PROGRESS IN GALOIS THEORY

Proceedings of John Thompson's
70th Birthday Conference

Developments in Mathematics

VOLUME 12

Series Editor:

Krishnaswami Alladi, *University of Florida, U.S.A.*

Aims and Scope

Developments in Mathematics is a book series publishing

(i) Proceedings of Conferences dealing with the latest research advances,

(ii) Research Monographs, and

(iii) Contributed Volumes focussing on certain areas of special interest

Editors of conference proceedings are urged to include a few survey papers for wider appeal. Research monographs, which could be used as texts or references for graduate level courses, would also be suitable for the series. Contributed volumes are those where various authors either write papers or chapters in an organized volume devoted to a topic of special/current interest or importance. A contributed volume could deal with a classical topic, which is once again in the limelight owing to new developments.

PROGRESS IN GALOIS THEORY

Proceedings of John Thompson's 70th Birthday Conference

Edited by

HELMUT VOELKLEIN
University of Florida, U.S.A.

TANUSH SHASKA
University of Idaho, U.S.A.

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

ISBN 0-387-23533-7 e-ISBN 0-387-23534-5 Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 11332459

springeronline.com

Contents

Preface

The legacy of Galois was the beginning of Galois theory as well as group theory. From this common origin, the development of group theory took its own course, which led to great advances in the latter half of the 20th century. It was John Thompson who shaped finite group theory like no-one else, leading the way towards a major milestone of 20th century mathematics, the classification of finite simple groups.

After the classification was announced around 1980, it was again J. Thompson who led the way in exploring its implications for Galois theory. The first question is whether all simple groups occur as Galois groups over the rationals (and related fields), and secondly, how can this be used to show that all finite groups occur (the 'Inverse Problem of Galois Theory'). What are the implications for the structure and representations of the absolute Galois group of the rationals (and other fields)? Various other applications to algebra and number theory have been found, most prominently, to the theory of algebraic curves (e.g., the Guralnick-Thompson Conjecture on the Galois theory of covers of the Riemann sphere).

All the above provided the general theme of the Year of Algebra at the University of Florida (2002/2003): the beauty and power of group theory, and how it applies to problems of arithmetic via the basic principle of Galois. The recent award of the National Medal of Science to J. Thompson made this all the more fitting, and provided the final backdrop for the celebration of the 70th birthday of our revered colleague John Thompson. To celebrate this occasion with the mathematical community, we organized a conference at the University of Florida, Nov. 4-8, 2002.

The conference continued a major line of work about covers of the projective line (and other curves), their fields of definition and parameter spaces, and associated questions about arithmetic fundamental groups. This is intimately tied up with the Inverse Problem of Galois Theory, and uses methods of algebraic geometry, group theory and number theory. Here is a brief summary of some highlights in the area:

- The classification of finite simple groups is announced around 1980; Fried, Matzat, Thompson and others begin to explore applications to the Inverse Galois Problem.

- Thompson (1984) realizes the monster, the largest sporadic simple group, as a Galois group over the rationals. All other sporadic simple groups follow, with one exception (M_{23}). More generally, Malle, Matzat, Fried, Thompson, Voelklein and others construct covers of the projective line defined over the rationals, by using rigidity, Hurwitz spaces and the braid group, in order to realize simple (and related) groups as Galois groups over the rationals. One is still far from realizing all simple groups.

- Harbater and Raynaud win the Cole Prize in 1995 for solving Abhyankar's Conjecture on unramified covers of affine curves in positive characteristic.

- The Guralnick-Thompson Conjecture on monodromy groups of genus zero covers of the projective line: Proof completed by Frohard and Magaard in 1999, building on work of Aschbacher, Guralnick, Liebeck, Thompson and other group-theoretists.

- The MSRI semester 'Galois groups and fundamental groups', fall '99, organized by Fried, Harbater, Ihara, Thompson and others, defines the area, its methods, goals and open problems.

Here is a brief description of the contents of this volume. It is a recent trend to tie the previous theory of curve coverings (mostly of the Riemann sphere) and Hurwitz spaces (moduli spaces for such covers) with the theory of algebraic curves and their moduli spaces $\mathcal{M}_g$. A general survey of this is given in the article by Voelklein. Further exemplifications come in the articles of Guralnick on automorphisms of modular curves in positive characteristic, of Zarhin on the Galois module structure of the 2-division points of hyperelliptic curves and of Krishnamoorthy, Shaska and Voelklein on invariants of genus 2 curves.

Abhyankar continues his work on explicit classes of polynomials in characteristic $p > 0$ whose Galois groups comprise entire families of Lie type groups in characteristic p. In his article, he proves a characterization of symplectic groups required for the identification of the Galois group of certain polynomials.

The more abstract aspects come into play when considering the totality of Galois extensions of a given field. This leads to the study of absolute Galois groups and (profinite) fundamental groups. Haran and Jarden present a result on the problem of finding a group-theoretic characterization of absolute Galois groups. In a similar spirit, Boston studies infinite p-extensions of number fields

unramified at p and makes a conjecture about a group-theoretic characterization of their Galois groups. He notes connections with the Fontaine-Mazur conjecture, knot theory and quantum field theory. Nakamura continues his work on relationships between the absolute Galois group of the rationals and the Grothendieck-Teichmüller group.

Finally, Fried takes us on a tour of places where classical topics like modular curves and j-line covers connect to the genus zero problem which was the starting point of the Guralnick-Thompson conjecture.

