INFORMATION TO USERS

This dissertation was produced from a microfilm copy of the original document. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the original submitted.

The following explanation of techniques is provided to help you understand markings or patterns which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting thru an image and duplicating adjacent pages to insure you complete continuity.

2. When an image on the film is obliterated with a large round black mark, it is an indication that the photographer suspected that the copy may have moved during exposure and thus cause a blurred image. You will find a good image of the page in the adjacent frame.

3. When a map, drawing or chart, etc., was part of the material being photographed the photographer followed a definite method in "sectioning" the material. It is customary to begin photoing at the upper left hand corner of a large sheet and to continue photoing from left to right in equal sections with a small overlap. If necessary, sectioning is continued again – beginning below the first row and continuing on until complete.

4. The majority of users indicate that the textual content is of greatest value, however, a somewhat higher quality reproduction could be made from "photographs" if essential to the understanding of the dissertation. Silver prints of "photographs" may be ordered at additional charge by writing the Order Department, giving the catalog number, title, author and specific pages you wish reproduced.

University Microfilms

300 North Zeeb Road
Ann Arbor, Michigan 48106

A Xerox Education Company

Downloaded from SHAREOK. Persistent Handle URL: https://hdl.handle.net/11244/3360

72-29,900

McQUEEN, Henry Leon, 1938-
AUTOMORPHISMS OF THE SYMPLECTIC GROUP OVER LOCAL RINGS.

The University of Oklahoma, Ph.D., 1972
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED

THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

AUTOMORPHISMS OF THE SYMPLECTIC GROUP OVER LOCAL RINGS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirement for the

degree of

DOCTOR OF PHILOSOPHY

BY

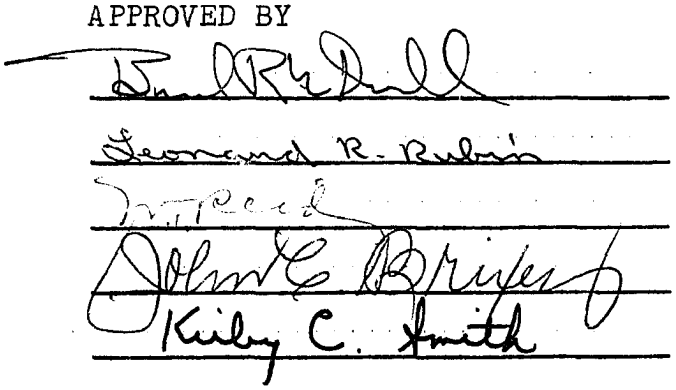
HENRY LEON MCQUEEN

Norman, Oklahoma

1972

AUTOMORPHISMS OF THE SYMPLECTIC GROUP OVER LOCAL RINGS

APPROVED BY



DISSERTATION COMMITTEE

PLEASE NOTE:

Some pages may have

indistinct print.

Filmed as received.

University Microfilms, A Xerox Education Company

ACKNOWLEDGMENTS

I express my gratitude to my thesis advisor, Bernard McDonald, who suggested the topic and provided assistance and encouragement throughout the course of the research.

I also thank my wife, Harriett, for her help in editing and typing and for her encouragement throughout the degree program.

TABLE OF CONTENTS

Page

INTRODUCTION 1

Chapter

I. SYMPLECTIC GROUPS 5

II. INVOLUTIONS 25

III. TRANSVECTIONS 36

IV. AUTOMORPHISMS 50

BIBLIOGRAPHY 62

AUTOMORPHISMS OF THE SYMPLECTIC GROUP OVER LOCAL RINGS

INTRODUCTION

The term "classical groups" has been used traditionally to mean the general linear group, $GL_n(V)$, and its subgroups which leave various forms invariant. In this paper, we shall investigate the symplectic group, $Sp_n(V)$, that is, the subgroup which leaves invariant a certain alternating form. In particular we shall determine the automorphisms of $Sp_n(V)$. Motivation is provided by the general observation that results for the general linear group can be carried over, in many instances, to the symplectic group.

The first book devoted to the theory of linear groups was Jordan's Traité des Substitutions in the 19th Century which developed earlier ideas of Galois. These results were subsequently refined by Dickson and others to the point that the structure of the general linear group, in the case where the space under consideration is a field, is relatively well known. For example, see Artin [1] and Dieudonné [7]. Following a natural course, many of these results have been generalized to modules over rings. Of particular interest to us is the specialization to local rings. Klingenberg [13], after earlier work on the structure

of the general linear group, studied the structure of the symplectic group. He showed that the symplectic group is generated by the transvections and that the only invariant subgroups are the congruence subgroups. We are able to use these facts to relate the local ring case to the field case.

The study of the automorphisms of the linear groups dates back to 1925 when Schreier and van der Waerden [23] determined the automorphisms of the general linear group over an arbitrary commutative field. Nearly a quarter of a century later Dieudonné [6] described the automorphisms of the general linear group over a non-commutative field. This was followed by investigations of the form of the automorphisms of $GL_n(V)$ where V is a free R-module for various rings R. Due to their related work on the symplectic group, we call attention to the work of Hua and Reiner [8] over the integers and O'Meara [17] and Chien [4] over integral domains. Recently Pomfret [19] described the automorphisms of the general linear group over local rings where the characteristic of the ring is other than 2 and the dimension of the module is at least 3.

As for the automorphisms of $Sp_n(V)$, the division ring case is virtually complete and can be found in Dieudonné [5]. We further note that many of those who had researched $GL_n(V)$ turned their attention to $Sp_n(V)$. The automorphisms of $Sp_n(V)$ over the ring of integers were

found by Reiner [20]. O'Meara [18] indicates that Wan has found the automorphisms over a commutative Euclidean ring of characteristic not 2 when $n \geq 6$. O'Meara then described all automorphisms of $Sp_n(V)$ over any commutative integral domain of any characteristic when $n \geq 4$. Throughout these studies of the linear groups, it is apparent that arguments, if they exist, in the cases for "small" dimension and rings of characteristic 2 require somewhat different methods than the other cases.

The approaches in determining automorphisms seem to be in two main veins. One is a highly computational argument as in Chien, Reiner, and Pomfret. The other, as exemplified by O'Meara, relies more on geometry.

We shall concern ourselves with the automorphisms of $Sp_n(V)$ where V is a free module over a local ring R with characteristic of $R/m \neq 2$ and $R/m \neq F_3$ where $n \geq 6$. (F_3 is the finite field of three elements.) The method is to determine the images of involutions and then the images of transvections. Recent work by Ojanguren and Sridharan [16] enables us to proceed à la O'Meara [18] and Dieudonné [6] in applying the fundamental theorem of projective geometry.

We conclude that the automorphisms of $Sp_n(V)$ are of the same general type as in the cases above, that is, $\sigma \to \chi(\sigma)g\sigma g^{-1}$ where g is a semi-linear isomorphism of V onto V and χ is a homomorphism of $Sp_n(V)$ into its center.

Notation and Terminology

Throughout this paper all rings are assumed to have identity element which is denoted by 1 or by I in the case of matrix rings. The symbol R always denotes a local ring with maximal ideal denoted by m.

The following is a list of symbols and a brief description of their use. Precise definitions are given in the text of the paper.

$GL_n(V)$, the group of invertible linear transformations of the free R-module V of dimension n.

Ω_n, the group of invertible n x n matrices.

$Sp_n(V)$, the symplectic group over V (dim V = n).

Γ_n, the subset of Ω_n corresponding to $Sp_n(V)$.

ρ_J, the natural morphism of $R \to R/J$ where J is an ideal of R.

g_J, the morphism $V \to V/JV$ induced by ρ_J.

h_J, the morphism of $Sp_n(V) \to Sp_n(V/JV)$ induced by g_J.

GSp(V,J), the general congruence subgroup mod J.

SSp(V,J), the special congruence subgroup mod J.

P(V), the collection of lines of V.

$SL_n(V)$, the subgroup of $GL_n(V)$ consisting of elements of determinant 1.

CHAPTER I

SYMPLECTIC GROUPS

Let R be a local ring with maximal ideal m and let $V = V(R)$ be an n-dimensional free R-module. If $\Phi: V \times V \to R$ is a bilinear form on V, then Φ induces homomorphisms d_Φ and ${}_\Phi d$ of V into its dual V^*. The mapping $d_\Phi: V \to V^*$ is given by $d_\Phi(x)(y) = \Phi(y,x)$ and the mapping ${}_\Phi d: V \to V^*$ is given by ${}_\Phi d(x)(y) = \Phi(x,y)$. Suppose $B = \{b_1, \ldots, b_n\}$ is an R-basis for V and let $b_{ij} = \Phi(b_i, b_j)$, then the matrix $[b_{ij}]$ is called the matrix of the form Φ relative to B and is denoted by $\mathrm{Mat}_B(\Phi)$. These concepts are related by:

Theorem 1.1. With the above notation, the following are equivalent.

(i) d_Φ is an isomorphism.

(ii) ${}_\Phi d$ is an isomorphism.

(iii) $\mathrm{Mat}_B(\Phi)$ is invertible.

Proof: See Lang [14].

Definition 1.1. A bilinear form on V satisfying any of the above equivalent conditions is called non-singular. The free module V is a symplectic space of dimension n if V is an n-dimensional free R-module on which is given a

non-singular bilinear form Φ satisfying $\Phi(x,x) = 0$ for all x in V.

Throughout this paper V will be a symplectic space with form Φ and R will be a local ring. Often instead of $\Phi(x,y)$, we write (x,y).

Definition 1.2. A submodule U of V is called a subspace if U is a direct summand of V. A subspace U is called non-isotropic if $d_\Phi|_U : U \to U^*$ is an isomorphism. An $(n-1)$-dimensional subspace of V is called a hyperplane of V; a 1-dimensional subspace is called a line of V; and a 2-dimensional subspace is called a plane of V.

Definition 1.3. Let U, U_1, U_2 be subspaces of V. We say that U is the orthogonal sum of U_1 and U_2, notation $U = U_1 \perp U_2$, if

(i) $U = U_1 \oplus U_2$ (U is the direct sum of U_1 and U_2)

(ii) $(u_1,u_2) = 0$ for every u_1 in U_1 and u_2 in U_2.

Let $U^o = \{v \text{ in } V \mid (v,u) = 0 \text{ for all } u \text{ in } U\}$. Note that $(x,x) = 0$ for all x in V implies $(x,y) = -(y,x)$ for x in V and y in V. Thus $(v,u) = 0$ implies $(u,v) = 0$.

Theorem 1.2. Let U be a subspace of V. Then

(i) U^o is a subspace of V.

(ii) $\dim U + \dim U^o = \dim V$.

(iii) $(U^o)^o = U$.

(iv) $\operatorname{Ker}(d_\Phi|_U : U \to U^*) = U \cap U^o$.

Proof: Since $d_\Phi : V \to V^*$ is an isomorphism, $d_\Phi(U)$ is a direct summand of V^*, say $V^* = d_\Phi(U) \oplus W$. Let $\pi_1 : V^* \to d_\Phi(U)$

and $\pi_2: V^* \to W$ be the natural projections. For σ in V^{**}, define σ_1 and σ_2 satisfying $\sigma = \sigma_1 + \sigma_2$ by $\sigma_1(f) = \sigma(\pi_1 f)$ and $\sigma_2(f) = \sigma(\pi_2 f)$ for any f in V^*. Note that if f is in W then $\sigma_1(f) = \sigma(\pi_1 f) = 0$ and if f is in $d_\Phi(U)$ then $\sigma_2(f) = \sigma(\pi_2 f) = 0$. Letting $S = \{\sigma \text{ in } V^{**} | \sigma(f) = 0 \text{ for all } f \text{ in } W\}$ and $T = \{\sigma \text{ in } V^{**} | \sigma(f) = 0 \text{ for all } f \text{ in } d_\Phi(U)\}$, it is clear that $V^{**} = S + T$.

Suppose that σ is in $S \cap T$. Then $\sigma(f) = 0$ for all f in $V^* = d_\Phi(U) \oplus W$. Thus $\sigma = 0$ and $V^{**} = S \oplus T$.

But there is a natural isomorphism between V and V^{**} given by $x \to x^{**}$ where $x^{**}(f) = f(x)$ for any f in V^*.

Suppose σ in T and x in V are such that $\sigma = x^{**}$. If u is in U, then $d_\Phi(u)(x) = x^{**}(d_\Phi(u)) = \sigma(d_\Phi(u)) = 0$, so that x is in U^o. Conversely if x is in U^o then $d_\Phi(u)(x) = 0$ for every u in U. Then $x^{**}(d_\Phi(u)) = 0$ so that x^{**} is in T. Thus we identify U^o in V with T in V^{**} and conclude that U^o is a direct summand of V. The module U^o is thus a subspace.

If $f_1, \ldots, f_m, f_{m+1}, \ldots, f_n$ form a dual basis for V^* with $f_1, \ldots, f_m$ a basis for $d_\Phi(U)$; and, if $\sigma_1, \ldots, \sigma_n$ are in V^{**} with $\sigma_i(f_j) = \delta_{ij}$, then $\sigma_1, \ldots, \sigma_n$ is a basis for V^{**} and T is spanned by $\sigma_{m+1}, \ldots, \sigma_n$. Thus dim U^o = dim T = codim U.

Observe that $U \subseteq U^{oo}$. Since both U and U^{oo} are direct summands with dim U = dim U^{oo}, it follows that $U = U^{oo}$.

Clearly $U \cap U^o = \ker(d_\Phi|_U)$.

Theorem 1.3. Let U be a subspace of V. The following are equivalent:

(i) U is non-isotropic.

(ii) U^o is non-isotropic.

(iii) $V = U \perp U^o$.

Proof: Assume U is non-isotropic. Then $d\Phi|_U : U \to U^*$ is an isomorphism. Let x be in V. Then there is a y in U satisfying $d\Phi(x)|_U = d\Phi|_U(y)$. Thus $d\Phi(x-y) = 0$ on U so that $x - y$ is in U^o. Hence there is a z in U^o with $x - y = z$, that is $x = y + z$. Thus $V = U + U^o$. Further, $0 = \ker(d\Phi|_U) = U \cap U^o$ so that $V = U \perp U^o$. Thus (i) implies (iii).

On the other hand, assume $V = U \perp U^o$. Then $d\Phi|_U$ is injective since $d\Phi|_U$ is a homomorphism with $\ker(d\Phi|_U) = U \cap U^o = 0$.

Observe that $d\Phi(V)|_U = U^*$. Let f be in U^*. Then there is an x in V satisfying $d\Phi(x)|_U = f$. Since $V = U \oplus U^o$, $x = u_1 + u_2$ with u_1 in U and u_2 in U^o. If u is in U, then $d\Phi(x)(u) = d\Phi(u_1+u_2)(u) = (u, u_1+u_2) = (u, u_1)$. Thus $f(u) = (u, u_1) = d\Phi(u_1)(u)$. Since $d\Phi|_U$ is injective, $d\Phi(x)(u) = f(u) = d\Phi(u_1)(u)$ implies $x = u_1$. Thus x is in U and $d\Phi|_U$ is surjective.

