国家出版基金项目

中国科学院华罗庚数学重点实验室丛书

华罗庚文集

代数卷 II

华罗庚 /著

李福安 /审校

科学出版社

纪念华罗庚先生诞辰100周年

《华罗庚文集》编委会

国家出版基金项目

中国科学院华罗庚数学重点实验室丛书

华罗庚文集

代数卷 II

华罗庚　著

李福安　审校

科学出版社

北　京

内 容 简 介

本书汇集了华罗庚先生 1930–1952 年关于代数和矩阵几何的代表性论文 22 篇, 以及万哲先关于华罗庚在代数和几何领域成就的一篇介绍文章.

华罗庚的论文内容深刻, 技巧性很强, 要求的预备知识并不多. 本书适合数学专业的研究生和研究人员阅读, 大学数学系的高年级学生也能读懂其中大部分内容.

图书在版编目(CIP)数据

华罗庚文集：代数卷 II/华罗庚著, 李福安审校. —北京：科学出版社，2011
(中国科学院华罗庚数学重点实验室丛书)
ISBN 978–7–03–030014–0

Ⅰ. ①华… Ⅱ. ①华… Ⅲ. ①数学–文集②代数–文集 Ⅳ. O1-53

中国版本图书馆 CIP 数据核字 (2011) 第 008066 号

责任编辑: 赵彦超 / 责任校对: 宋玲玲
责任印制: 钱玉芬 / 封面设计: 黄华斌

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

中国科学院印刷厂印刷
科学出版社发行　　各地新华书店经销
*
2011 年 2 月第 一 版　　开本: B5(720×1000)
2011 年 2 月第一次印刷　　印张: 24 1/4
印数: 1—2 000　　字数: 475 000

定价: 98.00 元

(如有印装质量问题, 我社负责调换)

《华罗庚文集》序言

2010 年是著名数学家华罗庚先生诞辰 100 周年. 值此机会, 我们编辑出版《华罗庚文集》, 作为对他的美好纪念.

华罗庚先生是他那个时代的国际领袖数学家之一, 也是中国现代数学的主要奠基人和领导者. 无论是在和平建设时期, 还是在政治动荡甚至是战争年代, 他都抱定了为国家和人民服务的宗旨, 为中国数学的发展倾注了毕生精力, 受到了中国人民的广泛尊敬.

华罗庚先生最初研究数论, 后将研究兴趣拓展至代数和多复变等多个领域, 取得了一系列国际一流的成果, 引领了这些领域的学术发展, 产生了广泛持久的影响. 他从一名自学青年成长为著名数学家, 其传奇经历激励了几代中国数学家投身于数学事业.

华罗庚先生为我们留下了丰富的精神遗产, 包括大量的学术著作和研究论文. 我们认为, 认真研读这些著作和论文, 是深刻把握华罗庚学术思想精髓的最佳途径. 无论对于数学工作者还是青年学生, 其中许多内容都是很有启发和裨益的.

华罗庚先生担任中国科学院数学研究所所长 30 余年, 他言传身教, 培养和影响了一批国际水平的数学家, 他的学术思想和治学精神已经成为数学所文化的核心. 自 2008 年起以中国科学院数学研究所为基础成立的中国科学院华罗庚数学重点实验室, 旨在继承和弘扬华罗庚先生的学术思想和治学精神, 积极推动中国数学的发展. 为此, 我们选择华罗庚先生的著作和论文作为实验室的首批出版物, 今后还将陆续推出更多优秀的数学出版物.

在出版《华罗庚文集》的过程中, 我们得到了各方面的关心和支持, 包括国家出版基金的资助, 在此我们表示深深的感谢. 同时, 对于有关人员在策划、翻译和审校等方面付出的辛勤劳动, 对于科学出版社所作的大量工作, 我们表示诚挚的谢意.

中国科学院华罗庚数学重点实验室

《华罗庚文集》编委会

2010 年 3 月

目　　录

Algebra and geometry*

Z. X. Wan

Finite Groups. Early in 1938, while Hua taught at the Southwest Association Associated University in Kunming, he conducted a seminar on finite groups; among the topics studied were p-groups. In [46, 81], he introduced the concept of the rank of a p-group. A p-group $\mathfrak{g}$ of order p^n is said to be of rank α, if the maximum of the orders of its elements is $p^{n-\alpha}$. Using this concept he proved that a pseudo-basis exists in p-groups, i.e., if $p \geqslant 3$ and $n \geqslant 2\alpha + 1$, then every element of $\mathfrak{g}$ can be expressed uniquely as

$$G = A^{\delta} A_{\alpha}^{\delta_\alpha} A_{\alpha-1}^{\delta_{\alpha-1}} \cdots A_1^{\delta_1}, \quad 0 \leqslant \delta \leqslant p^{n-\alpha} - 1, \quad 0 \leqslant \delta_i \leqslant p - 1,$$

where A is of order $p^{n-\alpha}$ and $A_i^{p^i} = 1$. With the aid of pseudo-bases, and of a modified form of the enumeration principle of P. Hall, he proved several "Anzahl" theorems. For instance, if $\mathfrak{g}$ is a group of order p^n and rank $\alpha\,(p \geqslant 3,\, n \geqslant 2\alpha+1)$, then (i)$\mathfrak{g}$ contains one and only one subgroup of order p^m and rank $\alpha\,(2\alpha + 1 \leqslant m \leqslant n)$; (ii) $\mathfrak{g}$ contains p^α cyclic subgroups of order $p^m\,(\alpha < m < n - \alpha - 1)$; (iii) the number of elements of order $\leqslant p^m\,(\alpha \leqslant m \leqslant n - \alpha)$ in $\mathfrak{g}$ is equal to $p^{m+\alpha}$. The second and third results improved theorems of G. A. Miller and A. A. Kulakoff respectively.

Skew Fields. Since Hamilton's first example of a non-commutative division algebra——the quaternion algebra——division algebras have received a great deal of attention. By comparison, infinite dimensional division algebras——skew fields ——were neglected; until, around 1950, with his perceptive direct algebraic method Hua proved several remarkable theorems in this area.

First, in 1949, Hua[88] proved that "every semi-automorphism of a skew field is either an automorphism or an anti-automorphism" (by a semi-automorphism of a skew field we mean a one-to-one mapping σ from the skew field into itself with the properties $(a + b)^\sigma = a^\sigma + b^\sigma$, $(aba)^\sigma = a^\sigma b^\sigma a^\sigma$ and $1^\sigma = 1$). This theorem was referred to as the beautiful theorem of Hua by E. Artin in his book *Geometric*

* Reprinted from *Loo-Keng Hua Selected Papers*. New York: Springer-Verlag, 1983: 281-284. The references in this article are those in this book.

