})$ is not larger than the number of integral solutions $\mathfrak{u}, \mathfrak{v}$ of

(114) $$\mathfrak{Y}^{-1}[\mathfrak{u} - \mathfrak{X}\mathfrak{v}] \leq \rho, \qquad \mathfrak{Y}[\mathfrak{v}] \leq \rho.$$

Put $\mathfrak{Y}^{-1} = \mathfrak{P}[\mathfrak{Q}]$ with $\mathfrak{P} = [p_1, \cdots, p_n]$ and $\mathfrak{Q} = (q_{kl})$, $q_{kl} = 0$ $(k > l)$, $q_{kk} = 1$, and let u_k, v_k, r_k $(k = 1, \cdots, n)$ denote the elements of the columns $\mathfrak{u}, \mathfrak{v}, \mathfrak{r} = \mathfrak{X}\mathfrak{v}$. The first condition (114) involves

$$p_k\{(u_k - r_k) + \sum_{l=k+1}^{n} q_{kl}(u_l - r_l)\}^2 \leq \rho \qquad (k = 1, \cdots, n);$$

this proves that the number of integral $\mathfrak{u}$ is

$$\leq \prod_{k=1}^{n} (1 + 2p_k^{-\frac{1}{2}}\rho^{\frac{1}{2}}),$$

for any given $\mathfrak{v}$. On the other hand, the second condition (114) involves

$$p_k^{-1}(v_k + \sum_{l=1}^{k-1} q^*_{kl}v_l)^2 \leq \rho,$$

where $(q^*_{kl}) = \mathfrak{Q}^{-1}$; this proves that the number of integral $\mathfrak{v}$ is

$$\leq \prod_{k=1}^{n} (1 + 2p_k^{\frac{1}{2}}\rho^{\frac{1}{2}}).$$

It follows that

$$h(\rho, \mathfrak{Z}) \leq \prod_{k=1}^{n} (1 + 2\rho^{\frac{1}{2}}(p_k^{\frac{1}{2}} + p_k^{-\frac{1}{2}}) + 4\rho).$$

Let $\gamma_1, \cdots, \gamma_4$ denote positive numbers which depend only upon n. By (93) and (94), we have $p_k < \gamma_1$ $(k = 1, \cdots, n)$, for all $\mathfrak{Z}$ in F; hence

$$h(\rho, \mathfrak{Z}) < \gamma_2(1 + \rho)^n \prod_{k=1}^{n} p_k^{-\frac{1}{2}}. \tag{115}$$

Now $0 \leq f(x) \leq f(0)$ $(0 \leq x \leq 1)$ and $f(x) = 0$ $(x \geq 1)$; consequently we infer from the definition (112) that

$$\phi(\epsilon, \mathfrak{Z}) \leq \epsilon^{2n} f(0) h(\epsilon^{-2}, \mathfrak{Z}). \tag{116}$$

By (115) and (116),

$$\phi(\epsilon, \mathfrak{Z}) < f(0)\gamma_2(1 + \epsilon^2)^n \prod_{k=1}^{n} p_k^{-\frac{1}{2}} < f(0)\gamma_3 \prod_{k=1}^{n} p_k^{-\frac{1}{2}} \qquad (0 < \epsilon \leq 1).$$

We define

$$g(\mathfrak{Z}) = f(0)\gamma_3 \prod_{k=1}^{n} p_k^{-\frac{1}{2}};$$

then (113) is fulfilled and it remains only to prove the convergence of the integral

$$\gamma_4 = \int_F \prod_{k=1}^{n} p_k^{-\frac{1}{2}} dv.$$

Instead of the elements Y_{kl} $(k \leq l)$ of $(Y_{kl}) = \mathfrak{Y}^{-1} = \mathfrak{P}[\mathfrak{Q}]$, we introduce the new variables $p_k^{\frac{1}{2}}$ $(k = 1, \cdots, n)$ and q_{kl} $(k < l)$. The functional determinant has the value

$$2^n \prod_{k=1}^{n} p_k^{n-k+\frac{1}{2}},$$

whence

$$\gamma_4 = 2^n \int_F \prod_{k=1}^{n} p_k^{n-k} dv_1$$

with

$$dv_1 = \prod_{k \leq l} dx_{kl} \prod_{k < l} dq_{kl} \prod_{k} dp_k^{\frac{1}{2}}.$$

Since $\mathfrak{X}$, $\mathfrak{P}$, $\mathfrak{Q}$ are bounded in F, the convergence is obvious.

Applying a well-known theorem of integral calculus, we obtain from Lemmata 12 and 13 the important

LEMMA 14. *The integral*

$$\psi(\epsilon) = \int_F \phi(\epsilon, \mathfrak{Z}) dv = \epsilon^{2n} \sum_{\mathfrak{w} \neq 0} \int_F f(\mathfrak{S}[\epsilon\mathfrak{w}]) dv$$

converges and

$$\lim_{\epsilon\to 0}\psi(\epsilon)=\frac{\pi^n}{(n-1)\,!}\int_F dv=\frac{\pi^n}{(n-1)\,!}V_n$$

where $V_n=V(\Gamma_n)$ *is the symplectic volume of the fundamental domain for the modular group* $\Gamma=\Gamma_n$ *of degree* n.

42. We denote by W the set of all columns $\mathfrak{w}^{(2n)}$ with coprime integral elements and by $\mathfrak{e}$ the first column of the unit matrix $\mathfrak{E}^{(2n)}$; obviously $\mathfrak{e}$ belongs to W.

LEMMA 15. *There exists a modular matrix* $\mathfrak{M}$ *with the first column* $\mathfrak{w}$, *if and only if* $\mathfrak{w}$ *belongs to* W.

The necessity of the condition is obvious, since $\mathfrak{M}$ has integral elements and the determinant 1. Therefore we have only to prove the existence of a modular matrix $\mathfrak{M}$ satisfying $\mathfrak{M}^{-1}\mathfrak{w}=\mathfrak{e}$, where $\mathfrak{w}$ is a given column of the set W.

Consider the column

$$\mathfrak{M}^{-1}\mathfrak{w}=\mathfrak{w}_1=\begin{pmatrix}\mathfrak{u}^{(n)}\\ \mathfrak{v}^{(n)}\end{pmatrix},$$

where $\mathfrak{M}$ is an arbitrary modular matrix, and let u, v denote the greatest common divisors of the n elements of $\mathfrak{u}, \mathfrak{v}$; we define $u=0$ or $v=0$ if $\mathfrak{u}=0$ or $\mathfrak{v}=0$. We choose now the matrix $\mathfrak{M}$, such that the sum $u+v=w$ is as small as possible. If $u<v$, we replace $\mathfrak{M}, \mathfrak{u}, \mathfrak{v}$ by $\mathfrak{M}\mathfrak{J}, -\mathfrak{v}, \mathfrak{u}$ and obtain the case $u>v$, with the same value of w; hence we may assume $u\geq v$.

If $v>0$, we determine a unimodular matrix $\mathfrak{U}$ with the first row $v^{-1}\mathfrak{v}'$ and an integral column $\mathfrak{t}$, such that all elements of the column $\mathfrak{U}\mathfrak{u}-v\mathfrak{t}=\mathfrak{u}_1$ have an absolute value $\leq(v/2)$; then the greatest common divisor u_1 of these elements satisfies $u_1\leq(v/2)<u$. Let $\mathfrak{T}$ be an integral symmetric matrix having $\mathfrak{t}$ as its first column and

$$\mathfrak{M}_1=\begin{pmatrix}\mathfrak{U}^{-1} & \mathfrak{U}^{-1}\mathfrak{T}\\ 0 & \mathfrak{U}'\end{pmatrix}.$$

Since $\mathfrak{U}'^{-1}\mathfrak{v}=v\mathfrak{e}_1$ and $\mathfrak{T}\mathfrak{U}'^{-1}\mathfrak{v}=v\mathfrak{t}$, where $\mathfrak{e}_1$ denotes the first column of the unit matrix $\mathfrak{E}^{(n)}$, we find

$$(\mathfrak{M}\mathfrak{M}_1)^{-1}\mathfrak{w}=\mathfrak{M}_1{}^{-1}\mathfrak{w}_1=\begin{pmatrix}\mathfrak{u}_1\\ v\mathfrak{e}_1\end{pmatrix}.$$

But $\mathfrak{M}_1$ and $\mathfrak{M}\mathfrak{M}_1$ are again modular matrices and $u_1+v<w$, in contradiction to the minimum property of w.

Consequently $v = 0$ and $u = 1$, the elements of $\mathfrak{w}_1$ being coprime. Let $\mathfrak{U}_1$ be a unimodular matrix with the first row $\mathfrak{u}'$ and

$$\mathfrak{M}_2 = \begin{pmatrix} \mathfrak{U}'_1 & 0 \\ 0 & \mathfrak{U}_1^{-1} \end{pmatrix}.$$

Then $(\mathfrak{M}\mathfrak{M}_2)^{-1}\mathfrak{w} = \mathfrak{e}$ and $\mathfrak{M}\mathfrak{M}_2$ is unimodular, q. e. d.

We denote by Δ_1 the subgroup of Γ consisting of all modular matrices $\mathfrak{M}$ with the first column $\mathfrak{e}$. Obviously two arbitrary modular matrices are then and only then in the same left coset of Δ_1 relative to the homogeneous modular group Γ_0, if they have the same first column. Applying Lemma 15, we find the decomposition

$$\Gamma_0 = \sum_{\mathfrak{w} \subset W} \mathfrak{M}_{\mathfrak{w}} \Delta_1 = \sum_{\mathfrak{w} \subset W} \Delta_1 \mathfrak{M}_{\mathfrak{w}}^{-1},$$

where $\mathfrak{w}$ runs over all elements of the set W and $\mathfrak{M}_{\mathfrak{w}}$ denotes a modular matrix with the first column $\mathfrak{w}$. We choose $\mathfrak{M}_{-\mathfrak{w}} = -\mathfrak{M}_{\mathfrak{w}}$, such that $\mathfrak{M}_{\mathfrak{w}}$ and $\mathfrak{M}_{-\mathfrak{w}}$ give the same element of Γ. Let $F_{\mathfrak{w}}$ be the image of F under the transformation $\mathfrak{M}_{\mathfrak{w}}^{-1}$; then the domains $F_{\mathfrak{w}}$ cover exactly twice a fundamental domain F_0 of the group Δ_1. On the other hand

$$\int_F f(\mathfrak{S}[\epsilon\mathfrak{w}])\,dv = \int_{F_{\mathfrak{w}}} f(\mathfrak{S}[\epsilon\mathfrak{e}]\,dv,$$

by Lemma 6. Using the abbreviation $p = \mathfrak{S}[\mathfrak{e}]$ for the first diagonal element of $\mathfrak{S}$, we obtain

$$\sum_{\mathfrak{w} \subset W} \int_F f(\mathfrak{S}[\epsilon\mathfrak{w}])\,dv = 2 \int_{F_0} f(\epsilon^2 p)\,dv.$$

Now we replace ϵ by ϵl and sum over all positive integers l; then $l\mathfrak{w}$ runs exactly over all lattice points $\neq 0$, and we have

$$\psi(\epsilon) = 2\epsilon^{2n} \sum_{l=1}^{\infty} \int_{F_0} f(\epsilon^2 l^2 p)\,dv, \tag{117}$$

where $\psi(\epsilon)$ is the function defined in Lemma 14.

43. Any element of Δ_1 has the form

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}, \quad \mathfrak{A} = \begin{pmatrix} 1 & * \\ 0 & \mathfrak{A}_1 \end{pmatrix}, \quad \mathfrak{B} = \begin{pmatrix} * & * \\ * & \mathfrak{B}_1 \end{pmatrix}, \tag{118}$$
$$\mathfrak{C} = \begin{pmatrix} 0 & * \\ 0 & \mathfrak{C}_1 \end{pmatrix}, \quad \mathfrak{D} = \begin{pmatrix} * & * \\ * & \mathfrak{D}_1 \end{pmatrix}.$$

It follows from (7) that also

$$\mathfrak{A}_1\mathfrak{B}'_1 = \mathfrak{B}_1\mathfrak{A}'_1, \quad \mathfrak{C}_1\mathfrak{D}'_1 = \mathfrak{D}_1\mathfrak{C}'_1, \quad \mathfrak{A}_1\mathfrak{D}'_1 - \mathfrak{B}_1\mathfrak{C}'_1 = \mathfrak{E};$$

hence

$$\mathfrak{M}_1 = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{C}_1 & \mathfrak{D}_1 \end{pmatrix}$$

belongs to the homogeneous modular group of degree $n-1$. We define

$$\mathfrak{A}_2 = \begin{pmatrix} 1 & 0 \\ 0 & \mathfrak{A}_1 \end{pmatrix}, \quad \mathfrak{B}_2 = \begin{pmatrix} 0 & 0 \\ 0 & \mathfrak{B}_1 \end{pmatrix}, \quad \mathfrak{C}_2 = \begin{pmatrix} 0 & 0 \\ 0 & \mathfrak{C}_1 \end{pmatrix},$$

$$\mathfrak{D}_2 = \begin{pmatrix} 1 & 0 \\ 0 & \mathfrak{D}_1 \end{pmatrix}, \quad \mathfrak{M}_2 = \begin{pmatrix} \mathfrak{A}_2 & \mathfrak{B}_2 \\ \mathfrak{C}_2 & \mathfrak{D}_2 \end{pmatrix},$$

$$\mathfrak{M}_0 = \mathfrak{M}\mathfrak{M}_2^{-1} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix} \begin{pmatrix} \mathfrak{D}'_2 & -\mathfrak{B}'_2 \\ -\mathfrak{C}'_2 & \mathfrak{A}'_2 \end{pmatrix} = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_0 \\ \mathfrak{C}_0 & \mathfrak{D}_0 \end{pmatrix},$$

where

$$\mathfrak{A}_0 = \begin{pmatrix} 1 & * \\ 0 & \mathfrak{E} \end{pmatrix}, \quad \mathfrak{B}_0 = \begin{pmatrix} * & * \\ * & 0 \end{pmatrix}, \quad \mathfrak{C}_0 = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}, \quad \mathfrak{D}_0 = \begin{pmatrix} * & * \\ * & \mathfrak{E} \end{pmatrix}.$$

Since $\mathfrak{M}_0$ is symplectic, we have $\mathfrak{C}_0\mathfrak{D}'_0 = \mathfrak{D}_0\mathfrak{C}'_0$, whence $\mathfrak{C}_0 = 0$; moreover $\mathfrak{A}_0\mathfrak{D}'_0 = \mathfrak{E}$ and $\mathfrak{A}_0\mathfrak{B}'_0 = \mathfrak{B}_0\mathfrak{A}'_0$ so that $\mathfrak{A}_0 = \mathfrak{U}'$, $\mathfrak{D}_0 = \mathfrak{U}^{-1}$, $\mathfrak{B}_0 = \mathfrak{T}\mathfrak{U}^{-1}$ with

(119) $$\mathfrak{U} = \begin{pmatrix} 1 & 0 \\ \mathfrak{a} & \mathfrak{E} \end{pmatrix}, \quad \mathfrak{T} = \begin{pmatrix} b & \mathfrak{b}' \\ \mathfrak{b} & 0 \end{pmatrix}$$

and integral $\mathfrak{a}, \mathfrak{b}, b$.

On the other hand, if $\mathfrak{U}$ and $\mathfrak{T}$ are defined by (119) with arbitrary integral $\mathfrak{a}, \mathfrak{b}, b$, then

(120) $$\mathfrak{M}_0 = \begin{pmatrix} \mathfrak{U}' & \mathfrak{T}\mathfrak{U}^{-1} \\ 0 & \mathfrak{U}^{-1} \end{pmatrix}$$

is a modular matrix and $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_2$ has again the form (118). It is obvious that the matrices $\mathfrak{M}_2$ constitute a group Δ_2 which is isomorphic to the homogeneous modular group of degree $n-1$ and is a subgroup of Δ_1. The left cosets of Δ_2 relative to Δ_1 are of the form $\mathfrak{M}_0\Delta_2$, where $\mathfrak{M}_0$ runs over all matrices defined by (119) and (120).

This result enables us to construct another fundamental domain of Δ_1. Let $\hat{\mathfrak{Z}} = (\mathfrak{A}_2\mathfrak{Z} + \mathfrak{B}_2)(\mathfrak{C}_2\mathfrak{Z} + \mathfrak{D}_2)^{-1}$ be the modular transformation with the matrix $\mathfrak{M}_2$. We decompose

$$\mathfrak{Z} = \begin{pmatrix} * & * \\ * & \mathfrak{Z}_1 \end{pmatrix}, \quad \hat{\mathfrak{Z}} = \begin{pmatrix} * & * \\ * & \hat{\mathfrak{Z}}_1 \end{pmatrix}$$

and obtain

$$\mathfrak{A}_2\mathfrak{Z} + \mathfrak{B}_2 = \begin{pmatrix} * & * \\ * & \mathfrak{A}_1\mathfrak{Z}_1 + \mathfrak{B}_1 \end{pmatrix}, \quad \mathfrak{C}_2\mathfrak{Z} + \mathfrak{D}_2 = \begin{pmatrix} 1 & 0 \\ * & \mathfrak{C}_1\mathfrak{Z}_1 + \mathfrak{D}_1 \end{pmatrix},$$

$$(\mathfrak{C}_2\mathfrak{Z} + \mathfrak{D}_2)^{-1} = \begin{pmatrix} 1 & 0 \\ * & (\mathfrak{C}_1\mathfrak{Z}_1 + \mathfrak{D}_1)^{-1} \end{pmatrix};$$

consequently $\hat{\mathfrak{Z}}_1 = (\mathfrak{A}_1\mathfrak{Z}_1 + \mathfrak{B}_1)(\mathfrak{C}_1\mathfrak{Z}_1 + \mathfrak{D}_1)^{-1}$ is the image of $\mathfrak{Z}_1$ under the modular transformation with the matrix $\mathfrak{M}_1$, of degree $n-1$. For any $\mathfrak{Z}$ in H, we determine $\mathfrak{M}_1$, such that $\hat{\mathfrak{Z}}_1$ lies in the fundamental domain F_1 of the modular group of degree $n-1$. Since we may replace $\mathfrak{M}_1$ by $-\mathfrak{M}_1$, there are always two different possibilities for the choice of the corresponding element $\mathfrak{M}_2$ of Δ_2.