Hence $d\Phi|_U$ is an isomorphism and U is non-isotropic. Thus (iii) implies (i).

To show that (ii) and (iii) are equivalent, we observe that U^o is also a subspace of V and use the same argument as in the equivalence of (i) and (iii).

Theorem 1.4. Let x be in V. The following are equivalent:

(i) $g_m x \neq 0$ where $g_m : V \to V/mV$ is the natural projection.

(ii) If $x = \sum_{i=1}^{n} a_i u_i$ and $\{u_i\}_{i=1}^{n}$ is a basis of V, then $R = Ra_1 + \ldots + Ra_n$.

(iii) If $x = \sum_{i=1}^{n} a_i u_i$ and $\{u_i\}$ is a basis of V, then a_i is a unit for some i.

(iv) $Rx = L$ is a direct summand of V.

(v) There is an R-morphism $\sigma : V \to R$ satisfying $\sigma(x) = 1$.

(vi) $\{\sigma(x) | \sigma \text{ in } V^*\} = R$.

(vii) The map $h : R \to V$ given by $h(r) = rx$ is a split monomorphism.

Proof: Straightforward.

Definition 1.4. An element x in V satisfying any of the above is called unimodular.

We will make use of the following theorem for finitely generated modules over local rings.

Theorem 1.5. Let R be a local ring with maximal ideal m and let V be a finitely generated R-module.

(i) A subset $\{u_i\}_{i=1}^{n}$ of V is a generating set for V if and only if their residue classes $\{\bar{u}_i\}_{i=1}^{n}$ generate the R/m-vector space V/mV.

(ii) A subset $\{u_i\}_{i=1}^n$ of V is a minimal generating set for V if and only if $\{\bar{u}_i\}_{i=1}^n$ is a linearly independent R/m-basis for V/mV.

(iii) Any generating set for V contains a minimal generating set; if $u_1,\ldots,u_n$ and $v_1,\ldots,v_m$ are both minimal generating sets for V then m = n and there is an R-isomorphism of V → V that maps $u_i \to v_i$, $1 \leq i \leq n$.

Proof: See Nagata [15], pages 13, 14.

If J is an ideal of R ($J \neq R$), let V/JV denote the n-dimensional free module over R/J. The canonical homomorphism ρ_J:R → R/J induces a natural morphism g_J:V → V/JV. When a basis has been fixed, g_J reduces components of a vector modulo J.

If V is a symplectic space, then V/JV is a symplectic space over R/J formed by the vectors $g_J x$, x in V. The form $\bar{\Phi}$ on V/JV is given by $\bar{\Phi}(g_J x, g_J y) = \rho_J \Phi(x,y)$ where Φ is the form on V. If J = R, we extend these concepts by putting V/RV = 0.

Theorem 1.6. Let x in V be unimodular. Then there exists a y in V satisfying

(i) P = Rx + Ry is a plane and

(ii) $V = P \perp P^o$.

Proof: Since d_Φ:V → V* is an isomorphism and x in V is unimodular, there is a y' in V such that $d_\Phi(x)(y')$ is a unit. Thus there is a y in V satisfying (x,y) = 1.

It is easily seen that $\{x,y\}$ is R-free. The set $\{x,y\}$ may be extended to a basis for V. Let $\pi = g_m : V \to V/mV$ and note that $\overline{\Phi}(\pi x, \pi y) = \rho_m(x,y) = 1$. Thus $\pi x \neq \pi y$ and $\pi x \neq 0$, $\pi y \neq 0$. Thus extend πx, πy to a basis of V/mV and take their pre-images to obtain a basis for V.

By the above $P = Rx + Ry$ is a direct summand of V and hence a subspace. Considering $\Phi|_P$ and the basis $B = \{x,y\}$,

$$\mathrm{Mat}_B(\Phi|_P) = \begin{bmatrix} (x,x) & (x,y) \\ (y,x) & (y,y) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$\mathrm{Mat}_B(\Phi|_P)$ has unit determinant and thus by (1.1), P is non-isotropic. Hence by (1.3), $V = P \perp P^o$.

A pair $\{x,y\}$ of elements of V satisfying $(x,y) = 1$ is called <u>hyperbolic</u>. Thus the R-module $P = Rx + Ry$ spanned by a hyperbolic pair $\{x,y\}$ is a non-isotropic subspace of dimension 2; P is called a <u>hyperbolic plane</u>.

<u>Theorem</u> 1.7. A symplectic space V of dimension n is a direct sum of hyperbolic planes.

<u>Proof</u>: Since V is non-isotropic, $\dim V \neq 1$. For $\dim V = 2$, apply (1.6). For $\dim V > 2$, by (1.6), there is a hyperbolic plane P such that $V = P \perp P^o$. By (1.3) and (1.2), P^o is non-isotropic with dimension n-2. The proof is completed by induction. That is, we consider the symplectic space P^o and as in the proof of (1.6) conclude that P^o is the

orthogonal sum of a plane P_1 and its orthogonal complement in P^o.

Since a symplectic space is then a direct sum of hyperbolic planes, the dimension of V must be even, (say $n = 2r$). Further V must possess a basis $B = \{x_1, y_1, x_2, y_2, \ldots, x_r, y_r\}$ with $(x_i, y_i) = 1$, $(y_i, x_i) = -1$ for $1 \leq i \leq r$, with all other combinations of basis elements yielding zero. Thus with respect to the basis B,

$$\mathrm{Mat}_B(\Phi) = \begin{bmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & -1 & 0 \end{bmatrix}$$

The basis B is called a hyperbolic basis for V.

Let $B' = \{x_1, \ldots, x_r, y_1, \ldots, y_r\}$ be the set B with elements listed in the described order. Then with respect to the basis B',

$$\mathrm{Mat}_{B'}(\Phi) = \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix} \quad \text{where}$$

I_r denotes the r x r identity matrix and 0 is the r x r matrix with each element 0. The basis B' is called a symplectic basis for V.

The following examples illustrate some non-standard difficulties.

Example 1.1. Suppose U is a non-isotropic subspace of V and x in U is unimodular. Then there is a y in U satisfying $(x,y) = 1$. Thus if L is a 1-dimensional free R-module which is a direct summand of V, then L is not non-isotropic.

Example 1.2. It is possible that an element x in V is R-free but not unimodular. Consider the domain $Z_p = \{a/b \mid (b,p) = 1\}$, that is, the localization of the integers Z at a prime p. Note Z_p is a local ring. Let $V = Z_p \oplus Z_p$ and denote a standard basis by $e_1 = \langle 1,0\rangle$ and $e_2 = \langle 0,1\rangle$. Take x in V to be $x = \langle p,0\rangle = pe_1$. Since there are no torsion elements, we have x is Z_p-free. However modulo the maximal ideal, $g_m x = 0$, thus x is not unimodular.

Example 1.3. We may have elements not contained in any 1-dimensional summand. Let $R = (Z/Zp)[X,Y]/(X^2,XY,Y^2)$ $= \{a + bX + cY \mid a,b,$ and c in $Z/Zp\}$ (Z/Zp denotes the integers Z modulo a prime p). Let $V = R \oplus R = Re_1 \oplus Re_2$; $e_1 = \langle 1,0\rangle$, $e_2 = \langle 0,1\rangle$. Let a in V be given by $a = Xe_1 + Ye_2$. Suppose b is in V, b unimodular, and $rb = a$. Then $b = s_1e_1 + s_2e_2$ and thus $a = rb = rs_1e_1 + rs_2e_2$. Hence $X = rs$, and $Y = rs_2$ with s_1 or s_2 a unit. But this is impossible. Thus a is not contained in any 1-dimensional summand.

Definition 1.5. Let V and V' be symplectic spaces over the local ring R with bilinear forms Φ and Φ' respectively.

An R-isomorphism $\sigma: V \to V'$ satisfying $\Phi(x,y) = \Phi'(\sigma x, \sigma y)$ shall be called an isometry and we say V and V' are isometric.

If V and V' have the same dimension, then each must have a hyperbolic basis, say B and B' respectively. Then there is a linear map carrying B onto B' which is an isometry. We thus have the following corollary.

Corollary 1.8. Let V be a symplectic space. Then the dimension of V is even. Further, any two symplectic spaces with the same dimension are isometric.

Definition 1.6. Let V by a symplectic space with dimension $n = 2r$. Let $Sp_n(V)$ denote the set of isometries of V onto V. Observe $Sp_n(V)$ contains both 1_V (identity on V) and -1_V and further $Sp_n(V)$ forms a group. The group $Sp_n(V)$ is called the symplectic group over V.

Consider a symplectic space V with dimension $n = 2r$ and let B be a symplectic basis of V. Let

$$\mathrm{Mat}_B(\Phi) = \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix}$$

be designated by F. Let Ω_n denote the group of all invertible matrices over R. If M is in Ω_n, M^t shall denote the transpose of M. Let Γ_n consist of all n x n matrices M in Ω_n satisfying $MFM^t = F$. We observe that Γ_n forms a subgroup of Ω_n. Lang ([14], page 344) shows that an n x n matrix M is the matrix of an automorphism of the form Φ

(relative to our basis) if and only if $MFM^t = F$. That is, an element σ is in $Sp_n(V)$ if and only if the matrix of σ, relative to the symplectic basis B of V, is an element of Γ_n.

The following provides criteria for determining when n x n matrices belong to Γ_n.

Let $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, where A, B, C, and D are r x r matrices with entries in R.

Lemma 1.9. For the above setting, M is in Γ_n if and only if the following conditions are satisfied:

(i) AB^t is symmetric.

(ii) CD^t is symmetric.

(iii) $AD^t - BC^t = I$.

Proof: If M is in Γ_n, then $MFM^t = F$.

Thus $\begin{bmatrix} A & B \\ C & D \end{bmatrix}\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}\begin{bmatrix} A^t & C^t \\ B^t & D^t \end{bmatrix} = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$.

So $\begin{bmatrix} -BA^t + AB^t & -BC^t + AD^t \\ -DA^t + CB^t & -DC^t + CD^t \end{bmatrix} = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$

Then $BA^t = AB^t$, $DC^t = CD^t$, and $AD^t - BC^t = I$.

Conversely if AB^t is symmetric, CD^t is symmetric, and $AD^t - BC^t = I$, then $DA^t - CB^t = I$. Thus from the above

computation $MFM^t = F$.

We now record Klingenberg's [13] results on normal subgroups of $Sp_n(V)$. The map $g_J: V \to V/JV$ (J ideal of R) determines a homomorphism $h_J: Sp_n(V) \to Sp_n(V/JV)$. When a basis has been fixed, h_J merely reduces entries of a matrix modulo J. More precisely h_J is defined by $(h_J\sigma)(g_Jx) = g_J(\sigma x)$ for all σ in $Sp_n(V)$ and x in V. Let $Sp_n(V/RV)$ be the identity group.

Let J be an ideal in R.

Definition 1.7. The general congruence subgroup mod J of $Sp_n(V)$, denoted by $GSp(V,J)$, is the group $h_J^{-1}(\text{center } Sp_n(V/JV))$.

Definition 1.8. The special congruence subgroup mod J of $Sp_n(V)$, denoted by $SSp(V,J)$ is the group $h_J^{-1}(1) = \text{kernel } h_J$.

For the extreme cases we have, $GSp(V,R) = SSp(V,R) = Sp_n(V)$; $GSp(V,0) = \text{center } (Sp_n(V))$; $SSp(V,0) = $ identity group.

Definition 1.9. A (symplectic) transvection is an element τ in $Sp_n(V)$ of the form $\tau x = x + \lambda(a,x)a$ for x in V where a is a unimodular element of V and λ is in R. If λ is a unit in R, then τ is a regular transvection.

Let $\tau_{a,\lambda}$ denote the transvection given by $\tau_{a,\lambda}(x) = x + \lambda(a,x)a$ for x in V. Note that $\tau_{a,\lambda}$ is an R-linear map. Further, if x and y are elements of V, then

$$(\tau x, \tau y) = (x + \lambda(a,x)a,\ y + \lambda(a,y)a)$$

$$= (x,y) + (x,\lambda(a,y)a) + (\lambda(a,x)a,y) + (\lambda(a,x)a,\lambda(a,y)a)$$

$$= (x,y) + \lambda(a,y)(x,a) - \lambda(x,a)(a,y)$$

$$= (x,y).$$

Thus, since V is a symplectic space, $\tau_{a,\lambda}$ is an isometry and $\tau_{a,\lambda}$ is indeed an element of $Sp_n(V)$.

Definition 1.10. The line Ra is called a line of τ ($\tau = \tau_{a,\lambda}$). Note that $(\tau - 1_V)V \subseteq Ra$. Further $H = (Ra)^o$ is a hyperplane satisfying $\tau x = x$ for x in H. The subspace H is called a hyperplane of τ. (Note dim (Ra) = 1 implies dim H = n - 1).

Lemma 1.10. Let V be a symplectic space of dimension n and let τ be in $Sp_n(V)$. Then there exists a hyperplane H on which τ is the identity map if and only if there is a line L such that $\tau x - x$ is in L for all x in V.

Proof: Let H be a hyperplane on which τ is the identity. Since dim H + dim H^o = n implies dim H^o = 1, there is a unimodular a in V with H^o = Ra. Let L = H^o. If x in V and h in H, then $(\tau x - x, h) = (\tau x,h) - (x,h) = (x,\tau^{-1}h) - (x,h) = (x,h) - (x,h) = 0$. Thus $\tau x - x$ is an element of H^o = L for all x in V.

On the other hand, suppose there is a line L = Ra such that $\tau x - x$ is in L for all x in V. Then $H = L^o$ is a hyperplane of V. Recall, since V is symplectic, if $(x,y) = (x,y')$ for all x in V then $y = y'$. Let y be in H. Then for any x in V, $0 = (\tau x - x, y) = (\tau x,y) - (x,y)$ so that $(\tau x,y) = (x,y)$. But then $(x, \tau^{-1}y) = (x,y)$ for all x

in V. Hence $\tau^{-1}y = y$ and $\tau y = y$, that is τ is the identity on H.

Thus if $\tau_{a,\lambda}$ is a transvection, it acts like the identity on the hyperplane $H = (Ra)^{\circ}$ and $(\tau_{a,\lambda} - 1_V)V \subseteq Ra$. We observe in the following theorem that if an element of $Sp_n(V)$ has these properties, then it is a transvection.

Theorem 1.11. Let τ be an element of $Sp_n(V)$ satisfying $\tau x = x$ for all x in a hyperplane H. Then τ has the form $\tau_{a,\lambda}$ for some unimodular a in V and λ in R.

Proof: Let τ in $Sp_n(V)$ be the identity on the hyperplane H in V. Then $H^{\circ} = Ra$ for some unimodular a in V. Since V is symplectic, there exists a b in V with $(a,b) = 1$ and $V = \langle a,b\rangle \perp P$, ($\langle a,b\rangle$ denotes the plane generated by the pair $\{a,b\}$). Then by (1.10) $\tau b - b$ is in Ra. Thus $\tau b = b + \lambda a$ for some λ in R. We claim $\tau = \tau_{a,\lambda}$.

