Oberwolfach Preprints

OWP 2009 - 07

S. De Winter, E. E. Shult and K. Thas

Singer Quadrangles

Mathematisches Forschungsinstitut Oberwolfach gGmbH
Oberwolfach Preprints (OWP) ISSN 1864-7596

Oberwolfach Preprints (OWP)

Starting in 2007, the MFO publishes a preprint series which mainly contains research results related to a longer stay in Oberwolfach. In particular, this concerns the Research in Pairs-Programme (RiP) and the Oberwolfach-Leibniz-Fellows (OWLF), but this can also include an Oberwolfach Lecture, for example.

A preprint can have a size from 1 - 200 pages, and the MFO will publish it on its website as well as by hard copy. Every RiP group or Oberwolfach-Leibniz-Fellow may receive on request 30 free hard copies (DIN A4, black and white copy) by surface mail.

Of course, the full copy right is left to the authors. The MFO only needs the right to publish it on its website *www.mfo.de* as a documentation of the research work done at the MFO, which you are accepting by sending us your file.

In case of interest, please send a **pdf file** of your preprint by email to *rip@mfo.de* or *owlf@mfo.de*, respectively. The file should be sent to the MFO within 12 months after your stay as RiP or OWLF at the MFO.

There are no requirements for the format of the preprint, except that the introduction should contain a short appreciation and that the paper size (respectively format) should be DIN A4, "letter" or "article".

On the front page of the hard copies, which contains the logo of the MFO, title and authors, we shall add a running number (20XX - XX).

We cordially invite the researchers within the RiP or OWLF programme to make use of this offer and would like to thank you in advance for your cooperation.

Imprint:

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany

Tel +49 7834 979 50
Fax +49 7834 979 55
Email admin@mfo.de
URL www.mfo.de

The Oberwolfach Preprints (OWP, ISSN 1864-7596) are published by the MFO.

Singer Quadrangles

S. De Winter, E. E. Shult and K. Thas

To Our Families

Contents

Preface

Imagine a geometry $(\mathcal{P}, \mathcal{L})$ of points and lines. It is said to admit a *Singer group* (w.r.t. points) if there is a group G of automorphisms which acts freely and transitively (= sharply transitively = regularly) on the points. That means G acts transitively on the points and no non-identity element of G fixes a point, forcing $|G| = |\mathcal{P}|$. The objective is to classify geometries of a particular type by specifying the existence of a Singer group. This project seems to be hopeless in the case that $|\mathcal{P}|$ is infinite, so, from here on, we (usually) assume that the geometries being considered possess only finitely many points. Of course that makes the group G finite, a very important fact.

Unfortunately, there exists so far just one "classical" case: that of finite projective planes. As of today the only known projective planes admitting a Singer group are Desarguesian — that is, they are defined as the geometry of 1-spaces and 2-spaces of a 3-dimensional right vector space over a division ring D. Thus such a plane admits the much larger group $\mathbf{P\Gamma L}_3(D)$, rather than just the Singer group.

Of course there is no need to test the hypothesis of a Singer group on projective spaces of higher rank since the Veblen-Young Theorem already tells us that Singer groups exist, as long as D is finite.

Where does one look next? Well first of all, our Singer geometry should not already be characterized by the axioms imposed on it. Among the spherical buildings, these would be the geometries of rank two. The reason for this, is that the connected geometries of higher rank have all been essentially classified by Tits in his famous lecture notes [32].

The rank two spherical buildings of interest are

(i) the projective planes just discussed,

(ii) the generalized quadrangles,

(iii) the generalized hexagons, and

(iv) the generalized octagons.

A finite (thick) *generalized n-gon* $\mathcal{S}$ of order (s,t), $n \geq 2$, $s > 1$, $t > 1$ (where all the parameters are finite), is a 1-$(v, s+1, t+1)$ design whose incidence graph has girth $2n$ and diameter n. The (finite) generalized 3-gons are precisely the (finite) projective planes. Recall from [11] that (i)-(ii)-(iii)-(iv) (when finite) are the only thick finite generalized polygons that actually occur!

The theory of Singer groups for projective planes has been especially popular and productive. Many questions concerning Singer groups stand among the truly fundamental ones in the theory of projective planes, the most notable being perhaps the classification of planes admitting an abelian Singer group. Conjecturally, those should always be Desarguesian. In the past 15 years, the question whether there are fruitful Singer group theories for other types of (building-like) geometries has been posed several times, especially for the other generalized n-gons.

After the finite projective planes, the next case seems to be that of the finite generalized quadrangles, the focus of our research. For generalized quadrangles (GQs), such a theory was initiated by D. Ghinelli in [13], where it was shown that a finite GQ of order s cannot admit an abelian Singer group. In [7] the first and last author further developed the theory by determining all GQs admitting an abelian Singer group. In fact, they showed that a GQ admitting an abelian Singer group G must always arise by "Payne-derivation" from a so-called translation GQ (cf. the monograph [26]) of even order s. It follows that G is necessarily elementary abelian.

So far, including the present research, there have been three approaches to a Singer group theory for GQs. In the first approach one starts with a given (type of) group and looks for all possible GQs that can admit this group as a Singer group. Two results of this type have been obtained previously by the first and last author ([7, 9]) and will be presented in detail in Chapter 5. These results basically consist of the complete structural classification of GQs that can admit an abelian group or an odd order Heisenberg group (of dimension 3) as a Singer group. Also Chapter 9 fits in this approach, and presents some first results on nilpotent groups as possible Singer groups for GQs.

The second approach aims at excluding the existence of a Singer group for GQs with specific parameters. It are the results of Ghinelli [13] — who initiated a Singer group theory for GQs (from the difference set point of view) — and Yoshiara [35] that address the theory in this context. As mentioned already above, D. Ghinelli specifically looked at GQs of order s and obtained restrictions for such GQs that admit a Singer group. The beautiful result of S. Yoshiara shows that no GQ of order (s^2, s) can admit a Singer group. In Chapter 6 these results will be treated.

Finally, the core of this report deals with the results that came out of our Research in Pairs (RiP) research project. We investigated which of the *known GQs* admits a Singer group, something that (strangely enough) had not been done before, and that turned out to be much harder than one would expect. In Chapter 7 we first reduce the problem to the classical GQs — those GQs that are associated to a classical group — by showing that no known non-classical GQ can admit a Singer group, unless it is a Payne-derived GQ. In Chapter 8 we then deal with the classical GQs. Using a mixture of projective geometry, group theory and representation theory, we prove that the only classical GQ that admits a Singer group is $\mathbf{Q}(5,2)$, which is in fact the only classical GQ that is also a Payne-derived GQ. In our proofs we do not use the classification of finite simple groups. It is not so much a matter of (not) trusting its truth as it is that one cannot teach it. A proof that utilizes the classification of finite simple groups is bound to rely on a case-by-case analysis with unique (ad hoc) arguments geared for each case. If this were not true, one would have to have at hand a fairly universal argument that handled all simple groups; if that *were* the case, one would not even *need* the classification of finite simple groups!

What we have written up in this RiP report is more than just a copy of the article that was the final result of our RiP research; we have opted to give a rather complete and self-contained overview of the theory of Singer GQs in these notes. However, when it comes to results that were obtained prior to our RiP stay, we will only give sketches of proofs, whereas rather complete proofs of our newly obtained results will be given (of course, the version presented here could eventually differ slightly from the final journal version).

ACKNOWLEDGEMENT. This research was done at the Mathematisches Forschungsinstitut Oberwolfach during a stay within the Research in Pairs Programme from April 1 to April 21, 2007.