We replace $\hat{\mathfrak{Z}}$ again by $\mathfrak{Z}$ and consider now the modular transformation $\hat{\mathfrak{Z}} = \mathfrak{Z}[\mathfrak{U}] + \mathfrak{T}$ with the matrix $\mathfrak{M}_0$. By (119),

$$\hat{\mathfrak{Z}}_1 = \mathfrak{Z}_1, \quad \hat{\mathfrak{Y}}^{-1} = \mathfrak{Y}^{-1}\begin{bmatrix} 1 & -\mathfrak{a}' \\ 0 & \mathfrak{E} \end{bmatrix}, \quad \hat{\mathfrak{X}} = \mathfrak{X}\begin{bmatrix} 1 & 0 \\ \mathfrak{a} & \mathfrak{E} \end{bmatrix} + \begin{pmatrix} b & \mathfrak{b}' \\ \mathfrak{b} & 0 \end{pmatrix},$$

where $\hat{\mathfrak{X}} + i\hat{\mathfrak{Y}} = \hat{\mathfrak{Z}}$. On account of the definition (77), the matrices $\mathfrak{Y}^{-1}$ and $\mathfrak{S}$ have the same first diagonal element p. Putting $\mathfrak{Y}^{-1} = (Y_{kl})$ and $\hat{\mathfrak{Y}}^{-1} = (\hat{Y}_{kl})$, we obtain $\hat{Y}_{1l} = Y_{1l} - pa_l$ $(l = 2, \cdots, n)$, where $a_2, \cdots, a_n$ denote the elements of $\mathfrak{a}$. We determine first $\mathfrak{a}$, such that $-(p/2) \leq \hat{Y}_{1l} \leq p/2$ $(l = 2, \cdots, n)$, and then $b, \mathfrak{b}$, such that the elements $\hat{x}_{1l}$ of the first row of $\hat{\mathfrak{X}}$ satisfy $-\frac{1}{2} \leq \hat{x}_{1l} \leq \frac{1}{2}$ $(l = 1, \cdots, n)$.

It follows that any point of H has, relative to Δ_1, an equivalent point in the domain defined by the conditions

$$\text{(121)} \qquad \begin{array}{lll} \mathfrak{Z}_1 \subset F_1, & -(p/2) \leq Y_{1l} \leq p/2 & (l = 2, \cdots, n), \\ & -\frac{1}{2} \leq x_{1l} \leq \frac{1}{2} & (l = 1, \cdots, n). \end{array}$$

On account of the ambiguity in the choice of $\mathfrak{M}_2$, this domain is not yet a fundamental domain of Δ_1. It is transformed into itself by the particular mapping $z_{1l} \to -z_{1l}$ $(l = 2, \cdots, n)$, $z_{11} \to z_{11}$, $\mathfrak{Z}_1 \to \mathfrak{Z}_1$, obtained from $\mathfrak{M}_1 = -\mathfrak{E}$, $\mathfrak{M}_0 = \mathfrak{E}$. By the additional condition

$$\text{(122)} \qquad Y_{12} \geq 0$$

together with (121), we obtain now a fundamental domain F^* of Δ_1.

In the special case $n = 1$, the condition (122) does not exist, and (121) reduces to $-\frac{1}{2} \leq x_{11} \leq \frac{1}{2}$.

44. By Lemma 6, the first element p of $\mathfrak{S}$ is invariant under all transformations of the group Δ_1. Since F_0 and F^* are both fundamental domains of Δ_1, we obtain

$$\text{(123)} \qquad \int_{F_0} f(\epsilon^2 l^2 p)\, dv = \int_{F^*} f(\epsilon^2 l^2 p)\, dv.$$

We use now the decomposition

$$\mathfrak{Y}^{-1} = \begin{pmatrix} p^{-1} & 0 \\ 0 & \mathfrak{Y}_1^{-1} \end{pmatrix}\begin{bmatrix} p & \mathfrak{y}' \\ 0 & \mathfrak{E} \end{bmatrix} = \begin{pmatrix} p & \mathfrak{y}' \\ \mathfrak{y} & \mathfrak{Y}_0 \end{pmatrix},$$

where

$$\mathfrak{Y}_1^{-1} = \mathfrak{Y}_0 - p^{-1}\mathfrak{y}\mathfrak{y}' \tag{124}$$

and $\mathfrak{Y}_1$ denotes the imaginary part of $\mathfrak{Z}_1$. Introducing as new variables the elements η_{kl} $(1 \leq k \leq l \leq n-1)$ of $\mathfrak{Y}_1^{-1} = (\eta_{kl})$ instead of the elements Y_{kl} $(2 \leq k \leq l \leq n)$ of $\mathfrak{Y}_0$, we obtain, by (124),

$$\begin{aligned} dv &= \prod_{1 \leq k \leq l \leq n} (dx_{kl}dY_{kl}) \\ &= \prod_{2 \leq k \leq l \leq n} (dx_{kl}d\eta_{kl}) \prod_{l=1}^{n} (dx_{1l}dY_{1l}) = dv_1 \prod_{l=1}^{n} (dx_{1l}dY_{1l}), \end{aligned} \tag{125}$$

where dv_1 is the symplectic volume element for $\mathfrak{Z}_1$ instead of $\mathfrak{Z}$; moreover $Y_{11} = p$.

Define $\eta_n = 1$ for $n = 1$ and $= 2$ for $n > 1$. By (111), (121), (122) and (125),

$$\begin{aligned} \eta_n \int_{F^*} f(\epsilon^2 l^2 p)\,dv &= V_{n-1} \int_0^\infty p^{n-1} f(\epsilon^2 l^2 p)\,dp \\ &= V_{n-1}(\epsilon l)^{-2n} \int_0^1 x^{n-1} f(x)\,dx = V_{n-1}(\epsilon l)^{-2n}, \end{aligned} \tag{126}$$

where V_{n-1} is the volume $V(\Gamma_{n-1})$ of the fundamental domain F_1 for the modular group of degree $n-1$ and $V_0 = 1$. By (117), (123) and (126),

$$\psi(\epsilon) = 2\eta_n^{-1} V_{n-1} \zeta(2n),$$

independent of ϵ. Lemma 14 leads now to the recursion formula

$$V_n = 2\eta_n^{-1}(n-1)!\,\pi^{-n}\zeta(2n)\,V_{n-1},$$

whence

$$V_n = 2\prod_{k=1}^{n} \{(k-1)!\,\pi^{-k}\zeta(2k)\}, \tag{127}$$

and Theorem 11 is proved.

45. By a well-known result of Euler,

$$2(2\pi)^{-2k}\zeta(2k) = \frac{B_{2k}}{(2k)!} \qquad (k = 1, 2, \cdots),$$

where B_{2k} is the absolute value of the Bernoulli numbers

$$B_2 = \frac{1}{6}, \quad -B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad -B_8 = -\frac{1}{30}, \cdots.$$

Thus we obtain the expression

$$V_n = 2^{n^2+1}\pi^{n(n+1)/2} \prod_{k=1}^{n} \left\{ \frac{(k-1)!}{(2k)!} B_{2k} \right\}$$

and in particular

$$V_1 = \frac{\pi}{3}, \quad V_2 = \frac{\pi^3}{270}, \quad V_3 = \frac{\pi^6}{127575}, \quad V_4 = \frac{\pi^{10}}{200930625}.$$

Consider now the congruence subgroup $\Gamma_n(p)$ of the modular group of degree n, defined by $\mathfrak{M} \equiv \mathfrak{E} \pmod{p}$, where p is a prime number. Its index has the value

$$(128) \qquad j_n(p) = \prod_{k=1}^{n} p^{2k-1}(p^{2k} - 1).$$

For $p \neq 2$, this group has no fixed point in H, by Theorem 10. *If* Theorem 5 still holds good for the non-compact fundamental domain of $\Gamma_n(p)$, then this open manifold has the Euler number

$$\chi = c_n(-\pi)^{-n(n+1)/2} V_n j_n(p).$$

We denote by $\chi_n(p)$ the right-hand side of this hypothetic formula. Using the values of c_1, c_2, c_3 given in Theorem 5, we find

$$c_1 V_1 = -\frac{\pi}{3!}, \qquad c_2 V_2 = -\frac{\pi^3}{6!}, \qquad c_3 V_3 = \frac{\pi^6}{2 \cdot 9!}$$

and consequently

$$\chi_1(p) = -\frac{1}{6} p(p^2 - 1), \quad \chi_2(p) = -\frac{1}{720} p^4(p^2 - 1)(p^4 - 1),$$
$$\chi_3(p) = \frac{1}{2 \cdot 9!} p^9(p^2 - 1)(p^4 - 1)(p^6 - 1).$$

It is easily proved that these rational numbers are integers for all prime numbers p; in particular $\chi_1(2) = -1$, $\chi_2(2) = -1$, $\chi_3(2) = 2$.

46. Let $q = p^a$ $(a \geq 1)$ be a power of a prime number p. For any integral skew-symmetric matrix $\mathfrak{S}^{(2n)}$, we denote by $A_q(\mathfrak{S})$ the number of integral solutions $\mathfrak{L}$, modulo q, of the congruence

$$(129) \qquad \mathfrak{J}[\mathfrak{L}] \equiv \mathfrak{S} \pmod{q}.$$

In particular, $A_q(\mathfrak{J}) = E_q$ is the order of the homogeneous modular group modulo q, namely the number of incongruent solutions $\mathfrak{M}$ of

$$(130) \qquad \mathfrak{J}[\mathfrak{M}] \equiv \mathfrak{J} \pmod{q}.$$

It is known that $E_p = j_n(p)$ has the value (128), and more generally

$$E_q = q^{n(2n+1)} \prod_{k=1}^{n} (1 - p^{-2k}).$$

By (129) and (130), $\mathfrak{M}\mathfrak{L}$ is also a solution of (129); we call it equivalent to $\mathfrak{L}$, relative to the group of the $\mathfrak{M}$. Since there are exactly E_q matrices in each class of equivalent solutions, the number of different classes of solutions of (129) is $A_q(\mathfrak{S})/E_q$. On the other hand, the number of incongruent skew-symmetric matrices $\mathfrak{S}$ is $q^{n(2n-1)}$, and

$$\sum_{\mathfrak{S}} A_q(\mathfrak{S}) = q^{4n^2}$$

is the number of incongruent $\mathfrak{L}$. The average number of classes of solutions is therefore

$$(131) \qquad q^{-n(2n-1)} \sum_{\mathfrak{S}} \frac{A_q(\mathfrak{S})}{E_q} = \prod_{k=1}^{n} (1 - p^{-2k})^{-1} = d_p,$$

independent of the exponent a.

By Euler's formula

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}; \qquad (s > 1),$$

the result (127) may be written

$$d_0 = \prod_p d_p,$$

where p runs over all prime numbers and

$$(132) \qquad d_0 = \tfrac{1}{2} V_n \prod_{k=1}^{n} \frac{\pi^k}{(k-1)!}.$$

Now the main formula in the analytic theory of quadratic forms suggests that d_0 can be defined independently as a density connected with the real solutions $\mathfrak{L}$ of the equation $\mathfrak{J}[\mathfrak{L}] = \mathfrak{S}$. We shall prove that d_0 has the value defined in (4); this is the statement of Theorem 12.

47. Let

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1 & \mathfrak{S}_2 \\ -\mathfrak{S}'_2 & \mathfrak{S}_3 \end{pmatrix}$$

be a real skew-symmetric matrix and

$$(133) \qquad \mathfrak{F} = \begin{pmatrix} \mathfrak{E} & \mathfrak{E} \\ -i\mathfrak{E} & i\mathfrak{E} \end{pmatrix}, \qquad \frac{1}{2i}\mathfrak{S}\{\mathfrak{F}\} = \begin{pmatrix} \mathfrak{H}_1 & -\bar{\mathfrak{A}} \\ \mathfrak{A} & -\bar{\mathfrak{H}}_1 \end{pmatrix} = \mathfrak{K}_1;$$

then $\mathfrak{H}_1 = \frac{1}{2}(\mathfrak{S}_2 + \mathfrak{S}'_2) + \frac{1}{2i}(\mathfrak{S}_1 + \mathfrak{S}_3)$ is hermitian and $\mathfrak{A} = \frac{1}{2}(\mathfrak{S}_2 - \mathfrak{S}'_2) + \frac{1}{2i}(\mathfrak{S}_1 - \mathfrak{S}_3)$ is complex skew-symmetric. For $\mathfrak{S} = \mathfrak{J}$, we have $\mathfrak{H}_1 = \mathfrak{E}$ and $\mathfrak{A} = 0$. We choose a neighborhood G of $\mathfrak{S} = \mathfrak{J}$, such that $|\mathfrak{H}_1| \neq 0$ and that the characteristic roots $b_1, \cdots, b_m$ of the matrix

$$(134) \qquad \mathfrak{B} = -\bar{\mathfrak{A}}\bar{\mathfrak{H}}_1^{-1}\mathfrak{A}\mathfrak{H}_1^{-1}$$

are of absolute value < 1, for all $\mathfrak{S} \subset G$.

The series

$$(135) \qquad \mathfrak{W} = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} \mathfrak{B}^k$$

converges and satisfies the equation

$$\mathfrak{W}^2 = \mathfrak{E} + \mathfrak{B}.$$

The characteristic roots of the matrix $\mathfrak{E} + \mathfrak{W}$ are $1 + (1 + b_\kappa)^{\frac{1}{2}} \neq 0$ $(k = 1, \cdots, n)$. We define

$$(136) \qquad \mathfrak{H} = \tfrac{1}{2}(\mathfrak{E} + \mathfrak{W})\mathfrak{H}_1;$$

then $|\mathfrak{H}| \neq 0$ and $|2\mathfrak{H} - \mathfrak{H}_1| \neq 0$.

LEMMA 16. *The matrix* $\mathfrak{H}$ *is hermitian and*

$$(137) \qquad \mathfrak{H} + \tfrac{1}{4}\bar{\mathfrak{A}}\bar{\mathfrak{H}}^{-1}\mathfrak{A} = \mathfrak{H}_1.$$

We have

$$\mathfrak{B}\bar{\mathfrak{A}} = -\bar{\mathfrak{A}}\bar{\mathfrak{H}}_1{}^{-1}\mathfrak{A}\mathfrak{H}_1{}^{-1}\bar{\mathfrak{A}} = \bar{\mathfrak{A}}\bar{\mathfrak{B}}' \quad \text{and} \quad \mathfrak{B}\mathfrak{H}_1 = -\bar{\mathfrak{A}}\bar{\mathfrak{H}}_1{}^{-1}\mathfrak{A} = \mathfrak{H}_1\bar{\mathfrak{B}}',$$

whence

$$\bar{\mathfrak{H}}' = \tfrac{1}{2}\mathfrak{H}_1(\mathfrak{E} + \bar{\mathfrak{W}}') = \tfrac{1}{2}(\mathfrak{E} + \mathfrak{W})\mathfrak{H}_1 = \mathfrak{H}$$

and

$$\begin{aligned} \tfrac{1}{2}\bar{\mathfrak{A}}\bar{\mathfrak{H}}^{-1}\mathfrak{A} = \bar{\mathfrak{A}}(\mathfrak{E} + \bar{\mathfrak{W}}')\bar{\mathfrak{H}}_1{}^{-1}\mathfrak{A} &= -(\mathfrak{E} + \mathfrak{W})^{-1}\mathfrak{B}\mathfrak{H}_1 \\ &= (\mathfrak{E} - \mathfrak{W})\mathfrak{H}_1 = 2\mathfrak{H}_1 - 2\mathfrak{H}, \end{aligned}$$

q. e. d.

We define now

$$\mathfrak{K} = \begin{pmatrix} \mathfrak{H} & 0 \\ 0 & -\bar{\mathfrak{H}} \end{pmatrix}, \qquad \mathfrak{C} = \begin{pmatrix} \mathfrak{E} & -\frac{1}{2}\bar{\mathfrak{H}}^{-1}\mathfrak{A} \\ -\frac{1}{2}\mathfrak{H}^{-1}\bar{\mathfrak{A}} & \mathfrak{E} \end{pmatrix}$$

and obtain, by (133) and (137), $\mathfrak{K}\{\mathfrak{C}\} = \mathfrak{K}_1$ and

$$\mathfrak{C}\begin{pmatrix} \mathfrak{E} & \frac{1}{2}\bar{\mathfrak{H}}^{-1}\mathfrak{A} \\ \frac{1}{2}\mathfrak{H}^{-1}\bar{\mathfrak{A}} & \mathfrak{E} \end{pmatrix} = \begin{pmatrix} 2\mathfrak{E} - \bar{\mathfrak{H}}^{-1}\bar{\mathfrak{H}}_1 & 0 \\ 0 & 2\mathfrak{E} - \mathfrak{H}^{-1}\mathfrak{H}_1 \end{pmatrix},$$

whence in particular $|\mathfrak{C}| \neq 0$.