HELMUT VOELKLEIN

Progress in Galois Theory, pp. 1-23
H. Voelklein and T. Shaska, Editors

SUPPLEMENTARY THOUGHTS ON SYMPLECTIC GROUPS

Shreeram S. Abhyankar
Mathematics Department, Purdue University, West Lafayette, IN 47907, USA.
ram@cs.purdue.edu

Nicholas F. J. Inglis
Queens' College, Cambridge University, Cambridge CB3 9ET, UK.
n.f.j.inglis@dpmms.cam.ac.uk

Umud D. Yalcin
Mathematics Department, Purdue University, West Lafayette, IN 47907, USA.
uyalcin@math.purdue.edu

Abstract Let b be a nondegenerate symplectic form on a vector space V over a finite field. It is well-known that every intermediate group between $\mathrm{Sp}(V,b)$ and $\Gamma Sp(V,b)$ (i.e. the isometry and the semisimilarity groups of b, respectively) is Rank 3 in its action on the projective space $\mathscr{P}(V)$. We prove that this property characterizes such subgroups of $\Gamma Sp(V,b)$ when the dimension of V is greater than 2.

1. Introduction

In this paper, we will prove the following theorem:

Theorem 1.1. *Let $G \leq \Gamma L(V)$ be transitive Rank 3 on $\mathscr{P}(V)$ with subdegrees $1, q+q^2+\cdots+q^{n-2}, q^{n-1}$ where V is an n-dimensional vector space over the field $k = GF(q)$ with $n = 2m \geq 4$, and $\mathscr{P}(V)$ is the set of all 1-spaces in V. Then there exists a symplectic form b on V such that either $Sp(V,b) \leq G$ or $A_6 \approx G \leq Sp(V,b) \approx S_6$ with $(n,q) = (4,2)$.*

By Lemma (5.5), which we will prove in Section 5, if there exists a subgroup G of $\Gamma L(V)$ that satisfies the hypothesis of Theorem (1.1), then we can define a symplectic form b on V such that $G \leq \Gamma Sp(V,b)$. Therefore, Theorem (1.1) can be restated as follows:

Symplectic Rank Three Theorem (1.2). *Let $G \leq \Gamma L(V,b)$ be transitive Rank 3 on $\mathscr{P}(V)$, where b is a nondegenerate symplectic form on an n-dimensional vector space V over $k = GF(q)$ with $n = 2m \geq 4$. Then either $Sp(V,b) \lhd G$ or $A_6 \approx G \leq Sp(V,b) \approx S_6$ with $(n,q) = (4,2)$.*

The quest for the Rank 3 subgroups of symplectic groups was started by the 1965 paper [HMc] of Higman-McLaughlin. In that paper they proved for $4 \leq n \leq 8$ and q odd that the only Rank 3 subgroup of $\mathrm{Sp}(V,b)$ was $\mathrm{Sp}(V,b)$ itself. In his 1972 paper [Per], Perin extended this result to any $n \geq 4$ and $q > 2$. Then, in their 1979 paper [CKa], Cameron and Kantor claimed the above stated Theorem (1.2), but their proof is very difficult to understand. Here our goal is to give a transparent proof for this theorem by using methods similar to the ones used by Abhyankar and Inglis in [AIn] to prove that any subgroup G of $\mathrm{GSp}(V,b)$ satisfying the hypothesis of Theorem (1.2) has to contain $\mathrm{Sp}(V,b)$ except when $A_6 \approx G \leq Sp(V,b) \approx S_6$ with $(n,q) = (4,2)$; for a correction to [AIn] see Remark (6.8) at the end of section 6.

In the first four sections, some introductory material about symplectic groups, orbits, orbitals and antiflags is given. Section 5 sketches the action of the symplectic groups on $\mathscr{P}(V)$ and on the lines in $\mathscr{P}(V)$. In Section 6, we will describe the structures of the normalizers of some Sylow subgroups of $\Gamma Sp(V,b)$, which will be used in Section 7 for the proof of Theorem (1.2).

Now, let V be a vector space of dimension n over a field k. A bivariate form on V is a map $b : V \times V \to k$. A bilinear form on V is a bivariate form b which is linear with respect to both terms; i.e. $b(\cdot, v) \to k$ and $b(u, \cdot) \to k$ are linear transformations for all $u, v \in V$. A bivariate form is

$$\begin{aligned} \textit{symmetric if} \quad & b(u,v) = b(v,u) \textit{ for all } u,v \in V \\ \textit{anti-symmetric if} \quad & b(u,v) = -b(v,u) \textit{ for all } u,v \in V \\ \textit{alternating if} \quad & b(u,u) = 0 \textit{ for all } u \in V. \end{aligned}$$

An alternating bilinear form is called a symplectic form. It is easy to see that a symplectic form is always anti-symmetric and if $\mathrm{char}(k) \neq 2$, then any anti-symmetric bilinear form is symplectic.

For an automorphism σ of k, a map $g : V \to V$ is called σ-linear if $g(u+v) = g(u) + g(v)$ and $g(\lambda v) = \sigma(\lambda) g(v)$ for all $u, v \in V$ and for all $\lambda \in k$. A map $h : V \to V$ is called a semilinear transformation if it is t_h-linear for some $t_h \in Aut(k)$. The group of all semilinear transformations is denoted by $\Gamma L(V)$.

Let b be a nondegenerate symplectic form and let g be a σ-linear transformation on V. Then $\mathrm{Sp}(V,b)$, $\mathrm{GSp}(V,b)$ and $\Gamma Sp(V,b)$, which are the groups of all b-isometries, b-similarities and b-semisimilarities, respectively, are defined as follows:

$g \in Sp(V,b)$ if and only if $b(g(u), g(v)) = b(u,v)$;

$g \in GSp(V,b)$ if there exists $\lambda \in k$ such that $b(g(u), g(v)) = \lambda b(u,v)$;

$g \in \Gamma Sp(V,b)$ if there exists $\lambda \in k$ such that $b(g(u), g(v)) = \lambda \sigma(b(u,v))$.