We would like to express our gratitude towards the Mathematisches Forschungsinstitut Oberwolfach for giving us the opportunity to spend three weeks at the institute to discuss our problem(s), device a "plan de campagne" to attack it, and obtain already some of our results. At the institute it is easy to concentrate and focus on research, but when back in the "real world", all problems of daily life return. So, although the rough strategy to finish our proofs was already there after the stay, the process of filling in all the gaps and details was a time consuming one that was also delayed on several occasions by non-mathematical issues. So we are also very grateful to the MFO for its patience in waiting on this manuscript.

This RiP stay meant something special to each of the three authors. For the first author it was his first visit ever to the MFO, an institute of which he already had heard so much. The quiet and motivating environment, in the institute and the surrounding nature, left a deep impression on him. The second (and senior) author had been to Oberwolfach on various occasions in his career. Not only was this stay for him a happy return to a place where so many great mathematicians had passed and so much great mathematics was presented, it also was a great occasion to reminiscence about the people he had met and the mathematics he had been involved in. The third author already visited the institute several times as a young boy (his father being also a mathematician), and

later came back as a researcher. Although the RiP period represented a particularly difficult period in his personal life, he is grateful to have spend it in the MFO with two of his great friends, under the 2007 April sun.

This stay brought the three authors together not only as mathematicians, but also as great friends.

STEFAAN DE WINTER AND KOEN THAS
Ghent University, Department of Pure Mathematics
and Computer Algebra
Krijgslaan 281, S25, B-9000 Ghent, Belgium
sgdwinte@cage.UGent.be; kthas@cage.UGent.be

ERNIE SHULT
Kansas State University
Department of Mathematics
138 Cardwell Hall, Manhattan, KS 66506-2602
Kansas, US
ernest_shult@yahoo.com

Chapter 1

Combinatorial Preliminaries

We begin this chapter with introducing some combinatorial notions in GQ theory. We then define the stereotypes of generalized quadrangles, and introduce elation generalized quadrangles.

1.1 Generalized quadrangles

We tersely review some basic notions taken from the theory of generalized quadrangles, for the sake of convenience.

Finite Generalized Quadrangles. A (finite) *generalized quadrangle* (GQ) *of order* (s,t) is a point-line incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ in which $\mathcal{P}$ and $\mathcal{B}$ are disjoint (non-empty) sets of objects called *points* and *lines* respectively, and for which I is a symmetric point-line incidence relation satisfying the following axioms:

(i) each point is incident with $t+1$ lines ($t \geq 1$) and two distinct points are incident with at most one line;

(ii) each line is incident with $s+1$ points ($s \geq 1$) and two distinct lines are incident with at most one point;

(iii) if p is a point and L is a line not incident with p, then there is a unique point-line pair (q, M) such that $p \mathrel{\mathrm{I}} M \mathrel{\mathrm{I}} q \mathrel{\mathrm{I}} L$.

If $s = t$, then $\mathcal{S}$ is also said to be *of order* s. If $s, t > 1$, $\mathcal{S}$ is *thick*.

Suppose $p \not\mathrm{I}\ L$. Then by $\mathrm{proj}_L p$, we denote the unique point on L collinear with p. Dually, $\mathrm{proj}_p L$ is the unique line incident with p concurrent with L.

Point-Line Duality. There is a *point-line duality* for GQs of order (s, t) for which in any definition or theorem the words "point" and "line" are interchanged and also the parameters. (If $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is a GQ of order (s, t), $\mathcal{S}^D = (\mathcal{B}, \mathcal{P}, \mathrm{I})$ is a GQ of order (t, s).)

Collinearity/Concurrency/Regularity. Let p and q be (not necessarily distinct) points of the GQ $\mathcal{S}$; we write $p \sim q$ and call these points *collinear*, provided that there is some line L such that $p \mathrm{\ I\ } L \mathrm{\ I\ } q$. Dually, for $L, M \in \mathcal{B}$, we write $L \sim M$ when L and M are *concurrent*.
For $p \in \mathcal{P}$, put

$$p^\perp = \{q \in \mathcal{P} \parallel q \sim p\}$$

(and note that $p \in p^\perp$). For a pair of distinct points $\{p, q\}$, we denote $p^\perp \cap q^\perp$ also by $\{p, q\}^\perp$. Then $|\{p, q\}^\perp| = s + 1$ or $t + 1$, according as $p \sim q$ or $p \not\sim q$, respectively. For $p \neq q$, we define

$$\{p, q\}^{\perp\perp} = \{r \in \mathcal{P} \parallel r \in s^\perp \text{ for all } s \in \{p, q\}^\perp\}.$$

When $p \not\sim q$, we have that $|\{p, q\}^{\perp\perp}| = s + 1$ or $|\{p, q\}^{\perp\perp}| \leq t + 1$ according as $p \sim q$ or $p \not\sim q$, respectively. If $p \sim q$, $p \neq q$, or if $p \not\sim q$ and $|\{p, q\}^{\perp\perp}| = t + 1$, we say that the pair $\{p, q\}$ is *regular*. The point p is *regular* provided $\{p, q\}$ is regular for every $q \in \mathcal{P} \setminus \{p\}$. Regularity for lines is defined dually. One easily proves that either $s = 1$ or $t \leq s$ if $\mathcal{S}$ has a regular pair of non-collinear points; see 1.3.6 of [23].

Throughout, "FGQ" refers to "Finite Generalized Quadrangles" [23].

Theorem 1.1.1 (FGQ, 1.3.1) *Let p be a regular point of a GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ of order (s, t), $s \neq 1 \neq t$. Then the incidence structure with point set $p^\perp \setminus \{p\}$, with line set the set of spans $\{q, r\}^{\perp\perp}$, where q and r*

are non-collinear points of $p^\perp \setminus \{p\}$*, and with the natural incidence, is the dual of a net of order* s *and degree* $t+1$.
If in particular $s = t$*, there arises a dual affine plane of order* s*. (Also, in the case* $s = t$*, the incidence structure* π_p *with point set* $p^\perp$*, with line set the set of spans* $\{q, r\}^{\perp\perp}$*, where* q *and* r *are different points in* $p^\perp$*, and with the natural incidence, is a projective plane of order* s*).* ■

Automorphisms. An *automorphism* of a GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is a permutation of $\mathcal{P} \cup \mathcal{B}$ which preserves P, B and I. The set of automorphisms of a GQ $\mathcal{S}$ is a group, called the *automorphism group* of $\mathcal{S}$, which is denoted by $\mathrm{Aut}(\mathcal{S})$.
A *whorl* about a point x is just an automorphism fixing it linewise. A point x is a *center of transitivity* provided that the group of whorls about x is transitive on the points of $\mathcal{P} \setminus p^\perp$.

SubGQs. A *subquadrangle*, or also *subGQ*, $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', \mathrm{I}')$ of a GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is a GQ for which $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{B}' \subseteq \mathcal{B}$, and where I' is the restriction of I to $(\mathcal{P}' \times \mathcal{B}') \cup (\mathcal{B}' \times \mathcal{P}')$.

The following results will sometimes be used without further reference.

Theorem 1.1.2 (FGQ, 2.2.1) *Let* $\mathcal{S}'$ *be a proper subquadrangle of order* (s', t') *of the GQ* $\mathcal{S}$ *of order* (s, t)*. Then either* $s = s'$ *or* $s \geq s't'$*. If* $s = s'$*, then each external point of* $\mathcal{S}'$ *is collinear with the* $st' + 1$ *points of an ovoid of* $\mathcal{S}'$*; if* $s = s't'$*, then each external point of* $\mathcal{S}'$ *is collinear with exactly* $1 + s'$ *points of* $\mathcal{S}'$*.* ■

Theorem 1.1.3 (FGQ, 2.2.2) *Let* $\mathcal{S}'$ *be a proper subquadrangle of the GQ* $\mathcal{S}$*, where* $\mathcal{S}$ *has order* (s, t) *and* $\mathcal{S}'$ *has order* (s, t') *(so* $t > t'$*). Then we have*

(1) $t \geq s$*; if* $s = t$*, then* $t' = 1$.