48. We consider now the set L of real matrices $\mathfrak{L}$ satisfying $\mathfrak{J}[\mathfrak{L}] = \mathfrak{G} \subset G$. Putting

$$(138) \qquad \mathfrak{L}\mathfrak{F} = \mathfrak{V}_1 = \begin{pmatrix} \mathfrak{P}_1 & \bar{\mathfrak{P}}_1 \\ \mathfrak{Q}_1 & \bar{\mathfrak{Q}}_1 \end{pmatrix}, \qquad \mathfrak{V}_1\mathfrak{C}^{-1} = \begin{pmatrix} \mathfrak{P} & \bar{\mathfrak{P}} \\ \mathfrak{Q} & \bar{\mathfrak{Q}} \end{pmatrix} = \mathfrak{V},$$

we have

$$\frac{1}{2i}\mathfrak{J}\{\mathfrak{V}\} = \frac{1}{2i}\mathfrak{G}\{\mathfrak{F}\mathfrak{C}^{-1}\} = \mathfrak{K}_1\{\mathfrak{C}^{-1}\} = \mathfrak{K}$$

and consequently

$$(139) \qquad \frac{1}{2i}(\mathfrak{P}'\bar{\mathfrak{Q}} - \mathfrak{Q}'\bar{\mathfrak{P}}) = \mathfrak{H}, \qquad \mathfrak{P}'\mathfrak{Q} - \mathfrak{Q}'\mathfrak{P} = 0;$$

moreover

$$\mathfrak{P}_1 = \mathfrak{P} - \tfrac{1}{2}\bar{\mathfrak{P}}\mathfrak{H}^{-1}\bar{\mathfrak{A}}, \qquad \mathfrak{Q}_1 = \mathfrak{Q} - \tfrac{1}{2}\bar{\mathfrak{Q}}\mathfrak{H}^{-1}\bar{\mathfrak{A}}.$$

By (133), (134), (135), (136) and (137), the neighborhood G of $\mathfrak{S} = \mathfrak{I}$ is mapped onto a neighborhood G^* of $\mathfrak{H} = \mathfrak{E}$, $\mathfrak{A} = 0$ in the $(\mathfrak{H}, \mathfrak{A})$ space. Since $|\mathfrak{H}| \neq 0$, we have $\mathfrak{H} > 0$. By (139), $|\mathfrak{Q}| \neq 0$ and

$$\mathfrak{P}\mathfrak{Q}^{-1} = \mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$$

is a point of H with the imaginary part $\mathfrak{Y} = \mathfrak{H}\{\mathfrak{Q}^{-1}\}$. Then

(140) $\quad \mathfrak{P}_1 = (\mathfrak{Z} - \tfrac{1}{2}\bar{\mathfrak{Z}}\mathfrak{Y}^{-1}\bar{\mathfrak{A}}[\mathfrak{Q}^{-1}])\mathfrak{Q}, \quad \mathfrak{Q}_1 = (\mathfrak{E} - \tfrac{1}{2}\mathfrak{Y}^{-1}\bar{\mathfrak{A}}[\mathfrak{Q}^{-1}])\mathfrak{Q}.$

It follows, from (138) and (140), that L is mapped onto the set L^* of the $(\mathfrak{Z}, \mathfrak{Q}, \mathfrak{A})$ space defined by the conditions $\mathfrak{Z} \subset H$, $(\mathfrak{Y}\{\mathfrak{Q}\}, \mathfrak{A}) \subset G^*$.

If

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{M}_1 & \mathfrak{M}_2 \\ \mathfrak{M}_3 & \mathfrak{M}_4 \end{pmatrix}$$

is any modular matrix, then the mapping

(141) $\quad \mathfrak{Z} \to (\mathfrak{M}_1\mathfrak{Z} + \mathfrak{M}_2)(\mathfrak{M}_3\mathfrak{Z} + \mathfrak{M}_4)^{-1}, \qquad \mathfrak{Q} \to (\mathfrak{M}_3\mathfrak{Z} + \mathfrak{M}_4)\mathfrak{Q}$

transforms L^* into itself and leaves every point of G^* invariant. We restrict now $\mathfrak{Z}$ to the fundamental domain F of the modular group Γ. Since the particular mapping with $\mathfrak{M} = -\mathfrak{E}$ leaves $\mathfrak{Z}$ invariant and changes $\mathfrak{Q}$ into $-\mathfrak{Q}$, we obtain in L^* a fundamental domain L^*_0 for all mappings (141), if we impose on $\mathfrak{Q}$ a linear homogeneous condition, e. g., $\sigma(\mathfrak{Q} + \bar{\mathfrak{Q}}) \geqq 0$; then L^*_0 is defined by $\mathfrak{Z} \subset F$, $(\mathfrak{Y}\{\mathfrak{Q}\}, \mathfrak{A}) \subset G^*$, $\sigma(\mathfrak{Q} + \bar{\mathfrak{Q}}) \geqq 0$. Let L_0 be the corresponding domain in L. Obviously L_0 is a fundamental domain in L relative to the homogeneous modular group Γ_0, such that the images of L_0 under the mappings $\mathfrak{L} \to \mathfrak{M}\mathfrak{L}$ cover L completely without gaps and overlappings.

Denote by $v(L_0)$ the euclidean volume of L_0, the elements of $\mathfrak{L}$ being considered as rectangular cartesian coördinates, and by $v(G)$ the euclidean volume of G, where the elements of the skew-symmetric matrix $\mathfrak{S} = \mathfrak{I}[\mathfrak{L}]$ above the diagonal are the coördinates. Theorem 12 asserts that

(142) $$\lim_{G \to \mathfrak{I}} \frac{v(L_0)}{v(G)} = d_0,$$

if G runs over any sequence of neighborhoods tending to the single point $\mathfrak{I}$, with the value d_0 defined in (132). Obviously the left-hand side of (142) is the analogue of the expression in (131), for the real valuation instead of the p-adic valuation.

49. In order to simplify the notation, we introduce cartesian coördinates for a matrix $\mathfrak{T}^{(m)} = (t_{kl})$ in the following way: If $\mathfrak{T}$ is arbitrarily real, we choose the m^2 coördinates t_{kl} $(k, l = 1, \cdots, m)$; if $\mathfrak{T}$ is symmetric, we take the $\frac{1}{2}m(m+1)$ coördinates t_{kl} $(1 \leq k \leq l \leq m)$; if $\mathfrak{T}$ is skew-symmetric, we take the $\frac{1}{2}m(m-1)$ coördinates t_{kl} $(1 \leq k < l \leq m)$. If $\mathfrak{T}$ is complex, we split

$$\mathfrak{T} = \mathfrak{T}_1 + i\mathfrak{T}_2, \qquad \mathfrak{T}_1 = \tfrac{1}{2}(\mathfrak{T} + \bar{\mathfrak{T}}), \qquad \mathfrak{T}_2 = \frac{1}{2i}(\mathfrak{T} - \bar{\mathfrak{T}}),$$

and proceed in the same manner with the real part $\mathfrak{T}_1$ and the imaginary part $\mathfrak{T}_2$. In particular, a hermitian matrix $\mathfrak{T}$ has then the m^2 coördinates

$$t_{kk}\ (k = 1, \cdots, m), \quad \tfrac{1}{2}(t_{kl} + \bar{t}_{kl}), \quad \frac{1}{2i}(t_{kl} - \bar{t}_{kl}) \qquad (1 \leq k < l \leq m).$$

In all these cases, we denote by $d\mathfrak{T}$ the euclidean volume element in the space of the coördinates of $\mathfrak{T}$.

By (133), (138) and (140), we have

$$v(L_0) = \int_{L_0} d\mathfrak{L}, \qquad d\mathfrak{L} = d\mathfrak{P}_1 d\mathfrak{Q}_1 = |\mathfrak{Q}_1\bar{\mathfrak{Q}}_1|^n\, d\mathfrak{R}\, d\mathfrak{Q}_1$$

with

$$\mathfrak{R} = \mathfrak{P}_1\mathfrak{Q}_1^{-1} = (\mathfrak{Z} + \tfrac{1}{2}\bar{\mathfrak{Z}}\mathfrak{Y}^{-1}\bar{\mathfrak{A}}[\mathfrak{Q}^{-1}])(\mathfrak{E} - \tfrac{1}{2}\mathfrak{Y}^{-1}\bar{\mathfrak{A}}[\mathfrak{Q}^{-1}])^{-1}.$$

In a sufficiently small neighborhood of $\mathfrak{A} = 0$, the power series

$$\mathfrak{R} = \mathfrak{Z} - i\bar{\mathfrak{A}}[\mathfrak{Q}^{-1}] + \cdots$$

converges, whence

$$d\mathfrak{R} \sim 2^{n(n-1)}\, |\mathfrak{Q}\bar{\mathfrak{Q}}|^{1-n}\, d\mathfrak{Z}\, d\mathfrak{A}, \qquad d\mathfrak{Q}_1 \sim d\mathfrak{Q} \qquad (\mathfrak{A} \rightarrow 0).$$

It follows that

$$v(L_0) \sim 2^{n(n-1)} \int_{L^*_0} |\mathfrak{Q}\bar{\mathfrak{Q}}|\, d\mathfrak{X}\, d\mathfrak{Y}\, d\mathfrak{Q}\, d\mathfrak{A} \qquad (G \rightarrow \mathfrak{H}).$$

We choose a real matrix $\mathfrak{C}_1^{(n)}$, such that $\mathfrak{C}'_1\mathfrak{C}_1 = \mathfrak{Y}$. Then the condition $\mathfrak{Y}\{\mathfrak{Q}\} = \mathfrak{H}$ is replaced by $\mathfrak{Q}'_2\bar{\mathfrak{Q}}_2 = \mathfrak{H}$ with $\mathfrak{Q}_2 = \mathfrak{C}_1\mathfrak{Q}$. Since

$$d\mathfrak{Q}_2 = |\mathfrak{C}_1|^{2n}\, d\mathfrak{Q} = |\mathfrak{Y}|^n\, d\mathfrak{Q}, \qquad |\mathfrak{Q}\bar{\mathfrak{Q}}| = |\mathfrak{Q}_2\bar{\mathfrak{Q}}_2|\ |\mathfrak{Y}|^{-1},$$

we obtain

$$(143) \quad v(L_0) \sim 2^{n(n-1)} \int_F |\mathfrak{Y}|^{-n-1}\, d\mathfrak{X}\, d\mathfrak{Y} \cdot \tfrac{1}{2} \int_{(\mathfrak{Q}'_2\bar{\mathfrak{Q}}_2, \mathfrak{A}) \subset G^*} |\mathfrak{Q}_2\bar{\mathfrak{Q}}_2|\, d\mathfrak{Q}_2\, d\mathfrak{A} \quad (G \rightarrow \mathfrak{H}).$$

On the other hand, by (133) and (136),

$$v(G) = \int_G d\mathfrak{G}, \qquad d\mathfrak{G} = d\mathfrak{G}_1 d\mathfrak{G}_2 d\mathfrak{G}_3 = 2^{n(n-1)} d\mathfrak{H}_1 d\mathfrak{A},$$
$$d\mathfrak{H}_1 \sim d\mathfrak{H} \qquad (G \to \mathfrak{Z});$$

hence

$$v(G) \sim 2^{n(n-1)} \int_{(\mathfrak{H},\mathfrak{A}) \subset G^*} d\mathfrak{H} d\mathfrak{A}. \tag{144}$$

The first integral in (143) has the value $V_m = V(\Gamma)$. By (132), (143) and (144), the proof of (142) is reduced to the proof of the following lemma.

LEMMA 17. *Let H_1 be a domain in the space of the positive hermitian matrices and $\mathfrak{H}^* > 0$; then*

$$\int_{\mathfrak{H}^*\{\mathfrak{Q}\} \subset H_1} d\mathfrak{Q} = c_n \,|\, \mathfrak{H}^* \,|^{-n} \int_{\mathfrak{H} \subset H_1} d\mathfrak{H}, \qquad c_n = \prod_{k=1}^{n} \frac{\pi^k}{(k-1)\,!}\,. \tag{145}$$

We determine a matrix $\mathfrak{C}^*$ satisfying $\mathfrak{H}^*\{\mathfrak{C}^*\} = \mathfrak{E}$ and replace $\mathfrak{Q}$, $d\mathfrak{Q}$ by $\mathfrak{C}^*\mathfrak{Q}$, $|\, \mathfrak{C}^*\bar{\mathfrak{C}}^* \,|^n d\mathfrak{Q}$. Then we have only to prove (145) in the special case $\mathfrak{H}^* = \mathfrak{E}$.

We apply induction and assume first $n > 1$. Let $\mathfrak{Q}_0$ be a matrix having the same first column $\mathfrak{q}$ as $\mathfrak{Q}$ and $|\, \mathfrak{Q}_0 \,| \neq 0$; then

$$\mathfrak{Q} = \mathfrak{Q}_0 \begin{pmatrix} 1 & \mathfrak{t}' \\ 0 & \mathfrak{T} \end{pmatrix},$$
$$d\mathfrak{Q} = |\, \mathfrak{Q}_0 \bar{\mathfrak{Q}}_0 \,|^{n-1} d\mathfrak{q} d\mathfrak{t} d\mathfrak{T}.$$

Introducing

$$\mathfrak{Q}'_0 \bar{\mathfrak{Q}}_0 = \mathfrak{H}_0 = \begin{pmatrix} h & \bar{\mathfrak{d}}'_0 \\ \mathfrak{d}_0 & \mathfrak{D}_0 \end{pmatrix} = \begin{pmatrix} h & 0 \\ 0 & \mathfrak{R}_0 \end{pmatrix} \left\{ \begin{matrix} 1 & h^{-1}\bar{\mathfrak{d}}'_0 \\ 0 & \mathfrak{E} \end{matrix} \right\},$$
$$\mathfrak{Q}' \bar{\mathfrak{Q}} = \mathfrak{H} = \begin{pmatrix} h & \bar{\mathfrak{d}}' \\ \mathfrak{d} & \mathfrak{D} \end{pmatrix} = \begin{pmatrix} h & 0 \\ 0 & \mathfrak{R} \end{pmatrix} \left\{ \begin{matrix} 1 & h^{-1}\bar{\mathfrak{d}}' \\ 0 & \mathfrak{E} \end{matrix} \right\}, \tag{146}$$

we have

$$\begin{gathered} h = \mathfrak{q}'\bar{\mathfrak{q}}, \quad \mathfrak{R} = \mathfrak{D} - h^{-1}\mathfrak{d}\bar{\mathfrak{d}}', \\ h \,|\, \mathfrak{R}_0 \,| = |\, \mathfrak{H}_0 \,| = |\, \mathfrak{Q}_0 \bar{\mathfrak{Q}}_0 \,|, \quad \mathfrak{R} = \mathfrak{R}_0\{\mathfrak{T}\}, \quad \mathfrak{d} = \mathfrak{T}'\mathfrak{d}_0 + h\mathfrak{t}. \end{gathered} \tag{147}$$

We replace $\mathfrak{t}$ by the new variable $\mathfrak{d}$ and obtain

$$dt = h^{2-2n} d\mathfrak{d},$$
$$d\mathfrak{Q} = |\, \mathfrak{Q}_0 \bar{\mathfrak{Q}}_0 \,|^{n-1} h^{2-2n} d\mathfrak{q} d\mathfrak{d} d\mathfrak{T}.$$

Using (145) with $n - 1$, $\mathfrak{R}_0$, $\mathfrak{T}$, $\mathfrak{R}$ instead of n, $\mathfrak{H}^*$, $\mathfrak{Q}$, $\mathfrak{H}$, we find

$$\int_{\mathfrak{Q}'\bar{\mathfrak{Q}} \subset H_1} d\mathfrak{Q} = c_{n-1} \int |\, \mathfrak{Q}_0 \bar{\mathfrak{Q}}_0 \,|^{n-1} h^{2-2n} \,|\, \mathfrak{R}_0 \,|^{1-n} d\mathfrak{q} d\mathfrak{d} d\mathfrak{R}, \tag{148}$$

where the domain of integration for the variables $\mathfrak{q}$, $\mathfrak{d}$, $\mathfrak{N}$ is given by (146), (147) and the condition $\mathfrak{H} \subset H_1$. We take the new variable $\mathfrak{D}$ instead of $\mathfrak{N}$, with $d\mathfrak{D} = d\mathfrak{N}$, and perform the integration over $\mathfrak{q}$, for fixed values of $\mathfrak{d}$ and $\mathfrak{D}$. Now

$$\int_{\mathfrak{q}'\bar{\mathfrak{q}} \leq g} d\mathfrak{q} = J(g) = \frac{\pi^n}{n!} g^n; \qquad (g > 0),$$

whence

$$\int_{h_1 \leq h \leq h_2} h^{1-n} d\mathfrak{q} = \int_{h_1}^{h_2} h^{1-n} \frac{dJ(h)}{dh}\, dh = \frac{\pi^n}{(n-1)!} \int_{h_1}^{h_2} dh. \tag{149}$$

But

$$|\,\mathfrak{Q}_0\bar{\mathfrak{Q}}_0\,|^{n-1} h^{2-2n}\,|\,\mathfrak{N}_0\,|^{1-n} = h^{1-n}, \qquad c_{n-1}\frac{\pi^n}{(n-1)!} = c_n$$

and consequently, by (148) and (149),

$$\int_{\mathfrak{Q}'\bar{\mathfrak{Q}} \subset H_1} d\mathfrak{Q} = c_n \int_{\mathfrak{H} \subset H_1} d\mathfrak{H}. \tag{150}$$

It remains to prove (150) in the case $n = 1$. Then it is contained in formula (149) which holds good also in this case.

50. The relationship

$$d_0 = \prod_p d_p$$

constitutes another example of the "integral formulae" of analytic number theory which appear in the theory of class fields and in the theory of quadratic forms. The formula also holds good in the case of an arbitrary group $\Delta(\mathfrak{S}, \mathfrak{H})$, if the densities d_0 and d_p are defined in an analogous manner. But we do not go into detail since the proof of this statement depends upon the analytic theory of hermitian forms, of which no complete account has hitherto been given.

We proved in Section **31**, that the matrix $\mathfrak{Y}^{-1}$ is bounded in the fundamental domain F of the modular group. Theorem 11 may be used for an estimation of the maximum μ_n of $|\,\mathfrak{Y}\,|^{-1}$ in F. It follows from (80), (90) and (91), that F is contained in the domain F_1 defined by the conditions

$$|\,\mathfrak{Y}\,|^{-1} \leq \mu_n, \quad \mathfrak{Y}^{-1} \subset R, \quad -\tfrac{1}{2} \leq x_{kl} \leq \tfrac{1}{2} \qquad (1 \leq k \leq l \leq n),$$

where R is the Minkowski domain of Section **29**. Consequently the symplectic volume of F_1 is equal to the euclidean volume of that part of R which is defined by $|\,\mathfrak{T}\,| \leq \mu_n$, $\mathfrak{T} \subset R$. By an important result of Minkowski, this volume is

$$\frac{2}{n+1} \mu_n^{(n+1)/2} \prod_{k=2}^{n} \{\pi^{-k/2}\Gamma\left(\frac{k}{2}\right) \zeta(k)\}. \tag{151}$$

Hence this number is an upper bound of V_n. Using (127), we obtain the estimation

$$(152) \qquad \mu_n \geq \nu_n, \qquad \nu_n^{(n+1)/2} = \frac{n+1}{6}\,\pi \prod_{k=2}^{n} \left\{ \pi^{-k/2} \frac{\Gamma(k)\zeta(2k)}{\Gamma(k/2)\zeta(k)} \right\}$$

and in particular

$$\mu_1 \geq \frac{\pi}{3}, \qquad \mu_2^{3/2} \geq \frac{\pi^2}{30}, \qquad \mu_3^2 \geq \frac{8\pi^6}{42525\zeta(3)},$$

the exact value of μ_1 being $2/3^{1/2}$. By Stirling's formula, for $n \to \infty$,

$$\log \nu_n = \frac{n}{2}\left(\log \frac{2n}{\pi} - \frac{3}{2}\right) + O(1); \quad \log \mu_n > \frac{n}{2} \log n + O(n).$$

This proves that μ_n increases rapidly, as a function of n.