Some basic properties of $\mathrm{Sp}(V,b)$, $\mathrm{GSp}(V,b)$ and $\Gamma Sp(V,b)$ which can be found in [Tay] are as follows:

(1.3). Let b be a nondegenerate symplectic form on an n-dimensional vector space V over a finite field $k = GF(q)$. Then

(1.3.1) There exists a basis $\{e_1, e_2, \ldots, e_m, f_1, f_2, \ldots, f_m\}$ of V such that

$$b(e_i, e_j) = b(f_i, f_j) = 0 \text{ and } b(e_i, f_j) = \delta_{ij}$$

for all $i, j \in \{1, 2, \ldots, m\}$.

(1.3.2) $n = 2m$ is even.

(1.3.3) $Sp(V,b) = \Gamma Sp(V,b) \cap SL(V)$ and $GSp(V,b) = \Gamma Sp(V,b) \cap GL(V)$.

(1.3.4) If $n = 2$, $Sp(V,b) \approx SL(V)$.

(1.3.5) $|Sp(V,b)| = q^{m^2} \prod (q^{2i} - 1)$,

(1.3.6) When $\mathrm{char}(k) = p$ and $q = p^f$ we have:

$$\begin{aligned} |GSp(V,b) : Sp(V,b)| &= |k^\times| = q - 1, \\ |\Gamma Sp(V,b) : GSp(V,b)| &= |Aut(k)| = f. \end{aligned}$$

By (1.2.1), we see that if

$$u = \sum_{i=1}^{m} u_i e_i + \sum_{i=1}^{m} u_{m+i} f_i \quad \text{and} \quad v = \sum_{i=1}^{m} v_i e_i + \sum_{i=1}^{m} v_{m+i} f_i,$$

then

$$b(u,v) = \sum_{i=1}^{m} (u_i v_{m+i} - u_{m+i} v_i).$$

Therefore, when we consider the symplectic groups in general, we can write $Sp(n,q)$, $GSp(n,q)$ and $\Gamma Sp(n,q)$ in place of $Sp(V,b)$, $GSp(V,b)$ and $\Gamma Sp(V,b)$, respectively.

2. Orbit Counting

Let G be a finite group acting on a finite set X. Recall that for any $x \in X$, the G-stabilizer and the G-orbit of x are defined by putting $G_x = \{g \in G : g(x) = x\}$ and $\mathrm{orb}_G(x) = \{y \in X : g(x) = y \text{ for some } g \in G\}$, respectively. Also an orbit of G on X is a subset Y of X such that $Y = orb_G(x)$ for some $x \in X$ and the set of all orbits of G on X is denoted by $\mathrm{orbset}_G(X)$. The size of the orbit and the size of the stabilizer are related by the following well-known lemma.

Lemma 2.1 (Orbit-Stabilizer Lemma). *For any $x \in X$ we have $|orb_G(x)| = |G|/|G_x|$.*

The idea of the G-stabilizer can be generalized by defining the G-stabilizer of a subset Y of X as $G_Y = \{g \in G : g(Y) = Y\}$, this is also called the setwise

G-stabilizer of Y. Then we can define the pointwise G-stabilizer of Y as $G_{[Y]} = \{g \in G : g(y) = y \text{ for all } y \in Y\}$. In the case $G_Y = G$, we say G stabilizes Y or Y is G-invariant. It is easy to see that this is the case if and only if Y is a union of some G-orbits on X.

Note that, for any prime p, $|X|_p$ denotes the highest power p^a of p which divides $|X|$. Also note that a p-group is a finite group whose order is a power of p, and that a Sylow p-subgroup of G is a p-subgroup P of G such that $|P|_p = |G|_p$. Letting $\mathrm{Syl}_p(G)$ denote the set of all Sylow p-subgroups of G, we get the following consequence (2.2) of (2.1).

Lemma 2.2 (Sylow Transitivity Lemma). *If $P \in Syl_p(G)$ then for every $x \in X$ we have $|orb_P(x)|_p \geq |orb_G(x)|_p$, and, in particular, if Y is any orbit of G on X such that $|Y|$ is a power of p then P is transitive on Y.*

3. Orbitals

Let G be a finite group acting on a nonempty finite set X. Then G acts on $X \times X$ componentwise; i.e. for all $(x',x'') \in X \times X$ and $g \in G$, we have $g((x',x'')) = (g(x'),g(x''))$. The orbits of G on $X \times X$ are called orbitals of G on X. For any $Y \subset X \times X$ and $x' \in X$, we define $Y(x') = \{x'' \in X : (x',x'') \in Y\}$.

Lemma 3.1. *If G is a finite group acting on a nonempty finite set X, then for any orbital Y of G and for any $x \in X$ satisfying $Y(x) \neq \emptyset$, we have:*

(3.1.1). $Y(x)$ is an orbit of G_x on X,

(3.1.2). $g(Y(x)) = Y(g(x))$.

Now assume that the action of G on X is transitive and that Y is an orbital of G on X. Then for any $x,y \in X$, there exists $g \in G$ such that $g(x) = y$ and it induces a bijection $Y(x) \to Y(y)$. This shows that $Y(x) = Y(y)$ for all $x,y \in X$. If Z is another orbital of G on X, then $Z(x) \cap Y(x) = \emptyset$ and so there exists a bijection between the orbits of G_x and the orbitals of G on X. This proves the following lemma.