Note $\tau_{a,\lambda}(b) = b + \lambda(a,b)a = b + \lambda a = \tau(b)$. If x is in V, then $x = ra + sb + p$ for r and s in R and p in P. Then

$$\begin{aligned}\tau(x) &= r\tau a + s\tau b + \tau p \\ &= ra + s\tau b + p \text{ (since a and p are in H)} \\ &= ra + sb + s\lambda a + p \text{ (since } \tau b = b + \lambda a).\end{aligned}$$

$$\begin{aligned}\text{But } \tau_{a,\lambda}(x) &= x + \lambda(a,x)a \\ &= ra + sb + p + \lambda(a, ra + sb + p)a \\ &= ra + sb + p + \lambda sa.\end{aligned}$$

Thus $\tau = \tau_{a,\lambda}$.

Consequently if τ is an element of $Sp_n(V)$ and if H is

a hyperplane such that $\tau x = x$ for all x in H, then τ is a transvection. Conversely, if τ is a transvection, then clearly τ fixes some hyperplane of V. However the representation of τ may not be unique. For $\tau_{a,\lambda} = \tau_{b,\mu}$ for any pair $\langle b,\mu\rangle$ in $V \times R$ with b unimodular satisfying $\lambda(a,x)a = \mu(b,x)b$ for all x in V. In the case of regular transvections we can establish a "form" of uniqueness.

Lemma 1.12. Let $\tau_{a,\lambda}$ be a regular transvection in $Sp_n(V)$. Let $\tau_{b,\mu}$ be a transvection in $Sp_n(V)$ such that $\tau_{b,\mu} = \tau_{a,\lambda}$. Then there exists a unit α in R satisfying $a = \alpha b$ and $\alpha^{-2}\mu = \lambda$ (then $\tau_{b,\mu}$ must be regular).

Proof: From $\tau_{b,\mu} = \tau_{a,\lambda}$ we have $\tau_{a,\lambda}(x) = \tau_{b,\mu}(x)$ for all x in V. Thus $x + \lambda(a,x)a = x + \mu(b,x)b$ and finally $\lambda(a,x)a = \mu(b,x)b$ for all x in V.

Since a is unimodular, there is an x_1 in V satisfying $(a,x_1) = 1$. Since λ is a unit, $a = \lambda^{-1}\mu(b,x_1)b$. Since b is unimodular, there is an x_2 in V satisfying $(b,x_2) = 1$. Thus $\mu b = \lambda(a,x_2)a$. Then $a = \lambda^{-1}\mu(b,x_1)b = \lambda^{-1}\lambda(a,x_2)(b,x_1)a$. Since $\{a\}$ may be extended to a basis of V, we have $(a,x_2)(b,x_1) = 1$. Thus (a,x_2) and (b,x_1) are units, indeed are inverses.

Let $\alpha = \mu\lambda^{-1}(b,x_1)$. Then $a = \alpha b$. Further $(b,x_1)^{-1} = (a,x_2) = (\alpha b,x_2) = \alpha(b,x_2) = \alpha$. Thus α is a unit and hence μ is a unit. Thus $\tau_{b,\mu}$ is a regular transvection.

Noting that $\mu = \lambda(b,x_1)^{-2}$ we compute $\alpha^{-2}\mu$; $\alpha^{-2}\mu = (\mu\lambda^{-1}(b,x_1))^{-2}\mu = (b,x_1)^{-2}\lambda^2\mu^{-2}\mu = (b,x_1)^{-2}\lambda^2\mu^{-1} = (b,x_1)^{-2}\lambda^2(b,x_1)^2\lambda^{-1} = \lambda$.

Corollary 1.13. If $\tau_{a,\lambda}$ is a regular transvection, then $\tau_{a,\lambda}$ has exactly one line and hence one hyperplane.

Proof: Immediate using lemma 1.12.

Let u be an element of R. Then o(u) denotes the ideal generated by u. Let x be in V; the order of x, o(x), is the smallest ideal $J \subseteq R$ such that $g_J x = 0$. Let σ be in $Sp_n(V)$; the order of σ, $o(\sigma)$, is the smallest ideal $J \subseteq R$ such that $h_J\sigma$ is in $Sp_n(V/mV)$, that is σ in $GSp(V,J)$. Note that o(x) is generated by the components of x with respect to any basis of V. Thus if o(x) = R, then x is unimodular.

Theorem 1.14. Center $Sp_n(V) = \{1_V, -1_V\}$.

Proof: Klingenberg [13].

Corollary 1.15. For $J \neq R$, $GSp(V,J)/SSp(V,J) \simeq \{1_V, -1_V\}$.

Corollary 1.16. Let $\tau_{a,\lambda}$ be a transvection. Then $o(\tau) = o(\lambda)$.

Theorem 1.17. SSp(V,J) is generated by the symplectic transvections of order contained in J. In particular, $Sp_n(V)$ is generated by the transvections.

Proof: Klingenberg [13].

Klingenberg discusses the structure of $Sp_n(V)$. For this study, we are restricted to local rings R with characteristic of $(R/m) \neq 2$ and $R/m \neq F_3 = Z/3Z$.

Theorem 1.18. The only normal proper subgroups of the symplectic group $Sp_n(V)$ over V are the congruence subgroups GSp(V,J) and SSp(V,J), J an ideal not R.

Proof: Klingenberg [13].

Corollary 1.19. $SSp(V,J)$ = commutator $(Sp_n(V),GSp(V,J))$ = commutator $(Sp_n(V),SSp(V,J))$. In particular, commutator $(Sp_n(V), Sp_n(V)) = Sp_n(V)$.

Proof: Klingenberg [13].

Theorem 1.20. The group $GSp(V,m)$ is characteristic under a group automorphism $\Lambda: Sp_n(V) \to Sp_n(V)$.

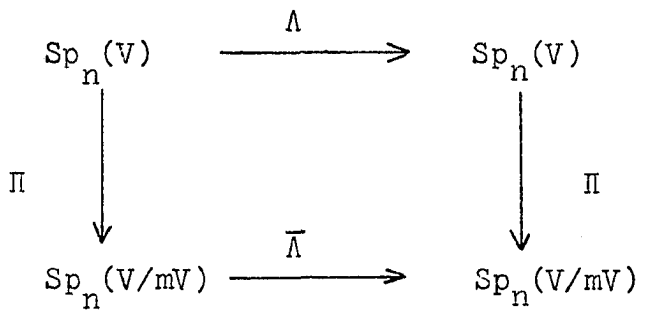
Proof: By theorem 1.18, the maximal normal subgroup of $Sp_n(V)$ is $GSp(V,m)$. Let $\Lambda: Sp_n(V) \to Sp_n(V)$ be a group automorphism. Since normal subgroups are carried to normal subgroups under Λ we have that $\Lambda(GSp(V,m)) \subseteq GSp(V,m)$. Thus $GSp(V,m)$ is characteristic under Λ.

Theorem 1.21. The normal subgroup $SSp(V,m)$ is characteristic under group automorphisms of $Sp_n(V)$.

Proof: By corollary 1.19, $SSp(V,m)$ is the commutator of $Sp_n(V)$ and $GSp(V,m)$. Let Λ be a group automorphism of $Sp_n(V)$. Let g be in $Sp_n(V)$ and h in $GSp(V,m)$. By theorem 1.20, Λh is in $GSp(V,m)$. Thus $\Lambda(ghg^{-1}h^{-1}) = \Lambda g \Lambda h \Lambda g^{-1} \Lambda h^{-1}$ is in the commutator $SSp(V,m)$ of $Sp_n(V)$ and $GSp(V,m)$. Thus $\Lambda(SSp(V,m))$ is contained in $SSp(V,m)$; that is $SSp(V,m)$ is characteristic.

Let $\Pi = h_m: Sp_n(V) \to Sp_n(V/mV)$. For Λ an automorphism of $Sp_n(V)$ define $\overline{\Lambda}: Sp_n(V/mV) \to Sp_n(V/mV)$ by $\overline{\Lambda}(\Pi\sigma) = \Pi(\Lambda\sigma)$ for σ in $Sp_n(V)$. We show that $\overline{\Lambda}$ is well defined. Suppose σ and β are in $Sp_n(V)$ such that $\Pi\sigma = \Pi\beta$. Then $\Pi(\sigma\beta^{-1}) = 1_V$ and $\sigma\beta^{-1} = \tau$ with τ in $\Pi^{-1}(1_V) = SSp(V,m)$. Thus $\Lambda(\sigma\beta^{-1}) = \Lambda\tau$ is in $SSp(V,m)$ by theorem 1.21. Then $\Lambda\sigma\Lambda\beta^{-1} = \Lambda\tau$ and

$\Pi(\Lambda\sigma\Lambda\beta^{-1}) = \Pi(\Lambda\tau) = 1_V$. Hence $\Pi(\Lambda\sigma) = \Pi(\Lambda\beta)$ and $\overline{\Lambda}$ is well defined. This provides the following important commutative diagram:



For the remainder of this chapter, R will denote a finite local ring. We let m denote the maximal ideal of R and put $k = R/m$. We will determine $|Sp_n(V)|$.

If $\tau_{a,\lambda}$ is a transvection in $Sp_n(V)$, then $h_m(\tau_{a,\lambda}) = \tau_{\bar{a},\,\bar{\lambda}}$ is a transvection in $Sp_n(V/mV)$, ($\bar{a}$ denotes $g_m a$ and $\bar{\lambda}$ denotes $\rho_m \lambda$). Since every transvection in $Sp_n(V/mV)$ can be obtained in this fashion and since these transvections generate $Sp_n(V/mV)$, we have $h_m: Sp_n(V) \to Sp_n(V/mV)$ is surjective.

Artin [1], page 146-147, calculates $|Sp_n(V/mV)| = |k|^{r^2} \prod_{i=1}^{r} (|k|^{2i} - 1)$, $(n = 2r)$. Further we have $(|k|^n - 1)|m|^n = |R|^n - |m|^n$ unimodular elements v in V. For each of these v, there are $(|k|^n - |k|^{n-1})|m|^n = |R|^n - |R|^{n-1}|m|$ unimodular vectors w such that (v,w) is a unit and $(|k|^2 - |k|)|m|^2 = |R|^2 - |R||m|$ of them span the same plane $\langle v,w \rangle$. Thus we have $|R|^{n-2}$ hyperbolic planes $\langle v,w \rangle$.

Now, in each plane there are $(|k|^2 - |k|)|m|^2 = |R|^2 - |R||m|$ vectors w with (v,w) a unit and these vectors w determine lines Rw with $(|k| - 1)|m| = |R| - |m|$ of them giving the same line. Now the plane $\langle v,w \rangle$ contains $|R| = |k||m|$ lines Rz with (v,z) a unit. On each line there exists an x with (v,x) = 1. Thus there exists $|k|^{n-1}|m|^{n-1} = |R|^{n-1}$ pairs with first component x. Since there are $(|k|^n - 1)(|m|)^n = |R|^n - |m|^n$ such vectors v, we have that the number of hyperbolic pairs, λ_n, is given by $\lambda_n = |R|^{n-1}(|R|^n - |m|^n)$.

Let $\Delta_n = |Sp_n(V)|$. A given hyperbolic pair $\{v,w\}$ can be moved to any other hyperbolic pair by a σ in $Sp_n(V)$, that is into any of λ_n pairs. If σ and τ move $\{v,w\}$ to the same pair, then $\tau^{-1}\sigma$ will leave $\langle v,w \rangle$ fixed. Let $V = \langle v,w \rangle \perp \langle v,w \rangle^o$. Then if $\rho = \tau^{-1}\sigma$, we have $\rho = 1_U \perp \rho_{U^o}$ where $U = \langle v,w \rangle$ and ρ_{U^o} is in the group of U^o. Thus $\Delta_n = \lambda_n \Delta_{n-2}$. So $\Delta_n = \lambda_n \lambda_{n-2} \cdots \lambda_2$

$$= |R|^{(n-1) + (n-3) + \ldots + 1} \prod_{i=1}^{(\frac{n}{2})} (|R|^{2i} - |m|^{2i})$$

$$= |R|^{(\frac{n}{2})^2} \prod_{i=1}^{\frac{n}{2}} (|R|^{2i} - |m|^{2i})$$

$$= |m|^{(\frac{n}{2})^2} |m|^{2(1+2+\ldots+\frac{n}{2})} \left[|k|^{(\frac{n}{2})^2} \prod_{i=1}^{\frac{n}{2}} (|k|^{2i} - 1) \right]$$

$$= |m|^{(\frac{n}{2})^2} |m|^{\frac{n(n+2)}{4}} |Sp_n(V/mV)|$$

$$= |m|^{\frac{n(n+1)}{2}} |Sp_n(V/mV)|.$$

CHAPTER II

INVOLUTIONS

An element σ in $Sp_n(V)$ is called an <u>involution</u> if $\sigma^2 = 1_V$. In this chapter we investigate the action of automorphisms of $Sp_n(V)$ on involutions. We shall assume that the characteristic of the field R/m is other than 2. Thus we have $r = -r$ implies $r = 0$ and $r^2 = 1$ implies $r = \pm 1$.

Let σ be an involution in $Sp_n(V)$. With σ, associate two submodules of V:

$$U = \{x \text{ in } V \mid \sigma(x) = -x\} \qquad \text{and}$$

$$W = \{x \text{ in } V \mid \sigma(x) = x\} .$$

Obviously $U \cap W = 0$. If x is in V,

$$x = 1/2(x - \sigma(x)) + 1/2(x + \sigma(x)).$$

Since $x - \sigma(x)$ is in U and $x + \sigma(x)$ is in W, we have $V = U \oplus W$. Thus the involution σ in $Sp_n(V)$ determines a unique splitting $\sigma: V = U \oplus W$. The spaces U and W are called the <u>proper spaces of σ</u>. We define the <u>index of σ</u>, denoted ind σ, by ind σ = min{dim U, dim W}.

Since $\sigma^2 = 1_V$, we have

$$\Phi((\sigma + 1_V)x, (\sigma - 1_V)y) = \Phi(\sigma x + x, \sigma y - y)$$

$$= \Phi(\sigma x, \sigma y) - \Phi(\sigma x, y) + \Phi(x, \sigma y) - \Phi(x, y)$$

$$= \Phi(x,y) - \Phi(x,\sigma y) + \Phi(x,\sigma y) - \Phi(x,y)$$

$$= 0$$

Further if v is in V then v = u + w for some u in U, w in W. Then $(\sigma + 1_V)(v) = \sigma v + v = \sigma u + \sigma w + u + w = w + w$ is in W. If w is in W, then $(\sigma + 1_V)(1/2\ w) = 1/2\ \sigma(w) + 1/2\ w = w$. Thus $(\sigma + 1_V)V = W$. Similarly $(\sigma - 1_V)V = U$. We have $V = U \perp W$.