(2) *If* $s > 1$*, then* $t' \leq s$*; if* $t' = s \geq 2$*, then* $t = s^2$.

(3) *If* $s = 1$*, then* $1 \leq t' < t$ *is the only restriction on* t'.

(4) *If* $s > 1$ *and* $t' > 1$*, then* $\sqrt{s} \leq t' \leq s$ *and* $s^{3/2} \leq t \leq s^2$.

(5) *If* $t = s^{3/2} > 1$ *and* $t' > 1$*, then* $t' = \sqrt{s}$*.*

(6) *Let* $\mathcal{S}'$ *have a proper subquadrangle* $\mathcal{S}''$ *of order* (s, t'')*,* $s > 1$*. Then* $t'' = 1$*,* $t' = s$ *and* $t = s^2$*.* ∎

Theorem 1.1.4 (FGQ, 2.3.1) *Let* $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', \mathrm{I}')$ *be a substructure of the GQ* $\mathcal{S}$ *of order* (s, t) *so that the following two conditions are satisfied:*

(i) *if* $x, y \in \mathcal{P}'$ *are distinct points of* $\mathcal{S}'$ *and* L *is a line of* $\mathcal{S}$ *such that* $x \mathrm{~I~} L \mathrm{~I~} y$*, then* $L \in \mathcal{B}'$*;*

(ii) *each element of* $\mathcal{B}'$ *is incident with* $s + 1$ *elements of* $\mathcal{P}'$*.*

Then there are four possibilities:

(1) $\mathcal{S}'$ *is a dual grid, so* $s = 1$*;*

(2) *the elements of* $\mathcal{B}'$ *are lines which are incident with a distinguished point of* $\mathcal{P}$*, and* $\mathcal{P}'$ *consists of those points of* $\mathcal{P}$ *which are incident with these lines;*

(3) $\mathcal{B}' = \emptyset$ *and* $\mathcal{P}'$ *is a set of pairwise non-collinear points of* $\mathcal{P}$*;*

(4) $\mathcal{S}'$ *is a subquadrangle of order* (s, t')*.* ∎

The following result is now easy to prove.

Theorem 1.1.5 (FGQ, 2.4.1) *Let* θ *be an automorphism of the GQ* $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ *of order* (s, t)*. The substructure* $\mathcal{S}_\theta = (\mathcal{P}_\theta, \mathcal{B}_\theta, \mathrm{I}_\theta)$ *of* $\mathcal{S}$ *which consists of the fixed elements of* θ *must be given by (at least) one of the following:*

(i) $\mathcal{B}_\theta = \emptyset$ *and* $\mathcal{P}_\theta$ *is a set of pairwise non-collinear points;*

(i)′ $\mathcal{P}_\theta = \emptyset$ *and* $\mathcal{B}_\theta$ *is a set of pairwise non-concurrent lines;*

(ii) $\mathcal{P}_\theta$ *contains a point* x *so that* $y \sim x$ *for each* $y \in \mathcal{P}_\theta$*, and each line of* $\mathcal{B}_\theta$ *is incident with* x*;*

(ii)$'$ *$\mathcal{B}_\theta$ contains a line L so that $M \sim L$ for each $M \in \mathcal{B}_\theta$, and each point of $\mathcal{P}_\theta$ is incident with L;*

(iii) *$\mathcal{S}_\theta$ is a grid;*

(iii)$'$ *$\mathcal{S}_\theta$ is a dual grid;*

(iv) *$\mathcal{S}_\theta$ is a subGQ of $\mathcal{S}$ of order (s', t'), $s', t' \geq 2$.* ■

Next, we recall a result on fixed elements structures of whorls.

Theorem 1.1.6 (FGQ, 8.1.1) *Let θ be a non-trivial whorl about p of the GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ of order (s, t), $s \neq 1 \neq t$. Then one of the following must hold for the fixed element structure $\mathcal{S}_\theta = (\mathcal{P}_\theta, \mathcal{B}_\theta, \mathrm{I}_\theta)$.*

(1) *$y^\theta \neq y$ for each $y \in \mathcal{P} \setminus p^\perp$.*

(2) *There is a point y, $y \not\sim p$, for which $y^\theta = y$. Put $V = \{p, y\}^\perp$ and $U = V^\perp$. Then $V \cup \{p, y\} \subseteq \mathcal{P}_\theta \subseteq V \cup U$, and $L \in \mathcal{B}_\theta$ if and only if L joins a point of V with a point of $U \cap \mathcal{P}_\theta$.*

(3) *$\mathcal{S}_\theta$ is a subGQ of order (s', t), where $2 \leq s' \leq s/t \leq t$, and hence $t < s$.* ■

Finally, we mention the following result of Benson.

Theorem 1.1.7 (Benson [2]) *Let $\mathcal{S}$ be a thick finite GQ of order (s, t), and let θ be a nonidentity automorphism of $\mathcal{S}$. Let f be the number of fixed points of θ, and g the number of points which are mapped onto a collinear but different point. Then*

$$(t+1)f + g \equiv st + 1 \mod s + t.$$

■

1.2 The classical examples and their duals

Consider a nonsingular quadric $\mathbf{Q}$ of Witt index 2, that is, of projective index 1, in $\mathbf{PG}(3,q)$, $\mathbf{PG}(4,q)$, $\mathbf{PG}(5,q)$, respectively. The points and lines of the quadric form a generalized quadrangle which is denoted by $\mathbf{Q}(3,q)$, $\mathbf{Q}(4,q)$, $\mathbf{Q}(5,q)$, respectively, and has order $(q,1)$, (q,q), (q,q^2), respectively. As $\mathbf{Q}(3,q)$ is a grid, its structure is trivial.

Recall that $\mathbf{Q}$ has the following canonical form:

(1) $X_0X_1 + X_2X_3 = 0$ if $d = 3$;

(2) $X_0^2 + X_1X_2 + X_3X_4 = 0$ if $d = 4$;

(3) $f(X_0, X_1) + X_2X_3 + X_4X_5 = 0$ if $d = 5$, where f is an irreducible binary quadratic form.

Next, let $\mathbf{H}$ be a nonsingular Hermitian variety in $\mathbf{PG}(3,q^2)$, respectively $\mathbf{PG}(4,q^2)$. The points and lines of $\mathbf{H}$ form a generalized quadrangle $\mathbf{H}(3,q^2)$, respectively $\mathbf{H}(4,q^2)$, which has order (q^2,q), respectively (q^2,q^3).

The variety $\mathbf{H}$ has the following canonical form:

$$X_0^{q+1} + X_1^{q+1} + \cdots + X_d^{q+1} = 0.$$

The points of $\mathbf{PG}(3,q)$ together with the totally isotropic lines with respect to a symplectic polarity, form a GQ $\mathbf{W}(q)$ (or $\mathbf{W}(3,q)$) of order q.

A symplectic polarity Θ of $\mathbf{PG}(3,q)$ has the following canonical form:

$$X_0Y_3 + X_1Y_2 - X_2Y_1 - X_3Y_0.$$

The generalized quadrangles defined in this section are the "classical generalized quadrangles". Their point-line duals are called the *dual classical generalized quadrangles*. It was Jacques Tits who first identified them as generalized quadrangles.