Algebra. From it Hua[88,97] deduced also the fundamental theorem of l-dimensional projective geometry over a skew field. In 1950[97] he extended his theorem to semi-homomorphisms of rings without zero divisors.

Secondly, in 1949 L. K. Hua[91] gave a straightforward proof that "every proper normal subfield of a skew field is contained in its center". This result appears in the literature as the Cartan-Brauer-Hua theorem. Before the work of Hua and Richard Brauer, Henri Cartan's proof had used the complicated device of Galois extensions over subfields. By contrast, Hua's proof requires only the elementary identity: If $ab \neq ba$, then

$$a = \Big(b^{-1} - (a-1)^{-1}b^{-1}(a-1)\Big)\Big(a^{-1}b^{-1}a - (a-1)^{-1}b^{-1}(a-1)\Big)^{-1}.$$

In 1950, Hua[96] proved also that "if a skew field is not a field, then its multiplicative group is not meta-abelian".

Classical Groups. Early in 1946, L. K. Hua[73] published his first paper on automorphisms of classical groups, in which he determined the automorphisms of a real symplectic group. Subsequently, in 1948, he[85] determined the automorphisms of a symplectic group over any field of characteristic not 2. The method of Hua for determining the automorphisms of symplectic groups can be applied also to classical groups of other types; but since Dieudonné published his results on the automorphisms of classical groups in 1951, Hua[101] restricted himself to publishing only solutions, by his own method, to a series of problems left open by Dieudonné. The first of these was the determination of automorphisms of $\mathrm{GL}_2(K)$, K being an arbitrary skew field of characteristic $\neq 2$.

Besides $\mathrm{GL}_2(K)$, Hua[101] determined also the automorphisms of $\mathrm{SL}_4(K)$ and $\mathrm{PSL}_4(K)$, where K is a skew field of characteristic not 2, and the automorphism of $\mathrm{O}_4^+(K, f)$, where K is a field of characteristic not 2 and f is a quadratic form of index 2. Afterwards, Hua and Z. X. Wan[105] determined the automorphisms of $\mathrm{SL}_2(K)$ and $\mathrm{PSL}_2(K)$, where K is a skew field of characteristic $\neq 0$, the automorphisms of $\mathrm{SL}_4(K)$ and $\mathrm{PSL}_4(K)$, where K is a skew field of characteristic 2, and they proved also the nonisomorphism of certain linear groups.

Hua's work on the automorphisms of classical groups, shows mastery of the techniques of matrix calculation. The procedure is to start with the low-dimensional cases and to proceed to the higher-dimensional cases by induction, as in [85], for $\mathrm{SP}_{2n}(K)$.

About the structure of classical groups, Hua extended the usual unitary group to

the case when the basic field is not necessarily commutative but has an involutive anti-automorphism. He proved that the group $TU_n(K_1S)$ generated by unitary transvections modulo its center is a simple group, if S has index $\geqslant 1$ and that $TU_n(K_1S)$ is the commutator subgroup of $U_n(K_1S)$, if the index of S satisfies $n \geqslant 2V \geqslant 4$.

Hua and I. Reiner[102,106] also determined the automorphisms of $\mathrm{GL}_n(\mathbb{Z})$ and $\mathrm{DGL}_n(\mathbb{Z})$, which was the start of the work on the automorphisms of classical groups over rings. They[92] also proved that $\mathrm{GL}_n(\mathbb{Z})$ is generated by three elements, $\mathrm{SL}_n(\mathbb{Z})$ by two elements, and $\mathrm{Sp}_{2n}(\mathbb{Z})$ by four elements for $n \geqslant 2$. Formerly Poincaré* had stated without proof that $\mathrm{Sp}_{2n}(\mathbb{Z})$ is generated by elementary matrices of two simple types, and later Brahana† had proved this by showing that every element of $\mathrm{Sp}_{2n}(\mathbb{Z})$ is expressible as a product of matrices taken from some finite set of matrices.

Geometry of Matrices[67,76−78,93,99]. Study of this topic was initiated by Hua and relates to Siegel's work on fractional linear transformations. In it, the points of the space are matrices of a certain kind, for instance, rectangular matrices, symmetric matrices or skew-symmetric matrices of the same size. There is then a group of motions in this space, and the problem is to characterize the group of motions by as few geometric invariants as possible. First, he studied the geometry of matrices of various types over the complex or real fields. Later, he extended his results to the case when the basic field is not necessarily commutative and discovered that the invariant "coherence" is alone sufficient to characterize the group of motions of the space. Take his paper [99] as an example. He proved the fundamental theorem of affine geometry of rectangular matrices: *Let* $1 < n \leqslant m$. *Then the one-to-one mappings from the set of* $n \times m$ *matrices over a skew field* K *onto itself preserving coherence* (*two matrices* M *and* N *are said to be coherent, if the rank of* $M-N$ *is* 1) *is necessarily of the form*

$$Z_1 = PZ^{\sigma}Q + R, \tag{1}$$

where $P = P^{(n)}$ *and* $Q = Q^{(m)}$ *are invertible matrices,* R *is an* $n \times m$ *matrix, and* σ *is an automorphism of* K; *if* $n = m$, *then besides* (1) *we have also*

$$Z_1 = PZ'^{\tau}Q + R,$$

where τ *is an anti-automorphism of* K. From this theorem he deduced the fundamental theorem of the projective geometry of rectangular matrices (the Grassmann space),

∗ Poincaré H. *Rend Circ Mat Palermo*, 1904, **18**: 45–110.

† Brahana R R. *Ann of Math*, 1923, **24** (2): 265–270.

and he determined the Jordan isomorphism of total matrix rings over skew fields of characteristic $\neq 2$ and the Lie isomorphism of total matrix rings over skew fields of characteristic $\neq 2, 3$.

Arising from the geometry of matrices and the theory of functions of several complex variables, Hua went on to study the classification problem of matrices; for instance, the classification of complex symmetric and skew-symmetric matrices under the unitary group, of a pair of Hermitian matrices under congruence[66], and of Hermitian matrices under the orthogonal group[76] (*editorial note*: by "elementary divisors of a characteristic matrix" is meant, in current usage, "Jordan blocks" in a Jordan normal form, in the sense that $(X-\alpha)^d$ is an elementary divisor of multiplicity m if and only if the Jordan form has exactly m blocks of $d \times d$ matrices

$$J_d(\alpha) = \begin{pmatrix} \alpha & 1 & & 0 & \\ & \alpha & 1 & & \\ & & & \ddots & 1 \\ 0 & & & & \alpha \end{pmatrix}.$$

In [76], on p. 509 four lines from the bottom, read $\overline{\Gamma}'Q(\overline{\Gamma}')^{-1} = T$ for $\overline{\Gamma}Q(\overline{\Gamma}')^{-1} = T$, and on p. 512 line four, read $H = KT_0$ for $K = HT_0$).