Further observe that $W = U^{\circ}$. For if x is an element of W, then $(x,U) = 0$ so that $W \subseteq U^{\circ}$. On the other hand, if x is in U°, then $(x,U) = 0$. Now x in V implies $x = u + w$ with u in U and w in W. Then $0 = (x,U) = (u + w,U) = (u,U) + (w,U) = (u,U)$. But $d_{\Phi}: V \to V^*$ is an isomorphism. For v in V, $v = u_1 + w_1$ for some u_1 in U and w_1 in W. Then $d_{\Phi}(u)(v) = (v,u) = (u_1 + w_1,u) = (u_1,u) + (w_1,u) = 0$. Thus $d_{\Phi}(u)$ is the zero map on V and $u = 0$. Therefore $x = u + w = w$ and $U^{\circ} \subseteq W$. Thus $W = U^{\circ}$ and $V = U \perp W = U \perp U^{\circ}$. In particular, U and W are non-isotropic subspaces of V. Further dim U and dim W must then be even. So if σ is an involution in $Sp_n(V)$, the index of σ must be even.

The following facts are evident.

(i) If σ_1 and σ_2 are involutions in $Sp_n(V)$, then $\sigma_1 = \pm\sigma_2$ if and only if they have the same proper spaces.

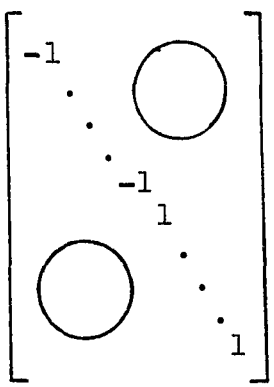
(ii) Let σ_1 and σ_2 be involutions in $Sp_n(V)$. Then $\sigma_1\sigma_2$ is an involution if and only if $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

(iii) Let β be an element of $Sp_n(V)$ and let σ be an involution in $Sp_n(V)$ with proper spaces U and W. Then

$\beta\sigma\beta^{-1}$ is an involution with proper spaces βU and βW.

(iv) Let β be in $\mathrm{Hom}_R(V,V)$ and σ in $Sp_n(V)$ with proper spaces U and W. Then $\beta\sigma = \sigma\beta$ if and only if $\beta U \subseteq U$ and $\beta W \subseteq W$.

Theorem 2.1. Let V be a symplectic space with dimension $n = 2r$ and let B be a symplectic basis of V. Let σ be an involution in $Sp_n(V)$ and let A be the matrix representation of σ with respect to B. Then there exists an integer t such that A is similar to $P \oplus P$ where P is a matrix of the form

$P =$  with t -1's,

that is $P = -I_t \oplus I_{r-t}$.

Proof: The involution σ determines a splitting of V, $\sigma: V = U \perp W$ with $\sigma = -1_U \oplus 1_W$. By the previous discussion, we have that U and W are non-isotropic subspaces and thus each must have a symplectic basis. Let $\{x_1,\ldots,x_t,y_1,\ldots,y_t\}$ be a symplectic basis for U and $\{x_{t+1},\ldots,x_r,y_{t+1},\ldots,y_r\}$ be a symplectic basis for W. Since R is local, it follows that $\{x_1,\ldots,x_r,y_1,\ldots,y_r\}$ is a symplectic basis for V.

Let $B = \{v_1,\ldots,v_r,v_1',\ldots,v_r'\}$ be our original

symplectic basis for V. Define a change of basis matrix Q by $Q(v_i) = x_i$ and $Q(v_i') = y_i$ for $i = 1,2,\ldots,r$. Since Q maps a symplectic basis of V to a symplectic basis, it is an element of Γ_n. But $Q^{-1}AQ = P \oplus P$ where P is of the form described in the statement of the theorem.

Note that dim U = 2t and dim W = n - 2t. Recall ind σ = min{dim U, dim W} = min{2t, n-2t}. Thus if ind σ = k, then the matrix of σ is similar to a diagonal matrix with either k or (n-k) -1's; the other entries being 1's. If the matrix has k -1's, we shall say σ is of <u>type</u> (k, n-k) and if the matrix has (n-k) -1's, we say σ has <u>type</u> (n-k, k). Thus σ has index k if and only if σ is either of type (k, n-k) or (n-k, k).

For computational purposes, the notion of <u>symplectic direct sum</u> is sometimes useful. If M_1 and M_2 are given by

$$M_1 = \begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} A_2 & B_2 \\ C_2 & D_2 \end{bmatrix}$$

then the symplectic direct sum of M_1 and M_2, denoted $M_1 * M_2$, is given by

$$M_1 * M_2 = \begin{bmatrix} A_1 & 0 & B_1 & 0 \\ 0 & A_2 & 0 & B_2 \\ C_1 & 0 & D_1 & 0 \\ 0 & C_2 & 0 & D_2 \end{bmatrix}$$

A straightforward computation shows that if

$$Y_i = \begin{bmatrix} A_i & B_i \\ C_i & D_i \end{bmatrix} \quad (i = 1,2) \text{ is in } \Gamma_{n_1} \text{ and}$$

$$Z_i = \begin{bmatrix} E_i & F_i \\ G_i & H_i \end{bmatrix} \quad (i = 1,2) \text{ is in } \Gamma_{n_2}$$

then $(Y_1 * Z_1)(Y_2 * Z_2) = Y_1Y_2 * Z_1Z_2$.

Note if σ is an involution in $Sp_n(V)$ with mat $(\sigma) = A$, then A is similar to a matrix in the form $-I^{(2t)} * I^{2(n-t)}$.

Let Ψ_n be the collection of matrices in Γ_n with the form $E_n = F_r \oplus F_r$ where F_r is a matrix in Ω_r having 1 or -1 in any combination on the main diagonal and zeroes elsewhere. By (1.9) it is clear that E_n in Ψ_n is an element of Γ_n. Further any two elements of Ψ_n commute and any E_n in Ψ_n is an involution.

Theorem 2.2. If $\{A_i\}_{i=1}^{s}$ is a collection of pairwise commutative involutions in Γ_n, then there is a P in Γ_n for which $P^{-1}A_iP$ is in Ψ_n for all $i = 1,2,\ldots,s$.

Proof: Consider first the case $n = 2$. Let A be an involution in Γ_2 given by

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ so that

$a^2 = 1$. But then $a = \pm 1$, so that $A = \pm I$.

Proceeding by induction, assume the theorem holds in Γ_{2k} for $1 \leq k \leq r$ $(n=2r)$. If A_i is an involution with index 0 or n, then $A_i = \pm I$. Thus we may assume that A_1 has index t for some t satisfying $2 \leq t \leq n-2$, otherwise the result would be trivial.

Since A_1 has index t, there is a Q in Γ_n such that $Q^{-1}A_1Q = -I^{(t)} * I^{(n-t)}$, (or $-I^{(n-t)} * I^{(t)}$, in which case the argument is similar). For each i, $i \leq i \leq s$, the matrix $Q^{-1}A_iQ$ commutes with $Q^{-1}A_1Q$ and therefore has the form $Q^{-1}A_iQ = B_i^{(t)} * B_i^{(n-t)}$ where $B_i^{(q)}$ denotes a q by q matrix block. Checking the criteria for membership in Γ_t and Γ_{n-t} yields that $B_i^{(t)}$ is an involution in Γ_t and $B_i^{(n-t)}$ is an involution in Γ_{n-t}. Also since $\{A_i\}_{i=1}^{s}$ is a pairwise commutative collection, we have that $\{B_i^{(t)}\}_{i=1}^{s}$ and $\{B_i^{(n-t)}\}_{i=1}^{s}$ are collections of pairwise commutative involutions from Γ_t and Γ_{n-t} respectively.

By induction, there exist $Q^{(t)}$ in Γ_t and $Q^{(n-t)}$ in Γ_{n-t} such that

$$Q^{(t)^{-1}} B_i^{(t)} Q^{(t)} \text{ is in } \Psi_n$$

and

$$Q^{(n-t)^{-1}} B_i^{(n-t)} Q^{(n-t)} \text{ is in } \Psi_{n-t}.$$

Therefore for all i, $1 \leq i \leq s$,

$$(Q^{(t)^{-1}} * Q^{(n-t)^{-1}}) Q^{-1} A_i Q (Q^{(t)} * Q^{(n-t)})$$

is in Ψ_n and the proof is complete.

Our discussion of involutions to this point has involved in most cases the use of symplectic basis. We recall that a symplectic basis $\{x_1,\ldots,x_r,y_1,\ldots,y_r\}$ gives rise to a hyperbolic basis $\{x_1,y_1,\ldots,x_r,y_r\}$ (and conversely). That is, we may assume that there is a splitting of V into hyperbolic planes, $V = P_1 \perp P_2 \perp \ldots \perp P_r$. In this context an involution $\sigma: V \to V$ is of index $k = 2t$ if σ is similar to

$$\sigma' = -1_{P_1} \oplus \ldots \oplus -1_{P_t} \oplus 1_{P_{t+1}} \oplus \ldots \oplus 1_{P_r} \quad \text{or}$$

$$\sigma'' = -1_{P_1} \oplus \ldots \oplus -1_{P_{r-t}} \oplus 1_{P_{r-t+1}} \oplus \ldots \oplus 1_{P_r}.$$

In this case an element of Ψ_n as described above will consist of the set of involutions

$$(\pm 1_{P_1}) \oplus (\pm 1_{P_2}) \oplus \ldots \oplus (\pm 1_{P_r}).$$

If we consider matrix representations of elements of Ψ_n in terms of a hyperbolic basis of V, we see that such an element is a direct sum of 2 x 2 block matrices, where each block is $\pm$ I.

Theorem 2.3. Let X be a set of involutions in $Sp_n(V)$. Then the following are equivalent:

(i) The elements of X are pairwise commutative.

(ii) There is a splitting of V into hyperbolic planes, $V = P_1 \perp \ldots \perp P_r$, such that $\sigma P_i = \pm P_i$ (that is $\sigma = \pm 1_{P_i}$) for $i = 1,2,\ldots,r$ and all σ in X. Thus each σ in X will have the form $\sigma = (\pm 1_{P_1}) \perp \ldots \perp (\pm 1_{P_r})$.

(iii) There is an element β in $Sp_n(V)$ such that $mat(\beta^{-1}\sigma\beta)$ is in Ψ_n for all σ in X.

Proof: ((i) implies (iii)). This is the result of (2.2) when translated to $Sp_n(V)$ and formulated with a hyperbolic basis.

((iii) implies (i)). If σ_1 and σ_2 are in X, then there is a β in $Sp_n(V)$ such that $\beta^{-1}\sigma_1\beta$ and $\beta^{-1}\sigma_2\beta$ are in Ψ_n. Since elements of Ψ_n are pairwise commutative, we have $(\beta^{-1}\sigma_1\beta)(\beta^{-1}\sigma_2\beta) = (\beta^{-1}\sigma_2\beta)(\beta^{-1}\sigma_1\beta)$. But then $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

((ii) implies (iii)). Letting $\beta = 1_V$ will suffice.

((iii) implies (ii)). Let $\{x_1,\ldots,x_n\}$ be a hyperbolic basis for V. By (iii) there is a change of basis map β so that $\beta^{-1}\sigma\beta$ is in Ψ_n for all σ in X. Thus the new basis gives a splitting of V with the desired condition.

Corollary 2.4. Let V be a symplectic space of dimension $n = 2r$. Let X be a collection of pairwise commutative involutions in $Sp_n(V)$, each of index $k = 2t$. Then there are at most $2\binom{r}{t}$ elements in X.

Proof: Let $V = P_1 \perp \ldots \perp P_r$ be a splitting of V

into hyperbolic planes. Then we can choose t of these planes in $\binom{r}{t}$ ways. If $2k \neq r$, there are $2\binom{r}{t}$ elements of Ψ_n of index k. If $2k = r$, there are $\binom{r}{t}$ elements of Ψ_n of index k. In either case (2.3) yields our result.

Corollary 2.5. Let V be a symplectic space of dimension $n = 2r$. Let X be a collection of pairwise commutative involutions in $Sp_n(V)$, each of type $k = 2t$. Then there are at most $\binom{r}{t}$ elements in X.

Proof: Immediate.

Let σ_i be the element of $Sp_n(V)$ with representation in Γ_n a diagonal matrix with -1 in both the (i,i) and (i+r, i+r) positions and 1 elsewhere for $i = 1,2,\ldots,r$ (where dim V = n = 2r). Noting that matrices of the form

$$\begin{bmatrix} U & 0 \\ 0 & U^{t^{-1}} \end{bmatrix} \qquad (U \text{ in } \Omega_r)$$

are elements of Γ_n, we see that σ_i is similar to σ_j for all $i, j, 1 \leq i, j \leq r$. Thus, if $\Lambda: Sp_n(V) \to Sp_n(V)$ is a group automorphism, then $\Lambda\sigma_i$ is similar to $\Lambda\sigma_j$ for all $i, j, 1 \leq i, j \leq r$. Thus the involutions $\{\Lambda\sigma_i\}_{i=1}^{r}$ are all of the same type, say (k, n-k), $k = 2t$.

We claim that $t = 1$ or $t = r - 1$. Clearly $t \neq 0$ and $t \neq r$ since $\sigma_i \neq \pm 1_V$. Thus suppose $1 < t < r - 1$. But $\binom{r}{1} < \binom{r}{t}$ implies there is an involution B of type k not in the set $\{\Lambda\sigma_i\}$ and commuting with each $\Lambda\sigma_i$. Then $\Lambda^{-1}B$ commutes

with all σ_i and has type (2, n-2). But this is impossible. Thus t = 1 or t = r - 1. That is, $\Lambda\sigma_i$ is either of type (2, n-2) or (n-2, 2).

Now let σ in $Sp_n(V)$ have type (2, n-2). Then there is a γ in $Sp_n(V)$ such that $\gamma^{-1}\sigma\gamma = \sigma_i$ for some i. Then $\Lambda(\gamma^{-1}\sigma\gamma) = \Lambda\sigma_i$ has type (2, n-2) or (n-2, 2). Thus $\Lambda\sigma = (\Lambda\gamma)(\Lambda\sigma_i)(\Lambda\gamma)^{-1}$ is either of type (2, n-2) or of type (n-2, 2). Similarly, if σ is of type (n-2, 2), then $\Lambda\sigma$ is of type (n-2, 2) or (2, n-2).

Let $I_{(2)} = \{\sigma | \text{ind } \sigma = 2\}$. That is, there is a splitting of V such that for σ in $I_{(2)}$

$$\sigma = 1_{P_1} \oplus \ldots \oplus 1_{P_{i-1}} \oplus -1_{P_i} \oplus 1_{P_{i+1}} \oplus \ldots \oplus 1_{P_r} \quad \text{for}$$

some i or

$$\sigma = -1_{P_1} \oplus \ldots \oplus -1_{P_{j-1}} \oplus 1_{P_j} \oplus -1_{P_{j+1}} \oplus \ldots \oplus -1_{P_r} \quad \text{for}$$

some j.

Observing that Λ^{-1} is also an automorphism, we have the following lemma.

Lemma 2.6. If Λ is a group automorphism of $Sp_n(V)$, then $\Lambda I_{(2)} = I_{(2)}$.