The following result will be very important in this text.

Theorem 1.2.1 (FGQ, 3.2.1, 3.2.2 and 3.2.3) (i) $\mathbf{Q}(4,q) \cong \mathbf{W}(q)^D$;

(ii) $\mathbf{Q}(4,q) \cong \mathbf{W}(q)$ *if and only if* q *is even;*

(iii) $\mathbf{Q}(5,q) \cong \mathbf{H}(3,q^2)^D$. ■

1.3 Elation and translation quadrangles

It appears that all finite classical GQs and their point-line duals have, for each point, an automorphism group that fixes it linewise and has a sharply transitive action on the points which are non-collinear with that point.

For a general "abstract" GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$, we call a point $x \in \mathcal{S}$ with this property an *elation point*, and a group H that fixes x linewise and acts sharply transitively on $\mathcal{P} \setminus x^{\perp}$ is an *elation group*. If a GQ has an elation point, it is called an *elation generalized quadrangle* or, shortly, "EGQ". We frequently will use the notation $(\mathcal{S}^x, H)$ to indicate that x is an elation point with associated elation group H. Sometimes we also write $\mathcal{S}^x$ if we don't want to specify the elation group. If H is abelian, we call $\mathcal{S}^x$ a *translation generalized quadrangle* (TGQ) with *translation point* x and *translation group* H.

1.4 Kantor families

Suppose $(\mathcal{S}^p, G) = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is an EGQ of order (s,t), $s \neq 1 \neq t$, with elation point p and elation group G, and let q be a point of $\mathcal{P} \setminus p^{\perp}$. Let $L_0, L_1, \ldots, L_t$ be the lines incident with p, and define r_i and M_i by $L_i \,\mathrm{I}\, r_i \,\mathrm{I}\, M_i \,\mathrm{I}\, q$, $0 \leq i \leq t$. Put

$$H_i = \{\theta \in G \parallel M_i^{\theta} = M_i\}$$

and

$$H_i^* = \{\theta \in G \parallel r_i^{\theta} = r_i\},$$

and $\mathcal{J} = \{H_i \parallel 0 \leq i \leq t\}$. Then $|G| = s^2 t$ and $\mathcal{J}$ is a set of $t+1$ subgroups of G, each of order s. Also, for each i, H_i^* is a subgroup of G

of order st containing H_i as a subgroup. Moreover, the following two conditions are satisfied:

(K1) $H_iH_j \cap H_k = \{\mathbf{1}\}$ for distinct i, j and k;

(K2) $H_i^* \cap H_j = \{\mathbf{1}\}$ for distinct i and j.

Conversely, if G is a group of order s^2t and $\mathcal{J}$ (respectively $\mathcal{J}^*$) is a set of $t+1$ subgroups H_i (respectively H_i^*) of G of order s (respectively of order st), and if the Conditions (K1) and (K2) are satisfied, then the H_i^* are uniquely defined by the H_i (H_i^* is sometimes called the *tangent space* at H_i), and $(\mathcal{J}, \mathcal{J}^*)$ is said to be a *Kantor family* or 4-*gonal family* of Type (s, t) in G. Sometimes we will also say that $\mathcal{J}$ is a (Kantor, 4-gonal) family of Type (s, t) *in* G.

Let $(\mathcal{J}, \mathcal{J}^*)$ be a Kantor family of Type (s, t) in the group G of order s^2t, $s \neq 1 \neq t$. Define an incidence structure $\mathcal{S}(G, \mathcal{J})$ as follows.

- POINTS of $\mathcal{S}(G, \mathcal{J})$ are of three kinds:
  - (i) elements of G;
  - (ii) right cosets H_i^*g, $g \in G$, $i \in \{0, 1, \ldots, t\}$;
  - (iii) a symbol (∞).
- LINES are of two kinds:
  - (a) right cosets H_ig, $g \in G$, $i \in \{0, 1, \ldots, t\}$;
  - (b) symbols $[H_i]$, $i \in \{0, 1, \ldots, t\}$.
- INCIDENCE. A point g of Type (i) is incident with each line H_ig, $0 \leq i \leq t$. A point H_i^*g of Type (ii) is incident with $[H_i]$ and with each line H_ih contained in H_i^*g. The point (∞) is incident with each line $[H_i]$ of Type (b). There are no further incidences.

It is straightforward to check that the incidence structure $\mathcal{S}(G, \mathcal{J})$ is a GQ of order (s, t). Moreover, if we start with an EGQ $(\mathcal{S}^p, G)$ to obtain the family $\mathcal{J}$ as above, then we have that

$$(\mathcal{S}^p, G) \cong \mathcal{S}(G, \mathcal{J}).$$

We thus have:

Theorem 1.4.1 *A group of order s^2t admitting a 4-gonal family is an elation group for a suitable elation generalized quadrangle.* ■

This result was first noted by W. M. Kantor [16].

1.5 Generalized ovoids

Suppose $H = \mathbf{PG}(2n + m - 1, q)$ is the finite projective $(2n + m - 1)$-space over $\mathbb{F}_q$, and let H be embedded in a $\mathbf{PG}(2n+m, q)$, say H'. Now define a set $\mathcal{O} = \mathcal{O}(n, m, q)$ of subspaces as follows: $\mathcal{O}$ is a set of $q^m + 1$ $(n - 1)$-dimensional subspaces of H, denoted $\mathbf{PG}(n - 1, q)^{(i)}$, so that

(i) every three generate a $\mathbf{PG}(3n - 1, q)$;

(ii) for every $i = 0, 1, \ldots, q^m$, there is a subspace $\mathbf{PG}(n + m - 1, q)^{(i)}$ of H of dimension $n + m - 1$, which contains $\mathbf{PG}(n - 1, q)^{(i)}$ and which is disjoint from any $\mathbf{PG}(n - 1, q)^{(j)}$ if $j \neq i$.

If $\mathcal{O}$ satisfies these conditions for $n = m$, then $\mathcal{O}$ is called a *pseudo-oval* or a *generalized oval* or an $[n - 1]$-*oval* of $\mathbf{PG}(3n - 1, q)$. A $[0]$-oval of $\mathbf{PG}(2, q)$ is an *oval* of $\mathbf{PG}(2, q)$. For $n \neq m$, $\mathcal{O}(n, m, q)$ is called a *pseudo-ovoid* or a *generalized ovoid* or an $[n - 1]$-*ovoid* or an *egg* of $\mathbf{PG}(2n + m - 1, q)$. A $[0]$-ovoid of $\mathbf{PG}(3, q)$ is an *ovoid* of $\mathbf{PG}(3, q)$.

Then S. E. Payne and J. A. Thas prove in [24, 23] that from any $\mathcal{O} = \mathcal{O}(n, m, q)$ there arises a GQ $\mathbf{T}(n, m, q) = \mathbf{T}(\mathcal{O})$ which is a TGQ of order (q^n, q^m) for some special point (∞). This goes as follows.

- The POINTS are of three types.
  (1) A symbol (∞).
  (2) The subspaces $\mathbf{PG}(n + m, q)$ of H' which intersect H in a $\mathbf{PG}(n + m - 1, q)^{(i)}$.
  (3) The points of $H' \setminus H$.
- The LINES are of two types.

(a) The elements of $\mathcal{O}(n, m, q)$.

(b) The subspaces $\mathbf{PG}(n, q)$ of $\mathbf{PG}(2n + m, q)$ which intersect H in an element of the egg.