苏家驹之代数的五次方程式解法不能成立之理由*

五次方程式经 Abel, Galois 之证明后, 一般算学者均认为不可以代数解矣, 而《学艺》七卷十号载有苏君之 "代数的五次方程式之解法" 一文, 罗欣读之而研究之, 于去年冬亦仿得 "代数的六次方程式之解法" 矣. 罗对此欣喜异常, 意为果能成立, 则于算学史中亦可占一席地也, 惟自思若不将 Abel 言论驳倒, 终不能完全此种理论, 故罗沉思于 Abel 之论中, 凡一阅月, 见其条例精严, 无懈可击, 后经本社编辑员之暗示, 遂从事于苏君解法确否之工作, 于六月中遂得其不能成立之理由, 罗安敢自秘, 特公之于世, 尚祈示正焉.

解 法 简 述

用 Sylvester 之分离消去法 (diabylic method of elemination) 将普通形

$$x^5+p_1x^4+p_2x^3+p_3x^2+p_4x+p_5=0$$

化为可解形 $X^5+P_1X^4+P_2X^3+P_3X^2+P_4X+P_5=0$ (中有 $P_1=0, P_3=0, P_2^2=5P_4$), 而 x, X 有 $X=n_0+n_1x+n_2x^2+n_3x^3+n_4x^4$ 之关系. P_1, P_2, P_3, P_4, P_5 为 n_0, n_1, n_2, n_3, n_4 之一次、二次、三次、四次、五次齐次函数. $P_1=0$, 即 n_0 可以 n_1, n_2, n_3, n_4 之一齐次函数表之, 以之代入 P_2, P_3, P_4, P_5, 则得 n_1, n_2, n_3, n_4 之二、三、四、五次齐次函数, 而 P_3 之一般形可写为

$$\begin{aligned}&A_1n_1^3+A_2n_2^3+A_3n_3^3+A_4n_4^3+A_5n_1^2n_2+A_6n_1^2n_3+A_7n_1^2n_4+A_8n_2^2n_1+A_9n_2^2n_3\\&+A_{10}n_2^2n_4+A_{11}n_3^2n_5+A_{12}n_3^2n_2+A_{13}n_3^2n_4+A_{14}n_4^2n_1+A_{15}n_4^2n_2+A_{16}n_4^2n_3\\&+A_{17}n_1n_2n_3+A_{18}n_1n_2n_4+A_{19}n_1n_2n_4+A_{20}n_2n_3n_4,\end{aligned}\tag{I}$$

式中 $A_1, \cdots, A_{20}$ 为 $p_1, \cdots, p_5$ 之函数为已知者.

若令等于下式

$$\begin{aligned}&(a_1n_1+a_2n_2)(a_3n_1^2+a_4n_2^2+a_5n_3^2+a_6n_4^2+a_7n_1n_2+a_8n_1n_3+a_9n_1n_4+a_{10}n_2n_3\\&+a_{11}n_2n_4+a_{12}n_3n_4)+(a_{13}n_3+a_{14}n_4)(a_{15}n_1^2+a_{16}n_2^2+a_{17}n_3^2+a_{18}n_4^2+a_{19}n_1n_2\\&+a_{20}n_1n_3+a_{21}n_1n_4+a_{22}n_2n_3+a_{23}n_2n_4+a_{24}n_3n_4),\end{aligned}\tag{II}$$

式中 $a_1, \cdots, a_{24}$ 为未定系数.

* 科学, 1930, **15**: 307-309.

再设 $a_1n_1+a_2n_2=0$, $a_{13}n_3+a_{14}n_4=0$, 代入 $P_2^2=5P_4$ 式中, 则此式为 n_2,n_4 之四次齐次函数, 解之, 则得 n_2,n_4 之比值, 由此可作得 $n_0:n_1:n_2:n_3:n_4$ 之值, 故普通形可化为上之可解形, 换言之, 即五次方程式可得而解矣.

谬　误　点

罗研究上意知其谬误在 P_3 中, 即 (I) 不能等于 (II) 也. 夫求未定系数 $a_1,\cdots,a_{24}$, 原文亦有求之之二十方程式, 罗为便利讨探计, 特分之为四类, 转录于下：

(一) $a_1a_3=A_1$, $a_2a_4=A_2$,

$a_3a_2+a_1a_7=A_5$, $a_4a_1+a_2a_7=A_8$;

(二) $a_{13}a_{17}=A_3$, $a_{14}a_{18}=A_4$,

$a_{17}a_{14}+a_{13}a_{24}=A_{13}$, $a_{18}a_{13}+a_{14}a_{24}=A_{16}$;

(三) $a_{13}a_{15}+a_1a_3=A_6$, $a_{14}a_{15}+a_1a_9=A_7$,

$a_1a_{11}+a_2a_9=a_{18}-a_{14}a_{19}$, $a_2a_{11}+a_{14}a_{16}=A_{10}$,

$a_2a_{10}+a_{13}a_{16}=A_9$, $a_1a_{10}+a_2a_8=a_{17}-a_{13}a_{19}$;

(四) $a_1a_5+a_{13}a_{20}=A_{11}$, $a_2a_5+a_{13}a_{22}=A_{12}$,

$a_2a_{12}+a_{14}a_{22}=A_{19}-a_{13}a_{23}$, $a_1a_{12}+a_{13}a_{21}=A_{20}-a_{14}a_{20}$,

$a_1a_6+a_{14}a_{21}=A_{14}$, $a_2a_6+a_{14}a_{23}=A_{15}$.