Let now $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$ be an arbitrary point of H and let $\mathfrak{Z}^* = \mathfrak{X}^* + i\mathfrak{Y}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ be the image of $\mathfrak{Z}$ under any modular transformation. By Section **30**, the expression

$$|\,\mathfrak{Y}^*\,|^{-1} = |\,\mathfrak{Y}\,|^{-1} \operatorname{abs} (\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^2$$

has its minimum value, if and only if $\mathfrak{Z}^*$ lies in F. Hence μ_n is the maximum of these minima, for the set of all $\mathfrak{Z}$ in H. A fortiori, there exists a matrix $\mathfrak{Z}$ in H, such that the inequality

$$\operatorname{abs} (\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^2 \geq \nu_n \,|\,\mathfrak{Y}\,|$$

holds for all second matrix rows $(\mathfrak{C}\mathfrak{D})$ of modular matrices, where ν_n is the number defined in (152). Writing $\mathfrak{Z} = \mathfrak{P}\mathfrak{Q}^{-1}$, we have

$$\mathfrak{P}'\mathfrak{Q} - \mathfrak{Q}'\mathfrak{P} = 0, \quad \frac{1}{2i}(\mathfrak{P}'\bar{\mathfrak{Q}} - \mathfrak{Q}'\bar{\mathfrak{P}}) > 0$$

and

$$\operatorname{abs} (\mathfrak{C}\mathfrak{P} + \mathfrak{D}\mathfrak{Q})^2 \geq \nu_n \left|\frac{1}{2i}(\mathfrak{P}'\bar{\mathfrak{Q}} - \mathfrak{Q}'\bar{\mathfrak{P}})\right|.$$

IX. COMMENSURABLE GROUPS.

51. We proved in Chapter V that the group $\Delta_0(\mathfrak{G}, \mathfrak{H})$ is commensurable with $\Delta_0(r, s)$. In order to demonstrate Theorem 13, we have now to discuss the necessary and sufficient conditions for the commensurability of two groups $\Delta_0(r, s)$ and $\Delta_0(r_1, s_1)$. We assumed that the numbers r and s are integers of the totally real field K; all conjugates of s except s itself are negative, whereas r is totally positive. Obviously s generates the field K. The numbers r_1 and s_1 have the same properties with respect to the totally real field K_1.

Hence this number is an upper bound of V_n. Using (127), we obtain the estimation

$$(152) \qquad \mu_n \geq \nu_n, \qquad \nu_n^{(n+1)/2} = \frac{n+1}{6}\,\pi \prod_{k=2}^{n} \left\{ \pi^{-k/2} \frac{\Gamma(k)\zeta(2k)}{\Gamma(k/2)\zeta(k)} \right\}$$

and in particular

$$\mu_1 \geq \frac{\pi}{3}, \qquad \mu_2^{3/2} \geq \frac{\pi^2}{30}, \qquad \mu_3^2 \geq \frac{8\pi^6}{42525\zeta(3)},$$

the exact value of μ_1 being $2/3^{1/2}$. By Stirling's formula, for $n \to \infty$,

$$\log \nu_n = \frac{n}{2}\left(\log \frac{2n}{\pi} - \frac{3}{2}\right) + O(1); \quad \log \mu_n > \frac{n}{2} \log n + O(n).$$

This proves that μ_n increases rapidly, as a function of n.

Let now $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$ be an arbitrary point of H and let $\mathfrak{Z}^* = \mathfrak{X}^* + i\mathfrak{Y}^* = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}$ be the image of $\mathfrak{Z}$ under any modular transformation. By Section **30**, the expression

$$|\mathfrak{Y}^*|^{-1} = |\mathfrak{Y}|^{-1} \operatorname{abs}(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^2$$

has its minimum value, if and only if $\mathfrak{Z}^*$ lies in F. Hence μ_n is the maximum of these minima, for the set of all $\mathfrak{Z}$ in H. A fortiori, there exists a matrix $\mathfrak{Z}$ in H, such that the inequality

$$\operatorname{abs}(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^2 \geq \nu_n |\mathfrak{Y}|$$

holds for all second matrix rows $(\mathfrak{C}\mathfrak{D})$ of modular matrices, where ν_n is the number defined in (152). Writing $\mathfrak{Z} = \mathfrak{P}\mathfrak{Q}^{-1}$, we have

$$\mathfrak{P}'\mathfrak{Q} - \mathfrak{Q}'\mathfrak{P} = 0, \quad \frac{1}{2i}(\mathfrak{P}'\bar{\mathfrak{Q}} - \mathfrak{Q}'\bar{\mathfrak{P}}) > 0$$

and

$$\operatorname{abs}(\mathfrak{C}\mathfrak{P} + \mathfrak{D}\mathfrak{Q})^2 \geq \nu_n \left| \frac{1}{2i}(\mathfrak{P}'\bar{\mathfrak{Q}} - \mathfrak{Q}'\bar{\mathfrak{P}}) \right|.$$

IX. COMMENSURABLE GROUPS.

51. We proved in Chapter V that the group $\Delta_0(\mathfrak{G}, \mathfrak{H})$ is commensurable with $\Delta_0(r, s)$. In order to demonstrate Theorem 13, we have now to discuss the necessary and sufficient conditions for the commensurability of two groups $\Delta_0(r, s)$ and $\Delta_0(r_1, s_1)$. We assumed that the numbers r and s are integers of the totally real field K; all conjugates of s except s itself are negative, whereas r is totally positive. Obviously s generates the field K. The numbers r_1 and s_1 have the same properties with respect to the totally real field K_1.

With the groups $\Delta_0(r,s)$ and $\Delta_0(r_1,s_1)$ we associate the two quadratic forms

$$Q(r,s) = rsx^2 - ry^2 + sz^2 \quad \text{and} \quad Q(r_1,s_1) = r_1s_1x_1^2 - r_1y_1^2 + s_1z_1^2$$

in 3 variables.

LEMMA 18. *If $Q(r,s)$ and $Q(r_1,s_1)$ are equivalent in K, then $K = K_1$ and the groups $\Delta_0(r,s)$, $\Delta_0(r_1,s_1)$ are commensurable.*

Under the assumption of the lemma, s_1 is certainly a number of K; therefore $K_1 \subset K$. Since all conjugates of $Q(r,s)$ are negative definite except $Q(r,s)$ itself, the same holds good for $Q(r_1,s_1)$ considered as a quadratic form in K; consequently s_1 is also a generating number of K and $K = K_1$.

Using the quaternion units $\epsilon_0, \epsilon_1, \epsilon_2, \epsilon_3$ defined in (74), we have $Q(r,s)\epsilon_0 = (x\epsilon_1 + y\epsilon_2 + z\epsilon_3)^2$. Let $\mathfrak{F} = (f_{kl})$ be the matrix of the linear substitution transforming $Q(r,s)$ into $Q(r_1,s_1)$ and let

$$\eta_k = \sum_{l=1}^{3} f_{lk}\epsilon_l \qquad (k = 1, 2, 3).$$

Then

$$\eta_1^2 = r_1s_1\epsilon_0, \quad \eta_2^2 = -r_1\epsilon_0, \quad \eta_3^2 = s_1\epsilon_0, \quad \eta_k\eta_l = -\eta_l\eta_k \quad (1 \leq k < l \leq 3)$$

and consequently there exists a real matrix $\mathfrak{L}^{(2)}$ satisfying

$$|\mathfrak{L}| = 1, \qquad \mathfrak{L}^{-1}\eta_k\mathfrak{L} = \omega_k \qquad (k = 1, 2, 3),$$

$$\omega_1 = \sqrt{r_1s_1}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \qquad \omega_2 = \pm\sqrt{r_1}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \qquad \omega_3 = \pm\sqrt{s_1}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

The elements of $\Delta_0(r,s)$ are defined by

$$\mathfrak{M} = \sum_{k=0}^{3} \mathfrak{A}_k \times \epsilon_k, \qquad \mathfrak{J}[\mathfrak{M}] = \mathfrak{J},$$

with integral $\mathfrak{A}_k$ $(k = 0, \cdots, 3)$ in K. Putting

$$(153) \qquad (\mathfrak{E}^{(n)} \times \mathfrak{F}^{-1})(\mathfrak{A}_1\mathfrak{A}_2\mathfrak{A}_3)' = (\mathfrak{B}_1\mathfrak{B}_2\mathfrak{B}_3)', \qquad \mathfrak{E}^{(n)} \times \mathfrak{L} = \mathfrak{R},$$

we obtain

$$\mathfrak{M} = \mathfrak{A}_0 \times \epsilon_0 + \sum_{k=1}^{3} \mathfrak{B}_k \times \eta_k = \mathfrak{R}\mathfrak{M}_1\mathfrak{R}^{-1}$$

with

$$(154) \qquad \mathfrak{M}_1 = \mathfrak{A}_0 \times \epsilon_0 + \sum_{k=1}^{3} \mathfrak{B}_k \times \omega_k,$$

and $\mathfrak{R}$ is symplectic.

Let q be an even positive rational integer, such that the matrix $q\mathfrak{F}^{-1}/2rs$ is integral. If $\mathfrak{M} \equiv \mathfrak{E} \pmod{q}$, then $\mathfrak{A}_0 + \sqrt{rs}\mathfrak{A}_1 \equiv \mathfrak{E}$, $\mathfrak{A}_0 - \sqrt{rs}\mathfrak{A}_1 \equiv \mathfrak{E}$,

$\sqrt{r}\mathfrak{A}_2 + \sqrt{s}\mathfrak{A}_3 \equiv 0$, $-\sqrt{r}\mathfrak{A}_2 + \sqrt{s}\mathfrak{A}_3 \equiv 0$; hence $\mathfrak{A}_0$ is integral and $\mathfrak{A}_k \equiv 0 \pmod{q/2rs}$ $(k = 1, 2, 3)$. By (153) and (154), $\mathfrak{B}_k$ is also integral and $\mathfrak{M}_1 = \mathfrak{K}^{-1}\mathfrak{M}\mathfrak{K}$ is an element of the group $\Delta_0(r_1, s_1)$. Consider now in $\Delta_0(r, s)$ the subgroup of all $\mathfrak{M}$, such that $\mathfrak{M}_1$ is contained in $\Delta_0(r_1, s_1)$. Since this subgroup Δ^*_0 contains the congruence subgroup of $\Delta_0(r, s)$, for the module q, it is of finite index in $\Delta_0(r, s)$. On the other hand, $\mathfrak{K}^{-1}\Delta^*_0\mathfrak{K}$ consists of all $\mathfrak{M}_1$ in $\Delta_0(r_1, s_1)$, such that $\mathfrak{M} = \mathfrak{K}\mathfrak{M}_1\mathfrak{K}^{-1}$ is an element of $\Delta_0(r, s)$; hence the same argument shows that $\mathfrak{K}^{-1}\Delta^*_0\mathfrak{K}$ is a subgroup of finite index in $\Delta_0(r_1, s_1)$. It follows that $\Delta_0(r, s)$ and $\Delta_0(r_1, s_1)$ are commensurable.

52. On account of Lemma 18, the condition of Theorem 13 is sufficient for the commensurability of $\Delta_0(r, s)$ and $\Delta_0(r_1, s_1)$. It remains to prove that this condition is also necessary, which is a little more difficult.

LEMMA 19. *Let a and b be two numbers of K, $ab \neq 0$ and K_0 an arbitrary algebraic number field. There exists an integral number t in K, such that $at^2 - b$ is not the square of a number of K_0 and $a(at^2 - b)$ is totally positive.*

We may obviously assume that a, b are integral and $K \subset K_0$. We choose in K a prime ideal λ having the following 3 properties: λ is not divisible by the square of a prime ideal of K_0, i. e., λ is not a factor of the relative discriminant of K_0 with respect to K; $2ab$ is not divisible by λ; ab is a quadratic residue modulo λ in K. Then there exists an integer t in K, such that $at^2 - b$ is divisible by λ, but not by λ^2, and that, moreover, $a(at^2 - b)$ is totally positive. Since $at^2 - b$ is divisible by exactly the first power of a prime ideal in K_0, it cannot be a square number in K_0.

LEMMA 20. *There exists a quadratic form $Q(r_0, s_0)$ equivalent with $Q(r, s)$ in K and a quadratic form $Q(r_2, s_2)$ equivalent with $Q(r_1, s_1)$ in K_1, such that the field $K^*(\sqrt{r_0}, \sqrt{s_0}, \sqrt{r_2}, \sqrt{s_2})$ has the degree 16 relative to K^*, where K^* is the union of the fields K and K_1.*

Using Lemma 19, we choose an integral number t in K, such that $rt^2 - s = r_0$ is totally positive and no square in K^*. Then the quadratic form $Q(r, s) = rsx^2 - ry^2 + sz^2$ is equivalent with $rsx^2 - r_0y^2 + r_0rsz^2$ in K. Applying again Lemma 19, we construct an integer u in K, such that $r_0rsu^2 + rs = s_0$ is no square in $K^*(\sqrt{r_0})$ and ss_0 is totally positive. Then $Q(r, s)$ is equivalent with $Q(r_0, s_0)$ in K and the field $K^*(\sqrt{r_0}, \sqrt{s_0})$ has the degree 4 relative to K^*. We complete the proof of the lemma by using the same argument for $Q(r_1, s_1)$, K_1, $K^*(\sqrt{r_0}, \sqrt{s_0})$ instead of $Q(r, s)$, K, K^*.

By Lemmata 18 and 20, we can assume for the rest of the proof of Theorem 13, that $K^*(\sqrt{r}, \sqrt{s}, \sqrt{r_1}, \sqrt{s_1})$ has the degree 16 relative to the union K^* of K and K_1.

Lemma 21. *Let G_1 be a subgroup of another group G, of finite index j. For any element A of G, there exists a positive rational integer $g \leq j$, such that A^g is an element of G_1.*

Let $G_1, G_2, \cdots, G_j$ be the right cosets of G_1 relative to G and consider the $j+1$ powers A^k $(k = 0, \cdots, j)$. Then two of these powers A^k and A^l $(0 \leq k < l \leq j)$ lie in the same coset, and A^g, with $g = l - k$, is an element of G_1, q. e. d.

53. Lemma 22. *Let Δ^* be a subgroup of $\Delta_0(r, s)$ of finite index. Then there exists in Δ^* a diagonal matrix $\mathfrak{P}$, such that all diagonal elements of $\mathfrak{P}$ are different one from another and that no conjugate of $\mathfrak{P}$, different from $\mathfrak{P}$ and $\mathfrak{P}^{-1}$, has a diagonal element in common with $\mathfrak{P}$.*

Let h be the degree of the field K with the conjugates $K^{(1)}, \cdots, K^{(h)}$ and $K^{(1)} = K$. The number of algebraic fundamental units in K is $h - 1$. The field $K(\sqrt{rs})$ has the degree $2h$; since it has 2 real conjugates and $h - 1$ pairs of conjugate complex conjugates, the number of algebraic fundamental units in $K(\sqrt{rs})$ is h. Consequently there exists an algebraic unit $\lambda = a + b\sqrt{rs}$, where a and b are numbers of K, such that no power λ^q $(q = \pm 1, \pm 2, \cdots)$ is a number of K.

Denoting by N the norm relative to K, we have $N(\lambda) = a^2 - rsb^2 = c$, where c is an algebraic unit in K, and $N(c^{-1}\lambda^2) = 1$. We replace $c^{-1}\lambda^2$ again by λ; then λ is an algebraic unit in $K(\sqrt{rs})$, no power λ^q $(q = \pm 1, \pm 2, \cdots)$ is a number of K, and $N(\lambda) = 1$, $\lambda^{-1} = a - b\sqrt{rs}$. By Fermat's theorem, we may, moreover, assume $\lambda \equiv 1 \pmod{2\sqrt{rs}}$; hence a and b are integers of K.

Let $q_1, \cdots, q_n$ be different positive rational integers and let

$$\mathfrak{P}_1 = [\lambda^{q_1}, \cdots, \lambda^{q_n}].$$

Then the matrix

$$\mathfrak{P} = \begin{pmatrix} \mathfrak{P}_1 & 0 \\ 0 & \mathfrak{P}_1^{-1} \end{pmatrix} = \tfrac{1}{2}(\mathfrak{P}_1 + \mathfrak{P}_1^{-1}) \times \epsilon_0 + \frac{1}{2\sqrt{rs}}(\mathfrak{P}_1 - \mathfrak{P}_1^{-1}) \times \epsilon_1$$

is an element of the group $\Delta_0(r,s)$. By Lemma 21, a certain power $\mathfrak{P}^g$ with positive exponent g lies in the subgroup Δ^*. Replacing gq_k $(k=1,\cdots,n)$ by q_k, we may assume that already $\mathfrak{P}$ is an element of Δ^*. The diagonal elements of $\mathfrak{P}$ are $\lambda^{q_k}, \lambda^{-q_k}$ $(k=1,\cdots,n)$. Since the exponents $q_k, -q_k$ are all different and λ is no root of unity, these diagonal elements are all different.

For any number t of K, we denote by $t^{(l)}$ the conjugate of t in $K^{(l)}$. The $2h$ conjugates of $\lambda^{q_k}=a_k+b_k\sqrt{rs}$ are $a_k^{(l)}\pm b_k^{(l)}\sqrt{r^{(l)}s^{(l)}}$ $(l=1,\cdots,h)$. Since $b_k\neq 0$ and $r^{(l)}s^{(l)}<0$ for $l=2,\cdots,h$, only the two conjugates $a_k+b_k\sqrt{rs}=\lambda^{q_k}$ and $a_k-b_k\sqrt{rs}=\lambda^{-q_k}$ are real. If a conjugate $\mathfrak{P}^*$ of $\mathfrak{P}$ has a diagonal element in common with $\mathfrak{P}$, then the substitution $\mathfrak{P}\rightarrow\mathfrak{P}^*$ arises either from the identical mapping $\lambda\rightarrow\lambda$ or from $\lambda\rightarrow\lambda^{-1}$, hence $\mathfrak{P}^*=\mathfrak{P}$ or $\mathfrak{P}^*=\mathfrak{P}^{-1}$, q. e. d.