- INCIDENCE is defined as follows: the point (∞) is incident with all the lines of Type (a) and with no other lines; a point of Type (2) is incident with the unique line of Type (a) contained in it and with all the lines of Type (b) which it contains (as subspaces); finally, a point of Type (3) is incident with the lines of Type (b) that contain it.

Conversely, any TGQ can be seen as a $\mathbf{T}(n, m, q)$ associated to an egg $\mathcal{O}(n, m, q)$ in $\mathbf{PG}(2n + m - 1, q)$ [26].

It is clear that $\mathbf{T}(1, 1, q)$ is a $\mathbf{T}_2(\mathcal{O})$ of Tits, and that $\mathbf{T}(1, 2, q)$ is a $\mathbf{T}_3(\mathcal{O})$ of Tits.

1.6 Payne-derived quadrangles and further notation

In a GQ $\mathbf{Q}$ of order (s, t) a point p is said to be a *center of symmetry* if there exists a group G of size t of automorphisms of $\mathbf{Q}$ fixing all points of $p^\perp$ and acting freely on the points not collinear with p. Each center of symmetry is a regular point. The following beautiful construction of GQs is due to S. E. Payne [19]. Let $\mathbf{Q}$ be a GQ of order s with a regular point p. Define a point-line incidence geometry $\mathcal{P} = \mathcal{P}(\mathbf{Q}, p)$ as follows.

- The POINTS of $\mathcal{P}$ are the points of $\mathbf{Q}$ not collinear with p.
- The LINES of $\mathcal{P}$ are the lines of $\mathbf{Q}$ not through p together with all sets $\{p, r\}^{\perp\perp} \setminus \{p\}$, where $p \not\sim r$.

We have the following theorem.

Theorem 1.6.1 (Payne [19]) *The point-line geometry $\mathcal{P}$ is a GQ of order $(s - 1, s + 1)$.*

Proof. Is left as an exercise to the reader. ■

The GQ $\mathcal{P}$ is the so-called *Payne-derived GQ* of $\mathbf{Q}$ (with respect to p).

A *spread of symmetry* T of a GQ $\mathbf{Q}$ is a partition T of the point set of $\mathbf{Q}$ into lines, for which there is an automorphism group of $\mathbf{Q}$ (called the "associated group") fixing T linewise and acting sharply transitively on the points of any of its lines. (Note that "any" implies "every".)

The following theorem allows one to reverse the construction of S. E. Payne.

Theorem 1.6.2 (De Soete and J. A. Thas [6]) *Let $\mathcal{P}$ be a GQ of order $(s-1, s+1)$ with a spread of symmetry T. Then $\mathcal{P}$ can be obtained by Payne derivation from a GQ of order s with a center of symmetry.*

Proof. Exercise. ■

An EGQ $(\mathbf{Q}^x, G)$ is called *skew translation GQ (STGQ)* provided the point x is a center of symmetry and all symmetries about x are in G.

Chapter 2

Group Theoretical Background

We introduce some notation and aspects of finite group theory needed for this book.

2.1 General background

If x and y are elements of a group, the element $[x, y] := x^{-1}y^{-1}xy$ is called the *commutator* of x and y. Since $xy = yx[x, y]$, the commutator measures how far x and y are from commuting. If A and B are subgroups of a group G, the symbol $[A, B]$ denotes the subgroup generated by the set $\{[a, b] \parallel (a, b) \in A \times B\}$. It is a convention to write $[A, B, C]$ for the subgroup $[A, [B, C]]$, for any subgroups A, B and C of G.

A subgroup N of G is *normal* in G if and only if $[G, N] \leq N$. In this case each right coset of N is also a left coset of N, so $Ng = gN$ for all elements $g \in G$. Thus the cosets themselves form a so-called *factor group* G/N under the group operation — that is, $NgNh = Ngh$; moreover the mapping $g \mapsto Ng$ defines a surjective group homomorphism $G \to G/N$ of G onto this factor group G/N.

The bijective homomorphisms $G \to G$ are called *automorphisms* of G. These can be composed to form the *automorphism group* of G, denoted by Aut(G). Any subgroup A of G that is invariant under all the automorphisms of G is said to be *characteristic* in G, and this condition is written A char G.

If A and B are subgroups of G, and $\sigma \in$ Aut(G), our definition of automorphism implies

$$[A, B]^\sigma = [A^\sigma, B^\sigma].$$

It follows that the members of the following two descending chains are all characteristic subgroups of G:

(*The lower central series*)

$$G^{(0)} := G \geq G^{(1)} \geq G^{(2)} \geq \cdots$$

where $G^{(n+1)} := [G, G^{(n)}]$ for all natural numbers n.

(*The derived series*)

$$\Gamma^0(G) := G \geq \Gamma^1(G) \geq \Gamma^2(G) \geq \cdots$$

where $\Gamma^{n+1}(G) := [\Gamma^n(G), \Gamma^n(G)]$ for all natural numbers n.

The second member of each series is $G^{(1)} = \Gamma^1(G) = [G, G]$, the *commutator subgroup* of G. If this subgroup is the identity subgroup, then all elements of G obey the commutative law, and G is said to be *abelian*. More generally, if the lower central series terminates at the identity subgroup in a finite number of steps — say $G^{(k)} = \{\mathbf{1}\}$ and either $k = 0$ or $G^{(k-1)} \neq \{\mathbf{1}\}$ — we say that G is *nilpotent of class* k, or simply *nilpotent* if the integer k is not specified.

We say G is *solvable* if and only if the derived series reaches the identity subgroup in a finite number of steps.

The *center* of a group G is the set

$$Z(G) := \{g \in G \parallel [g, G] = \{\mathbf{1}\}\}$$

consisting of those elements which commute with all elements of the group. This is clearly a characteristic subgroup. The interesting thing is that any non-identity nilpotent group possesses a non-trivial center.

Suppose $\{A_i \parallel i = 1, \ldots, n\}$ is a collection of groups, and let $Z_i = Z(A_i)$ be the center of A_i. The direct product of this collection of groups is the group $\Sigma A_i := A_1 \times \cdots \times A_n$ whose elements are those of the indicated Cartesian product and whose binary operation is performed coordinatewise. Its center is then

$$Z(A_1 \times \cdots \times A_n) = Z_1 \times \cdots \times Z_n.$$

A *central product* of the groups $A_1, \ldots, A_n$ is any group of the form

$$(A_1 \times \cdots \times A_n)/Z_0$$

where Z_0 is any subgroup of the center $Z_1 \times \cdots \times Z_n$ and is denoted by the symbol $A_1 * \cdots * A_n$. Note that unlike the direct product, the central product only loosely specifies the group since its actual isomorphism type depends upon the choice of the kernel, Z_0, in the center. (Roughly speaking, the central product is simply the direct product with some products of elements of the Z_i being identified with one another.)

A group G is *perfect* if and only if $G = [G, G]$ — or, equivalently, it has no non-trivial abelian factor groups. A group G is *simple* if and only if its identity subgroup is the only proper normal subgroup of G. (Note that this definition does not allow the group of order 1 to be a simple group.) A group is *quasisimple* if and only if these two conditions hold:

(1) G is perfect,

(2) $G/Z(G)$ is a simple group.

For example, the special linear groups $\mathbf{SL}_2(q)$, q an odd prime power greater than 3, are all quasisimple groups with a center of order 2.

Similarly, we say that G is *semi-quasisimple* if and only if

(1) G is perfect,

(2') $G/Z(G)$ is a direct product of simple groups.

Suppose now that A and B are normal subgroups of a group G. Then $AB = \{ab \parallel a \in A, b \in B\}$ is also a normal subgroup of G. (If $A \cap B = \{\mathbf{1}\}$, the identity group, then AB is isomorphic to the direct product $A \times B$.) In any case, we say that AB is a *normal product* of A and B, even though the term does not precisely identify the isomorphism class of the group — one needs to know G for that.