依原所谓假 a_7,a_{24} 则由 (一), (二) 得 $a_1,a_2,a_3,a_4,a_{13},a_{14},a_{17},a_{18}$ 之值, 则第二类乃为 $a_8,a_{15},a_9,a_{11},a_{16},a_{10}$ 之联立一次方程式 (设 a_{19} 为已知), 以行列式解之, 知其各分母悉为

$$\Delta=\begin{vmatrix} a_1 & a_{13} & 0 & 0 & 0 & 0\\ 0 & a_{14} & a_1 & 0 & 0 & 0\\ 0 & 0 & a_2 & a_1 & 0 & 0\\ 0 & 0 & 0 & a_2 & a_{14} & 0\\ 0 & 0 & 0 & 0 & a_{13} & a_2\\ a_2 & 0 & 0 & 0 & 0 & a_1 \end{vmatrix}.$$

然

$$\begin{vmatrix} a_1 & a_{13} & 0 & 0 & 0 & 0\\ 0 & a_{14} & a_1 & 0 & 0 & 0\\ 0 & 0 & a_2 & a_1 & 0 & 0\\ 0 & 0 & 0 & a_2 & a_{14} & 0\\ 0 & 0 & 0 & 0 & a_{13} & a_2\\ a_2 & 0 & 0 & 0 & 0 & a_1 \end{vmatrix} = a_1\begin{vmatrix} a_{14} & a_1 & 0 & 0 & 0\\ 0 & a_2 & a_1 & 0 & 0\\ 0 & 0 & a_2 & a_{14} & 0\\ 0 & 0 & 0 & a_{13} & a_2\\ 0 & 0 & 0 & 0 & a_1 \end{vmatrix}$$

$$-a_{13}\begin{vmatrix} 0 & a_1 & 0 & 0 & 0 \\ 0 & a_2 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & a_{14} & 0 \\ 0 & 0 & 0 & a_{13} & a_2 \\ a_2 & 0 & 0 & 0 & a_1 \end{vmatrix} = 0,$$

而 $a_8, a_{15}, a_9, a_{11}, a_{16}, a_{10} = \delta/\Delta$.

因 $\Delta = 0$, 故 $a_8, a_{15}, a_9, a_{11}, a_{16}, a_{10}$ 非不定即无限大, 故 (I) 等 (II) 之谬论不攻自破矣. 换言之, 即 P_3 为零不能解得二一次式, 故此法亦不能解五次方程式也.

Geometries of matrices. I. Generalizations of von Staudt's theorem*

It was first shown in the author's recent investigations on the theory of automorphic functions of a matrix-variable that there are three types of geometry playing important roles. Besides their applications, the author obtained a great many results which seem to be interesting in themselves.

The main object of the paper is to generalize a theorem due to von Staudt, which is known as the fundamental theorem of the geometry in the complex domain. The statement of the theorem is:

Every topological transformation of the complex plane into itself, which leaves the relation of harmonic separation invariant, is either a collineation or an anti-collineation.

Since the fields and groups may be varied, several generalizations of von Staudt's theorem will be given. The proofs of the theorems have interesting corollaries.

The paper contains also some fundamental results which will be useful in succeeding papers.

The interest of the paper seems to be not only geometric but also algebraic, for example we shall establish the following purely algebraic theorem:

Let $\mathfrak{M}$ *be the module formed by n-rowed symmetric matrices over the complex field. Let* Γ *be a continuous* (*additive*) *automorphism of* $\mathfrak{M}$ *leaving the rank unaltered and* $\Gamma(iX) = i\Gamma(X)$. *Then* Γ *is an inner automorphism of* $\mathfrak{M}$, *that is, we have a nonsingular matrix* T *such that*

$$\Gamma(X) = TXT'.$$

The author makes the paper self-contained in the sense that no knowledge of the author's contributions to the theory of automorphic functions is assumed.

* Presented to the Society, April 28, 1945; received by the editors November 20, 1944. Reprinted from Transactions of the *American Mathematical Society*, 1945, **57**: 441-481.

I. Geometry of symmetric matrices

Let Φ be any field. In I, II, and III, capital Latin letters denote $n \times n$ matrices unless the contrary is stated. But on the contrary, we use $M^{(n,m)}$ to denote an $n \times m$ matrix, and $M^{(n)} = M^{(n,n)}$. I and 0 denote the identity and zero matrices respectively.

Throughout I, we use

$$\mathfrak{F} = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}, \quad \mathfrak{T} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix},$$

which are $2n$-rowed matrices.

1. Definitions

We make the following definitions.

A pair of matrices (Z_1, Z_2) is said to be *symmetric* if

$$(Z_1, Z_2)\mathfrak{F}(Z_1, Z_2)' = 0,$$

that is, if $Z_1 Z_2' = Z_2 Z_1'$. The pair is said to be *nonsingular* if (Z_1, Z_2) is of rank n.

A $2n \times 2n$ matrix $\mathfrak{T}$ is said to be *symplectic* if

$$\mathfrak{T}\mathfrak{F}\mathfrak{T}' = \mathfrak{F}.$$

Explicitly, let

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

then we have

$$AB' = BA', \quad CD' = DC', \quad AD' - BC' = I.$$

Further, it may be easily verified that

$$\mathfrak{T}^{-1} = \begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix}$$

is also symplectic.

We define

$$(W_1, W_2) = Q(Z_1, Z_2)\mathfrak{T}$$

to be a *symplectic transformation*, where Q is nonsingular and $\mathfrak{T}$ is symplectic.

Since

$$(W_1, W_2)\mathfrak{F}(W_1, W_2)' = Q(Z_1, Z_2)\mathfrak{T}\mathfrak{F}\mathfrak{T}'(Z_1, Z_2)'Q',$$

a symplectic transformation carries symmetric (nonsingular) pairs into symmetric (nonsingular) pairs.

We identify two nonsingular symmetric pairs of matrices (Z_1, Z_2) and (W_1, W_2) by means of the relation

$$(Z_1, Z_2) = Q(W_1, W_2).$$

It is called a point of the space. The space so defined is unaltered under symplectic transformations, which may be considered as the motions of the space.

If Z_1 and W_1 are both nonsingular and if $(W_1, W_2) = Q(Z_1, Z_2)\mathfrak{T}$, let

$$W = -W_1^{-1}W_2, \quad Z = -Z_1^{-1}Z_2,$$

then W and Z are both symmetric and

$$Z = (AW + B)(CW + D)^{-1}.$$

Thus a symmetric pair of matrices may be considered as homogeneous coordinates of a symmetric matrix. The terminology "geometry of symmetric matrices" is thus justified.

2. Equivalence of points

Theorem 1 *Any two nonsingular symmetric pairs of matrices are equivalent. Or what is the same thing: every nonsingular symmetric pair is equivalent to* $(I, 0)$.

Proof Let (Z_1, Z_2) be a nonsingular symmetric pair.

(1) If Z_1 is nonsingular, we have

$$(Z_1, Z_2) = Z_1(I, Z_1^{-1}Z_2) = Z_1(I, 0)\begin{pmatrix} I & S \\ 0 & I \end{pmatrix},$$

where $S = Z_1^{-1}Z_2$ is symmetric, and then

$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}$$

is symplectic.