Lemma 3.2. *Let G be a finite group acting transitively on a nonempty finite set X and let Y be an orbital of G on X. Then for any $x \in X$, we have:*

(3.2.1) $|Y(x)| = |Y| / |X|$

(3.2.2) $|orbset_G(X \times X)| = |orbset_{G_x}(X)|$

When the action of G on X is transitive, the number of orbitals of G on X is called the rank (or, permutation rank) of G on X, and we denote it by $\mathrm{Rank}_G(X)$. By (3.2.2), this number is equal to the number of orbits of G_x on X, for any $x \in X$. The subdegrees of G on X are the sizes of the orbits of G_x on X, which are independent of x by (3.2.1).

Lemma 3.3. *If for an orbital Y of a finite group G acting transitively on a nonempty finite set X, and for some $x \in X$, the size of the orbit $Y(x)$ of G_x on*

X is different from the size of every other orbit of G_x on X, then $(x,y) \in Y \Leftrightarrow (y,x) \in Y$; or, equivalently $y \in Y(x) \Leftrightarrow x \in Y(y)$.

Proof. Assume that $|Y(x)| \neq |Z(x)|$ for any other orbital Z of G on X. Then $|Y| \neq |Z|$ for any $Z \in orbset_G(X \times X) \setminus \{Y\}$. Therefore $(x,y) \in Y$ if and only if $(y,x) \in Y$, since $Y = orb_G((x,y))$ and $|orb_G((x,y))| = |orb_G((y,x))|$. □

4. Flags and Antiflags

Let V be an n-dimensional vector space over a field k with $n \geq 2$. A full flag in V is a sequence of subspaces $V_1 \subset V_2 \subset \cdots \subset V_n$ where $\dim_k V_i = i$. A projective full flag in $\mathscr{P}(V)$ is a sequence of subspaces $\mathscr{P}(V_1) \subset \mathscr{P}(V_2) \subset \cdots \subset \mathscr{P}(V_n)$ where $V_1 \subset V_2 \subset \cdots \subset V_n$ is a full flag in V. The projective sizes of $V_1, V_2 \setminus V_1, \ldots, V_n \setminus V_{n-1}$ are the sizes of $\mathscr{P}(V_1), \mathscr{P}(V_2) \setminus \mathscr{P}(V_1), \ldots, \mathscr{P}(V_n) \setminus \mathscr{P}(V_{n-1})$. An antiflag in V is a pair (U,U') such that U is a 1-space and U' is a hyperplane of $\mathscr{P}(V)$ and $U \not\subset U'$. Similarly, an antiflag in $\mathscr{P}(V)$ is a pair (x,H) such that H is a hyperplane and x is a point of $\mathscr{P}(V)$ and $x \notin H$.

Let $\mathrm{UL}(n,q)$ be the set of all $n \times n$ uniuppertriangular matrices (i.e., upper-triangular matrices with 1 everywhere on the diagonal) with entries in $\mathrm{GF}(q)$ where q is a power of a prime number p. Since $|GL(n,q)| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)$ and $|UL(n,q)| = q^{n(n-1)/2}$, we have $|UL(n,q)| = |GL(n,q)|_p$ and this proves:

Lemma 4.1 (Sylow Subgroup Lemma). *$UL(n,q)$ is a Sylow p-subroup of $GL(n,q)$.*

Letting $e_1, e_2, \ldots, e_n$ be the unit vectors in $\mathrm{GF}(q)^n$ and L_i be the subspace generated by $e_1, e_2, \ldots, e_i$, we see that $orb_{UL(n,q)}(\langle e_i \rangle) = \mathscr{P}(L_i) \setminus \mathscr{P}(L_{i-1})$. Therefore, the orbits of $\mathrm{UL}(n,q)$ in $\mathscr{P}(V)$ are $\mathscr{P}(L_1), \mathscr{P}(L_2) \setminus \mathscr{P}(L_1), \ldots, \mathscr{P}(L_n) \setminus \mathscr{P}(L_{n-1})$.

Lemma 4.2 (Flag Stabilization Lemma). *The orbits of any $P \in Syl_p(\Gamma L(n,q))$ in $\mathscr{P}(n-1,q)$ are the complements of a projective full flag, and hence the largest orbit of P has size q^{n-1}, and it is the complement of a unique hyperplane in $\mathscr{P}(n-1,q)$.*

Proof. By Sylow's Theorem, there exists a Sylow p-subgroup P' of $\Gamma L(n,q)$ such that $UL(n,q) \leq P'$. Then each orbit of P' is a disjoint union of some orbits of $\mathrm{UL}(n,q)$. Let $\Omega = \mathscr{P}(L_{i_1}) \setminus \mathscr{P}(L_{i_1-1}) \cup \mathscr{P}(L_{i_2}) \setminus \mathscr{P}(L_{i_2-1}) \cup \cdots \cup \mathscr{P}(L_{i_j}) \setminus \mathscr{P}(L_{i_j-1})$ be an orbit of P' in $\mathscr{P}(V)$ (here, we can define $\mathscr{P}(L_0) = \emptyset$), then $|\Omega| = q^{i_1-1} + q^{i_2-1} + \cdots + q^{i_j-1}$ which is a p-power if and only if $j = 1$. Since P' is a p-group, $|\Omega|$ is a p-power and so $j = 1$. This implies that $\Omega = \mathscr{P}(L_{i_1}) \setminus \mathscr{P}(L_{i_1-1})$; i.e. Ω is an orbit of $\mathrm{UL}(n,q)$ in $\mathscr{P}(V)$. Hence the orbits of P' are the complements of the projective full flag $\mathscr{P}(L_1) \subset \mathscr{P}(L_2) \subset \cdots \subset \mathscr{P}(L_n)$. By Sylow's Theorem, any $P \in Syl_p(\Gamma L(n,q))$ is a conjugate of P' and so the theorem follows. □

As applications of Lemmas (2.2), (3.1), (3.3), and (4.2), we shall now prove the following two Lemmas (4.3) and (4.4).