Occasionally one encounters classes of groups — such as nilpotent or semi-quasisimple groups — which are closed under taking normal products. Thus, if the poset of normal subgroups of G which belong to such a class possesses the *ascending chain condition* (ACC), then G possesses a unique (necessarily characteristic) maximal normal subgroup of this class. In the case of the nilpotent groups, this maximal element is called the *Fitting subgroup* of G, and is denoted $\mathbf{F}(G)$. In the case of normal semi-quasisimple subgroups of G, the unique maximal poset element is denoted $\mathbf{E}(G)$. Recall that $\mathbf{E}(G)$ must have the form of a central product $X_1 * \cdots * X_n$ where the X_i are quasisimple normal subgroups of $\mathbf{E}(G)$ (they might not be normal in G). Then $\mathbf{E}(G)$ is a perfect group which, modulo its center, is a direct product of the simple groups $X_i/Z(X_i)$.

2.2 Special results from finite groups

The arguments in this book utilize a number of results from finite group theory. We assume the reader is familiar with Sylow's theorem. If H is a subgroup of G, two subgroups are determined: first of all the *centralizer* of H in G, which is the subgroup $C_G(H)$ consisting of all elements of G which commute with all elements of H. The second is the *normalizer* of H in G consisting of all elements $g \in G$, for which $g^{-1}Hg = H$. This subgroup is denoted by the symbol $N_G(H)$.

Theorem 2.2.1 (Burnside Transfer Theorem) *Let G be a finite group with an abelian p-Sylow subgroup A. Then there is a surjective morphism*

$$G \to A/[N_G(A), A].$$

In particular, if $[N_G(A), A]$ is a proper subgroup of A, then G cannot be a simple group, unless A is cyclic of prime order. ■

The Burnside Fusion Theorem says that any two elements of the abelian p-Sylow subgroup A which are conjugate in G are in fact conjugate in the normalizer of A, forcing $[N_G(A), A]$ to be the "focal subgroup" of A, as introduced by Don Higman. (There is always a surjective morphism of G onto the factor of A by its focal subgroup, even when the p-Sylow subgroup A is not abelian.)

The following theorem is used so repeatedly that it is not always explicitly referred to.

Theorem 2.2.2 *Suppose G is a group of linear transformations of a finite vector space V, and suppose A is an abelian subgroup of G which acts irreducibly on V (that is, it stabilizes no proper non-zero subspace of V). Then the centralizer $C_G(A)$ is a cyclic group.* ■

(For a proof, we refer to [10].)

Finally we must invoke the following theorem of Gorenstein and Walter [14].

Theorem 2.2.3 (Gorenstein and Walter [14]) *Suppose G is a simple finite group whose 2-Sylow subgroups are dihedral (this notion is intended to include the "Klein four group" as a special case). Then G is isomorphic to one of the following:*

(i) $\mathbf{PSL}_2(q)$, *where $q = 4$ or q is an odd prime power;*

(ii) $\mathbf{A}_7$, *the alternating group on seven letters.* ■

Recall that $\mathbf{PSL}_2(4) \cong \mathbf{PSL}_2(5)$.

Chapter 3

Preparatory Results

In this chapter, we first introduce a property and prove some necessary lemmas for what is to come. Some auxiliary results on irreducible group modules and arithmetical properties are obtained.

3.1 Condition (C)

We introduce "Condition (C)" as follows: Let $\mathbf{Q}$ be GQ and let α be any automorphism of $\mathbf{Q}$ that acts fixed point freely. We say that α satisfies (C) if

(C) There is at least one point x such that $x^\alpha \sim x$.

Although (C) could appear to be very restrictive, the following observation shows that a general assumption on the parameters of a GQ is already sufficient to have (C) *for any automorphism without fixed points*. We say that a GQ $\mathbf{Q}$ satisfies (C) if every automorphism of $\mathbf{Q}$ that acts fixed point freely satisfies (C).

Lemma 3.1.1 *Let β be a non-trivial automorphism of a thick GQ $\mathbf{Q}$ of order (s,t) for which $s+t$ does not divide $st+1$. If β acts fixed point freely, then β satisfies (C).*

Proof. Let β be as above. Suppose that no point of **Q** is mapped onto a point collinear with it. Then applying Benson's theorem (Theorem 1.1.7), we obtain

$$st + 1 \equiv 0 \mod s + t. \quad (*)$$

■

If (s,t) is the order of a known GQ, then $t \in \{\sqrt{s}, s^{2/3}, s, s-2, s+2, s^{3/2}, s^2\}$ [27, Chapter 2]. So then (*) is only satisfied when $t = s \pm 2$ and t is odd.

Suppose that a GQ **Q** admits a Singer group G on the points which is transitive on the line set, and let the order of **Q** be (s,t). Suppose (C) is not satisfied (for the elements of G), so that $s+t$ divides $st+1$ and hence $s+t$ divides t^2-1. Since G acts transitively on the lines, we have

$$t + 1 \text{ divides } s + 1.$$

So $s+t$ divides $(t-1)(s+1)$ and then $s+t$ divides $s+2-t$ leads us to $t = s+2$, a contradiction.

Lemma 3.1.2 *If (C) does not hold for a Singer quadrangle $(\mathbf{Q}, G)$, then G cannot act transitively on lines.* ■

We also have

Lemma 3.1.3 *Let α and β be central elements of a Singer group G acting on a quadrangle.*

- *If α satisfies (C), then $x \sim x^\alpha$ for all points x.*
- *If α, β and $\alpha\beta$ all satisfy Condition (C), the group $\langle \alpha, \beta \rangle$ stabilizes a spread linewise.*
- *If **Q** satisfies Condition (C), $Z(G)$ stabilizes a spread linewise.* ■

3.2 Properties of the center

Let G be a Singer group of a GQ $\mathbf{Q}$ of order (s,t). Suppose that Condition (C) is satisfied.

We now specialize and consider elements of $Z(G)$.

Take $\alpha \in Z(G)^\times$. One easily deduces that $x^\alpha \sim x$ for all points x of $\mathbf{Q}$. Choose a point x and put $L = xx^\alpha$. Let y be a point incident with L and different from x, x^α. Furthermore, let $\beta \in G$ be the element that maps x onto y. Then we have

$$x \sim x^\beta \Longrightarrow x^\alpha \sim x^{\beta\alpha} = x^{\alpha\beta}; x \sim x^\alpha \Longrightarrow x^\beta \sim x^{\alpha\beta}.$$

Hence $x, x^\alpha, x^\beta, x^{\alpha\beta}$ are all on the same line, and $\{x, x^\beta\}^\alpha = \{x^\alpha, x^{\alpha\beta}\}$ implies that L is fixed by α. Since G acts transitively on the point set of $\mathbf{Q}$, one concludes that each point is incident with a unique line that is fixed by α, that is, α fixes a spread $T(\alpha)$ linewise.

Suppose $\alpha' \in Z(G)^\times$ for which $T(\alpha') \neq T(\alpha)$. Then there exists a line $M \in T(\alpha)$ such that each point of M is incident with a line of $T(\alpha')$ different from M. Take any point $z \mathrel{\mathrm{I}} M$. Then $z \sim z^\alpha \mathrel{\mathrm{I}} M$, $z^\alpha \sim z^{\alpha\alpha'} \not\mathrel{\mathrm{I}} M$, so that $z \not\sim z^{\alpha\alpha'}$. On the other hand, $\alpha\alpha' \in Z(G)$, while each element of $Z(G)$ maps a point onto a collinear point, contradiction. So $T(\alpha) = T(\alpha')$ and hence each element of $Z(G)$ fixes $T(\alpha)$ line wise. As G acts fixed point freely we obtain that $|Z(G)| \leq s+1$.