We assume that the groups $\Delta_0(r,s)$ and $\Delta_0(r_1,s_1)$ are commensurable; we shall now first prove, that then $K=K_1$. There exists a subgroup Δ^* of $\Delta_0(r,s)$, of finite index, and a symplectic matrix $\mathfrak{R}$, such that $\mathfrak{R}^{-1}\Delta^*\mathfrak{R}=\Delta_1$ is a subgroup of $\Delta_0(r_1,s_1)$, of finite index. Henceforth we do not need the existence of a *symplectic* matrix $\mathfrak{R}$ with this property; we have only to assume that there is a non-singular matrix $\mathfrak{R}$ with real or complex elements satisfying $\Delta^*\mathfrak{R}=\mathfrak{R}\Delta_1$ where Δ^* and Δ_1 are subgroups of $\Delta_0(r,s)$ and $\Delta_0(r_1,s_1)$, of finite indices. Obviously we may then, moreover, assume that $\mathfrak{R}$ lies in the field $K^*(\sqrt{r},\sqrt{s},\sqrt{r_1},\sqrt{s_1})=K_0$, of degree 16 over the union K^* of K and K_1.

Let $\mathfrak{P}$ be the matrix of Lemma 22. Since $\mathfrak{P}$ belongs to the subgroup Δ^* of $\Delta_0(r,s)$, the matrix $\mathfrak{R}^{-1}\mathfrak{P}\mathfrak{R}$ is an element of Δ_1 and lies therefore in the field $K_1(\sqrt{r_1},\sqrt{s_1})$. We consider any isomorphism A of K_0 which does not change the numbers of $K_1(\sqrt{r_1},\sqrt{s_1})$. Denoting the image under A by the subscript A, we have $\mathfrak{R}_A^{-1}\mathfrak{P}_A\mathfrak{R}_A=\mathfrak{R}^{-1}\mathfrak{P}\mathfrak{R}$; hence the matrix $\mathfrak{B}=\mathfrak{R}_A\mathfrak{R}^{-1}$ satisfies

$$\mathfrak{P}_A=\mathfrak{B}\mathfrak{P}\mathfrak{B}^{-1}. \tag{155}$$

This proves that the diagonal matrices $\mathfrak{P}_A$ and $\mathfrak{P}$ have the same diagonal elements, perhaps in different order. By Lemma 22, either $\mathfrak{P}_A=\mathfrak{P}$ or $\mathfrak{P}_A=\mathfrak{P}^{-1}$. If $a+b\sqrt{rs}$ is a diagonal element of $\mathfrak{P}$, then $b\neq 0$ and $(a+b\sqrt{rs})_A=a\pm b\sqrt{rs}$; whence $(rs)_A=rs$.

On the other hand, rs generates K, since all conjugates of rs except rs itself are negative. Consequently all numbers of K are invariant under A. This proves $K\subset K_1(\sqrt{r_1},\sqrt{s_1})$. Since $K^*(\sqrt{r_1},\sqrt{s_1})$ has the degree 4 relative to K^*, the intersection of $K_1(\sqrt{r_1},\sqrt{s_1})$ and K^* is K_1. Therefore

$K \subset K_1$. Interchanging K and K_1, we have also $K_1 \subset K$; consequently $K = K_1$.

54. We use the abbreviation

$$\mathfrak{C} = \begin{pmatrix} \mathfrak{E} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{E} \end{pmatrix}.$$

LEMMA 23. *There exists an element* $\mathfrak{M}$ *of* Δ^*, *such that* $\mathfrak{C}\mathfrak{M}\mathfrak{C}^{-1} = \mathfrak{Q}$ *is a diagonal matrix with different diagonal elements.*

Analogously to the proof of Lemma 22, we construct an algebraic unit $\mu = a + b\sqrt{s}$ in $K(\sqrt{s})$, such that a, b are integers of K, $a^2 - sb^2 = 1$ and all powers μ^q $(q = \pm 1, \pm 2, \cdots)$ are different one from another. Let $q_1, \cdots, q_n$ be different positive rational integers, $\mathfrak{Q}_1 = [\mu^{q_1}, \cdots \mu^{q_n}]$ and

$$\mathfrak{Q} = \begin{pmatrix} \mathfrak{Q}_1 & 0 \\ 0 & \mathfrak{Q}_1^{-1} \end{pmatrix}.$$

Then the matrix

$$\mathfrak{M} = \mathfrak{C}^{-1}\mathfrak{Q}\mathfrak{C} = \tfrac{1}{2}\begin{pmatrix} \mathfrak{Q}_1 + \mathfrak{Q}_1^{-1} & \mathfrak{Q}_1 - \mathfrak{Q}_1^{-1} \\ \mathfrak{Q}_1 - \mathfrak{Q}_1^{-1} & \mathfrak{Q}_1 + \mathfrak{Q}_1^{-1} \end{pmatrix}$$

$$= \tfrac{1}{2}(\mathfrak{Q}_1 + \mathfrak{Q}_1^{-1}) \times \epsilon_0 + \frac{1}{2\sqrt{s}}(\mathfrak{Q}_1 - \mathfrak{Q}_1^{-1}) \times \epsilon_3$$

is an element of $\Delta_0(r, s)$. By Lemma 3, a power $\mathfrak{M}^g = \mathfrak{C}^{-1}\mathfrak{Q}^g\mathfrak{C}$ lies in Δ^*. Replacing $\mathfrak{M}^g, \mathfrak{Q}^g$ by $\mathfrak{M}, \mathfrak{Q}$, we obtain the proof of Lemma 23.

Let again A denote an isomorphism of $K(\sqrt{r}, \sqrt{s}, \sqrt{r_1}, \sqrt{s_1}) = K_0$ which leaves invariant all numbers of $K(\sqrt{r_1}, \sqrt{s_1})$. Analogous to (155), we obtain

$$\mathfrak{Q}_A = (\mathfrak{C}\mathfrak{V}\mathfrak{C}^{-1})\mathfrak{Q}(\mathfrak{C}\mathfrak{V}\mathfrak{C}^{-1})^{-1} \qquad (156)$$

with the matrix $\mathfrak{Q}$ of Lemma 23 and $\mathfrak{V} = \mathfrak{R}_A\mathfrak{R}^{-1}$. Consider in particular the isomorphism A_s defined by $\sqrt{s} \to -\sqrt{s}$, $\sqrt{r} \to \sqrt{r}$ and write more shortly the subscript s instead of A_s; then

$$\mathfrak{P}_s = \mathfrak{P}^{-1}, \qquad \mathfrak{Q}_s = \mathfrak{Q}^{-1}.$$

By (155) the matrix $\mathfrak{R}_s\mathfrak{R}^{-1} = \mathfrak{V}$ has the form

$$\mathfrak{V} = \begin{pmatrix} 0 & \mathfrak{D}(1) \\ \mathfrak{D}(0) & 0 \end{pmatrix},$$

where $\mathfrak{D}(0)$ and $\mathfrak{D}(1)$ denote diagonal matrices; by (156), the matrix $\mathfrak{C}\mathfrak{V}\mathfrak{C}^{-1}$ has the same form, whence

$$\mathfrak{R}_s = \begin{pmatrix} 0 & \mathfrak{D}(1) \\ -\mathfrak{D}(1) & 0 \end{pmatrix} \mathfrak{R}, \tag{157}$$

$$\begin{gathered} \mathfrak{R} = \mathfrak{R}_{ss} = -(\mathfrak{D}_s(1)\mathfrak{D}(1) \times \epsilon_0)\mathfrak{R}, \\ \mathfrak{D}_s(1)\mathfrak{D}(1) = -\mathfrak{E}. \end{gathered} \tag{158}$$

Consider now the isomorphism A_r defined by $\sqrt{r} \to -\sqrt{r}$, $\sqrt{s} \to \sqrt{s}$; then

$$\mathfrak{P}_r = \mathfrak{P}^{-1}, \qquad \mathfrak{Q}_r = \mathfrak{Q},$$

and we obtain from (155) and (156) the formula

$$\mathfrak{R}_r = \begin{pmatrix} 0 & \mathfrak{D}(2) \\ \mathfrak{D}(2) & 0 \end{pmatrix} \mathfrak{R} \tag{159}$$

with a diagonal matrix $\mathfrak{D}(2)$, whence

$$\mathfrak{D}_r(2)\mathfrak{D}(2) = \mathfrak{E}. \tag{160}$$

Interchanging r, s and r_1, s_1, we find in an analogous manner

$$\mathfrak{R}_{s_1} = \mathfrak{R} \begin{pmatrix} 0 & \mathfrak{D}(3) \\ -\mathfrak{D}(3) & 0 \end{pmatrix}, \qquad \mathfrak{R}_{r_1} = \mathfrak{R} \begin{pmatrix} 0 & \mathfrak{D}(4) \\ \mathfrak{D}(4) & 0 \end{pmatrix}, \tag{161}$$

$$\mathfrak{D}(3)\mathfrak{D}_{s_1}(3) = -\mathfrak{E}, \qquad \mathfrak{D}(4)\mathfrak{D}_{r_1}(4) = \mathfrak{E} \tag{162}$$

with diagonal matrices $\mathfrak{D}(3)$ and $\mathfrak{D}(4)$. Moreover $\mathfrak{R}_{rr_1} = \mathfrak{R}_{r_1 r}$, whence

$$(\mathfrak{D}_{r_1}(2)\mathfrak{D}^{-1}(2) \times \epsilon_0)\mathfrak{R} = \mathfrak{R}(\mathfrak{D}_r(4)\mathfrak{D}^{-1}(4) \times \epsilon_0). \tag{163}$$

Since $|\mathfrak{R}| \neq 0$ at least one element r_{1l} of the first row of $\mathfrak{R} = (r_{kl})$ is $\neq 0$. We assume $r_{1l} \neq 0$ for $l = p_0$ and define $p = p_0$, if $p_0 \leq n$, and $p = p_0 - n$, if $p > n$. Let a be the first diagonal element of $\mathfrak{D}(2)$ and b be the p-th diagonal element of $\mathfrak{D}(4)$. By (160), (162) and (163),

$$aa_r = 1, \qquad bb_{r_1} = 1, \qquad ab_r = ba_{r_1}.$$

55. LEMMA 24. *There exists a number $c \neq 0$ in K_0 satisfying*

$$ac = c_r, \qquad bc = c_{r_1}. \tag{164}$$

If $a \neq 1$, we define $d = \dfrac{\sqrt{r}}{a-1}$, whence

$$d_r = \frac{-\sqrt{r}}{a_r - 1} = \frac{-a\sqrt{r}}{1-a} = ad;$$

if $a = 1$, we define $d = 1$. In both cases $ad = d_r$. Putting $\dfrac{bd}{d_{r_1}} = f$, we find $ff_{r_1} = 1$,

$$f_r = \frac{b_r d_r}{d_{r_1 r}} = \frac{b_r a d}{(ad)_{r_1}} = \frac{bd}{d_{r_1}} = f.$$

Let $g = \frac{\sqrt{r_1}}{f-1}$ for $f \neq 1$, and $g = 1$ for $f = 1$. In both cases

$$fg = g_{r_1}, \qquad g_r = g,$$

and $c = dg$ has the required propetries.

Since there is an arbitrary scalar factor $\neq 0$ in $\mathfrak{R}$, we may replace $\mathfrak{R}$ by $c\mathfrak{R}$, where c is defined in Lemma 24. It follows from (159), (161) and (164), that then a and b are both replaced by 1.

Let α be the first diagonal element of $\mathfrak{D}(1)$ and β the p-th diagonal element of $\mathfrak{D}(3)$. By (158) and (162),

$$\alpha\alpha_s = -1, \qquad \beta\beta_{s_1} = -1. \tag{165}$$

Calculating

$$\mathfrak{R}_{rs} = \mathfrak{R}_{sr}, \quad \mathfrak{R}_{sr_1} = \mathfrak{R}_{r_1 s}, \quad \mathfrak{R}_{rs_1} = \mathfrak{R}_{s_1 r}, \quad \mathfrak{R}_{r_1 s_1} = \mathfrak{R}_{s_1 r_1} \quad \text{and} \quad \mathfrak{R}_{ss_1} = \mathfrak{R}_{s_1 s}$$

by (157), (159) and (161), we obtain, moreover,

$$\alpha_r = -\alpha, \quad \alpha_{r_1} = \alpha, \quad \beta_r = \beta, \quad \beta_{r_1} = -\beta, \quad \beta\alpha_{s_1} = \alpha\beta_s. \tag{166}$$

By (165) and (166), the numbers $u = \alpha\sqrt{r}$ and $v = \beta\sqrt{r_1}$ lie in $K(\sqrt{s}, \sqrt{s_1})$ and satisfy

$$uu_s = -r, \qquad vv_{s_1} = -r_1, \qquad vu_{s_1} = uv_s.$$

Defining $w = u/u_{s_1} = v/v_s$, we have $w_{s_1} = w^{-1} = w_s$, and consequently w is a number of the field $K(\sqrt{ss_1})$. Let $\tau = \sqrt{ss_1}/(w-1)$ for $w \neq 1$, and $\tau = 1$ for $w = 1$; in both cases τ lies in $K(\sqrt{ss_1})$ and $\tau_s = \tau_{s_1} = w\tau$. Then the numbers $\rho = u\tau$ and $\sigma = v\tau$ satisfy

$$\rho_{s_1} = u_{s_1}\tau_{s_1} = \frac{u}{w} w\tau = u\tau = \rho, \qquad \sigma_s = v_s\tau_s = \frac{v}{w} w\tau = v\tau = \sigma,$$

$$\rho\rho_s = u\tau u_s\tau_s = -r\tau\tau_s, \qquad \sigma\sigma_{s_1} = v\tau v_{s_1}\tau_{s_1} = -r_1\tau\tau_{s_1},$$

whence

$$\rho = \xi + \eta\sqrt{s}, \quad \sigma = \xi_1 + \eta_1\sqrt{s_1}, \quad \tau = \zeta + \omega\sqrt{ss_1},$$

$$\xi^2 - s\eta^2 = -r(\zeta^2 - ss_1\omega^2), \quad \xi_1^2 - s_1\eta_1^2 = -r_1(\zeta^2 - ss_1\omega^2), \tag{167}$$

where $\xi, \eta, \xi_1, \eta_1, \zeta, \omega$ are numbers of K which are not all 0.

We consider first the case $\omega \neq 0$. Performing the 3 linear substitutions

$$x = \eta x_3 + \xi y_3, \qquad y = \xi x_3 + s\eta y_3, \qquad z = z_3$$

$$x_3 = \frac{x_2}{s\eta^2 - \xi^2}, \qquad y_3 = \frac{\zeta y_2}{s\omega(s\eta^2 - \xi^2)} + \frac{z_2}{rs\omega}, \qquad z_3 = \frac{y_2 + \zeta z_2}{s\omega}$$

$$x_2 = s_1\eta_1 x_1 + \xi_1 y_1, \qquad y_2 = \xi_1 x_1 + \eta_1 y_1, \qquad z_2 = z_1,$$

we obtain, by (167),

$$\begin{aligned} Q(r,s) &= rsx^2 - ry^2 + sz^2 = r(s\eta^2 - \xi^2)(x_3^2 - sy_3^2) + sz_3^2 \\ &= \frac{r}{s\eta^2 - \xi^2}(x_2^2 - s_1 y_2^2) + s_1 z_2^2 = r_1 s_1 x_1^2 - r_1 y_1^2 + s_1 z_1^2 = Q(r_1, s_1); \end{aligned}$$

hence $Q(r,s)$ and $Q(r_1, s_1)$ are equivalent in K.

In the remaining case $\omega = 0$, we have

$$\xi^2 - s\eta^2 = -r\zeta^2 \quad \text{and} \quad \xi_1^2 - s_1\eta_1^2 = -r_1\zeta^2.$$

Consequently the diophantine equation $Q(r,s) = 0$ has the non-trivial solution $x = \xi$, $y = s\eta$, $z = r\zeta$. Moreover it follows immediately from the signs of the conjugates of r and s, that K is the field of rational numbers. Applying the 2 linear substitutions

$$x = \frac{\eta x_2 + \xi y_2}{r\zeta}, \qquad y = \frac{\xi x_2 + s\eta y_2}{r\zeta}, \qquad z = z_2$$

$$x_2 = x_1, \qquad y_2 = \frac{s+1}{2s} y_1 + \frac{s-1}{2s} z_1, \qquad z_2 = \frac{s-1}{2s} y_1 + \frac{s+1}{2s} z_1,$$

we obtain

$$Q(r,s) = x_2^2 - sy_2^2 + sz_2^2 = x_1^2 - y_1^2 + z_1^2 = Q(1, 1);$$

hence $Q(r,s)$ and $Q(1,1)$ are equivalent in K. Since the same holds for $Q(r_1, s_1)$ instead of $Q(r,s)$, $Q(r,s)$ and $Q(r_1, s_1)$ are also equivalent in K.

Theorem 13 is now completely proved. In the particular case

$$\mathfrak{S}_1 = \mathfrak{J}, \quad \mathfrak{H}_1 = i\mathfrak{J}, \quad r_1 = 1, \quad s_1 = 1,$$

we have

$$\Delta(\mathfrak{S}_1, \mathfrak{H}_1) = \Gamma \quad \text{and} \quad Q(r_1, s_1) = x_1^2 - y_1^2 + z_1^2.$$

It follows that the group $\Delta(\mathfrak{S}, \mathfrak{H})$ is then and only then commensurable with the modular group, when the diophantine equation $x^2 + ry^2 = s$ has a solution x, y in K.

X. UNIT GROUPS OF QUINARY QUADRATIC FORMS.

56. For $n > 2$, the groups $\Delta(\mathfrak{G}, \mathfrak{H})$ and their subgroups are the only known examples of non-trivial discontinuous subgroups of the symplectic group. However, in the case $n = 2$, another set of examples is provided by the unit groups of certain quinary quadratic forms.