(2) Suppose Z_1 to be singular. We have nonsingular matrices P and Q such that

$$W_1 = PZ_1Q = \begin{pmatrix} I^{(r)} & 0^{(r,n-r)} \\ 0^{(n-r,r)} & 0^{(n-r)} \end{pmatrix}$$

and

$$(W_1, W_2) = P(Z_1, Z_2) \begin{pmatrix} Q & 0 \\ 0 & Q'^{-1} \end{pmatrix}$$

and

$$W_2 = PZ_2Q'^{-1} = \begin{pmatrix} s^{(r)} & m^{(r,n-r)} \\ q^{(n-r,r)} & t^{(n-r)} \end{pmatrix}.$$

Since

$$\begin{pmatrix} Q & 0 \\ 0 & Q'^{-1} \end{pmatrix}$$

is symplectic, (W_1, W_2) is nonsingular and symmetric. Consequently s is symmetric and q is a zero matrix.

Let

$$(U_1, U_2) = (W_1, W_2) \begin{pmatrix} I & -S \\ 0 & I \end{pmatrix},$$

where

$$S = \begin{pmatrix} s^{(r)} & 0 \\ 0 & I^{(n-r)} \end{pmatrix}.$$

Then

$$U_1 = W_1, \quad U_2 = -W_1S + W_2 = \begin{pmatrix} 0 & m \\ 0 & t \end{pmatrix}.$$

Since (U_1, U_2) is nonsingular, $t^{(n-r)}$ is nonsingular. Let

$$(V_1, V_2) = (U_1, U_2) \begin{pmatrix} I & 0 \\ I & I \end{pmatrix},$$

then

$$V_1 = U_1 + U_2 = \begin{pmatrix} I^{(r)} & m \\ 0 & t \end{pmatrix},$$

which is nonsingular. By (1), we have the theorem.

3. Equivalence of point-pairs

Definition Let (Z_1, Z_2) and (W_1, W_2) be two nonsingular symmetric pairs of matrices. We define the rank of

$$(Z_1, Z_2)\mathfrak{F}(W_1, W_2)' = Z_1W_2' - Z_2W_1'$$

to be the *arithmetic distance* between the two points represented. Evidently, the notion is independent of the choice of representation. Further, it is invariant under symplectic transformations. In fact, let

$$(Z_1^*, Z_2^*) = Q(Z_1, Z_2)\mathfrak{T}, \quad (W_1^*, W_2^*) = R(W_1, W_2)\mathfrak{T},$$

then

$$(Z_1^*, Z_2^*)\mathfrak{F}(W_1^*, W_2^*)' = Q(Z_1, Z_2)\mathfrak{T}\mathfrak{F}\mathfrak{T}'(W_1, W_2)'R' = Q(Z_1, Z_2)\mathfrak{F}(W_1, W_2)'R'.$$

In nonhomogeneous coordinates, the arithmetic distance between two symmetric matrices W, Z is equal to the rank of $W - Z$.

Theorem 2 *Two point-pairs are equivalent if and only if they have the same arithmetic distance. What is the same thing: every point-pair with arithmetic distance r is equivalent to*

$$(I, 0), \quad (I, I_r),$$

where

$$I_r = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}.$$

Proof By Theorem 1, we may assume that the point-pairs are of the form

$$(I, 0), \quad (Z_1, Z_2).$$

The arithmetic distance being r, it follows that Z_2 is of rank r. We have two nonsingular matrices P and Q such that

$$QZ_2P = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix} = I_r.$$

Then

$$Q(Z_1, Z_2)\begin{pmatrix} P'^{-1} & 0 \\ 0 & P \end{pmatrix} = (T, I_r)$$

and

$$Q(I, 0)\begin{pmatrix} P'^{-1} & 0 \\ 0 & P \end{pmatrix} = QP'^{-1}(I, 0).$$

Since (T, I_r) is a nonsingular symmetric pair, we have, consequently,

$$T = \begin{pmatrix} s^{(r)} & t \\ 0 & p^{(n-r)} \end{pmatrix},$$

where s is symmetric and p is nonsingular. Then

$$\begin{pmatrix} I^{(r)} & -tp^{-1} \\ 0 & p^{-1} \end{pmatrix} (T, I_r) = \left(\begin{pmatrix} s^{(r)} & 0 \\ 0 & I^{(n-r)} \end{pmatrix}, I_r \right).$$

Further

$$\left(\begin{pmatrix} s^{(r)} & 0 \\ 0 & I^{(n-r)} \end{pmatrix}, I_r \right) \begin{pmatrix} I & & 0 \\ \begin{pmatrix} I-s & 0 \\ 0 & 0 \end{pmatrix} & & I \end{pmatrix} = (I, I_r)$$

and

$$(I, 0) \begin{pmatrix} I & & 0 \\ \begin{pmatrix} I-s & 0 \\ 0 & 0 \end{pmatrix} & & I \end{pmatrix} = (I, 0).$$

Since

$$\begin{pmatrix} I & & 0 \\ \begin{pmatrix} I-s & 0 \\ 0 & 0 \end{pmatrix} & & I \end{pmatrix}$$

is symplectic, we have the result.

Definition The points (X_1, X_2) with singular X_1 are called *points at infinity* (or symmetric matrices at infinity). Finite points are those with nonsingular X_1.

Lemma *Any finite number of points may be carried simultaneously into finite points by a symplectic transformation, if Φ is the field of complex numbers.*

Proof (1) Given any symmetric pair of matrices (T_1, T_2), we have a symplectic matrix

$$\begin{pmatrix} P_1 & P_2 \\ T_1 & T_2 \end{pmatrix}.$$

In fact, by Theorem 2, we have a symplectic $\mathfrak{T}$ such that

$$(T_1, T_2) = Q(-I, 0)\mathfrak{T}.$$

Let

$$(P_1, P_2) = Q'^{-1}(0, I)\mathfrak{T}.$$

Then

$$\begin{pmatrix} P_1 & P_2 \\ T_1 & T_2 \end{pmatrix} = \begin{pmatrix} Q'^{-1} & 0 \\ 0 & Q \end{pmatrix} \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \mathfrak{T},$$

which is evidently symplectic.

(2) For a fixed point (X_1, X_2), the manifold

$$\det((X_1, X_2)\mathfrak{F}(Z_1, Z_2)') = 0$$

is of dimension $n(n+1) - 2$. Let

$$(A_1, A_2), \cdots, (L_1, L_2)$$

be p given points. Then we have p manifolds

$$\det((A_1, A_2)\mathfrak{F}(Z_1, Z_2)') = 0, \cdots, \det((L_1, L_2)\mathfrak{F}(Z_1, Z_2)') = 0.$$

In the space, there is a point (T_1, T_2) which is not on any one of the manifolds. The transformation

$$(Y_1, Y_2) = Q(X_1, X_2)\begin{pmatrix} P_1 & P_2 \\ T_1 & T_2 \end{pmatrix}^{-1} = Q(X_1, X_2)\begin{pmatrix} T_2' & -P_2' \\ -T_1' & P_1' \end{pmatrix}$$

carries evidently the p points into finite points simultaneously.