Observe that we have two cases. If σ and β have the same type, then $\Lambda\sigma$ and $\Lambda\beta$ have the same type; consequently

$$\text{(I)} \quad \text{type } (2, n-2) \xrightarrow{\Lambda} \text{type } (2, n-2) \quad \text{and}$$

$$\text{type } (n-2, 2) \xrightarrow{\Lambda} \text{type } (n-2, 2).$$

or (II) type $(2, n-2) \xrightarrow{\Lambda}$ type $(n-2, 2)$ and

type $(n-2, 2) \xrightarrow{\Lambda}$ type $(2, n-2)$.

CHAPTER III

TRANSVECTIONS

Let $\tau: V \to V$ be a transvection of the form $\tau_{a,\lambda}$ with unimodular a and λ in R. We can extend {a} to a hyperbolic basis of V. Then considering Mat(τ) relative to this basis, it is clear that τ is an element of the special linear group, $SL_n(V)$. Recalling that Klingenberg has shown that $Sp_n(V)$ is generated by the transvections, we see $Sp_n(V) \subseteq SL_n(V)$. In the case n = 2, $Sp_2(V) = SL_2(V)$.

Let T be the set of transvections in $Sp_n(V)$, and let Λ be an automorphism of $Sp_n(V)$. If $\Lambda(T) = T$, we say Λ preserves transvections. It is our intent in this chapter to show that any automorphism of $Sp_n(V)$ preserves transvections. First, we make some observations on transvections.

The identity 1_V is a transvection; namely, $1_V = \tau_{a,o}$ for some unimodular a. Further, if $\tau_{a,\lambda} = 1_V$, then $\lambda = 0$. For if $\tau x = x + \lambda(a,x)a = x$, then $\lambda(a,x)a = 0$ for all x in V. Selecting x such that (a,x) = 1, we have $\lambda a = 0$. Since a is unimodular, λ must be 0. However, since we are assuming that 2 is a unit in R, -1_V is not a transvection.

Lemma 3.1. Let $\tau_{a,\lambda}$ be a transvection. Then

$\sigma\tau_{a,\lambda}\sigma^{-1} = \tau_{\sigma a,\lambda}$ for every σ in $Sp_n(V)$.

Proof: $\sigma\tau_{a,\lambda}\sigma^{-1}(x) = \sigma\tau_{a,\lambda}(\sigma^{-1}x) = \sigma(\sigma^{-1}x + \lambda(a,\sigma^{-1}x)a) = x + \lambda(a,\sigma^{-1}x)\sigma a = x + \lambda(\sigma a, x)\sigma a = \tau_{\sigma a,\lambda}(x)$. Since $\sigma(a)$ is unimodular, the proof is complete.

Note that $\tau_{a,\lambda}$ has line $Ra = L$. Thus if σ is in $Sp_n(V)$, then $\sigma\tau_{a,\lambda}\sigma^{-1}$ is a transvection with line σL.

Lemma 3.2. Let $\tau_{a,\lambda}$ be a regular transvection. Then

(i) $\tau_{a,\lambda} = \tau_{b,\lambda}$ if and only if $b = \pm a$.

(ii) $\tau_{a,\lambda} = \tau_{a,\mu}$ if and only if $\lambda = \mu$.

Proof: By (1.12) $\tau_{a,\lambda} = \tau_{b,\lambda}$ implies there is a unit α in R such that $b = \alpha a$ and $\lambda = \alpha^{-2}\lambda$. Then $\alpha^2 = 1$, so that $\alpha = \pm 1$. Thus $b = \pm a$. Conversely if $b = \pm a$, then $\tau_{a,\lambda}(x) = x + \lambda(a,x)a$ while

$$\tau_{b,\lambda}(x) = x + \lambda(b,x)b = \begin{cases} x + \lambda(a,x)a & \text{if } b = a \\ x + \lambda(-a,x)(-a) = x + \lambda(a,x)a & \text{if } b = -a. \end{cases}$$

For (ii), if $\tau_{a,\lambda} = \tau_{a,\mu}$ then by (1.12) there is a unit α in R satisfying $a = \alpha a$ and $\mu = \alpha^{-2}\lambda$. But a is unimodular, $a = \alpha a$ implies $\alpha = 1$ and $\mu = \lambda$.

Lemma 3.3. Let τ_1 and τ_2 be transvections with the same line. Then $\tau_1\tau_2$ is a transvection (with the same line as τ_1 and τ_2).

Proof: Let $\tau_1 = \tau_{a,\lambda}$ and $\tau_2 = \tau_{a,\mu}$. Then

$\tau_1\tau_2(x) = \tau_2 x + \lambda(a, \tau_2 x)a$

$$= x + \mu(a,x)a + \lambda(a,\ x+\mu(a,x)a)a$$

$$= x + \mu(a,x)a + \lambda(a,x)a + \lambda\mu(a,x)(a,a)a$$

$$= x + \mu(a,x)a + \lambda(a,x)a$$

$$= x + (\mu+\lambda)(a,x)a.$$

Thus $\tau_1\tau_2 = \tau_{a,\mu+\lambda}$.

Note that if τ_1 and τ_2 are regular transvections with the same line, then $\tau_1\tau_2$ is a transvection with the same line. However $\tau_1\tau_2$ may not be regular.

Lemma 3.4. Let τ_1 and τ_2 be regular transvections. Then τ_1 and τ_2 permute if and only if their lines are orthogonal.

Proof: Let $\tau_1 = \tau_{a,\lambda}$ and $\tau_2 = \tau_{b,\mu}$. Then for all x in V, $\tau_1 x = x + \lambda(a,x)a$ and $\tau_2 x = x + \mu(b,x)b$ with a and b unimodular elements of V and λ and μ units in R. Suppose $\tau_1\tau_2 = \tau_2\tau_1$. Then $\tau_1\tau_2\tau_1^{-1} = \tau_2$. By (3.1) $\tau_1\tau_2\tau_1^{-1} = \tau_{\tau_1(b),\mu}$, thus $\tau_2 = \tau_{\tau_1(b),\mu}$; that is, $\tau_{b,\mu} = \tau_{\tau_1(b),\mu}$. By (3.2) $b = \pm\ \tau_1(b)$. So two cases arise.

(i) If $b = \tau_1(b)$, then $b = b + \lambda(a,b)b$ so $\lambda(a,b)b = 0$. But λ is a unit and b is unimodular, thus $(a,b) = 0$. Thus the lines Ra and Rb of τ_1 and τ_2, respectively, are orthogonal.

(ii) If $b = -\tau_1(b)$, then $b = -\ b - \lambda(a,b)a$ so that $b = -\ \lambda 2^{-1}(a,b)a$. Then $(a,b) = 0$ and the lines are orthogonal.

Conversely, suppose the proper lines of τ_1 and τ_2 are orthogonal. In particular, $(a,b) = 0$. Now $\tau_1\tau_2(x) = x + \mu(b,x)b + \lambda(a,x)a + \lambda\mu(b,x)(a,b)a$ and $\tau_2\tau_1(x) = x + \lambda(a,x)a + \mu(b,x)b + \mu\lambda(a,x)(b,a)b$. Thus $\tau_1\tau_2 = \tau_2\tau_1$.

Note that if the lines of τ_1 and τ_2 are orthogonal, then $\tau_1\tau_2 = \tau_2\tau_1$ without the requirement that τ_1 and τ_2 be regular. The other implication seems to require regularity.

Lemma 3.5. Let τ be a regular transvection with line Ra, say $\tau_{a,\lambda} = \tau$. Let $C(\tau) = \{\sigma \text{ in } Sp_n(V) | \sigma\tau = \tau\sigma\}$ Then $C(\tau) = \{\sigma \text{ in } Sp_n(V) | \sigma a = \pm a\}$.

Proof: Suppose $\sigma a = \pm a$. Then $\sigma\tau(x) =$

$\sigma(x + \lambda(a,x)a) = \sigma x + \lambda(a,x)\sigma a$

$$= \begin{cases} \sigma x + \lambda(a,x)a & \text{if } \sigma a = a, \\ \sigma x - \lambda(a,x)a & \text{if } \sigma a = -a, \end{cases}$$

and

$\tau\sigma(x) = \sigma x + \lambda(a,\sigma x)a = \sigma x + \lambda(\sigma^{-1}a,x)a$

$$= \begin{cases} \sigma x + \lambda(a,x)a \text{ if } \sigma a = a \text{ since this case has } \sigma^{-1}a = a. \\ \sigma x - \lambda(a,x)a \text{ if } \sigma a = -a \text{ since this case has } \sigma^{-1}a = -a. \end{cases}$$

Thus $\sigma\tau = \tau\sigma$ and σ is in $C(\tau)$.

Conversely, suppose σ is in $C(\tau)$. Then $\sigma\tau\sigma^{-1} = \tau$. Thus $\tau_{\sigma a,\lambda} = \tau_{a,\lambda}$ since $\sigma\tau\sigma^{-1} = \tau_{\sigma a,\lambda}$. By (1.12) there is a unit α in R satisfying $\sigma a = \alpha a$ and $\alpha^{-2}\lambda = \lambda$. Thus $\alpha^2 = 1$ and $\alpha = \pm 1$. Hence $\sigma a = \pm a$ and $C(\tau) \subseteq \{\sigma \text{ in } Sp_n(V) | \sigma a = \pm a\}$.

Observe that τ need not be regular to have that $\{\sigma \text{ in } Sp_n(V) | \sigma a = \pm a\} \subseteq C(\tau)$.

Lemma 3.6. Let τ_1 and τ_2 be regular transvections in $Sp_n(V)$. Then $C(\tau_1) = C(\tau_2)$ if and only if τ_1 and τ_2 have

the same line.

Proof: Suppose τ_1 and τ_2 have the same line, say Ra. Then by (3.5),

$$C(\tau_1) = \{\sigma \text{ in } Sp_n(V) \mid \sigma a = \pm a\} = C(\tau_2).$$

Conversely, suppose $C(\tau_1) = C(\tau_2)$ and $\tau_1 = \tau_{a,\lambda}$ and $\tau_2 = \tau_{b,\mu}$. Suppose the lines of τ_1 and τ_2 are distinct. Then the hyperplanes $(Ra)^\circ$ and $(Rb)^\circ$ are distinct, since $(U^\circ)^\circ = U$ for any subspace U of V. Thus there exists a c in V satisfying $(a,c) = 0$ and $(b,c) \neq 0$. We can assume c is unimodular and choose a unit ν in R, so $\tau_{c,\nu}$ is a transvection. But $\tau_{c,\nu}(a) = a + \nu(c,a)c = a$ implies that $\tau_{c,\nu}$ is in $C(\tau_1)$.

We claim however that $\tau_{c,\nu}(b) \neq \pm b$. Suppose $\tau_{c,\nu}(b) = b$. Then $b = b + \nu(c,b)c$ so that $\nu(c,b)c = 0$. But ν is a unit and c is unimodular so $(c,b) = 0$. This contradicts our choice of c. Suppose that $\tau_{c,\nu}(b) = -b$. Then $b + \nu(c,b)c = -b$, so $-2^{-1}\nu(c,b)c = b$. But then $(b,c) = 0$, again contradicting the choice of c. Thus we have $\tau_{c,\nu}(b) \neq \pm b$. Hence by (3.5), $\tau_{c,\nu}$ is not an element of $C(\tau_2)$. This is a contradiction to $C(\tau_1) = C(\tau_2)$. Therefore $Ra = Rb$, that is τ_1 and τ_2 have the same line.

Lemma 3.7. Let σ be an element of $Sp_n(V)$ such that $\sigma L = L$ for all lines L in V. Then $\sigma = \pm 1_V$.

Proof: Let L be a line in V, that is L is a free R-submodule of dimension 1 which is a direct summand of V. Thus $L = Rx$ for some unimodular x in V. Since $\sigma L = L$, there

exists r_x in R such that $\sigma x = r_x x$. If y is in Rx, then $y = sx$ for some s in R. Hence $\sigma y = \sigma(sx) = s\sigma x = sr_x x = r_x sx = r_x y$ and $\sigma y = r_x y$ for every y in $L = Rx$.

Let x and y be basis vectors of V. Then $\sigma(x+y) = a(x+y)$ for some a in R. But $\sigma(x+y) = \sigma x + \sigma y = r_x x + r_y y$. So $ax + ay = r_x x + r_y y$ and $r_x = a = r_y$. Thus if x is any basis vector in V and y is in Rx, then $\sigma y = ay$.

Select x and y satisfying $(x,y) = 1$. Then $1 = (x,y) = (\sigma x, \sigma y) = (ax, ay) = a^2(x,y) = a^2$. But $a^2 = 1$ implies $a = \pm 1$. Thus $\sigma = \pm 1_V$.

Lemma 3.8. Let $V = P_1 \perp \ldots \perp P_r$ be a splitting of V into planes. Let τ be a regular transvection such that $\tau P_i = P_i$ for $i = 1,2,\ldots,r$. Then the proper line of τ is contained in one of the P_i.

Proof: Let $\tau = \tau_{a,\lambda}$ be a regular transvection. Then there is a b in V with $(a,b) = 1$. But $V = P_1 \perp \ldots \perp P_r$ so $b = b_1 + \ldots + b_r$ with b_i in P_i. Then $1 = (a,b) = (a, b_1 + \ldots + b_r) = (a,b_1) + \ldots + (a,b_r)$. Since the sum of non-units in R cannot be a unit, we must have (a,b_i) a unit for some i.

Then, since $\tau P_i = P_i$ and b_i in P_i, we have $\tau b_i = b_i + \lambda(a,b_i)a$ in P_i. But (a,b_i) and λ are units; thus solving for a yields that a is in P_i. Hence $Ra \subseteq P_i$.

Theorem 3.9. Let $n \geq 6$. If Λ is a group automorphism of $Sp_n(V)$ and τ is a regular transvection in $Sp_n(V)$, then $\Lambda\tau$ is a transvection.

Proof: Let τ be a regular transvection with line $L = Ra$ and put $T = \Lambda\tau$. Say $\tau x = \lambda(a,x)a$ for x in V where a is unimodular and λ is a unit in R. Since a is unimodular, there is a hyperbolic basis of V, say $\{a = x_1, y_1, \ldots, x_r, y_r\}$ with $V = P_1 \perp \ldots \perp P_r$ where P_i, $1 \leq i \leq r$, is the hyperbolic plane spanned by $\{x_i, y_i\}$. Thus the line of τ, that is $L = Ra$, is contained in P_1.

Now choose σ to be an involution of index 2 whose plane contains L, say $\sigma = -1_{P_1} \oplus \ldots \oplus 1_{P_r}$. Let $\Sigma = \Lambda\sigma$. By (2.6), Σ is an involution of index 2. Thus Σ determines a splitting of V, $\Sigma: V = P \perp N$, with $\dim P = 2$ and either

$$\text{(i)} \quad \Sigma = -1_P \oplus 1_N \qquad \text{or}$$

$$\text{(ii)} \quad \Sigma = 1_P \oplus -1_N.$$

Note that L is contained in the proper plane of σ so that $\sigma(a) = -a$. Then for x in V,

$\sigma\tau(x) = \sigma(x+\lambda(a,x)a) = \sigma x + \lambda(a,x)\sigma a = \sigma x - \lambda(a,x)a$ and

$\tau\sigma(x) = \sigma x + \lambda(a,\sigma x)a = \sigma x + \lambda(\sigma a,x)a = \sigma x - \lambda(a,x)a$.