Consider the special quinary quadratic form

$$\mathfrak{S}[\mathfrak{w}] = w_1 w_2 - w_3^2 + w_4 w_5$$

and a complex column $\mathfrak{w}$ satisfying

$$(168) \qquad \mathfrak{S}[\mathfrak{w}] = 0, \qquad \mathfrak{S}\{\mathfrak{w}\} > 0.$$

If $w_5 = 0$, then $w_1 w_2 = w_3^2$ and $w_1 \bar{w}_2 + w_2 \bar{w}_1 - 2 w_3 \bar{w}_3 > 0$, whence $w_1 \neq 0$,

$$(w_1 \bar{w}_3 - w_3 \bar{w}_1)^2 = w_1 \bar{w}_1 (w_1 \bar{w}_2 + w_2 \bar{w}_1 - 2 w_3 \bar{w}_3) > 0,$$

which is impossible, the left-hand side being the square of a pure imaginary quantity; consequently $w_5 \neq 0$. Introducing inhomogeneous coördinates $w_5^{-1}\mathfrak{w} = \mathfrak{z} = \mathfrak{x} + i\mathfrak{y}$, we infer from

$$\mathfrak{S}[\mathfrak{z}] = 0 \quad \text{and} \quad \mathfrak{S}[\mathfrak{y}] = \mathfrak{S}\left[\frac{\mathfrak{z} - \bar{\mathfrak{z}}}{2i}\right] = \tfrac{1}{2}\mathfrak{S}\{\mathfrak{z}\} > 0$$

the relationships

$$(169) \qquad z_1 z_2 - z_3^2 = z_4, \qquad y_1 y_2 - y_3^2 > 0,$$

whence, in particular, $y_1 \neq 0$. On the other hand, (168) follows again from (169), if we define $\mathfrak{w} = w_5 \mathfrak{z}$ with arbitrary $w_5 \neq 0$.

The matrices

$$\mathfrak{Z} = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix}$$

with $y_1 y_2 - y_3^2 > 0$ and $y_1 > 0$ form the space H for $n = 2$; let $\bar{H}$ be the space defined by $y_1 y_2 - y_3^2 > 0$ and $y_1 < 0$.

Consider now a real linear transformation $\hat{\mathfrak{w}} = \mathfrak{B}\mathfrak{w}$, such that $\mathfrak{S}[\hat{\mathfrak{w}}] = 0$, $\mathfrak{S}\{\hat{\mathfrak{w}}\} > 0$ follows from (168). Since the equation $\mathfrak{S}[\mathfrak{w}] = 0$ is irreducible, we conclude that $\mathfrak{S}[\mathfrak{B}] = \lambda\mathfrak{S}$, with a scalar factor $\lambda \neq 0$. Consequently $|\mathfrak{B}| \neq 0$, and these transformations form a group. Since $w_1, \cdots, w_5$ are homogeneous coördinates, we may replace $\mathfrak{B}$ by $\mu\mathfrak{B}$, for any scalar $\mu \neq 0$. But $|\mu\mathfrak{B}| = \mu^5 |\mathfrak{B}|$; hence we may assume $|\mathfrak{B}| = 1$ and $\mathfrak{S}[\mathfrak{B}] = \mathfrak{S}$.

Put $\mathfrak{V} = (v_{kl})$ and $\hat{w}_5^{-1}\hat{\mathfrak{w}} = \hat{\mathfrak{z}} = \hat{\mathfrak{x}} + i\hat{\mathfrak{y}}$. Then the fractional linear substitution

$$\hat{z}_k = \frac{\sum_{l=1}^{5} v_{kl} z_l}{\sum_{l=1}^{5} v_{5l} z_l} \qquad (k = 1, 2, 3) \tag{170}$$

with $z_4 = z_1 z_2 - z_3^2$ and $z_5 = 1$ transforms the space H either into itself or into $\bar{H}$. We are only interested in the substitutions which leave H invariant; they form an invariant subgroup of index 2 in the whole group. We denote this subgroup by $\Omega(\mathfrak{S})$.

Obviously we obtain the solution of (170) with respect to z_1, z_2, z_3, if we replace $\mathfrak{V}$ by $\mathfrak{V}^{-1}$ and interchange $\mathfrak{z}, \hat{\mathfrak{z}}$. Hence (170) is a birational analytic mapping of H onto itself. A simple calculation gives the functional determinant

$$\frac{d(\hat{z}_1, \hat{z}_2, \hat{z}_3)}{d(z_1, z_2, z_3)} = \hat{w}_5^{-3} w_5^{3} \neq 0. \tag{171}$$

On account of Theorem 1, the transformation (170) is symplectic:

$$\begin{pmatrix} \hat{z}_1 & \hat{z}_3 \\ \hat{z}_3 & \hat{z}_2 \end{pmatrix} = \hat{\mathfrak{Z}} = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1}, \quad \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix} = \mathfrak{M}, \quad \mathfrak{I}[\mathfrak{M}] = \mathfrak{I}. \tag{172}$$

57. Let us now start from an arbitrary symplectic transformation (172). Defining

$$\mathfrak{I}_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

we have $\mathfrak{I}_2[\mathfrak{F}] = |\mathfrak{F}|\,\mathfrak{I}_2$ for any matrix $\mathfrak{F}^{(2)}$, and consequently

$$(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1} = |\mathfrak{C}\mathfrak{Z} + \mathfrak{D}|^{-1}\mathfrak{I}_2(\mathfrak{Z}\mathfrak{C}' + \mathfrak{D}')\mathfrak{I}_2^{-1}. \tag{173}$$

Moreover

$$|\mathfrak{F}_1 + \mathfrak{F}_2| = |\mathfrak{F}_1| + |\mathfrak{F}_2| + \sigma(\mathfrak{F}_1\mathfrak{I}_2\mathfrak{F}'_2\mathfrak{I}_2^{-1})$$

for any two matrices $\mathfrak{F}_1^{(2)}$ and $\mathfrak{F}_2^{(2)}$, whence

$$|\mathfrak{A}\mathfrak{Z} + \mathfrak{B}| = |\mathfrak{A}\mathfrak{Z}| + |\mathfrak{B}| + \sigma(\mathfrak{A}\mathfrak{Z}\mathfrak{I}_2\mathfrak{B}'\mathfrak{I}_2^{-1}) \tag{174}$$

$$|\mathfrak{C}\mathfrak{Z} + \mathfrak{D}| = |\mathfrak{C}\mathfrak{Z}| + |\mathfrak{D}| + \sigma(\mathfrak{C}\mathfrak{Z}\mathfrak{I}_2\mathfrak{D}'\mathfrak{I}_2^{-1}). \tag{175}$$

We apply (173), (174) and (175) for the calculation of

$$\hat{\mathfrak{Z}} = (\mathfrak{A}\mathfrak{Z} + \mathfrak{B})(\mathfrak{C}\mathfrak{Z} + \mathfrak{D})^{-1} \quad \text{and} \quad |\hat{\mathfrak{Z}}| = |\mathfrak{A}\mathfrak{Z} + \mathfrak{B}|\;|\mathfrak{C}\mathfrak{Z} + \mathfrak{D}|^{-1}.$$

It follows that

(176) $\hat{\mathfrak{W}} = (\mathfrak{A}\mathfrak{W}\mathfrak{J}_2\mathfrak{D}' + \mathfrak{B}\mathfrak{J}_2\mathfrak{W}\mathfrak{C}' + w_4\mathfrak{A}\mathfrak{J}_2\mathfrak{C}' + w_5\mathfrak{B}\mathfrak{J}_2\mathfrak{D}')\mathfrak{J}_2^{-1}$

(177) $\hat{w}_4 = \sigma(\mathfrak{A}\mathfrak{W}\mathfrak{J}_2\mathfrak{B}'\mathfrak{J}_2^{-1}) + |\mathfrak{A}|\, w_4 + |\mathfrak{B}|\, w_5$

(178) $\hat{w}_5 = \sigma(\mathfrak{C}\mathfrak{W}\mathfrak{J}_2\mathfrak{D}'\mathfrak{J}_2^{-1}) + |\mathfrak{C}|\, w_4 + |\mathfrak{D}|\, w_5$

with

$$\mathfrak{W} = \begin{pmatrix} w_1 & w_3 \\ w_3 & w_2 \end{pmatrix}, \qquad \hat{\mathfrak{W}} = \begin{pmatrix} \hat{w}_1 & \hat{w}_3 \\ \hat{w}_3 & \hat{w}_2 \end{pmatrix}$$

is a real linear substitution $\hat{\mathfrak{w}} = \mathfrak{V}\mathfrak{w}$ mapping the domain $\mathfrak{S}[\mathfrak{w}] = 0$, $\mathfrak{S}\{\mathfrak{w}\} > 0$ into itself. Hence $|\mathfrak{V}| = \nu \neq 0$, $|\nu^{-1/5}\mathfrak{V}| = 1$. Moreover, $\mathfrak{V}$ is not changed if we replace $\mathfrak{M}$ my $-\mathfrak{M}$. This proves the identity of $\Omega(\mathfrak{S})$ and the symplectic group Ω, for $n = 2$. By (171) and (178), the functional determinant of the transformation (172) has the value

$$(\nu^{-1/5}\hat{w}_5)^{-3} w_5{}^3 = \nu^{3/5}\, |\mathfrak{C}\mathfrak{Z} + \mathfrak{D}|^{-3};$$

on the other hand, by (24), $d\mathfrak{Z} = d\hat{\mathfrak{Z}}[\mathfrak{C}\mathfrak{Z} + \mathfrak{D}]$, which leads to the value $|\mathfrak{C}\mathfrak{Z} + \mathfrak{D}|^{-3}$ of that functional determinant; consequently $\nu = 1$, $|\mathfrak{V}| = 1$ and $\mathfrak{S}[\mathfrak{V}] = \mathfrak{S}$.

58. The formulae (176), (177), (178) and the identity of the groups $\Omega(\mathfrak{S})$ and Ω can be demonstrated in another way, without using Theorem 1.

Let us first determine all skew-symmetric symplectic matrices $\mathfrak{G}^{(4)}$. We have the conditions

(179) $$\mathfrak{G} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix} = -\mathfrak{G}'$$

(180) $\mathfrak{A}\mathfrak{B}' = \mathfrak{B}\mathfrak{A}', \qquad \mathfrak{C}\mathfrak{D}' = \mathfrak{D}\mathfrak{C}', \qquad \mathfrak{A}\mathfrak{D}' - \mathfrak{B}\mathfrak{C}' = \mathfrak{E}.$

By (179),

$$\mathfrak{A} = w_4\mathfrak{J}_2, \quad \mathfrak{D} = w_5\mathfrak{J}_2, \quad \mathfrak{B} = \mathfrak{W}\mathfrak{J}_2, \quad \mathfrak{C} = \mathfrak{J}_2\mathfrak{W}', \quad \mathfrak{W} = \begin{pmatrix} w_1 & w_3 \\ w_6 & w_2 \end{pmatrix}$$

with arbitrary $w_1, \cdots, w_6$; by (180), $w_4\mathfrak{W}$ and $w_5\mathfrak{W}$ are symmetric and $\mathfrak{W}\mathfrak{J}_2\mathfrak{W} = (w_4 w_5 - 1)\mathfrak{J}_2$. Hence either $\mathfrak{W}$ is non-symmetric and then, necessarily, $\mathfrak{G} = \pm\mathfrak{J}$ or $\mathfrak{W}$ is symmetric and

(181) $$w_1 w_2 - w_3{}^2 = w_4 w_5 - 1.$$

Omitting in the second case the condition (181), we obtain the identity

(182) $$(\mathfrak{J}\mathfrak{G})^2 = -\mathfrak{S}[\mathfrak{w}]\mathfrak{E}$$

with

$$\mathfrak{G} = \begin{pmatrix} w_4\mathfrak{J}_2 & \mathfrak{W}\mathfrak{J}_2 \\ \mathfrak{J}_2\mathfrak{W} & w_5\mathfrak{J}_2 \end{pmatrix}, \qquad \mathfrak{W} = \begin{pmatrix} w_1 & w_3 \\ w_3 & w_2 \end{pmatrix}$$

and arbitrary $w_1, \cdots, w_5$.

We substitute

$$\begin{aligned} w_1 &= -v_1 - v_2, \quad w_2 = v_1 - v_2, \quad w_3 = -v_3, \\ w_4 &= -v_4 - v_5, \quad w_5 = v_4 - v_5; \end{aligned} \tag{183}$$

then

$$\mathfrak{J}\mathfrak{G} = \begin{pmatrix} \mathfrak{J}_2\mathfrak{W} & w_5\mathfrak{J}_2 \\ -w_4\mathfrak{J}_2 & -\mathfrak{W}\mathfrak{J}_2 \end{pmatrix} \tag{184}$$

$$= \begin{pmatrix} -v_3 & v_1 - v_2 & 0 & v_4 - v_5 \\ v_1 + v_2 & v_3 & -v_4 + v_5 & 0 \\ 0 & v_4 + v_5 & -v_3 & v_1 + v_2 \\ -v_4 - v_5 & 0 & v_1 - v_2 & v_3 \end{pmatrix} = \sum_{k=1}^{5} v_k\mathfrak{F}_k,$$

$$\mathfrak{S}[\mathfrak{w}] = \sum_{k=1}^{5} (-1)^k v_k^2,$$

$$\begin{aligned} \mathfrak{F}_k^2 &= (-1)^{k-1}\mathfrak{E} \qquad (k = 1, \cdots, 5), \\ \mathfrak{F}_k\mathfrak{F}_l &= -\mathfrak{F}_l\mathfrak{F}_k \qquad (1 \leq k < l \leq 5), \end{aligned} \tag{185}$$

by (182). The 16 products $\mathfrak{F}_1^{e_1}\mathfrak{F}_2^{e_2}\mathfrak{F}_3^{e_3}\mathfrak{F}_4^{e_4}$ $(e_k = 0, 1;\ k = 1, \cdots, 4)$ form a basis for the four-dimensional complete matric representation of the well-known Clifford-Lipschitz algebra of order 16. The matrix $\mathfrak{F}_1\mathfrak{F}_2\mathfrak{F}_3\mathfrak{F}_4\mathfrak{F}_5$ is permutable with all matrices of the algebra and has the square $\mathfrak{E}$, hence it is equal to $\mathfrak{E}$ or $-\mathfrak{E}$; by direct calculation we find the value $\mathfrak{E}$ and therefore

$$\mathfrak{F}_5 = \mathfrak{F}_1\mathfrak{F}_2\mathfrak{F}_3\mathfrak{F}_4. \tag{186}$$

Let now $\hat{\mathfrak{w}} = \mathfrak{V}\mathfrak{w}$ be a real linear substitution with $\mathfrak{S}[\hat{\mathfrak{w}}] = \mathfrak{S}[\mathfrak{w}]$ and $|\mathfrak{V}| = 1$. We denote the matrix of the substitution (183) by $\mathfrak{L}$ and put $\mathfrak{L}^{-1}\mathfrak{V}\mathfrak{L} = \mathfrak{R} = (r_{kl})$. By (182) and (184), the matrices

$$\hat{\mathfrak{F}}_k = \sum_{l=1}^{5} r_{lk}\mathfrak{F}_l \qquad (k = 1, \cdots, 5) \tag{187}$$

satisfy again (185), and consequently their product is $\pm\mathfrak{E}$. It follows from (185), (186) and the linear independence of the 16 products that

$$\hat{\mathfrak{F}}_1\hat{\mathfrak{F}}_2\hat{\mathfrak{F}}_3\hat{\mathfrak{F}}_4\hat{\mathfrak{F}}_5 = |\mathfrak{R}|\,\mathfrak{E} = \mathfrak{E}; \tag{188}$$

hence (186) holds also for $\hat{\mathfrak{F}}_k$ instead of $\mathfrak{F}_k$.

Since the two representations generated by $\mathfrak{F}_k$ and $\hat{\mathfrak{F}}_k$ are necessarily equivalent, there exists a real matrix $\mathfrak{M}$, such that

$$\hat{\mathfrak{F}}_k = \mathfrak{M}^{-1}\mathfrak{F}_k\mathfrak{M} \qquad (k = 1, \cdots, 5). \tag{189}$$

Moreover, by (184) and (187), the matrices $\mathfrak{J}\mathfrak{F}_k$ and $\mathfrak{J}\hat{\mathfrak{F}}_k$ are skew-symmetric, and consequently (189) leads to

$$\mathfrak{J}\mathfrak{M}^{-1}\mathfrak{F}_k\mathfrak{M} = \mathfrak{M}'\mathfrak{J}\mathfrak{F}_k\mathfrak{J}\mathfrak{M}'^{-1}\mathfrak{J}^{-1} \qquad (k = 1, \cdots, 5).$$

This proves that $\mathfrak{M}\mathfrak{J}\mathfrak{M}'\mathfrak{J}^{-1}$ is a scalar multiple of $\mathfrak{E}$. There is an arbitrary real scalar factor in $\mathfrak{M}$; hence we may assume $\mathfrak{J}[\mathfrak{M}] = \pm\mathfrak{J}$. Putting

$$\hat{\mathfrak{G}} = \begin{pmatrix} \hat{w}_4\mathfrak{J}_2 & \hat{\mathfrak{W}}\mathfrak{J}_2 \\ \mathfrak{J}_2\hat{\mathfrak{W}} & \hat{w}_5\mathfrak{J}_2 \end{pmatrix} = \sum_{k=1}^{5} v_k\mathfrak{J}^{-1}\hat{\mathfrak{F}}_k, \tag{190}$$

we obtain

$$\hat{\mathfrak{G}} = \pm\mathfrak{G}[\mathfrak{M}] \tag{191}$$

or more explicitly

$$\begin{pmatrix} \hat{w}_4\mathfrak{J}_2 & \hat{\mathfrak{W}}\mathfrak{J}_2 \\ \mathfrak{J}_2\hat{\mathfrak{W}} & \hat{w}_5\mathfrak{J}_2 \end{pmatrix} = \pm\mathfrak{M}'\begin{pmatrix} w_4\mathfrak{J}_2 & \mathfrak{W}\mathfrak{J}_2 \\ \mathfrak{J}_2\mathfrak{W} & w_5\mathfrak{J}_2 \end{pmatrix}\mathfrak{M}. \tag{192}$$

On the other hand, if $\mathfrak{M}$ is any real matrix satisfying $\mathfrak{J}[\mathfrak{M}] = \pm\mathfrak{J}$, then the matrix $\hat{\mathfrak{G}}$ in (191) is again a skew-symmetric solution of (182) and consequently of the form (190), and (192) defines a real linear substitution $\hat{\mathfrak{w}} = \mathfrak{V}\mathfrak{w}$ with $\mathfrak{S}[\mathfrak{V}] = \mathfrak{S}$ and $|\mathfrak{V}| = 1$, by (188). We may replace $\mathfrak{M}$ by $-\mathfrak{M}$ and obtain the same matrix $\mathfrak{V}$, but the pair $\mathfrak{M}, -\mathfrak{M}$ is uniquely determined by $\mathfrak{V}$.