4. Equivalence of triples of points

Definition 1 A subspace is said to be *normal* if it is equivalent to the subspace formed by symmetric matrices (in nonhomogeneous coordinates) of the form

$$\begin{pmatrix} Z_0^{(r)} & 0 \\ 0 & 0^{(n-r)} \end{pmatrix}.$$

The least possible r is defined to be the *rank of the subspace.*

Definition 2 A triple of points is said to be of *degeneracy* $d = n - r$ if it belongs to a normal subspace of rank r.

Evidently degeneracy is invariant under symplectic transformations.

Theorem 3 *In the complex field, two triples of points are equivalent if and only if they have the same degeneracy and the arithmetic distances between any two corresponding pairs of points are equal.*

Proof Evidently, if two triples are equivalent, they have the same degeneracy and the arithmetic distances between any two corresponding pairs of points are equal.

We prove the converse in six steps.

(1) Every triple with arithmetic distances n, n, r is equivalent to

$$0, \quad I, \quad \begin{pmatrix} -I^{(r)} & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{(in nonhomogeneous coordinates)}$$

(notice that now the degeneracy is 0). We use $r(A, B)$ to denote the arithmetic distance between A and B. Let A, B, C be the three points of the triple. Then

$$r(A, B) = r(A, C) = n.$$

By Theorem 2, we may write in homogeneous coordinates

$$A = (I, 0), \quad B = (0, I), \quad C = (Z_1, Z_2).$$

Since $r(A, C) = n$ and Z_2 is nonsingular, we may write C as

$$(S, I),$$

where S is a symmetric matrix of rank r. We have a nonsingular matrix Γ such that

$$\Gamma S \Gamma' = I_r = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix},$$

then

$$\Gamma \begin{pmatrix} (I, 0) \\ (0, I) \\ (S, I) \end{pmatrix} \begin{pmatrix} \Gamma' & 0 \\ 0 & \Gamma^{-1} \end{pmatrix} = \begin{pmatrix} \Gamma\Gamma'(I, 0) \\ (0, I) \\ (I_r, I) \end{pmatrix}.$$

Thus the triple is equivalent to

$$(I, 0), \quad (0, I), \quad (I_r, I).$$

Since (in the nonhomogeneous coordinate system)

$$0, \ I, \ -I_r$$

is a triple with distances n, n, r, we have the theorem.

(2) Every triple of points with arithmetic distances n, s, t is equivalent to

$$0, \quad I, \quad \begin{pmatrix} -I^{(p)} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & I^{(q)} \end{pmatrix},$$

where $p + q = s$, $n - q = t$ (obviously, $s + t \geqslant n$).

In fact, we may assume that

$$A = (I, 0), \quad B = (I, I), \quad C = (Z_1, Z_2).$$

We may determine two nonsingular matrices U, V such that

$$UZ_2V = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix},$$

where r is the rank of Z_2. If we set

$$G = \begin{pmatrix} V'^{-1} & 0 \\ V - V'^{-1} & V \end{pmatrix},$$

the relations

$$\begin{aligned} U(I,0)G &= UV'^{-1}(I,0), \\ U(I,I)G &= UV(I,I), \\ U(Z_1,Z_2)G &= \left(P, \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}\right) \end{aligned}$$

imply that we may assume that

$$Z_1 = P, \quad Z_2 = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}.$$

Owing to the symmetry, we have

$$P = \begin{pmatrix} S^{(r)} & W \\ 0 & T \end{pmatrix},$$

where S is symmetric and T is nonsingular. Further, since

$$\begin{pmatrix} I & -WT^{-1} \\ 0 & T^{-1} \end{pmatrix} \left(\begin{pmatrix} S^{(r)} & W \\ 0 & T \end{pmatrix}, \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}\right) = \left(\begin{pmatrix} S^{(r)} & 0 \\ 0 & I \end{pmatrix}, \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}\right),$$

we may assume that

$$Z_1 = \begin{pmatrix} S^{(r)} & 0 \\ 0 & I \end{pmatrix}, \quad Z_2 = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}.$$

In the normal subspace of rank r, the points $(I^{(r)}, 0^{(r)}), (I^{(r)}, I^{(r)}), (S^{(r)}, I^{(r)})$ are, by (1), equivalent to

$$(I^{(r)}, 0^{(r)}), \quad (I^{(r)}, I^{(r)}), \quad \left(I^{(r)}, \begin{pmatrix} -I^{(p)} & 0 \\ 0 & 0^{(r-p)} \end{pmatrix}\right).$$

Thus, we have, in nonhomogeneous coordinates,

$$\begin{pmatrix} I^{(r)} & 0 \\ 0 & 0^{(n-r)} \end{pmatrix}, \quad \begin{pmatrix} 0^{(r)} & 0 \\ 0 & I^{(n-r)} \end{pmatrix}, \quad \begin{pmatrix} -I^{(p)} & 0 & 0 \\ 0 & 0^{(r-p)} & 0 \\ 0 & 0 & 0^{(n-r)} \end{pmatrix}.$$

The transformation

$$\begin{pmatrix} I^{(r)} & 0 \\ 0 & iI^{(n-r)} \end{pmatrix} \left(Z - \begin{pmatrix} 0^{(r)} & 0 \\ 0 & I^{(n-r)} \end{pmatrix} \right) \begin{pmatrix} I^{(r)} & 0 \\ 0 & iI^{(n-r)} \end{pmatrix} = W$$

carries the three points to the required form.

(3) Now we are going to prove that any three points are equivalent to

$$A = 0, \quad B = b_1 \dot{+} \cdots \dot{+} b_\lambda, \quad C = c_1 \dot{+} \cdots \dot{+} c_\lambda \text{①},$$

where b_ν and c_ν are unit matrices of degree (ν), multiplied with a factor 1, 0, or -1. (1) and (2) are special cases of this. We shall consider another special case with

$$A = 0, \quad B = \begin{pmatrix} 0 & M \\ M' & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & N \\ N' & 0 \end{pmatrix},$$

where

$$M = \begin{pmatrix} 0 & \cdots & 0 \\ & I^{(m)} & \end{pmatrix}, \quad N = \begin{pmatrix} & I^{(m)} & \\ 0 & \cdots & 0 \end{pmatrix}, \quad n = 2m + 1.$$

They form a triple with distances $2m$, $2m$, $2m$.