Thus τ permutes with σ and hence $\Sigma T = T\Sigma$.

We claim then that $T: P \to P$. If $\Sigma = -1_P \oplus 1_N$ and p in P then $T(p) = p_1 + n_1$ for some p_1 in P and n_1 in N. Then $\Sigma T(p) = \Sigma(p_1+n_1) = -p_1 + n_1$. But $T\Sigma(p) = T(-p) = -T(p) = -p_1-n_1$. Thus $-p_1 + n_1 = -p_1 - n_1$ implying that $n_1 = 0$. That is, $T(p) = p_1$ in P. Similarly if $\Sigma = 1_P \oplus -1_N$, we conclude that $T(p)$ in P. Thus we have $T: P \to P$.

By a similar argument we also have $T: N \to N$. We want

to show that T^2 is the identity on N.

Suppose we choose an involution Σ' ($\neq \pm \Sigma$) of index 2 which permutes with Σ. Then Σ' determines the splitting $\Sigma':V = P' \perp N'$ with plane P'. Note $\Sigma' = -1_{P'} \oplus 1_{N'}$, $P \subseteq N'$, and $P' \subseteq N$. We claim that $TP' = P'$.

Also Λ^{-1} is an automorphism of $Sp_n(V)$. Since Σ' is an involution of index 2, it follows that $\Lambda^{-1}\Sigma'$ is also of index 2. Further $\Sigma' \neq \pm \Sigma$ and $\Sigma\Sigma' = \Sigma'\Sigma$ implies that $\Lambda^{-1}\Sigma' \neq \pm \sigma$ and $(\Lambda^{-1}\Sigma')\sigma = \sigma(\Lambda^{-1}\Sigma')$. So by (2.3) there is a splitting of V such that $V = Q_1 \perp \ldots \perp Q_r$ where $\sigma Q_i = \pm Q_i$ and $\Lambda^{-1}\Sigma' Q_i = \pm Q_i$ for $1 \leq i \leq r$. We may assume then that the plane of σ is $Q_1 = P_1$ and the plane of $\Lambda^{-1}\Sigma'$ is Q_2 (that is, their planes are orthogonal). But L, the line of τ, is then contained in Q_1. An easy computation then shows that $\tau(\Lambda^{-1}\Sigma') = (\Lambda^{-1}\Sigma')\tau$. Hence, applying Λ, we have $T\Sigma' = \Sigma'T$. It follows that $T:P' \to P'$ and $T:N' \to N'$. Since T is an isomorphism, we have $TP' = P'$.

We now show that T actually acts as $\pm 1_{P'}$ on P'. Suppose P' is generated by $\{v,w\}$ where $(v,w) = 1$. Recall that $P' \subseteq N$ and consider the line $K = Rv$ (similarly for $K = Rw$). Since $n \geq 6$, there is an element u, a member of the hyperbolic basis of V, with u not in P or P', and u in N. Note that $u + v$ is a unimodular element of V and let J be the line $J = R(u+v)$.

Then observe the following:

(i) $J \subseteq N$; since u is in N and v is in N.

(ii) $J \perp K$; since $(u+v, v) = (u,v) + (v,v) = 0$.

(iii) $J \not\subseteq P'$; since $u + v$ is not in P'.

(iv) $J \not\perp P'$; since $(u+v , w) = 1$.

Let ϕ be a regular transvection in $Sp_n(V)$ with line J, and put $\Sigma'' = \phi\Sigma'\phi^{-1}$. Then Σ'' is an involution of index 2, since Σ' is of index 2. Also since the line J of ϕ is contained in N, we have $\phi\Sigma = \Sigma\phi$ or $\Sigma = \phi^{-1}\Sigma\phi$. Hence, since $\Sigma' \neq \pm \Sigma$, it is evident that $\Sigma'' \neq \pm \Sigma$.

Recall that the proper spaces of Σ' are P' and N' with $\dim P' = 2$. Since $\Sigma'' = \phi\Sigma'\phi^{-1}$, we have the proper plane of Σ'' is $P'' = \phi P'$. Now we have $\Sigma'' \neq \pm \Sigma$ and $\Sigma''\Sigma = \Sigma\Sigma''$ (since $\Sigma = \phi\Sigma\phi^{-1}$), thus we apply the same argument as in showing $TP' = P'$ to obtain that $TP'' = P''$. Now $TP' = P'$ and $TP'' = P''$ so $T(P' \cap P'') \subseteq P' \cap P''$. But T is an automorphism so $T(P' \cap P'') = P \cap P''$. We claim that $P' \cap P'' = P' \cap \phi P' = K$.

Since $K \perp J$ and $K \subseteq P'$, we see that ϕ acts as the identity on K. Hence $K \subseteq \phi P'$. Thus $K \subseteq P' \cap \phi P'$. Conversely, suppose x is in $P' \cap \phi P'$. Now x in P' implies $x = rv + sw$ for some r and s in R. Since x is in $\phi P'$, there exists a y in P' wuch that $\phi(y) = x$. Let $y = r_1v + s_1w$, with r_1 and s_1 in R. Recall that ϕ is a regular transvection with line $J = R(u+v)$, say $\phi(z) = z + \beta(u+v, z)(u+v)$ for all z in V where β is a unit. Then

$$\phi(y) = y + \beta(u+v, y)(u+v)$$

$$= (r_1v + s_1w) + \beta(u+v, r_1v + s_1w)(u+v)$$

$$= r_1v + s_1w + \beta s_1u + \beta s_1v$$
$$= (r_1 + \beta s_1)v + s_1w + \beta s_1u.$$

But $\phi(y) = rv + sw$, and u,v, and w are basis elements, so $\beta s_1u = 0$. Since β is a unit, $s_1 = 0$. Thus $y = r_1v$ implies $\phi(y) = \phi(r_1v) = r_1\phi(v) = r_1v$ (since $J \perp K$ implies ϕ fixes v). Thus $x = \phi(y) = r_1v$ is in $K = Rv$. Therefore $P' \cap \phi P' = K$. Hence $TK = K$. Similarly we have $T(Rw) = Rw$.

Now $P' = Rv \oplus Rw$, $T(Rv) = Rv$ and $T(Rw) = Rw$. Using the technique in the proof of (3.7) we have there exist r_v and r_w in R so that $T(y) = r_vy$ for all y in Rv and $T(y) = r_wy$ for all y in Rw.

Observe that (i) $(v+w, w) = 1$, (ii) $\{v+w, w\}$ is R-free, and (iii) $v + w$ is in P'. Thus P' is also $P' = R(v+w) \oplus Rw$. Thus there exist r_{v+w} in R such that $T(y) = r_{v+w}y$ for all y in $R(v+w)$. Then $r_{v+w}(v+w) = T(v+w) = Tv + Tw = r_vv + r_ww$. Thus $r_{v+w}v + r_{v+w}w = r_vv + r_ww$. So $r_v = r_w = r_{v+w} = r$. But $(v,w) = 1$. So $1 = (v,w) = (Tv,Tw) = (rv,rw) = r^2(v,w) = r^2$. Thus $r = \pm 1$. If $r = 1$ and x in P', then $x = r_1v + r_2w$ for some r_1 and r_2 in R. Then $Tx = r_1Tv + r_2Tw = r_1v + r_2w = x$. If $r = -1$, $Tx = r_1Tv + r_2Tw = -r_1v - r_2w = -x$. Thus $T = \pm 1_{P'}$.

We have τ a transvection with line L, $V = P_1 \perp \ldots \perp P_r$, and $L \subseteq P_1$. Let

$\sigma_i = 1_{P_1} \oplus \ldots \oplus 1_{P_{i-1}} \oplus -1_{P_i} \oplus 1_{P_{i+1}} \oplus \ldots \oplus 1_{P_r}$ and let

$S = \{\sigma_i\}_{i=1}^{r}$. Note that each $\Lambda\sigma_i$ is an involution of index 2.

Let $P_1', \ldots, P_r'$ be the planes of the set of involutions $\{\Lambda\sigma_i\}_{i=1}^{r}$. For each $i = 1, 2, \ldots, r$, fix an involution Σ_i, of index 2 with plane P_i'.

We chose $\sigma = \sigma_1 = -1_{P_1} \oplus 1_{P_2} \oplus \ldots \oplus 1_{P_r}$ and let $\Sigma = \Lambda\sigma$. We can then assume that $\Sigma = \Sigma_1$, so $P = P_1'$ and $N = P_2' \perp \ldots \perp P_r'$. Then we chose $\Sigma' \neq \pm \Sigma$ and showed that $T = \Lambda\tau$ acts like the identity on the plane of Σ'. Thus by using this argument for each of $\Sigma_2, \Sigma_3, \ldots, \Sigma_r$, we conclude that T must act like $\pm 1_{P_i'}$ on P_i' for $2 \leq i \leq r$. Thus T^2 acts like the identity on P_i' for $2 \leq i \leq r$ and hence like the identity on N.

In the splitting $V = P_1 \perp P_2 \perp \ldots \perp P_r$, let P_1 be generated by the hyperbolic pair $\{a,b\}$ and P_2 by the hyperbolic pair $\{c,d\}$, (note $r \geq 3$). Take $J' = R(a+c)$. Then

(i) J' is a line; since $a + c$ is unimodular.

(ii) $J' \perp L$; since $L = Ra$ and $(a+c, a) = 0$.

(iii) $J' \not\subseteq P_1$; since $a + c$ is not in P_1.

(iv) $J' \not\perp P_1$; since $(a+c, b) = 1$.

Let δ be a regular transvection with line J'.

Let $\sigma_o = \delta\sigma\delta^{-1}$. Then

(i) σ_o is an involution of index 2.

(ii) the plane of σ_o is $P_o = \delta P$.

(iii) $L \subseteq P_o$; since $J' \perp L$, $\delta L = L$. But $L \subseteq P$ so $\delta L \subseteq P_o$.

(iv) $\sigma_o \neq \pm \sigma$; for example $\sigma_o(b) \neq \pm \sigma(b)$.

Thus we have two distinct involutions σ and σ_o, each of index 2 with proper plane containing L.

Let $\Sigma = \Lambda\sigma$ and $\Sigma_o = \Lambda\sigma_o$. Then Σ and Σ_o determine splittings of V; $\Sigma:V = P \perp N$ and $\Sigma_o:V = P_o \perp N_o$. Let $T' = \Lambda\tau_{a,\lambda/2}$. Note 2 is a unit so $\lambda/2$ is a unit. Thus $\tau_{a,\lambda/2}$ is a regular transvection. Then the above argument shows that $T'^2 = (\Lambda\tau_{a,\lambda/2})^2 = \Lambda\tau_{a,\lambda}$ acts as the identity on N and N_o.

Now recall the following commutative diagram:

$$\begin{array}{ccc} Sp_n(V) & \xrightarrow{\Lambda} & Sp_n(V) \\ \Big\downarrow h_m & & \Big\downarrow h_m \\ Sp_n(V/mV) & \xrightarrow{\overline{\Lambda}} & Sp_n(V/mV) \end{array}$$

Let $N \to \overline{N}$ and $N_o \to \overline{N}_o$ under the map $g_m:V \to V/mV$. Then using the images of σ, σ_o, and δ under h_m, say $\overline{\sigma}$, $\overline{\sigma}_o$ and $\overline{\delta}$, and $\overline{L} = k\overline{a}$ $(k = R/m)$, and $\overline{J}' = k(\overline{a} + \overline{c})$, we repeat the above argument. Thus we conclude that the two spaces $\overline{N}$ and $\overline{N}_o$ of dimension $n - 2$ are distinct.

Since $\overline{N} \neq \overline{N}_o$, there exists an $\overline{x}$ in $\overline{N}_o - \overline{N}$. Thus there is an x in $N_o - N$. Let $\{\overline{b}_1, \ldots, \overline{b}_{n-2}\}$ be a basis for $\overline{N}$ obtained from the basis $\{b_1, \ldots, b_{n-2}\}$ of N. Then $\{\overline{b}_1, \ldots, \overline{b}_{n-2}\} \cup \{\overline{x}\} \cup \{\overline{y}\}$, for some $\overline{y}$, is a basis for V/mV. If y is a pre-image of $\overline{y}$, then $\{b_1, \ldots, b_{n-2}\} \cup \{x\} \cup \{y\}$ is a basis for V. But b_i is in N for $i = 1, 2, \ldots, n - 2$ and x is in N_o. Since $\Lambda\tau_{a,\lambda}$ fixes N and N_o we have that $\Lambda\tau_{a,\lambda}$

fixes the hyperplane $Rb_1 \oplus \ldots \oplus Rb_{n-2} \oplus Rx$. Thus $\Lambda\tau_{a,\lambda}$ is a transvection.

Corollary 3.10. If $\tau_{a,\lambda}$ is a regular transvection, then $\Lambda\tau_{a,\lambda}$ is a regular transvection where Λ is an automorphism of $Sp_n(V)$.

Proof: Recall the commutative diagram:

$$\begin{array}{ccc} Sp_n(V) & \xrightarrow{\Lambda} & Sp_n(V) \\ \downarrow{\scriptstyle h_m} & & \downarrow{\scriptstyle h_m} \\ Sp_n(V/mV) & \xrightarrow{\overline{\Lambda}} & Sp_n(V/mV). \end{array}$$

If $\tau_{a,\lambda}$ is a regular transvection, then $\Lambda\tau_{a,\lambda}$ is a transvection by (3.9). Now $\tau_{a,\lambda}$ regular implies $h_m\tau_{a,\lambda} \neq 1_{V/mV}$. Thus $\overline{\Lambda}h_m\tau_{a,\lambda} \neq 1_{V/mV}$. Hence $h_m\Lambda\tau_{a,\lambda} \neq 1_V$. Therefore $\Lambda\tau_{a,\lambda}$ is regular.

Theorem 3.11. Let $\Lambda: Sp_n(V) \to Sp_n(V)$ be a group automorphism. Then Λ preserves transvections.

Proof: Let $\tau = \tau_{a,\lambda}$ be a transvection in $Sp_n(V)$. If λ is a unit then $\Lambda\tau$ is a transvection by (3.10). Suppose then that λ is not a unit. Then $\tau_{a,\lambda} = \tau_{a,1}\tau_{a,\lambda-1}$. But 1 and $\lambda - 1$ are units, so $\tau_{a,1}$ and $\tau_{a,\lambda-1}$ are regular transvections with line $L = Ra$. By (3.5)

$$C(\tau_{a,1}) = \{\sigma \mid \sigma a = \pm a\} = C(\tau_{a,\lambda-1}).$$

By (3.10) $T_1 = \Lambda\tau_{a,1}$ and $T_2 = \Lambda\tau_{a,\lambda-1}$ are regular

transvections. Since $C(\tau_{a,1}) = C(\tau_{a,\lambda-1})$, we have $C(T_1) = C(T_2)$. Thus by (3.6), T_1 and T_2 have the same line. Then (3.3) implies T_1T_2 is a transvection with the same line. But $\Lambda\tau = \Lambda(\tau_{a,1}\tau_{a,\lambda-1}) = \Lambda\tau_{a,1}\,\Lambda\tau_{a,\lambda-1} = T_1T_2$. Thus $\Lambda\tau$ is a transvection. Therefore Λ preserves transvections.