Imposing on $\mathfrak{V}$ the condition $\mathfrak{J}[\mathfrak{M}] = +\mathfrak{J}$, we obtain a subgroup of index 2 in the group of all $\mathfrak{V}$; and this subgroup is isomorphic to the inhomogeneous symplectic group, by (192). If we write

$$\mathfrak{M}' = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$$

and calculate the single terms in (192), we find exactly the formulae (176), (177) and (178).

59. Let K be again a totally real algebraic number field of degree h. Let $\mathfrak{T}[\mathfrak{v}]$ be a quinary quadratic form with coefficients in K such that all conjugates except $\mathfrak{T}[\mathfrak{v}]$ itself are definite. We assume, moreover, that $\mathfrak{T}[\mathfrak{v}]$ has the signature 2, 3, i. e., that $\mathfrak{T}[\mathfrak{v}]$ can be transformed into $-v_1^2 + v_2^2 - v_3^2 + v_4^2 - v_5^2$ by a real linear substitution. Then there exists also a real matrix $\mathfrak{N}$, such that $\mathfrak{T}[\mathfrak{N}] = \mathfrak{S}$.

Consider now the units of $\mathfrak{T}$ in K, i. e., the integral matrices $\mathfrak{U}$ in K

satisfying $\mathfrak{T}[\mathfrak{U}] = \mathfrak{T}$. Since $|\mathfrak{U}| = \pm 1$ and $|-\mathfrak{U}| = -|\mathfrak{U}|$, we restrict ourselves to the case $|\mathfrak{U}| = +1$. Then the matrix $\mathfrak{R}^{-1}\mathfrak{U}\mathfrak{R} = \mathfrak{B}$ satisfies $\mathfrak{S}[\mathfrak{B}] = \mathfrak{S}$, $|\mathfrak{B}| = 1$, and the corresponding substitution (170) transforms H either into itself or into $\bar{H}$. We consider only the matrices $\mathfrak{U}$ with the first property; they form a subgroup of index 2 or 1 in the whole group of units with $|\mathfrak{U}| = 1$; we denote it by $\Lambda(\mathfrak{T})$, and by $\Delta(\mathfrak{T})$ the isomorphic subgroup of Ω.

Let us first prove that $\Delta(\mathfrak{T})$ is discontinuous. By Section **19**, it is sufficient to prove that $\Delta(\mathfrak{T})$ does not contain an infinite number of bounded elements. Otherwise $\Lambda(\mathfrak{T})$ would also contain infinitely many bounded matrices $\mathfrak{U}$, by (176), (177), (178) and $\mathfrak{U} = \mathfrak{R}\mathfrak{B}\mathfrak{R}^{-1}$. Since $\mathfrak{T}[\mathfrak{U}] = \mathfrak{T}$ and all conjugates of $\mathfrak{J}[\mathfrak{v}]$, except $\mathfrak{J}[\mathfrak{v}]$ itself, are definite, all conjugates of these matrices are bounded. Moreover their elements are integers, and this is a contradiction.

We apply now the following results from the theory of units of quadratic forms. Let Q be the space of real matrices $\mathfrak{Q}^{(32)}$ satisfying

$$\mathfrak{S}[\mathfrak{P}] > 0, \qquad \mathfrak{P}^{(52)} = \begin{pmatrix} \mathfrak{Q} \\ \mathfrak{E} \end{pmatrix}.$$

If

$$\mathfrak{B} = \begin{pmatrix} \mathfrak{B}_1 & \mathfrak{B}_2 \\ \mathfrak{B}_3 & \mathfrak{B}_4 \end{pmatrix}$$

is a real solution of $\mathfrak{S}[\mathfrak{B}] = \mathfrak{S}$, with $\mathfrak{B}_1 = \mathfrak{B}_1^{(3)}$, then the mapping

$$\mathfrak{Q} \rightarrow (\mathfrak{B}_1\mathfrak{Q} + \mathfrak{B}_2)(\mathfrak{B}_3\mathfrak{Q} + \mathfrak{B}_4)^{-1}$$

transforms Q into itself. We restrict $\mathfrak{B}$ to the matrices $\mathfrak{R}^{-1}\mathfrak{U}\mathfrak{R}$, where $\mathfrak{U}$ runs over the units of $\mathfrak{T}$ with $|\mathfrak{U}| = 1$. Then there exists in Q a fundamental domain Q_0, with respect to $\Lambda(\mathfrak{T})$, bounded by a finite number of algebraic surfaces and having only a finite number of neighbors. Moreover the integral

$$v(\mathfrak{T}) = \int_{Q_0} |\mathfrak{S}[\mathfrak{P}]|^{-5/2} d\mathfrak{Q} \tag{193}$$

has a finite value. As a matter of fact, a proof of these statements has been published only in the case of the field of rational numbers, instead of a totally real algebraic field K of arbitrary degree h; but the generalization of this proof offers no difficulties.

60. In order to derive the corresponding results for the group $\Delta(\mathfrak{T})$ and the space H, we have only to map Q onto H. If

(194) $$\mathfrak{Z} = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix} \subset H, \qquad z_4 = |\mathfrak{Z}|, \qquad z_5 = 1,$$

we define

$$\mathfrak{z} = \mathfrak{x} + i\mathfrak{y}, \qquad \mathfrak{P} = (\mathfrak{x}\mathfrak{y})\begin{pmatrix} x_4 & y_4 \\ 1 & 0 \end{pmatrix}^{-1} = \frac{1}{2iy_4^2}(\mathfrak{z}\bar{\mathfrak{z}})\begin{pmatrix} 1 & -\bar{z}_4 \\ -1 & z_4 \end{pmatrix};$$

then the elements of $\mathfrak{Q} = (q_{kl})$ are

$$q_{k1} = \frac{y_k}{y_4}, \qquad q_{k2} = \frac{x_k y_4 - y_k x_4}{y_4} \qquad (k = 1, 2, 3)$$

and

$$\mathfrak{S}[\mathfrak{P}] = \frac{1}{2y_4^2}\mathfrak{S}\{\mathfrak{z}\}\mathfrak{E}\begin{bmatrix} 0 & y_4 \\ 1 & -x_4 \end{bmatrix} > 0;$$

hence $\mathfrak{Q}$ is a point of Q. On the other hand, if $\mathfrak{Q}$ is an arbitrary point of Q, we determine z_4 from the quadratic equation

(195) $$\mathfrak{S}[\mathfrak{P}]\begin{bmatrix} z_4 \\ 1 \end{bmatrix} = 0$$

and put

(196) $$\mathfrak{P}\begin{pmatrix} z_4 \\ 1 \end{pmatrix} = \mathfrak{z};$$

then

$$\mathfrak{S}[\mathfrak{z}] = 0, \qquad \mathfrak{S}\{\mathfrak{z}\} = \mathfrak{S}[\mathfrak{P}]\left\{ \begin{matrix} z_4 \\ 1 \end{matrix} \right\} > 0.$$

If we replace z_4 by the other root $\bar{z}_4$ of (195), the column $\mathfrak{z}$ is replaced by $\bar{\mathfrak{z}}$; therefore we can choose the root z_4 of this quadratic equation, such that $y_1 > 0$, and then (194) is satisfied.

In this way, the fundamental domain Q_0 for $\Lambda(\mathfrak{T})$ in Q is mapped onto a fundamental domain F for $\Delta(\mathfrak{T})$ in H. It follows that F has only a finite number of neighbors $F_{\mathfrak{M}}$, for the elements $\mathfrak{M}$ of $\Delta(\mathfrak{T})$, and that any compact domain in H is covered by a finite number of images $F_{\mathfrak{M}}$; moreover F is bounded by a finite number of algebraic surfaces. Putting $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$ and introducing the new variables $\mathfrak{X}, \mathfrak{Y}$ into (193), by (195) and (196), we obtain

$$v(\mathfrak{T}) = 4\int_F |\mathfrak{Y}|^{-3} d\mathfrak{X} d\mathfrak{Y} = 4\int_F d\mathfrak{X} d\mathfrak{Y}^{-1}.$$

This proves that F has a finite symplectic volume.

The latter result is not trivial in the case $h = 1$, since then H is not compact relative to $\Delta(\mathfrak{T})$; this may be derived from the theorem of A. Meyer, that an indefinite quinary quadratic form with rational coefficients is a zero form. On the other hand, $\mathfrak{T}[\mathfrak{v}]$ is not a zero form in K in the case $h > 1$, since we assumed that the conjugates of $\mathfrak{T}[\mathfrak{v}]$ are definite except $\mathfrak{T}[\mathfrak{v}]$ itself; it can be proved as a simple consequence that then F is compact.

This is a sketch of the proof of Theorem 14; the details may be completed according to the scheme of Chapter VII.

Consider now the invariant subgroup $\Delta_\kappa(\mathfrak{T})$ of $\Delta(\mathfrak{T})$, defined by the condition $\mathfrak{U} \equiv \mathfrak{E} \pmod{\kappa}$ for the units $\mathfrak{U}$ of $\mathfrak{T}$, where κ denotes, as in Theorem 10, a certain power of an arbitrary prime ideal. It follows from Section **39**, that $\Delta_\kappa(\mathfrak{T})$ has no fixed points in H. The subgroup $\Delta_\kappa(\mathfrak{T})$ is of finite index j in $\Delta(\mathfrak{T})$, and the union of j images $F_{\mathfrak{M}}$ of F, for suitably chosen elements $\mathfrak{M}$ of $\Delta(\mathfrak{T})$, constitutes a fundamental domain F_κ of $\Delta_\kappa(\mathfrak{T})$. Since the domain F_κ is compact in the case $h > 1$, it gives another example of a closed manifold with the symplectic metric.

It is known that the volume $v(\mathfrak{T})$ appears in the formula for the measure of the genus of $\mathfrak{T}$. In this way an analogue of Theorem 12 might be found.

61. We proved in Section **27**, that $\Delta(\mathfrak{G}, \mathfrak{H})$ is commensurable with a group $\Delta(r, s)$ of symplectic quaternion matrices $\pm \mathfrak{M}$. We shall now derive a corresponding result for the group $\Delta(\mathfrak{T})$.

A matrix of rank r is called *primitive*, if its elements are algebraic integers and if the minors of degree r are relative prime. Let $\mathfrak{W}_0^{(24)}$ be a primitive matrix of rank 2. Then the matrix $\mathfrak{J}[\mathfrak{W}_0] = \mathfrak{G}^{(4)} = (g_{kl})$ is skew-symmetric and has the rank 2; its elements are the minors of $\mathfrak{W}_0$. It follows by an application of Laplace's theorem, that also $\mathfrak{G}$ is primitive.

LEMMA 25. *Let $\mathfrak{G}^{(4)}$ be a primitive skew-symmetric matrix of rank 2, with elements from an algebraic number field K_0. Then there exists in K_0 a primitive matrix $\mathfrak{W}_0$, such that $\mathfrak{J}_0[\mathfrak{W}_0] = \mathfrak{G}$.*

Since $\mathfrak{G}$ is a primitive matrix of rank 2 and degree 4, with elements from K_0, we can determine in K_0 a unimodular matrix $\mathfrak{U}_0$, such that the first two columns of $\mathfrak{G}\mathfrak{U}_0$ are zero. Moreover the matrix $\mathfrak{G}[\mathfrak{U}_0]$ is skew-symmetric and again primitive; hence

$$\mathfrak{G}[\mathfrak{U}_0] = \epsilon \begin{pmatrix} 0 & 0 \\ 0 & \mathfrak{J}_2 \end{pmatrix},$$

where ϵ is an algebraic unit in K_0. Obviously we may choose $\mathfrak{U}_0$, such that $\epsilon = 1$. Denoting by $\mathfrak{W}_0$ the matrix of the two last rows of $\mathfrak{U}_0^{-1}$, we obtain the statement of the lemma.

For any skew-symmetric $\mathfrak{G}^{(4)} = (g_{kl})$,

$$|\mathfrak{G}| = (g_{12}g_{34} - g_{13}g_{24} + g_{14}g_{23})^2$$

and consequently

$$g_{12}g_{34} - g_{13}g_{24} + g_{14}g_{23} = 0, \tag{197}$$

if the rank of $\mathfrak{G}$ is < 4. It follows from (197) that the 36 minors of $\mathfrak{G}$, of degree 2, have the values $\pm g_{kl}g_{pq}$ $(1 \leq k < l \leq 4;\ 1 \leq p < q \leq 4)$. This proves that the skew-symmetric matrix $\mathfrak{G}^{(4)}$ is a primitive matrix of rank 2, if and only if (197) holds and the six numbers g_{kl} $(1 \leq k < l \leq 4)$ are relative prime.

Let $\mathfrak{W}_0 = (\mathfrak{C}_1{}^{(2)}\mathfrak{D}_1{}^{(2)})$ be the matrix of Lemma 25; then $\mathfrak{C}_1\mathfrak{D}'_1 - \mathfrak{D}_1\mathfrak{C}'_1 = (g_{13} + g_{24})\mathfrak{J}_2$, and consequently the relationship $\mathfrak{C}_1\mathfrak{D}'_1 = \mathfrak{D}_1\mathfrak{C}'_1$ holds, if and only if the condition

$$g_{13} + g_{24} = 0 \tag{198}$$

is satisfied. Since $\mathfrak{W}_0\mathfrak{U}_0 = (0\mathfrak{E})$, the equation $\mathfrak{A}_0\mathfrak{D}'_1 - \mathfrak{B}_0\mathfrak{C}'_1 = \mathfrak{E}$ has an integral solution $\mathfrak{A}_0, \mathfrak{B}_0$ in K_0. Then the matrices $\mathfrak{A}_1 = \mathfrak{A}_0 - \mathfrak{B}_0\mathfrak{A}'_0\mathfrak{C}_1$ and $\mathfrak{B}_1 = \mathfrak{B}_0 - \mathfrak{B}_0\mathfrak{A}'_0\mathfrak{D}_1$ satisfy

$$\mathfrak{A}_1\mathfrak{B}'_1 - \mathfrak{B}_1\mathfrak{A}'_1 = \mathfrak{B}_0\mathfrak{A}'_0(\mathfrak{C}_1\mathfrak{D}'_1 - \mathfrak{D}_1\mathfrak{C}'_1)\mathfrak{A}_0\mathfrak{B}'_0,$$
$$\mathfrak{A}_1\mathfrak{D}'_1 - \mathfrak{B}_1\mathfrak{C}'_1 = \mathfrak{E} - \mathfrak{B}_0\mathfrak{A}'_0(\mathfrak{C}_1\mathfrak{D}'_1 - \mathfrak{D}_1\mathfrak{C}'_1),$$

and the matrix

$$\mathfrak{M}_1 = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{C}_1 & \mathfrak{D}_1 \end{pmatrix}, \tag{199}$$

with integral elements in K_0 and the second matrix row $\mathfrak{W}_0$, is symplectic, if (198) is fulfilled.

62. We consider again the substitution $\hat{\mathfrak{w}} = \mathfrak{V}\mathfrak{w}$ with $\mathfrak{S}[\hat{\mathfrak{w}}] = \mathfrak{S}[\mathfrak{w}]$ and $|\mathfrak{V}| = 1$. We assume now that the elements v_{kl} of $\mathfrak{V}$ are integers in a real algebraic field K_0 and that $\mathfrak{V} \equiv \mathfrak{E} \pmod 2$. We define

$$g_{14} = v_{51},\ g_{23} = -v_{52},\ g_{24} = \tfrac{1}{2}v_{53},\ g_{13} = -\tfrac{1}{2}v_{53},\ g_{12} = v_{54},\ g_{34} = v_{55}.$$

Then (198) is satisfied, and also (197), as a consequence of $\mathfrak{S}^{-1}[\mathfrak{V}'] = \mathfrak{S}^{-1}$. Since $|\mathfrak{V}| = 1$ and $v_{53} \equiv 0 \pmod 2$, the 6 numbers g_{kl} $(1 \leq k < l \leq 4)$ are relative prime. By the results of the last section, the matrix $\mathfrak{M}_1$ of (199) is symplectic with integral elements in K_0 and $\mathfrak{J}_2[\mathfrak{C}_1\mathfrak{D}_1] = \mathfrak{G} = (g_{kl})$, whence

$$\hat{w}_5 = \sum_{l=1}^{5} v_{5l}w_l = \sigma(\mathfrak{C}_1\mathfrak{W}\mathfrak{J}_2\mathfrak{D}'_1\mathfrak{J}_2^{-1}) + |\mathfrak{C}_1|\, w_4 + |\mathfrak{D}_1|\, w_5. \tag{200}$$

Let $\mathfrak{V}_1$ be the matrix of the linear transformation (176), (177), (178) with $\mathfrak{M}_1$ instead of $\mathfrak{M}$. By (178) and (200), the matrices $\mathfrak{V}$ and $\mathfrak{V}_1$ have the same fifth row, hence $(0\,0\,0\,0\,1)$ is the fifth row of $\mathfrak{V}\mathfrak{V}_1^{-1} = \mathfrak{V}_2$. Putting

$$\mathfrak{M}\mathfrak{M}_1^{-1} = \mathfrak{M}_2 = \begin{pmatrix} \mathfrak{A}_2 & \mathfrak{B}_2 \\ \mathfrak{C}_2 & \mathfrak{D}_2 \end{pmatrix},$$

we infer from (168) that

$$|\mathfrak{D}_2| = 1, \quad |\mathfrak{C}_2| = 0 \quad \text{and} \quad \sigma(\mathfrak{C}_2\mathfrak{W}\mathfrak{F}_2\mathfrak{D}'_2\mathfrak{F}_2^{-1}) = \sigma(\mathfrak{W}\mathfrak{D}_2^{-1}\mathfrak{C}_2) = 0,$$

whence $\mathfrak{C}_2 = 0$ and $\mathfrak{A}_2\mathfrak{D}'_2 = \mathfrak{E}$. The corresponding linear transformation (176) takes the simpler form

(201) $$\hat{\mathfrak{W}} = \mathfrak{W}[\mathfrak{A}'_2] + w_5\mathfrak{B}_2\mathfrak{A}'_2.$$

Obviously $\mathfrak{B}_1$ is unimodular in K_0, hence the same is true for the matrix $\mathfrak{B}_2$, and the coefficients in (201) are integers. Let

$$\mathfrak{A}_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then a^2, b^2, c^2, d^2 are necessarily integers, hence also a, b, c, d. Moreover $\mathfrak{B}_2\mathfrak{A}'_2$ is integral and $|\mathfrak{A}_2| = 1$; hence $\mathfrak{B}_2$ is integral. This proves that $\mathfrak{M} = \mathfrak{M}_2\mathfrak{M}_1$ has integral elements. Since $|\mathfrak{M}| = 1$, these elements are relative prime.