Now we are going to establish that there exists a symmetric matrix S such that the transformation

$$W = Z(SZ + I)^{-1}$$

will carry the three points to

$$A = 0, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & B_1^{(n-1)} \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 \\ 0 & C_1^{(n-1)} \end{pmatrix},$$

where B_1 is nonsingular. In fact S is given by

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

and so on. The general form may be obtained easily. Applying the results obtained in (2) to

$$0^{(n-1)}, \quad B_1^{(n-1)}, \quad C_1^{(n-1)},$$

① $\dot{+}$ and $\sum'$ denote direct sums.

we have the conclusion.

(4) Let B, C be a nonsingular pair of symmetric matrices (in the ordinary sense), that is, we have λ and μ such that

$$\det(\lambda B + \mu C) \neq 0.$$

Suppose C is nonsingular; the conclusion announced in (3) is true by (2). Otherwise ($\lambda \neq 0$) we have Γ such that

$$\Gamma'(\lambda B + \mu C)\Gamma = I,$$

$$\Gamma' C \Gamma = \begin{pmatrix} C_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix}, \quad C_1^{(r)} \text{ nonsingular.}$$

Then

$$\lambda \Gamma' B \Gamma = \begin{pmatrix} I^{(r)} - \mu C_1^{(r)} & 0 \\ 0 & I^{(n-r)} \end{pmatrix}.$$

Applying the results of (2) to

$$0, \quad \frac{1}{\lambda}(I^{(r)} - \mu C_1^{(r)}), \quad C_1^{(r)}$$

and

$$0, \quad \frac{1}{\lambda} I^{(n-r)}, \quad 0,$$

we have the result announced in (3).

(5) Finally, for any pair of symmetric matrices (cf. the lemma of §3)

$$B, \quad C,$$

we have a nonsingular matrix Γ such that

$$\Gamma B \Gamma' = b_1 \dot{+} \cdots \dot{+} b_\lambda$$

and

$$\Gamma C \Gamma' = c_1 \dot{+} \cdots \dot{+} c_\lambda,$$

where

$$(b_\nu, c_\nu)$$

is either the pair discussed in (4) or the pair discussed in (3), hence the results in (3).

(6) By a rearrangement and some evident modifications, for a triple of points with degeneracy t, we have

$$A = 0^{(p)} \dot{+} 0^{(q)} \dot{+} 0^{(r)} \dot{+} 0^{(s)} \dot{+} 0^{(t)},$$
$$B = I^{(p)} \dot{+} 0^{(q)} \dot{+} I^{(r)} \dot{+} I^{(s)} \dot{+} 0^{(t)},$$
$$C = -I^{(p)} \dot{+} I^{(q)} \dot{+} 0^{(r)} \dot{+} I^{(s)} \dot{+} 0^{(t)},$$

which is the only possible form. The arithmetic distances between two points are given by

$$a = r(B, C) = p + q + r,$$
$$b = r(C, A) = p + q + s,$$
$$c = r(A, B) = p + r + s.$$

Thus, for given t, a, b, c, if the equations are soluble, the solution is unique. We have therefore the theorem.

The conditions for solubility are

$$n - t \geqslant a,\ b,\ c,$$
$$a + b + c \geqslant 2(n - t). \tag{1}$$

In terms of a "triangle" we have the following theorem.

Theorem 4 *A triangle of degeneracy t with sides a, b, c exists if and only if* (1) *holds. If it exists, it is unique apart from equivalence.*

Incidentally, we have

$$a + b \geqslant 2(n - t) - c \geqslant c,$$

equality holds if and only if $c = a + b = n - t$.

The "triangle-relation"

$$a + b \geqslant c, \quad b + c \geqslant a, \quad c + a \geqslant b$$

does not guarantee the existence of triangles with a given degeneracy, for example, $n = 2$, $t = 0$, $a = b = c = 1$. But we have the following theorem.

Theorem 5 *Given the lengths of three sides a, b, c ($\leqslant n$), where the sum of every two is greater than the third one, there are λ non-equivalent triangles, where*

$$\lambda = \begin{cases} [(a + b + c)/2] - \max(a, b, c) + 1, & \text{for } n \geqslant [(a + b + c)/2]^{①}, \\ n - \max(a, b, c) + 1, & \text{for } n < [(a + b + c)/2]. \end{cases}$$

Proof From $a + b \geqslant c$, $b + c \geqslant a$, $c + a \geqslant b$, we have

① $[x]$ denotes the integral part of x.

$$a+b+c \geqslant 2\max(a,\, b,\, c).$$

There always exists a t such that

$$a+b+c \geqslant 2(n-t) \geqslant 2\max(a,\, b,\, c).$$

Then

$$\max(0,\, n-[(a+b+c)/2]) \leqslant t \leqslant n-\max(a,\, b,\, c).$$

Thus, the number of t's is equal to

$$\begin{aligned} &n-\max(a,\, b,\, c)-\max(0,\, n-[(a+b+c)/2])+1 \\ =&\min(n, [(a+b+c)/2])-\max(a,\, b,\, c)+1. \end{aligned}$$

Corollary 1 *If one of the sides is of length n, the triangle is unique.*

Corollary 2 *If the sum of two sides is equal to the third, then the triangle is unique.*

5. Equivalence of quadruples of points

Definition Let Z_1, Z_2, Z_3, Z_4 be four points in the nonhomogeneous coordinate-system. The matrix

$$(Z_1-Z_3)(Z_1-Z_4)^{-1}(Z_2-Z_4)(Z_2-Z_3)^{-1}$$

is defined to be the cross-ratio-matrix of the four points, and it is denoted by

$$(Z_1,\, Z_2;\, Z_3,\, Z_4).$$

It is defined only when Z_1-Z_4 and Z_2-Z_3 are nonsingular.

In the homogeneous coordinate-system, we let $P_1,\, P_2,\, P_3,\, P_4$ be four points with coordinates

$$(X_1, Y_1), \quad (X_2, Y_2), \quad (X_3, Y_3), \quad (X_4, Y_4).$$

In terms of

$$\langle P_i, P_j\rangle = (X_j, Y_j)\mathfrak{F}(X_i, Y_i)',$$

the cross-ratio-matrix is defined by

$$(P_1, P_2; P_3, P_4) = \langle P_1, P_3\rangle\langle P_1, P_4\rangle^{-1}\langle P_2, P_4\rangle\langle P_2, P_3\rangle^{-1},$$

provided that it is not meaningless.