We just proved the following lemma.

Lemma 3.2.1 *Let G be a Singer group of a GQ $\mathbf{Q}$ of order (s,t) satisfying Condition (C). Then*

- $|Z(G)| \leq s+1$.
- *If $Z(G)$ is not trivial, then $Z(G)$ fixes a spread linewise.* ■

3.3 A theorem from projective geometry

If a GQ has an even number of points, each Singer group of it must contain involutions, whence the following theorem — due to Wagner [34] — that classifies involutions in projective space will turn out to be very useful.

Theorem 3.3.1 (Wagner [34]) *Let ι be an involution of a projective space $\mathbf{PG}(k,q)$ of dimension $k \geq 2$, and let $\mathcal{F}$ be the set of all fixed points of ι. Then one of the following must occur:*

- *$\mathcal{F}$ consists of the points of two disjoint subspaces of dimension d_1 and d_2 respectively, such that $d_1 + d_2 = k - 1$. In this case q is odd.*
- *$\mathcal{F}$ consists of the points of a subspace of dimension at least $(k-1)/2$. In this case q is even.*
- *$\mathcal{F}$ is the point set of a Baer subspace $\mathbf{PG}(k, \sqrt{q})$. We call ι a* Baer involution*.*
- *$\mathcal{F}$ is empty. In this case k is odd.* ■

We will exploit this classification to prove that for odd q the GQs $\mathbf{Q}(4,q)$, $\mathbf{H}(4,q^2)$ and $\mathbf{H}(4,q^2)^D$ do not admit a Singer group.

3.4 Irreducible group modules, and arithmetic

The following theorem on representation theory, due to Clifford [4] (see also Curtis and Reiner [5]) will also appear to be useful.

Theorem 3.4.1 (Clifford [4]) *Let K be an arbitrary field, and let N be a normal subgroup of a finite group G. Suppose V is an irreducible KG-module. Then the KN-module V is isomorphic to the direct sum of KN-homogeneous components. Furthermore these homogeneous components are permuted transitively by G.* ■

The next lemma will turn out to be a key result for Chapter 8.

Lemma 3.4.2 *Suppose V is a faithful irreducible $G\mathbb{F}_q$-module, where G is a group of order prime to the characteristic of $\mathbb{F}_q$. We suppose G to have the form RN where R is a cyclic group of odd prime order r and N is an r'-group which is minimal with respect to being normalized but not centralized by R. Then R does not act irreducibly on V unless $r - 1 = \dim(V) = p^a$ and N is extra-special of order p^{2a+1}, for some prime p.*

Proof. We assume R acts irreducibly on V. We must show $r - 1 = p^a = \dim(V)$ and the conclusion about N. From the fact that r does not divide $|N|$, we see that R normalizes a p-Sylow subgroup N_p for each prime p dividing the order of N. If R centralized all these we should have that $|C_N(R)| = |N|$, where $C_N(R)$ is the biggest subgroup of N centralized by R, contradicting the fact that R does not centralize N. By the minimality of N we can conclude that N is a p-group, and that either N is an elementary p-group or that N is an extra-special group of order p^{2a+1} (N is special but its center is homogeneously represented on V, and so is cyclic). In either case, R acts irreducibly on the Frattini factor group $\overline{N}$ of N. In the first case RN is a Frobenius group, and R has copies of its regular representation on V, and so is not irreducible. In the latter case, V is a homogeneous N-module, with irreducible modules of dimension p^a. Also, because of the irreducible action of R on $\overline{N}$, r divides $p^{2a} - 1$, but does not divide $p^a - 1$ (since otherwise it would not act irreducibly on V). Hence r divides $p^a + 1$. Now $\dim(V) = mp^a$. If $m > 1$, we have $\dim(V) > r$, and so V is the sum of at least two R-modules, contradicting the irreducibility of R on V. Thus, $m = 1$ and $\dim(V) = p^a$. Since $\dim(V) < r$ by the irreducibility of R on V, and $r \leq p^a + 1$, we obtain $r = p^a + 1$. ■

We will use the following theorem of Zsigmondy to introduce the concept of a "Z-prime".

Theorem 3.4.3 (Zsigmondy [36]) *If $a > b > 0$ are coprime integers, then for any natural $n > 1$ there is a prime number p that divides $a^n - b^n$ and does not divide $a^k - b^k$ for any $k < n$, with the following two exceptions:*

- $(a, b, n) = (2, 1, 6)$*, and*
- $a + b$ *is a power of* 2 *while* $n = 2$. ■

A *Z-prime* for $q^n - 1$, q a prime power, $n \geq 1$, is a prime p such that p divides $q^n - 1$, but divides no $q^k - 1$ for $k < n$. By Zsigmondy's theorem we know that such a prime always exists, except when $(q, n) = (2, 6)$ or when $n = 2$ and $1 + q$ is a power of 2. If p is a Z-prime for $q^n - 1$ and G is a subgroup of $\mathbf{PGL}_n(q)$ of order p, then G will act irreducibly on $V(n, q)$. More generally if p is a Z-prime for $q^k - 1$ and G a subgroup of

$\mathbf{PGL}_n(q)$, $k \leq n$, of order p, acting freely on projective points, then G will act on $V(n,q)$ with irreducible modules of dimension a multiple of k. This observation will play a crucial role in what follows.

We conclude this section with three lemmas that will be used frequently throughout the book.

Lemma 3.4.4 *Let r be an odd prime dividing $1+p^{kr^a}$, with p, a and k natural numbers such that $(r,k)=1$, then r^{a+1} divides $1+p^{kr^a}$.*

Proof. Clearly $p^k \equiv -1 \pmod{r}$, and so $p^k = -1 + t_0 r$, with t_0 a natural number. It follows that $(p^k)^{r^a} = -1 + t_a r^{a+1}$, with t_a a natural number. Hence r^{a+1} divides $1 + p^{kr^a} = t_a r^{a+1}$. ■

Corollary 3.4.5 *Let r, p, k and a be as in the previous lemma. Suppose G is a group with order divisible by $1+p^{kr^a}$. If H is a subgroup of G whose index in G divides kr^a, then H contains an element of order r.* ■

Lemma 3.4.6 *Let q be a prime power. Suppose $e(u)$ is the highest power of the prime u such that $u^{e(u)}$ divides $q+1$. We suppose that $u^{e(u)} \neq 2$ and that $q^d \equiv 1 \pmod{u^{e(u)+m}}$ for some integer m such that $1 \leq m \leq e(u)$. Then u^m divides d.*

Proof. By hypothesis, $q = ku^{e(u)} - 1$ for some integer k relatively prime to u. Since $q \equiv -1 \pmod{u^{e(u)}}$ and $q^d \equiv 1 \pmod{u^{e(u)}}$, we see that d is even. Then the binomial expansion yields

$$\begin{aligned} q^d &= (-1 + ku^{e(u)})^d \\ &= 1 - d(ku^{e(u)}) + (d(d-1)/2)(ku^{e(u)})^2 + \dots \\ &= 1 - d(ku^{e(u)}) + N \cdot u^{2e(u)}, \end{aligned}$$

for some integer N. But as $q^d - 1$ is divisible by $u^{e(u)+m}$ and $e(u) + m \leq 2e(u)$, we see that $u^{e(u)+m}$ must divide $dku^{e(u)}$. But as k is prime to u, u^m must divide d. The proof is complete. ■