On the other hand, by (176), (177) and (178), the elements of $\mathfrak{M}$ satisfy a system of algebraic equations with coefficients in K_0, and the only solutions of these equations are $\mathfrak{M}$ and $-\mathfrak{M}$. It follows that $\sqrt{t}\mathfrak{M} = \mathfrak{F}$, where $\mathfrak{F}$ is a matrix in K_0 and t is a number $\neq 0$ in K_0.

Since $\sqrt{t}$ is the greatest common divisor of the elements of $\mathfrak{F}$, the principal ideal (t) is the square of an ideal $\mathfrak{a}$ in K_0. Let $A_1 = E, A_2, \cdots, A_g$ denote the ambiguous classes of ideals in K_0, i. e., the classes A satisfying $A^2 = E$, where E is the principal class. We choose an integral ideal $\mathfrak{a}_k$ in A_k $(k = 2, \cdots, g)$ and take $\mathfrak{a}_1 = (1)$; then $\mathfrak{a}_k^2 = (a_k)$ is a principal ideal and $a_1 = 1$. Let $u_1, \cdots, u_s$ be a complete system of fundamental units in K_0 and denote by f_l $(l = 1, \cdots, 2^{s+1})$ the 2^{s+1} products $(-1)^{e_0}u_1^{e_1} \cdots u_s^{e_s}$ $(e_k = 0, 1;\ k = 0, \cdots, s)$, in particular $f_1 = 1$. The products a_kf_l are all different; we denote them by $t_1, \cdots, t_m$ with $m = 2^{s+1}g$ and $t_1 = a_1f_1 = 1$. Obviously $t = t_qv^2$, where t_q is one of the numbers $t_1, \cdots, t_m$ and v is a number in K_0.

None of the numbers $t_2, \cdots, t_m$ is a square in K_0. We choose now an integral ideal ω_0 in K_0, such that none of those numbers is a quadratic residue modulo ω_0. If $\mathfrak{B} \equiv \mathfrak{E}$ (mod $2\omega_0$), then $|\mathfrak{D}| \equiv 1$, $|\mathfrak{A}| \equiv 1$, $\mathfrak{C} \equiv 0$, $\mathfrak{B} \equiv 0$, by (176), (177) and (178). Moreover $\mathfrak{A}\mathfrak{D}' \equiv \mathfrak{E}$, and the coefficients of $\mathfrak{W}[\mathfrak{A}'] - \mathfrak{W}$ are $\equiv 0$. Putting

$$\mathfrak{A} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \qquad \mathfrak{D} = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix},$$

we obtain

(202) $a_1^2 \equiv 1, \quad a_1 \equiv a_4 \equiv d_1 \equiv d_4, \quad a_2 \equiv a_3 \equiv d_2 \equiv d_3 \equiv 0 \pmod{2\omega_0}.$

But $\sqrt{t_q}\, a_1 = x$ is an integer in K_0; hence $x^2 \equiv t_q \pmod{\omega_0}$, $t_q = t_1 = 1$.

We have proved that $\mathfrak{M}$ is an integral matrix in K_0, if $\mathfrak{B}$ is an integral matrix in K_0 satisfying $\mathfrak{S}[\mathfrak{B}] = \mathfrak{S}$, $|\mathfrak{B}| = 1$ and $\mathfrak{B} \equiv \mathfrak{E} \pmod{2\omega_0}$.

63. Let $\mathfrak{T}[\mathfrak{v}]$ be the quinary quadratic form of Section **59**. There exists in K a matrix $\mathfrak{L}_0$, such that

$$\mathfrak{T}[\mathfrak{L}_0\mathfrak{v}] = m(-pv_1^2 + v_2^2 - qv_3^2 + rsv_4^2 - rv_5^2)$$

with integral positive m, p, q, r, s. Putting

$$(pqs)^{-1} = m_2, \quad pm_2 = m_1, \quad qm_2 = m_3, \quad rsm_2 = m_4, \quad rm_2 = m_5,$$

we have

$$\prod_{k=1}^{5} m_k = r^2 m_2^4, \qquad -m^{-1}m_2\mathfrak{T}[\mathfrak{L}_0\mathfrak{v}] = \sum_{k=1}^{5} (-1)^{k-1} m_k v_k^2. \tag{203}$$

Let $\mathfrak{L}_1$ be the matrix of the linear substitution

$$\begin{aligned} w_1 &= -v_1\sqrt{m_1} - v_2\sqrt{m_2}, \quad w_2 = v_1\sqrt{m_1} - v_2\sqrt{m_2}, \quad w_3 = -v_3\sqrt{m_3}, \\ w_4 &= -v_4\sqrt{m_4} - v_5\sqrt{m_5}, \quad w_5 = v_4\sqrt{m_4} - v_5\sqrt{m_5} \end{aligned} \tag{204}$$

and let $\mathfrak{L}_0\mathfrak{L}_1^{-1} = \mathfrak{R}_1$; then $m^{-1}m_2\mathfrak{T}[\mathfrak{R}_1] = \mathfrak{S}$.

By (185) and (186), the matrices

$$\mathfrak{Q}_k = \sqrt{m_k}\,\mathfrak{F}_k \qquad (k = 1, \cdots, 5)$$

satisfy the conditions

$$\mathfrak{Q}_k\mathfrak{Q}_l = -\mathfrak{Q}_l\mathfrak{Q}_k \ (1 \leq k < l \leq 5), \quad \mathfrak{Q}_k^2 = (-1)^{k-1}m_k\mathfrak{E} \ (k = 1, \cdots, 5), \qquad \prod_{k=1}^{5} \mathfrak{Q}_k = rm_2^2\mathfrak{E}. \tag{205}$$

Using the abbreviations

$$\mathfrak{J}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathfrak{J}_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathfrak{J}_3 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$\sqrt{p} = \rho_1, \quad \sqrt{s} = \rho_2, \quad \sqrt{q} = \rho_3, \quad \sqrt{r} = \rho_4,$$

we introduce the 16 linearly independent matrices

$$\mathfrak{P}_1 = \begin{pmatrix} \mathfrak{E} & 0 \\ 0 & \mathfrak{E} \end{pmatrix}, \qquad \mathfrak{P}_2 = m_2^{-1}\mathfrak{Q}_1\mathfrak{Q}_2 = \rho_1 \begin{pmatrix} -\mathfrak{J}_3 & 0 \\ 0 & \mathfrak{J}_3 \end{pmatrix},$$

$$\mathfrak{P}_3 = m_2^{-1}s\mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3 = \rho_2 \begin{pmatrix} -\mathfrak{E} & 0 \\ 0 & \mathfrak{E} \end{pmatrix}, \qquad \mathfrak{P}_4 = ps\mathfrak{Q}_3 = \rho_1\rho_2 \begin{pmatrix} \mathfrak{J}_3 & 0 \\ 0 & \mathfrak{J}_3 \end{pmatrix},$$

$$\mathfrak{P}_5 = m_2^{-1}\mathfrak{Q}_2\mathfrak{Q}_3 = \rho_3 \begin{pmatrix} -\mathfrak{J}_1 & 0 \\ 0 & \mathfrak{J}_1 \end{pmatrix}, \qquad \mathfrak{P}_6 = m_2^{-1}\mathfrak{Q}_1\mathfrak{Q}_3 = \rho_1\rho_3 \begin{pmatrix} \mathfrak{J}_2 & 0 \\ 0 & \mathfrak{J}_2 \end{pmatrix},$$

$$\mathfrak{P}_7 = qs\mathfrak{Q}_1 = \rho_2\rho_3 \begin{pmatrix} \mathfrak{J}_1 & 0 \\ 0 & \mathfrak{J}_1 \end{pmatrix}, \qquad \mathfrak{P}_8 = m_2^{-1}\mathfrak{Q}_2 = \rho_1\rho_2\rho_3 \begin{pmatrix} -\mathfrak{J}_2 & 0 \\ 0 & \mathfrak{J}_2 \end{pmatrix},$$

$$\mathfrak{P}_9 = m_2^{-1}\mathfrak{Q}_1\mathfrak{Q}_3\mathfrak{Q}_4 = \rho_4 \begin{pmatrix} 0 & -\mathfrak{E} \\ -\mathfrak{E} & 0 \end{pmatrix}, \qquad \mathfrak{P}_{10} = m_2^{-1}p\mathfrak{Q}_2\mathfrak{Q}_3\mathfrak{Q}_4 = \rho_1\rho_4 \begin{pmatrix} 0 & -\mathfrak{J}_3 \\ \mathfrak{J}_3 & 0 \end{pmatrix},$$

$$\mathfrak{P}_{11} = m_2^{-1}\mathfrak{Q}_2\mathfrak{Q}_4 = \rho_2\rho_4 \begin{pmatrix} 0 & \mathfrak{E} \\ -\mathfrak{E} & 0 \end{pmatrix}, \qquad \mathfrak{P}_{12} = m_2^{-1}\mathfrak{Q}_1\mathfrak{Q}_4 = \rho_1\rho_2\rho_4 \begin{pmatrix} 0 & \mathfrak{J}_3 \\ \mathfrak{J}_3 & 0 \end{pmatrix},$$

$$\mathfrak{P}_{13} = m_2^{-1}q\mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_4 = \rho_3\rho_4 \begin{pmatrix} 0 & \mathfrak{J}_1 \\ -\mathfrak{J}_1 & 0 \end{pmatrix}, \qquad \mathfrak{P}_{14} = pq\mathfrak{Q}_4 = \rho_1\rho_3\rho_4 \begin{pmatrix} 0 & \mathfrak{J}_2 \\ \mathfrak{J}_2 & 0 \end{pmatrix},$$

$$\mathfrak{P}_{15} = m_2^{-1}\mathfrak{Q}_3\mathfrak{Q}_4 = \rho_2\rho_3\rho_4 \begin{pmatrix} 0 & -\mathfrak{J}_1 \\ -\mathfrak{J}_1 & 0 \end{pmatrix}, \qquad \mathfrak{P}_{16} = m_2^{-2}\mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3\mathfrak{Q}_4 = \rho_1\rho_2\rho_3\rho_4 \begin{pmatrix} 0 & -\mathfrak{J}_2 \\ \mathfrak{J}_2 & 0 \end{pmatrix}.$$

Then any real matrix $\mathfrak{M}^{(4)}$ can be expressed in the form

$$\mathfrak{M} = \sum_{k=1}^{16} x_k \mathfrak{P}_k \tag{206}$$

with uniquely determined real scalar factors x_k.

We denote the real algebraic number field $K(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{s})$ by K_0. Let ω_0 be the ideal of the preceding section and choose in K an ideal ω having the corresponding properties with respect to K instead of K_0. We put $4pqrs\omega\omega_0 = \mu$.

On account of (203) and (204), the elements of the matrix $\mathfrak{N}_1$ lie in K_0. Let f be an integer $\neq 0$, such that $f\mathfrak{N}_1$ and $f\mathfrak{N}_1^{-1}$ are integral, and choose in K an ideal ν which is divisible by $f^2\mu$. We consider now the elements $\mathfrak{U}$ of the congruence subgroup $\Lambda_\nu(\mathfrak{T})$ of $\Lambda(\mathfrak{T})$ defined by condition $\mathfrak{U} \equiv \mathfrak{E} \pmod{\nu}$. Then $\mathfrak{V} = \mathfrak{N}_1^{-1}\mathfrak{U}\mathfrak{N}_1$ is an integral matrix in K_0 satisfying $\mathfrak{S}[\mathfrak{V}] = \mathfrak{S}$, $|\mathfrak{V}| = 1$ and $\mathfrak{V} \equiv \mathfrak{E} \pmod{\mu}$. The corresponding symplectic matrices $\pm\mathfrak{M}$ form a subgroup $\Delta_\nu(\mathfrak{T})$ of $\Delta(\mathfrak{T})$.

By Section **58**, the pair $\mathfrak{M}, -\mathfrak{M}$ is uniquely determined by the conditions

$$\hat{\mathfrak{Q}}_k = \mathfrak{M}^{-1}\mathfrak{Q}_k\mathfrak{M} \ (k = 1, \cdots, 5), \qquad \mathfrak{J}[\mathfrak{M}] = \mathfrak{J} \tag{207}$$

with

$$\hat{\mathfrak{Q}}_k = \sum_{l=1}^{5} r_{lk}\mathfrak{Q}_l \ (k = 1, \cdots, 5), \qquad (r_{kl}) = \mathfrak{L}_0^{-1}\mathfrak{U}\mathfrak{L}_0. \tag{208}$$

On account of the result of Section **62**, the coefficients x_k in (206) are numbers of K_0. We apply any isomorphism of K_0 which leaves all numbers of K

invariant and denote by $\mathfrak{P}^*_k$, $\mathfrak{Q}^*_k$, $\hat{\mathfrak{Q}}^*_k$, x^*_k the images of $\mathfrak{P}_k$, $\mathfrak{Q}_k$, $\hat{\mathfrak{Q}}_k$, x_k. Then (205) and (208) hold good with $\mathfrak{Q}^*_k$, $\hat{\mathfrak{Q}}^*_k$ instead of $\mathfrak{Q}_k$, $\hat{\mathfrak{Q}}_k$, and the same is true for the relationship

$$\mathfrak{Q}'_k = \mathfrak{J}^{-1}\mathfrak{Q}_k\mathfrak{J} = (\mathfrak{Q}_2\mathfrak{Q}_4)^{-1}\mathfrak{Q}_k(\mathfrak{Q}_2\mathfrak{Q}_4) \qquad (k = 1, \cdots, 5).$$

It follows that both matrices

$$\mathfrak{M}^* = \sum_{k=1}^{16} x^*_k\mathfrak{P}^*_k, \qquad \mathfrak{M}_0 = \sum_{k=1}^{16} x_k\mathfrak{P}^*_k$$

are solutions of (207), with $\mathfrak{Q}^*_k$, $\hat{\mathfrak{Q}}^*_k$ instead of $\mathfrak{Q}_k$, $\hat{\mathfrak{Q}}_k$, and consequently

$$\mathfrak{M}^* = \pm \mathfrak{M}_0, \qquad x^*_k = \pm x_k \qquad (k = 1, \cdots, 16).$$

Putting

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix},$$

we have

$$\mathfrak{A} = \begin{pmatrix} x_1 + x_2\rho_1 - x_3\rho_2 - x_4\rho_1\rho_2 & (-x_5 + x_6\rho_1 + x_7\rho_2 - x_8\rho_1\rho_2)\rho_3 \\ (-x_5 - x_6\rho_1 + x_7\rho_2 + x_8\rho_1\rho_2)\rho_3 & x_1 - x_2\rho_1 - x_3\rho_2 + x_4\rho_1\rho_2 \end{pmatrix},$$

$$\mathfrak{D} = \begin{pmatrix} x_1 - x_2\rho_1 + x_3\rho_2 - x_4\rho_1\rho_2 & (x_5 + x_6\rho_1 + x_7\rho_2 + x_8\rho_1\rho_2)\rho_3 \\ (x_5 - x_6\rho_1 + x_7\rho_2 - x_8\rho_1\rho_2)\rho_3 & x_1 + x_2\rho_1 + x_3\rho_2 + x_4\rho_1\rho_2 \end{pmatrix};$$

if we replace x_k by $(-1)^k x_{k+8}\rho_4$ $(k = 1, \cdots, 8)$, we obtain the expressions for $\mathfrak{B}$, $\mathfrak{C}$. By (176), (177) and (178), $\mathfrak{B} \equiv 0 \pmod{\mu}$ and $\mathfrak{C} \equiv 0 \pmod{\mu}$, hence $x_9, \cdots, x_{16}$ are integers. Moreover (202) holds now for the module μ instead of $2\omega_0$; consequently $x_1, \cdots, x_8$ are also integers and $x_1^2 \equiv 1 \pmod{\omega}$. Since $|\mathfrak{M}| = 1$, the numbers $x_1, \cdots, x_{16}$ are relative prime. We apply the argument of Section **62** and conclude that the coefficients x_k are numbers of the field K.

Let $\Delta(p, q, r, s)$ denote the group of all symplectic matrices $\pm \mathfrak{M}$ with integral $x_1, \cdots, x_{16}$ in K. We have proved that $\Delta_\nu(\mathfrak{T})$ is a subgroup of $\Delta(p, q, r, s)$. On the other hand, if $\mathfrak{M}$ is an element of $\Delta(p, q, r, s)$ satisfying $x_1 \equiv 1$, $x_k \equiv 0 \pmod{f^2}$ for $k = 2, \cdots, 16$, then $\mathfrak{B} \equiv \mathfrak{E} \pmod{f^2}$, by (176), (177) and (178), and $\mathfrak{U} = \mathfrak{R}_1\mathfrak{B}\mathfrak{R}_1^{-1}$ is an element of the group $\Lambda(\mathfrak{T})$. Consequently the groups $\Delta(\mathfrak{T})$ and $\Delta(p, q, r, s)$ are commensurable.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.