Lemma 4.3 (Hyperplanarity Lemma). *Let k be the finite field $GF(q)$ of order q and let $G \leq \Gamma L(V)$ be transitive on $\mathscr{P}(V)$. Assume that $n > 2$ and G has an orbital Δ on $\mathscr{P}(V)$ such that for $x \in \mathscr{P}(V)$ we have $|\Delta(x)| = q^{n-1}$. Then $\Delta(x)$ is the complement of a unique hyperplane in $\mathscr{P}(V)$, i.e., $\Delta(x) = \mathscr{P}(V) \setminus \mathscr{P}(H(x))$ for a unique hyperplane $H(x)$ in V.*

Let x be a point in $\mathscr{P}(V)$ and let P' be a Sylow p-subgroup of G_x; then, by Lemma (2.2), P' is transitive on $\Delta(x)$. By Sylow's Theorem, there exists $P \in Syl_p(\Gamma L(V))$ such that $P' \leq P$. It follows that P has an orbit in $\mathscr{P}(V)$ containing $\Delta(x)$. On the other hand, Lemma (4.2) shows that the largest orbit of P is the complement of a unique hyperplane $H(x)$ and its size is q^{n-1}. Therefore, we have $\Delta(x) = \mathscr{P}(V) \setminus \mathscr{P}(H(x))$.

Lemma 4.4 (Supplementary Hyperplanarity Lemma). *In the situation of (4.3) assume that $Rank_G(\mathscr{P}(V)) = 3$. Then:*

(4.4.1) If we let $\overline{H}(x) = \mathscr{P}(H(x))$, then for any $g \in G$ we have $g(\overline{H}(x)) = \overline{H}(g(x))$, or equivalently $g(\overline{H}(g^{-1}(x))) = \overline{H}(x)$,

(4.4.2) $x \mapsto H(x)$ gives a bijection $X_1 \to X_{n-1}$,

(4.4.3) For any $y \in \mathscr{P}(V)$ and $z \in \mathscr{P}(V)$ with $y \neq x$ and $z \subset x+y$, we have $H(x) \cap H(y) \subset H(z)$.

Let Γ be the orbital of G on $\mathscr{P}(V)$ different from $\{(y,y) : y \in \mathscr{P}(V)\}$ and Δ. It follows from the previous lemma that $\overline{H}(x) = \{x\} \cup \Gamma(x)$. Then we have $g(\overline{H}(x)) = \overline{H}(g(x))$, since by (3.1.2), $g(\Gamma(x)) = \Gamma(g(x))$.

To prove the second part, assume the contrary that there exists $y \neq x$ in $\mathscr{P}(V)$ satisfying $H(x) = H(y)$. This implies that $y \in \Gamma(x)$ and $\overline{H}(g(y)) = g(\overline{H}(y)) = \overline{H}(x)$ for all $g \in G_x$; i.e. $\overline{H}(z) = \overline{H}(x)$ for all $z \in \Gamma(x)$. Since G is transitive on $\mathscr{P}(V)$, this should hold for every point in $\mathscr{P}(V)$: $x' \in \mathscr{P}(V) \Rightarrow \overline{H}(z') = \overline{H}(x')$ for all $z' \in \overline{H}(x')$. But then it follows that $x' \notin \overline{H}(x) \Rightarrow \overline{H}(x) \cap \overline{H}(x') = \emptyset$ which cannot happen, since in $\mathscr{P}(V)$ with $n > 2$ any two hyperplanes meet.

It only remains to show that $z \subset x+y \Rightarrow H(x) \cap H(y) \subset H(z)$. By Lemma (3.3), we know that $s \in \overline{H}(r) \Leftrightarrow r \in \overline{H}(s)$. Therefore

$$\begin{aligned} w \in \overline{H}(x) \cap \overline{H}(y) &\Rightarrow w \in \overline{H}(x) \text{ and } w \in \overline{H}(y) \\ &\Rightarrow x \in \overline{H}(w) \text{ and } y \in \overline{H}(w) \\ &\Rightarrow x+y \subset H(w) \\ &\Rightarrow z \in \overline{H}(w) \text{ for all } z \subset x+y \\ &\Rightarrow w \in \overline{H}(z) \text{ for all } z \subset x+y \end{aligned}$$

and hence

$$\begin{aligned} z \subset x+y &\Rightarrow w \in \overline{H}(z) \text{ for all } w \in \overline{H}(x) \cap \overline{H}(y) \\ &\Rightarrow H(x) \cap H(y) \subset H(z). \end{aligned}$$