CHAPTER IV

AUTOMORPHISMS

In this section we determine the automorphisms of the symplectic group over a local ring. We require that the characteristic of R/m be other than 2, that $R/m \neq F_3$, and that V have dimension $n \geq 6$.

Theorem 4.1. Let ϕ be an automorphism of $Sp_n(V)$ with the following property: For each transvection τ in $Sp_n(V)$, $\phi\tau$ is a transvection with the same line as τ. Then there exists a homomorphism χ of $Sp_n(V)$ into its center $\{\pm 1_V\}$ such that $\phi(\sigma) = \chi(\sigma)\sigma$ for all σ in $Sp_n(V)$. In this case we write $\phi = P_\chi$.

Proof: We claim that $\phi\sigma = \pm\sigma$ for all σ in $Sp_n(V)$. Let σ be in $Sp_n(V)$; let L be a line in V, and let τ be a regular transvection in $Sp_n(V)$ with line L. Then $\phi\tau$ is a regular transvection with line L. Hence $(\phi\sigma)(\phi\tau)(\phi\sigma)^{-1}$ is a transvection with line $(\phi\sigma)L$.

On the other hand, $\sigma\tau\sigma^{-1}$ is a transvection with line σL. Thus $\phi(\sigma\tau\sigma^{-1})$ is a transvection with line σL. But $(\phi\sigma)(\phi\tau)(\phi\sigma)^{-1} = \phi(\sigma\tau\sigma^{-1})$ so that $(\phi\sigma)(\phi\tau)(\phi\sigma)^{-1}$ must have line σL. Hence $(\phi\sigma)L = \sigma L$. Therefore $\sigma^{-1}(\phi\sigma)L = L$ for

all lines L in V. Hence $\sigma^{-1}(\phi\tau) = \pm 1_V$ by (3.7). Thus $\phi\sigma = \pm \sigma$ for σ in $Sp_n(V)$. Define the homomorphism χ of $Sp_n(V)$ into $\{\pm 1_V\}$ by $\phi\sigma = \chi(\sigma)\sigma$ for σ in $Sp_n(V)$.

Let g be a semi-linear isomorphism of V onto itself. Let ϕ_g be the mapping defined by $\phi_g(\sigma) = g\sigma g^{-1}$ for all σ in $Sp_n(V)$. It is clear that ϕ_g is an injective homomorphism of $Sp_n(V)$ into $GL_n(V)$. We shall describe the automorphisms of $Sp_n(V)$ in terms of mappings of the types P_χ and ϕ_g.

Theorem 4.2. Let Λ be a group automorphism of $Sp_n(V)$. Then there are automorphisms P_χ and ϕ_g on $Sp_n(V)$ such that $\Lambda = P_\chi \circ \phi_g$.

Proof: Since Λ is an automorphism of $Sp_n(V)$, by (3.11) it preserves transvections. The proof consists of a sequence of steps, some of which will be stated as theorems.

For any line L in V, let $T(L)$ denote the collection of regular transvections in $Sp_n(V)$ with line L. Since Λ preserves transvections, every element of $\Lambda(T(L))$ is a transvection. Indeed, by (3.10), each element is a regular transvection.

Let τ_1' and τ_2' be elements of $\Lambda(T(L))$ with $\Lambda\tau_1 = \tau_1'$ and $\Lambda\tau_2 = \tau_2'$ for some τ_1 and τ_2 in $T(L)$. Since τ_1 and τ_2 are regular transvections each with line L, we have $C(\tau_1) = C(\tau_2)$. But then $C(\Lambda\tau_1) = C(\Lambda\tau_2)$. So τ_1' and τ_2' are regular transvections with $C(\tau_1') = C(\tau_2')$. Hence τ_1' and τ_2' have the same line. Thus there exists a line L' in V such that $\Lambda(T(L)) \subseteq T(L')$.

Let τ_1' be an element of $T(L')$. Select τ_2' in $\Lambda(T(L)) \subseteq T(L')$ with $\Lambda\tau_2 = \tau_2'$ for some τ_2 in $T(L)$. Since Λ^{-1} is an automorphism, the above argument shows that $\Lambda^{-1}\tau_2' = \tau_2$ and $\Lambda^{-1}\tau_1'$ have the same line; namely, L. Thus $\Lambda^{-1}(T(L')) \subseteq T(L)$ so that $T(L') \subseteq \Lambda(T(L))$. Hence $\Lambda(T(L)) = T(L')$.

We can therefore associate with each line L in V a unique line L' in V such that $\Lambda(T(L)) = T(L')$. Clearly for lines L and K in V with $L \neq K$, we have $L' \neq K'$. By considering Λ^{-1} we have that every line in V is an L' for some L. We have therefore established a bijection $\alpha: P(V) \to P(V)$ of the collection of lines of V onto itself.

We now show that α preserves orthogonal lines; that is, $\Phi(L_1, L_2) = 0$ implies $\Phi(L_1', L_2') = 0$. Let L_1 and L_2 be orthogonal lines in V. Let τ_1 and τ_2 be regular transvections with lines L_1 and L_2, respectively. Then $\Lambda\tau_1$ and $\Lambda\tau_2$ are regular transvections with lines L_1' and L_2'. Now $\Phi(L_1, L_2) = 0$ implies τ_1 and τ_2 permute by (3.4). Hence $\Lambda\tau_1$ and $\Lambda\tau_2$ permute. Thus, by (3.4) again, L_1' and L_2' are orthogonal. Similarly α^{-1} preserves orthogonal lines.

The above argument establishing the bijection α utilized the techniques used by O'Meara [18] in the case where R is an integral domain. Again, using these techniques and the automorphism $\bar{\Lambda}$ of $Sp_n(V/mV)$, there exists a bijection $\bar{L} \leftrightarrow \bar{L}'$ of the set of lines of V/mV onto itself given by the defining equation $\Lambda(T(\bar{L})) = T(\bar{L}')$.

Recall the automorphism $\Lambda: Sp_n(V) \to Sp_n(V)$ induces an automorphism $\bar{\Lambda}: Sp_n(V/mV) \to Sp_n(V/mV)$ such that the following diagram is commutative:

$$\begin{array}{ccc} Sp_n(V) & \xrightarrow{\Lambda} & Sp_n(V) \\ {\scriptstyle h_m}\downarrow & & \downarrow{\scriptstyle h_m} \\ Sp_n(V) & \xrightarrow{\bar{\Lambda}} & Sp_n(V) \end{array}$$

Observe that the following diagram is also commutative:

$$\begin{array}{ccc} P(V) & \xrightarrow{\alpha} & P(V) \\ {\scriptstyle \Pi}\downarrow & & \downarrow{\scriptstyle \Pi} \\ P(V/mV) & \xrightarrow{\bar{\alpha}} & P(V/mV) \end{array}$$

where Π is the natural projection $(Ra \xmapsto{\Pi} k\bar{a})$. Let L be a line in V and $\Pi L = \bar{L}$ be its image in V/mV. Let τ be a regular transvection in $Sp_n(V)$ with line L. Then $\Pi\tau = \bar{\tau}$ is a non-trivial transvection in $Sp_n(V/mV)$. Further $\Lambda\tau$ is a regular transvection in $Sp_n(V)$ with line αL. Now $\bar{\Lambda}(\Pi\tau) = \Pi(\Lambda\tau)$, so $\overline{\alpha L} = \Pi(\alpha L)$ must be the line of the transvection $\bar{\Lambda}(\Pi\tau)$, that is $\bar{L}'$. Thus the diagram is commutative.

O'Meara shows that the Fundamental Theorem of Projective Geometry (over fields) applies to the bijection $\bar{\alpha}$. Thus there is a semi-linear isomorphism $\bar{g}: V/mV \to V/mV$ such

that $g\bar{L} = \bar{L}'$ for all lines L in V/mV. Thus if $\{\bar{e}_1,\ldots,\bar{e}_t\}$ forms a basis for a subspace of V/mV then $k\bar{e}_1' \oplus \ldots \oplus k\bar{e}_t'$ is a subspace of dimension t, (that is $\{\bar{e}_1',\ldots,\bar{e}_t'\}$ is independent).

Let H be any hyperplane in V. Then any line L in H is orthogonal to the line H^o. Hence L' is orthogonal to the line $(H^o)'$. But then L' is contained in the hyperplane $((H^o)')^o$. Thus $\alpha H = \{\alpha L | L \text{ line in } H\}$ is contained in $((H^o)')^o$. Suppose $H = Re_1 \oplus \ldots \oplus Re_{n-1}$. Then there exist elements $e_1',\ldots,e_{n-1}'$ in V such that

$$\begin{array}{ccc} Re_i & \xrightarrow{\alpha} & Re_i' \\ \Pi \downarrow & & \downarrow \Pi \\ k\bar{e}_i & \xrightarrow{\bar{\alpha}} & k\bar{e}_i' \end{array}$$

is commutative, i = 1, ..., n - 1. Let $<\alpha H>$ be the submodule of V generated by αH. Then, by the diagram, $\{e_1',\ldots,e_{n-1}'\}$ is an independent set modulo mV in $<\alpha H>$ containing n-1 elements. But by the above discussion, $<\alpha H>$ is contained in a space of dimension n-1 and thus must actually be a hyperplane. Hence for any hyperplane H in V, $<\alpha H>$ is also a hyperplane.

Theorem 4.3. Let N be a subspace of V of dimension t. Then $<\alpha N>$ is a space of dimension t ($t<n$).

Proof: By the above, if t = n-1 then $<\alpha N>$ is a

space of dimension n-1. We proceed by induction and assume that subspaces of dimension t+1 are mapped by α to subspaces of dimension t+1. Let N be a subspace of dimension t. Note that $N = \bigcap\{M \mid \dim M = n+1,\ N \subseteq M\}$.

Select a basis $b_1,\ldots,b_t$ for N. Then $\{\Pi b_i = \bar{b}_i\}_{i=1}^{t}$ gives a basis for $\Pi N = \bar{N}$. Then if $\bar{\alpha}(k\bar{b}_i) = k\bar{b}_i'$, there exists b_i', $i=1,\ldots,t$, such that

$$\begin{array}{ccc} Rb_i & \xrightarrow{\alpha} & \alpha Rb_i = Rb_i' \text{ in } \alpha N \\ \Pi \downarrow & & \downarrow \Pi \\ k\bar{b}_i & \xrightarrow{\bar{\alpha}} & k\bar{b}_i'. \end{array}$$

Thus $Q = Rb_1' \oplus \ldots \oplus Rb_t' \subseteq \langle \alpha N \rangle \subseteq V$. Now extend $\{b_1',\ldots,b_t'\}$ to $\{b_1',\ldots,b_t',b_{t+1}',\ldots,b_n'\}$ a basis for V. Let $Rb_{t+1} = \alpha^{-1}Rb_{t+1}',\ldots,Rb_n = \alpha^{-1}Rb_n'$. Then as before, using α^{-1} instead of α, we conclude $b_1,\ldots,b_n$ is a basis of V.

Now suppose $\langle \alpha N \rangle \supsetneq Q$. Then there exists an x in $\langle \alpha N \rangle - Q$. Since x is in V, we have $x = s_1b_1' + \ldots + s_tb_t' + s_{t+1}b_{t+1}' + \ldots + s_nb_n'$ where $s_{t+1},\ldots,s_n$ are in the maximal ideal m. Let $M' = Rb_1' \oplus \ldots \oplus Rb_t' \oplus Rb_{t+1}'$ and $M'' = Rb_1' \oplus \ldots \oplus Rb_t' \oplus Rb_{t+2}'$. (Note $t \leq n-2$ so there are elements b_{t+1}' and b_{t+2}'.) Then M' and M'' are subspaces of dimension t+1. Thus $\langle \alpha^{-1}M' \rangle$ and $\langle \alpha^{-1}M'' \rangle$ are spaces of

dimension t+1 containing $\{b_1,\ldots,b_t,b_{t+1}\}$ and $\{b_1,\ldots,b_t,b_{t+2}\}$, respectively. Thus these two sets are bases for $<\alpha^{-1}M'>$ and $<\alpha^{-1}M">$. But $N \subseteq <\alpha^{-1}M'>$ and $N \subseteq <\alpha^{-1}M">$. Thus $<\alpha N> \subseteq M'$ and $<\alpha N> \subseteq M"$. Since x is in $<\alpha N>$, we have x in M' and x in M". But x in M' implies $s_{t+2} = \ldots = s_n = 0$ and x in M" implies $s_{t+1} = s_{t+3} = \ldots = s_n = 0$. That is, $x = s_1b_1' + \ldots + s_tb_t'$. But then x is in Q, a contradiction. Thus $<\alpha N> = Q$ and $<\alpha N>$ is a space of dimension t as desired.

Corollary 4.4. If P is a plane, then $<\alpha P>$ is a plane.

Proof: Suppose $P = Re_1 \oplus Re_2$. Then by (4.3), $<\alpha P> = Re_1' \oplus Re_2'$ where $\alpha Re_1 = Re_i'$, $i = 1,2$.

Corollary 4.5. Let $L = Re$, $L_1 = Re_1$, and $L_2 = Re_2$ be lines in V. Then $L \subseteq L_1 \oplus L_2$ if and only if $\alpha L \subseteq \alpha L_1 \oplus \alpha L_2$.

Proof: Assume $L \subseteq L_1 \oplus L_2$. By (4.4), $<\alpha(L_1 + L_2)> = \alpha L_1 \oplus \alpha L_2$. But $\alpha L \subseteq <\alpha(L_1 \oplus L_2)>$ so $\alpha L \subseteq \alpha L_1 \oplus \alpha L_2$. On the other hand, suppose $\alpha L \subseteq \alpha L_1 \oplus \alpha L_2$. By the above arguments, using α^{-1} instead of α, we have $L \subseteq L_1 \oplus L_2$.

Recently Ojanguren and Sridharan [16] have generalized to commutative rings the fundamental theorem of projective geometry. The setting is provided by the following definitions.

Let M and N be free modules over commutative rings A and B, respectively. A map $\alpha:P(M) \to P(N)$ is called a projectivity if α is bijective and for p_1, p_2, p_3 in P(M), we have $\alpha p_1 \subseteq \alpha p_2 + \alpha p_3$ in N if and only if $p_1 \subseteq p_2 + p_3$ in M. If $g:M \to N$ is a σ-semilinear isomorphism, then g induces a map $P(g):P(M) \to P(N)$ by setting $P(g)(Ae) = Bg(e)$ for any

unimodular element e of M. With this notation, if σ is an isomorphism, then P(g) is a projectivity. The following theorem ([16], page 311) then generalizes to commutative rings the classical "Fundamental Theorem of Projective Geometry."