Let P_i^* be the point with coordinates

$$(X_i^*, Y_i^*) = Q_i(X_i, Y_i)\mathfrak{T},$$

where $\mathfrak{T}$ is symplectic; then

$$\begin{aligned}\langle P_i^*, P_j^*\rangle =&(X_j^*, Y_j^*)\mathfrak{F}(X_i^*, Y_i^*)'\\ =&Q_j(X_j, Y_j)\mathfrak{F}(X_i, Y_i)'Q_i' = Q_j\langle P_i, P_j\rangle Q_i'.\end{aligned}$$

Therefore

$$\begin{aligned}(P_1^*, P_2^*; P_3^*, P_4^*) =&\langle P_1^*, P_3^*\rangle\langle P_1^*, P_4^*\rangle^{-1}\langle P_2^*, P_4^*\rangle\langle P_2^*, P_3^*\rangle^{-1}\\ =&Q_3\langle P_1, P_3\rangle Q_1'Q_1'^{-1}\langle P_1, P_4\rangle Q_4Q_4^{-1}\langle P_2, P_4\rangle Q_2'Q_2'^{-1}\langle P_2, P_3\rangle^{-1}Q_3^{-1}\\ =&Q_3(P_1, P_2; P_3, P_4)Q_3^{-1},\end{aligned}$$

and we now state the following theorem.

Theorem 6 *In an algebraically closed field, two quadruples of points, no two of the points having arithmetic distance less than n, are equivalent if and only if their cross-ratio-matrices are equivalent.*

In order to prove Theorem 6, we need to establish the following theorem.

Theorem 7 *In the algebraically closed field, any quadruple of points, no two of which have arithmetic distance less than n, is equivalent to*

$$0, \quad \infty, \quad \sum_{1\leqslant i\leqslant\nu}{}' a_i, \quad \sum_{1\leqslant i\leqslant\nu}{}' b_i,$$

where

$$a_i = \begin{pmatrix} 0 & \cdots & 0 & 1\\ 0 & \cdots & 1 & 0\\ \vdots & & \vdots & \vdots\\ 1 & \cdots & 0 & 0\end{pmatrix}, \quad b_i = \begin{pmatrix} 0 & 0 & \cdots & 0 & \lambda_i\\ 0 & 0 & \cdots & \lambda_i & 1\\ \vdots & \vdots & & \vdots & \vdots\\ \lambda_i & 1 & \cdots & 0 & 0\end{pmatrix}, \quad \lambda_i \neq 0 \text{ or } 1.$$

Proof In homogeneous coordinates, we may write the four points as

$$(0, I), \quad (I, 0), \quad (Z_1, Z_2), \quad (W_1, W_2).$$

Since no two of the arithmetic distances are less than n, $1, Z_1, Z_2, W_1, W_2$ are all nonsingular. We may write them in the nonhomogeneous coordinates as

$$0, \quad \infty, \quad S_1, \quad S_2.$$

We have a nonsingular matrix T such that

$$TS_1T' = \sum{}' a_i, \quad TS_2T' = \sum{}' b_i.$$

The theorem follows.

The proof of Theorem 6 is now evident.

Remark The equivalence of quadruples in any field seems to be more difficult. The condition in Theorem 6 is insufficient for the real case (a signature system is required).

Definition We define a quadruple of points satisfying

$$(P_1, P_2; P_3, P_4) = -I$$

to be a *harmonic range.*

Evidently a harmonic range is invariant under a symplectic transformation.

6. Von Staudt's theorem in the complex number field

Now we let Φ be the field formed by complex numbers.

We use $\overline{Z}$ to denote the conjugate complex matrix of Z. The transformation

$$(W_1, W_2) = Q(\overline{Z}_1, \overline{Z}_2)\mathfrak{T}$$

carrying a symmetric pair (W_1, W_2) into a symmetric pair (Z_1, Z_2) is called *anti-symplectic* if Q is nonsingular and $\mathfrak{T}$ symplectic.

Theorem 8 *A transformation satisfying the following conditions*:

(1) *one-to-one and continuous*;

(2) *carrying symmetric matrices into symmetric matrices*;

(3) *keeping arithmetic distance invariant*;

(4) *keeping the harmonic relation invariant*

is either a symplectic or an anti-symplectic transformation.

Proof Let Γ be the transformation considered. Taking three points A, B, C (symmetric matrices), no two of which have arithmetic distance less than n, let A_1, B_1, C_1 be their images. By (3), the arithmetic distance between any two of A_1, B_1, C_1 is n. Let $\mathfrak{T}_1$ and $\mathfrak{T}_2$ be two symplectic transformations carrying respectively A, B, C and A_1, B_1, C_1 into 0, I, ∞, in accordance with Theorem 3. Then, without loss of generality, we may assume that

$$0 = \Gamma(0), \quad I = \Gamma(I), \quad \infty = \Gamma(\infty).$$

Since

$$Z, \quad Z_1, \quad (Z + Z_1)/2, \quad \infty$$

form a harmonic range, we have

$$\Gamma(Z) + \Gamma(Z_1) = \Gamma(Z + Z_1).$$

Consequently,

$$\Gamma(rZ) = r\Gamma(Z)$$

for all rational r. By continuity, this holds for all real r.

Now we introduce the following notations:

$$E_{ii} = (p_{st}), \quad p_{st} = \begin{cases} 1, & \text{if } s = t = i, \\ 0, & \text{otherwise} \end{cases}$$

and

$$E_{ij} = (q_{st}), \quad q_{st} = \begin{cases} 1, & \text{if } s = i,\ t = j \text{ or } s = j,\ t = i, \\ 0, & \text{otherwise.} \end{cases}$$

Let

$$\Gamma(E_{ii}) = M_i.$$

Since M_i is of rank 1 and symmetric, we have

$$M_i = (\lambda_{i1}, \cdots, \lambda_{in})'(\lambda_{i1}, \cdots, \lambda_{in}).$$

Let

$$\Lambda = (\lambda_{ij}).$$

Then

$$\begin{aligned} I = \Gamma(I) =& \sum_{i=1}^{n} \Gamma(E_{ii}) = \sum_{i=1}^{n} M_i \\ =& \sum_{i=1}^{n} (\lambda_{i1}, \cdots, \lambda_{in})'(\lambda_{i1}, \cdots, \lambda_{in}) \\ =& \sum_{i=1}^{n} (\lambda_{ij}\lambda_{ik}) = \left(\sum_{i=1}^{n} \lambda_{ij}\lambda_{ik} \right) \\ =& \Lambda'\Lambda. \end{aligned}$$

That is, Λ is an orthogonal matrix

$$(\lambda_{i1}, \cdots, \lambda_{in})\Lambda' = (\delta_{i1}, \cdots, \delta_{in}),$$

where δ_{ij} is Kronecker's delta. Thus

$$\Lambda\Gamma(E_{ii})\Lambda' = E_{ii}.$$

Let

$$\Delta(Z) = \Lambda\Gamma(Z)\Lambda',$$

then Δ has the same property as Γ, that is,