5. Correlations

Let V and V' be n-dimensional vector spaces over fields k and k' respectively. By a collineation $\nu : \mathscr{P}(V) \to \mathscr{P}(V')$ we mean a bijection which sends lines in $\mathscr{P}(V)$ to lines in $\mathscr{P}(V')$. For an isomorphism $\sigma : k \to k'$, by a σ-linear transformation $V \to V'$ we mean an additive isomorphism such that for all $\lambda \in k$ and $v \in V$ we have $\mu(\lambda v) = \sigma(\lambda)\mu(v)$, and we note that then μ induces the collineation $\mu' : \mathscr{P}(V) \to \mathscr{P}(V')$ which, for every $0 \neq v \in V$, sends kv to $k'\mu(v)$. The Fundamental Theorem of Projective Geometry (see Theorem 3.1 on page 14 of [Tay]) says that conversely, for $n > 2$, given any collineation $\nu : \mathscr{P}(V) \to \mathscr{P}(V')$ there exists an isomorphism $\sigma : k \to k'$ and a σ-linear bijection $\mu : V \to V'$ such that $\nu = \mu'$; moreover, ν determines σ and it determines μ up to multiplication by a nonzero element of k', i.e., if there exists any other such then for some $0 \neq \kappa \in k'$ we have $\overline{\mu}(v) = \kappa\mu(v)$ for all $v \in V$. In particular, for $n > 2$, by taking $k' = k$ and $V' = V$ it follows that $\mathrm{P\Gamma L}(V)$ is (= is naturally isomorphic to) the group of all collineations of $\mathscr{P}(V)$, i.e., collineations of $\mathscr{P}(V)$ onto itself.

Now suppose that $k' = k$ and $V' =$ the dual of V which consists of all k-linear maps $V \to k$. By a correlation of $\mathscr{P}(V)$ we mean a collineation $\nu : \mathscr{P}(V) \to \mathscr{P}(V')$. Applying the above Theorem to such ν we find a unique $\sigma \in Aut(k)$ together with a σ-linear bijection $\mu : V \to V'$, which is determined upto multiplication in $k^\times$, such that $\nu = \mu'$. Let $b : V \times V \to k$ be defined by $b(v,w) = \mu(w)(v)$. Then the σ-linearity of μ implies the σ-sesquilinearity of b which means that b is k-linear in v, additive in w, and for all $\alpha \in k$ we have $b(v,\alpha w) = \sigma(\alpha)b(v,w)$. Also the bijectivity of μ implies the nondegeneracy of b which means that $b(v,w) = 0$ *for all* $w \in V \Rightarrow v = 0$ and $b(v,w) = 0$ *for all* $v \in V \Rightarrow w = 0$. Consequently (cf. page 52 of [Tay]), for any subspace W of V, upon letting $W^{\perp_b} = \{v \in V : b(v,w) = 0 \text{ for all } w \in W\}$, we see that $W^{\perp_b}$ is a subspace of V with $dim_k W^{\perp_b} = n - dim_k(W)$, and hence upon letting $W^\natural = \{v' \in V' : v'(v) = 0 \text{ for all } v \in W\}$ we see that. $(W^{\perp_b})^\natural$ is a subspace of V' with $dim_k(W^{\perp_b})^\natural = dim_k(W)$. In particular, for every $x \in \mathscr{P}(V)$ we have $(x^{\perp_b})^\natural = \nu(x) \in \mathscr{P}(V')$. The general fact that ν determines μ upto multiplication, says that if $b' : V \times V \to k$ is any σ-sesquilinear form such that $x^{\perp_b} = x^{\perp_{b'}}$ for all $x \in \mathscr{P}(V)$ then there exists $\alpha \in k^\times$ such that $b'(v,w) = \alpha b(v,w)$ for all v, w in V. Thus we have the following:

Lemma 5.1 (Correlation Lemma). *Let V be an n-dimensional vector space over a field k with $n > 2$, and let ν be a correlation of $\mathscr{P}(V)$. Then there exists $\sigma \in Aut(k)$ together with a nondegenerate σ-sesquilinear form $b : V \times V \to k$ such that $\nu(x) = (x^{\perp_b})^\natural$ for all $x \in \mathscr{P}(V)$. Moreover, if $b' : V \times V \to k$ is any σ-sesquilinear form such that $\nu(x) = (x^{\perp_{b'}})^\natural$ for all $x \in \mathscr{P}(V)$, then there exists $\alpha \in k^\times$ such that $b'(v,w) = \alpha b(v,w)$ for all v, w in V.*

Concerning a σ-sesquilinear form $b : V \times V \to k$, where V is an n-dimensional vector space over a field k and $\sigma \in Aut(k)$, note that: (i) if b is antisymmetric and $b(v,w) \neq 0$ for some v,w in V (which is certainly the case if b is nondegenerate), then for all $\alpha \in k$ we have $\alpha b(v,w) = b(\alpha v, w) = -b(w,\alpha v) = -\mu(\alpha)b(w,v) = \mu(\alpha)b(v,w)$ and dividing the extremities by $b(v,w)$ we get $\alpha = \mu(\alpha)$, and hence μ is identity and so b is bilinear; and (ii) the form b is alternating $\Leftrightarrow x \subset x^{\perp_b}$ *for all* $x \in \mathscr{P}(V)$; and hence (iii) if the form b is nondegenerate and for all $x \in \mathscr{P}(V)$ we have $x \subset x^{\perp_b}$, then n is even and b is a nondegenerate symplectic form on V.

Thus we conclude with the:

Lemma 5.2 (Sesquilinearity Lemma). *For a σ-sesquilinear form $b : V \times V \to k$, where V is an n-dimensional vector space over a field k and $\sigma \in Aut(k)$, we have the following.*

(5.2.1) If the form b is nondegenerate and antisymmetric then b is bilinear.

(5.2.2) The form b is alternating $\Leftrightarrow x \subset x^{\perp_b}$ for all $x \in \mathscr{P}(V)$.

(5.2.3) If the form b is nondegenerate and for all $x \in \mathscr{P}(V)$ we have $x \subset x^{\perp_b}$, then n is even and b is a nondegenerate symplectic form on V.