Theorem. Let M and N be free modules of rank ≥ 3 over commutative rings A and B respectively. If $\alpha:P(M) \to P(N)$ is a projectivity, then there exists an isomorphism $\sigma:A \to B$ and a σ-semilinear isomorphism $g:M \to N$ such that $\alpha = P(g)$.

We return to our setting and recall that we have established a bijection $\alpha:P(V) \to P(V)$. However we have not indicated that α is a projectivity. Instead of satisfying the condition $\alpha p_1 \subseteq \alpha p_2 + \alpha p_3$ if and only if $p_1 \subseteq p_2 + p_3$, we have been able to show for α that $Re \subseteq Re_1 \oplus Re_2$ if and only if $\alpha Re \subseteq \alpha Re_1 \oplus \alpha Re_2$ for Re, Re_1, and Re_2 lines in V. That is, we require that $Re_1 \oplus Re_2$ be a plane in V. Thus we are not able to apply the theorem to our setting directly. However, an examination of the proof of this "Fundamental Theorem" enables us to make the following observations concerning our setting.

Let $e_1, e_2, \ldots, e_n$ be a basis for V. We have previously indicated that if $\alpha Re_i = Re_i'$ for $i = 1,2,\ldots,n$, then $e_1',\ldots,e_n'$ is also a basis for V. Using the techniques of the proof of Ojanguren and Sridharan, we get a basis $f_1,\ldots,f_n$ of V such that

(i) $\alpha Re_1 = Rf_i$ $\quad 1 \leq i \leq n$ and

(ii) $\alpha R(e_1 + e_i) = R(f_1 + f_i) \quad 2 \leq i \leq n.$

Further for r in R, $\alpha R(e_1 + re_2) = R(b_1f_1 + b_2f_2)$ with b_1 a unit of R. Thus $\alpha R(e_1 + re_2) = R(f_1 + \sigma(r)f_2)$ where $\sigma:R \to R$ is a well-defined map. Proceeding, as in [16], one is able to conclude that $\sigma:R \to R$ is a ring isomorphism.

Next it is shown that for $r_2,\ldots,r_n$ in R we have $\sigma R(e_1+r_2e_2+\ldots+r_ne_n) = R(f_1+\sigma(a_2)f_2+\ldots+\sigma(a_n)f_n)$. Indeed for any $r_1,\ldots,r_{i-1},r_{i+1},\ldots,r_n$ and i = 2, ..., n,

$$\alpha R(e_i+r_1e_1+\ldots+r_{i-1}e_{i-1}+r_{i+1}e_{i+1}+\ldots+r_ne_n)$$

$$= R(f_i+\sigma(r_1)f_1+\ldots+\sigma(r_{i-1})f_{i-1}+\sigma(r_{i+1})f_{i+1}+\ldots+\sigma(r_n)f_n).$$

All of these statements can be verified using the properties of σ which are slightly weaker than those of Ojanguren and Sridharan.

At this point in the proof [16], it is necessary to show for a unimodular $e = r_1e_1+\ldots+r_ne_n$ in V, that $\alpha R(r_1e_1+\ldots+r_ne_n) = R(\sigma(r_1)f_1+\ldots+\sigma(r_n)f_n)$. In the case of arbitrary commutative rings, the proof requires the stronger condition on the bijection. However, in our setting, R is local and thus one of $r_1,\ldots,r_n$ must be a unit, say r_i. Thus $R(r_1e_1+\ldots+r_ne_n)$

$$= R(e_i+r_i^{-1}r_1e_1+\ldots+r_i^{-1}r_{i-1}e_{i-1}+r_i^{-1}r_{i+1}e_{i+1}+\ldots+r_i^{-1}r_ne_n).$$

Then αRe

$$= R(f_i+\sigma(r_i^{-1}r_i)f_1+\ldots+\sigma(r_i^{-1}r_{i-1})f_{i-1}+\sigma(r_i^{-1}r_{i+1})f_{i+1}+\ldots+$$
$$\sigma(r_i^{-1}r_n)f_n).$$

But σ is a ring isomorphism so that $\sigma(r_i^{-1})$ is a unit. Thus

$R(f_i+\sigma(r_i^{-1}r_1)f_1+\ldots+\sigma(r_i^{-1}r_n)f_n) = R(\sigma(r_1)f_1+\ldots+\sigma(r_n)f_n)$.
Therefore

$\alpha R(r_1e_1+\ldots+r_ne_n) = R(\sigma(r_1)f_1+\ldots+\sigma(r_n)f_n)$ for unimodular $r_1e_1+\ldots+r_ne_n$.

Now, let $g:V \to V$ be the σ-semilinear isomorphism defined by $g(e_i) = f_i$. The result of the preceeding paragraph shows that $\alpha = P(g)$. Thus the above gives the following theorem.

Theorem 4.6. In the setting described in this section, with $\alpha:P(V) \to P(V)$ the bijection defined by $\alpha L = L'$ where $\Lambda(T(L)) = T(L')$, there is a semilinear isomorphism g of V onto V such that $gL = L'$ for all lines L in V.

We have previously noted that α preserves orthogonal lines. Thus, since $gL = \alpha L$, g also must preserve orthogonal lines. Then if x and y are unimodular elements such that $(x,y) = 0$, then the lines Rx and Ry must be orthogonal. Thus $(g(Rx), g(Ry)) = 0$. In particular, $(gx,gy) = 0$.

Let $X = \{x_1,x_2,\ldots,x_n\}$ be a symplectic basis for V, $n=2r$. For $1 \leq i \leq r$, put $\alpha_i = (gx_i,gx_{i+r})$. Then

$$(x_i+x_j,\ x_{i+r} - x_{j+r}) = 0 \quad \text{for } 1 \leq j \leq r,\ 1 \leq i \leq r.$$

But note x_i, x_j, x_{i+r}, x_{j+r} are basis elements and hence unimodular. Further $x_i + x_j$ and $x_{i+r} - x_{j+r}$ are then unimodular. Thus by the above note $(g(x_i+x_j), g(x_{i+r}-x_{j+r})) = 0$. So $0 = (gx_i+gx_j,\ gx_{i+r}-gx_{j+r})$

$$= (gx_i, gx_{i+r}) - (gx_i, gx_{j+r}) + (gx_j, gx_{i+r}) - (gx_j, gx_{j+r}).$$

But since x_i and x_{j+r} are unimodular with $(x_i, x_{j+r}) = 0$, we have $(gx_i, gx_{j+r}) = 0$. Similarly $(gx_j, gx_{i+r}) = 0$. Thus $(gx_i - gx_{i+r}) - (gx_j - x_{j+r}) = 0$ so that $\alpha_i = \alpha_j$. Thus $(gx_i, gx_{j+r}) = \alpha\delta_{ij}$ for some α in R; namely, $\alpha = \alpha_i = \alpha_j$.

Thus, consider cases $(gx_k, gx_s) = \alpha(x_k, x_s)$ for $1 \leq k \leq n$, $1 \leq s \leq n$:

(i) If $k = s$, then $(x_k, x_s) = 0$ implies $(gx_k, gx_s) = 0$. Hence $(gx_k, gx_s) = \alpha(x_k, x_s)$.

(ii) If $k \neq s$, assume $k < s$.

(a) If $s \leq r$, then $(x_k, x_s) = 0$ implies $(gx_k, gx_s) = 0$. Hence $(gx_k, gx_s) = \alpha(x_k, x_s)$.

(b) If $k \leq r < s$ then there exists a j such that $x_{j+r} = x_s$. Then $(gx_k, gx_s) = (gx_k gx_{j+r})$. Hence

$$(gx_k, gx_s) = \begin{cases} 0 \ (j \neq k) = \alpha(x_k, x_{j+r}) = \alpha(x_k, x_s) \\ \\ \alpha \ (j = k) = \alpha(x_k, x_{k+r}) = \alpha(x_k, x_s). \end{cases}$$

(c) If $r < k$, then $(x_k, x_s) = 0$ implies $(gx_k, gx_s) = 0$. Thus $(gx_k, gx_s) = \alpha(x_k, x_s)$.

So in any case $(gx_k, gx_s) = \alpha(x_k, x_s)$.

By linearity, we have $(gx, gy) = \alpha[\sigma(x, y)]$ for x and y in V. For if $x = a_1x_1 + \ldots + a_nx_n$ and $y = b_1x_1 + \ldots + b_nx_n$, then

$$\begin{aligned}(gx, gy) &= (\sigma(a_1)g(x_1) + \ldots + \sigma(a_n)g(x_n), \sigma(b_1)g(x_1) + \ldots + \sigma(b_n)g(x_n)) \\ &= \sigma(a_1)\sigma(b_{1+r})(gx_1, gx_{1+r}) + \ldots + \sigma(a_r)\sigma(b_n)(gx_r, gx_n) \\ &\quad -\sigma(a_{r+1})\sigma(b_1)(gx_{r+1}, gx_1) - \ldots - \sigma(a_n)\sigma(b_r)(gx_n, gx_r)\end{aligned}$$

$$= \sigma(a_1)\sigma(b_{1+r})\alpha + \ldots + \sigma(a_r)\sigma(b_n)\alpha - \ldots - \sigma(a_{r+1})\sigma(b_1)\alpha$$
$$- \sigma(a_n)\sigma(b_r)\alpha$$
$$= \alpha[\sigma(a_1b_{1+r} + \ldots + a_rb_n - a_{r+1}b_1 - \ldots - a_nb_r)]$$
$$= \alpha[\sigma(x,y)].$$

Observe then that $\phi_g(\sigma)$ is in $Sp_n(V)$ for σ in $Sp_n(V)$. For if σ is in $Sp_n(V)$, then

$$(\phi_g(\sigma)(x), \phi_g(\sigma)(y)) = (g\sigma g^{-1}(x), g\sigma g^{-1}(y))$$
$$= \alpha[\sigma(\sigma g^{-1}(x), \sigma g^{-1}(y))]$$
$$= \alpha[\sigma(g^{-1}x, g^{-1}y)]$$
$$= (g(g^{-1}x), g(g^{-1}y))$$
$$= (x,y).$$

Thus $\phi_g(Sp_n(V)) \subseteq Sp_n(V)$. By considering g^{-1}, we have $\phi_g(Sp_n(V)) = Sp_n(V)$. Hence ϕ_g is an automorphism of $Sp_n(V)$.

Hence $\phi_g^{-1} \circ \Lambda$ defines an automorphism of $Sp_n(V)$. Suppose τ is a transvection with line L. Since Λ preserves transvections, $\Lambda\tau$ is a transvection with proper line $L' = \alpha L$. Observe that $\phi_g^{-1} = \phi_{g^{-1}}$ and $\phi_{g^{-1}}(\Lambda\tau) = g^{-1}(\Lambda\tau)g$. Hence $\phi_g^{-1} \circ \Lambda(\tau)$ is a transvection with line $g^{-1}L' = L$. That is, $\phi_g^{-1} \circ \Lambda(\tau)$ has the same line as τ. Thus by (4.1), there is a homomorphism $\chi: Sp_n(V) \to \{\pm 1_V\}$ such that $\phi_g^{-1} \circ \Lambda = P_\chi$. Therefore $\Lambda = \phi_g \circ P_\chi$. Using Λ^{-1} instead of Λ, we obtain $\Lambda = P_\chi \circ \phi_g$ as stated in theorem 4.2.

BIBLIOGRAPHY

1. Artin, Emil. Geometric Algebra. New York: Interscience Publishers, 1962.

2. Atiyah, M. F. and MacDonald, I. G. Introduction to Commutative Algebra. Reading Massachusetts: Addison-Wesley, 1969.

3. Bass, Hyman. Algebraic K-Theory. New York: W. A. Benjamin, 1968.

4. Chien, Yen Shih. "Linear Groups Over a Ring," Chinese Mathematics, 7(1965), 163-179.

5. Dieudonné, Jean. La Geometrie Des Groupes Classiques. Berlin: Springer-Verlag, 1955.

6. Dieudonné, Jean. On the Automorphisms of the Classical Groups. Memoirs 2. Providence: American Mathematical Society, 1951.

7. Dieudonné, Jean. Sur les Groupes Classiques. Paris: Hermann, 1958.

8. Hua, L. K. and Reiner, I. "Automorphisms of the Unimodular Group," Transactions of the American Mathematical Society, 71(1951), 331-348.

9. Hua, L. K. and Reiner, I. "On the Generators of the Symplectic Modular Group," Transactions of the American Mathematical Society, 65(1949), 415-426.

10. Hua, Loo-Keng. "Geometries of Matrices," Transactions of the American Mathematical Society, 57(1945), 441-490.

11. Hua, Loo-Keng. "On the Automorphisms of the Symplectic Group Over Any Field," Annals of Mathematics, 49(1948), 739-759.

12. Kaplansky, Irving. Linear Algebra and Geometry. Boston: Allyn and Bacon, 1969.

13. Klingenberg, Wilhelm. "Symplectic Groups Over Local Rings," American Journal of Mathematics, 85(1963), 232-240.

14. Lang, Serge. Algebra. Reading, Massachusetts: Addison-Wesley, 1965.

15. Nagata, Masayoshi. Local Rings. New York: Interscience Publishers, 1962.

16. Ojanguren, M. and Sridharan, R. "A Note on the Fundamental Theorem of Projective Geometry," Commentarii Mathematica Helvetici, 44(1969), 310-315.

17. O'Meara, O. T. "The Automorphisms of Linear Groups Over Any Integral Domain," Journal fur die reine und angewandte Mathematik, 223(1966), 56-100.

18. O'Meara, O. T. "The Automorphisms of the Standard Symplectic Group Over Any Integral Domain," Journal fur die reine und angewandte Mathematik, 230(1968), 103-138.

19. Pomfret, James Charles. "Linear Groups Over Local Rings." Unpublished Ph.D. dissertation, University of Oklahoma, 1971.

20. Reiner, Irving. "Automorphisms of the Symplectic Modular Group," Transactions of the American Mathematical Society, 80(1955), 35-50.

21. Reiner, Irving. "Real Linear Characters of the Symplectic Modular Group," Proceedings of the American Mathematical Society, 6(1955), 987-990.

22. Reiner, Irving. "Symplectic Modular Complements." Transactions of the American Mathematical Society, 77(1954), 498-505.

23. Schreier, O. and van der Waerder, B. L. "Die Automorphism der projectiven Gruppen," Abhandlungen aus dem mathematishen Seminar der Hamburgishen Universitat, 6(1928), 303-322.

24. Wan, C. H. "On the Automorphisms of Linear Groups Over A Non-Commutative Euclidean Ring of Characteristic 2," Sci. Record, 1(1957), 5-8.

25. Wan, Z. X. and Wang, Y. X. "On the Automorphisms of Symplectic Groups Over A Field of Characteristic 2," Sci. Sinica, 12(1963), 289-315.