Given a nondegenerate symplectic form b on an n-dimensional vector space V over a field k, and given any x,y in $\mathscr{P}(V)$, we write $x \perp_b y$ or $x \not\perp_b y$ according as $b(v,w) = 0$ or $b(v,w) \neq 0$ for some (and hence all) v,w in $V \setminus \{0\}$ with $\langle v \rangle = x$ and $\langle w \rangle = y$. For any subspace U of V, by b_U we denote the restriction of b to U (i.e., to $U \times U$); we call U degenerate or nondegenerate (relative to b) according as b_U is degenerate or nondegenerate. In case of $k = GF(q)$ we have the following:

Symplectic Rank Three Property (5.3) *Let $Sp(V,b) \leq G \leq \Gamma Sp(V,b)$ where b is a nondegenerate symplectic form on an n-dimensional vector space V over $k = GF(q)$ with $n = 2m \geq 4$. Then for any $x \in \mathscr{P}(V)$, the orbits of G_x on $\mathscr{P}(V)$ are*

$$\{x\},\ \{y \in \mathscr{P}(V) \setminus \{x\} : x \perp_b y\},\ \{y \in \mathscr{P}(V) : x \not\perp_b y\},$$

and these have sizes 1, $q + q^2 + \cdots + q^{2m-2}$ and q^{2m-1} respectively.

For $G = Sp(V,b)$ this is well-known. The other cases follow by noting that the three displayed subsets of $\mathscr{P}(V)$ are clearly stabilized by $\Gamma Sp(V,b)_x$.

As a sharpening of (5.3) we have the following:

Lemma 5.3 (Symplectic Rank Three Lemma). *Let $G \leq \Gamma Sp(V,b)$ be transitive Rank 3 on $\mathscr{P}(V)$ where b is a nondegenerate symplectic form on an n-dimensional vector space V over $k = GF(q)$ with $n = 2m \geq 4$. Then we have the following.*

(5.4.1) For any $x \in \mathscr{P}(V)$, the orbits of G_x on $\mathscr{P}(V)$ are

$$\{x\},\ \{y \in \mathscr{P}(V) \setminus \{x\} : x \perp_b y\},\ \{y \in \mathscr{P}(V) : x \not\perp_b y\},$$

and these have sizes 1, $q+q^2+\cdots+q^{2m-2}$ *and* q^{2m-1} *respectively.*

(5.4.2) G is transitive on nondegenerate 2*-spaces U, and for any such space,* G_U *is* 2*-transitive on* $\mathscr{P}(U)$.

(5.4.3) G is transitive on degenerate 2*-spaces U, and for any such space,* G_U *is* 2*-transitive on* $\mathscr{P}(U)$.

(5.4.4) G is antiflag transitive.

Proof. For any $x \in \mathscr{P}(V)$, the orbits of $\Gamma Sp(V,b)_x$ on $\mathscr{P}(V)$ are unions of those of G_x, so the first part follows from (5.3). Any nondegenerate 2-space containing $x \in \mathscr{P}(V)$ is generated by x and $y \in \mathscr{P}(V)$, where $x \not\perp_b y$, but G is transitive on $\mathscr{P}(V)$, and, G_x is transitive on the set of $y \in \mathscr{P}(V)$ with $x \not\perp_b y$, so G is transitive on nondegenerate 2-spaces. Let U be a nondegenerate 2-space and let $x,y,x',y' \in \mathscr{P}(U)$ with $x \neq y$ and $x' \neq y'$. Therefore $x \not\perp_b y$ and $x' \not\perp_b y'$. Since G is transitive on $\mathscr{P}(V)$, there exists $g \in G$ taking x' to x and y' to y'', say, with $x \not\perp_b y''$. Now G_x is transitive on $\mathscr{P}(V) \setminus x^{\perp_b}$, so there exists $h \in G_x$ taking y'' to y. Therefore hg takes (x',y') to (x,y), so $hg \in G_U$ and hence G_U is 2-transitive on $\mathscr{P}(U)$, completing the proof of the second part. Any degenerate 2-space containing $x \in \mathscr{P}(V)$ is generated by x and $y \in \mathscr{P}(V)$, where $x \perp_b y$, but G is transitive on $\mathscr{P}(V)$, and, G_x is transitive on the set of $y \in \mathscr{P}(V) \setminus \{x\}$ with $x \perp_b y$, so G is transitive on degenerate 2-spaces. Let U be a degenerate 2-space and let $x,y,x',y' \in \mathscr{P}(U)$ with $x \neq y$ and $x' \neq y'$. Therefore $x \perp_b y$ and $x' \perp_b y'$. Since G is transitive on $\mathscr{P}(V)$, there exists $g \in G$ taking x' to x and y' to y'', say, with $x \perp_b y''$. Now G_x is transitive on $x^{\perp_b} \setminus \{x\}$, so there exists $h \in G_x$ taking y'' to y. Therefore hg takes (x',y') to (x,y), so $hg \in G_U$ and hence G_U is 2-transitive on $\mathscr{P}(U)$, completing the proof of the third part. Any antiflag (x,H) is of the form $(x,y^{\perp_b})$ for some $y \in \mathscr{P}(V)$ and the condition that $x \not\subset H$ is equivalent to $x \not\perp_b y$. But G_x is transitive on the set of such y and G is transitive on $\mathscr{P}(V)$, so G is transitive on antiflags. □

As a further partial sharpening of (5.3) we have the following:

Lemma 5.4 (Vectorial Rank Three Lemma). *Let* $G \leq \Gamma L(V)$ *be transitive Rank 3 on* $\mathscr{P}(V)$ *with subdegrees* 1, $q+q^2+\cdots+q^{n-2}$ *and* q^{n-1}, *where V be an n-dimensional vector space over* $k = GF(q)$ *with* $n > 2$. *Then n is even and* $G \leq \Gamma Sp(V,b)$ *for a nondegenerate symplectic form b on V.*

Proof. To see this, let Γ and Δ be the orbitals of G on $\mathscr{P}(V)$ such that for every $x \in \mathscr{P}(V)$ the sizes of $\Gamma(x)$ and $\Delta(x)$ are $q+q^2+\cdots+q^{n-2}$ and q^{n-1} respectively. By the Hyperplanarity Lemma (4.3) we see that for each $x \in \mathscr{P}(V)$ there is a unique hyperplane $H(x)$ in V such that $\mathscr{P}(H(x)) = \{x\} \cup \Gamma(x)$, and by the Supplementary Hyperplanarity Lemma (4.4) we see that $x \mapsto (H(x))^\natural$ gives a correlation ν of $\mathscr{P}(V)$. By the Correlation Lemma (5.1) and the Sesquilinearity Lemma (5.2), n is even and there exists a nondegenerate symplectic form b on V such that $H(x) = x^{\perp_b}$ for all $x \in \mathscr{P}(V)$. Given any $g \in G$, associated with

$\sigma \in Aut(k)$ define $b' : V \times V \to k$ by putting $b'(v,w) = \sigma(b(g^{-1}(v), g^{-1}(w)))$ for all v, w in V. Then b' is obviously a nondegenerate symplectic form on V such that for all $x \in \mathscr{P}(V)$ we have $\mathscr{P}(x^{\perp_{b'}}) = g(\mathscr{P}(H(g^{-1}(x))))$, and hence by the Supplementary Hyperplanarity Lemma (4.4) we get $x^{\perp_{b'}} = x^{\perp_b}$. Therefore by the Correlation Lemma (5.1) there exists $\alpha \in k^\times$ such that $b'(v,w) = \alpha b(v,w)$ for all v, w in V; i.e. $b(g^{-1}(v), g^{-1}(w)) = \sigma^{-1}(\alpha b(v,w))$. Consequently $g \in \Gamma Sp(V,b)$. □

6. Preparation for Symplectic Rank Three Theorem

In this section we shall make some preparation for proving Theorem (1.2).

Lemma 6.1. *Let g be an element of $SL(2,q)$ and let C_G and C_S be the conjugacy classes of g in $GL(2,q)$ and $SL(2,q)$, respectively. Suppose also that $C_G \neq C_S$. Then q is odd and g has a repeated eigenvalue $\varepsilon = \pm 1$ with a 1-dimensional eigenspace. Moreover C_G is the union of two $SL(2,q)$-conjugacy classes with representatives*

$$\varepsilon \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \varepsilon \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

where λ is a non-square in $GF(q)$.

Proof. Let g be an element of $\mathrm{SL}(2,q)$ and let C_G and C_S be the conjugacy classes of g in $\mathrm{GL}(2,q)$ and $\mathrm{SL}(2,q)$, respectively. Let $m(t)$ be the minimal polynomial of g over $\mathbb{F} = GF(q)$. The scalar case is trivial, therefore we shall assume that $g \neq \lambda I$ for any $\lambda \in \mathbb{F}^\times$, where I is the identity element in $\mathrm{GL}(2,q)$. When q is even, every element in $\mathbb{F}^\times$ has a square root. It follows that for any $h \in GL(2,q)$, letting $h' = \frac{1}{\sqrt{D(h)}} h$, we get $h^{-1}gh = h'^{-1}gh'$, where D is the determinant map. This shows that $C_G = C_S$ when q is even. So we shall further assume that q is odd.

First we shall show that $C_G = C_S$ when g does not have any eigenvalues in $\mathbb{F}$. So suppose that $m(t)$ is an irreducible polynomial of degree 2 and that g is equal to $\left(\begin{smallmatrix} 0 & -1 \\ 1 & \lambda \end{smallmatrix}\right)$ for some $\lambda \in \mathbb{F}$. Every element of $\mathrm{GL}(2,q)$ centralizing g, also centralizes the multiplicative group $\mathbb{F}[g]^\times$ of the field $\mathbb{F}[g]$. It follows that $C_{GL(2,q)}(g)$, the centralizer of g in $GL(2,q)$, is equal to $\mathbb{F}[g]^\times$ and therefore we have $|C_G| = |GL(2,q) : C_{GL(2,q)}(g)| = q(q-1)$.

Now consider the determinant map $D : \mathbb{F}[g]^\times \to \mathbb{F}^\times : xI + yg \mapsto x^2 + xy\lambda + y^2 = (x + (\frac{\lambda}{2})y)^2 + (1 - \frac{\lambda^2}{4})y^2$ for all $x, y \in \mathbb{F}$ satisfying $(x,y) \neq (0,0)$, where I is the identity element in $\mathrm{GL}(2,q)$. Let $\mathbb{F}^{\times 2}$ denote the subgroup $\{\alpha^2 : \alpha \in \mathbb{F}^\times\}$ of $\mathbb{F}^\times$. Then the order of $\mathbb{F}^{\times 2}$ is $(q-1)/2$, when q is odd. For any $\nu \in \mathbb{F}^\times$, the sets $\{(x + (\frac{\lambda}{2})y)^2 : x, y \in \mathbb{F}\}$ and $\{\nu - (1 - \frac{\lambda^2}{4})y^2 : y \in \mathbb{F}\}$ have order $(q+1)/2$