Corollary 3.4.7 *Let q be a prime power. Suppose x is a linear transformation of an $\mathbb{F}_q$-vector space W, such that x is of prime power order $u^{e(u)+m}$, where $e(u)$ is the highest power of the prime u dividing $q+1$, and $1 \leq m \leq e(u)$. We suppose $u^{e(u)} \neq 2$ so $u^{e(u)}$ does not divide $q-1$. Then any irreducible faithful $\mathbb{F}_q\langle x\rangle$-module V has dimension divisible by $2u^m$.*
■

Lemma 3.4.8 *If $q > 2$ then there exists a prime $r \neq 3$ dividing $q^2 - q + 1$.*

Proof. Suppose 3 would be the only prime dividing $q^2 - q + 1$. Then $q^2 - q + 1 = 3^a$. Clearly 3 cannot divide $q - 1$ or q, and so must divide $q + 1$. Hence $q \equiv 2, 5$ or $8 \pmod 9$, and consequently $q^2 - q + 1 \equiv 3 \pmod 9$. If $a > 1$ this yields a contradiction. Hence $a = 1$, implying $q = 2$, a contradiction. ■

Chapter 4

The known GQs with a Singer group

In this chapter we will discuss the known GQs that admit a Singer group, as well as the Singer groups that arise from them.

4.1 The fundamental theorem for Singer quadrangles

There is in fact only one class of GQs with a Singer group known. We describe them in the following theorem.

Theorem 4.1.1 *Let* $\mathbf{Q}$ *be a thick GQ of order* s *with a regular point* r. *Suppose that there is a group* $G \leq \mathrm{Aut}(\mathbf{Q})$ *of order* s^3 *fixing* r *and acting sharply transitively on the points of* $\mathbf{Q}$ *not collinear with* r. *Then* $\mathcal{P} := \mathcal{P}(\mathbf{Q}, r)$, *that is, the Payne-derivative of* $\mathbf{Q}$ *with respect to* r, *is a GQ admitting a Singer group* $H \cong G$.

Proof. It is clear that G induces an automorphism group $H \cong G$ of $\mathcal{P}$ acting sharply transitively on its points. ■

We will now have a closer look at the GQs which satisfy the conditions of Theorem 4.1.1.

4.2 Translation quadrangles

A first possibility occurs when the GQ $\mathbf{Q}$ is a TGQ of order s with regular translation point r. In fact the translation point r is regular if and only if s is even [26, Theorem 2.1.5]. Hence the Payne-derivatives of these GQs are in one-to-one correspondence with generalized hyperovals [26] $\overline{\mathcal{O}(n,n,q)}$ in $\mathbf{PG}(3n-1,q)$. In this case the GQ $\mathcal{P}(\mathbf{Q},r)$ will have an elementary abelian Singer 2-group. In the next chapter we will prove that the converse is also true, that is, if a GQ admits an abelian Singer group, then it necessarily arises in the way just described.

4.3 EGQs with a regular point

The second class of known GQs satisfying the conditions of Theorem 4.1.1 are the EGQs of order s with a regular point r. If s is even, all known EGQs of order s are TGQs, and hence are described above. If s is odd, the only known example of an EGQ of order s is the classical GQ $\mathbf{W}(q)$, $q = s$ odd. We will discuss this case in more detail, but first we introduce Heisenberg groups.

The *(general) Heisenberg group* $\mathbf{H}_n$ of dimension $2n+1$ over $\mathbb{F}_q$, with n a natural number, is the group of square $(n+2)\times(n+2)$-matrices with entries in $\mathbb{F}_q$, of the following form (and with the usual matrix multiplication):

$$\begin{pmatrix} 1 & \alpha & c \\ 0 & \mathbb{I}_n & \beta^T \\ 0 & 0 & 1 \end{pmatrix},$$

where $\alpha,\beta \in \mathbb{F}_q^n$, $c \in \mathbb{F}_q$ and with $\mathbb{I}_n$ being the $n\times n$-unit matrix. Let $\alpha,\alpha',\beta,\beta' \in \mathbb{F}_q^n$ and $c,c' \in \mathbb{F}_q$; then

$$\begin{pmatrix} 1 & \alpha & c \\ 0 & \mathbb{I}_n & \beta^T \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & \alpha' & c' \\ 0 & \mathbb{I}_n & \beta'^T \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha+\alpha' & c+c'+\langle\alpha,\beta'\rangle \\ 0 & \mathbb{I}_n & \beta+\beta' \\ 0 & 0 & 1 \end{pmatrix}.$$

Here $\langle x, y\rangle$, with $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ elements of $\mathbb{F}_q^n$, denotes $x_1y_1 + x_2y_2 + \ldots + x_ny_n = xy^T$. Thus the group $\mathbf{H}_n$ is isomorphic to the group $\{(\alpha, c, \beta) \parallel \alpha, \beta \in \mathbb{F}_q^n, c \in \mathbb{F}_q\}$, where the group operation $\circ$ is given by $(\alpha, c, \beta) \circ (\alpha', c', \beta') = (\alpha + \alpha', c + c' + \alpha\beta'^T, \beta + \beta')$. The group $\mathbf{H}_n$ is a p-group of order q^{2n+1}, with elementary abelian center $Z(\mathbf{H}_n)$ of order q, and $\mathbf{H}_n/Z(\mathbf{H}_n)$ elementary abelian of order q^{2n}.

Since the full automorphism group of $\mathbf{W}(q)$ is transitive on the points of $\mathbf{W}(q)$, the Payne-derivatives of $\mathbf{W}(q)$ with respect to any point of $\mathbf{W}(q)$ are isomorphic. Hence let r be any fixed chosen point of $\mathbf{W}(q)$. Now $\mathbf{W}(q)$ can be described as an EGQ $(\mathbf{W}(q)^r, G)$. We will describe this in detail. Let the points and lines of $\mathbf{W}(q)$ be the absolute points and lines of the symplectic polarity ρ of $\mathbf{PG}(3, q)$ defined by

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Let the point r be the point $(0, 0, 1, 0)^T$. One easily checks that the matrices

$$S(c) := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{bmatrix}, T_1(\alpha) := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -\alpha \\ \alpha & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, T_2(\beta) := \begin{bmatrix} 1 & 0 & 0 & \beta \\ 0 & 1 & 0 & 0 \\ 0 & \beta & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

with $c, \alpha, \beta \in \mathbb{F}_q$, determine automorphisms of $\mathbf{W}(q)$ fixing each line through r. The group G generated by these matrices clearly has order q^3 and acts sharply transitively on the points of $\mathbf{W}(q)$ not collinear with r. So indeed $(\mathbf{W}(q)^r, G)$ is an EGQ. The matrices $S(c)$ determine the symmetries about r. We have

$$G = \left\{ \begin{bmatrix} 1 & 0 & 0 & \beta \\ 0 & 1 & 0 & -\alpha \\ \alpha & \beta & 1 & c \\ 0 & 0 & 0 & 1 \end{bmatrix} \parallel \alpha, \beta, c \in \mathbb{F}_q \right\},$$

with standard matrix multiplication as group action (note that the subgroup $Z = \{S(c) \parallel c \in \mathbb{F}_q\}$ is the center of G).

Consequently the group G is isomorphic to the group $K = \{(\alpha, c, \beta) \parallel \alpha, \beta, c \in \mathbb{F}_q\}$, where the group operation $\circ$ is given by $(\alpha, c, \beta) \circ (\alpha', c', \beta') = (\alpha + \alpha', c + c' + \alpha\beta' - \beta\alpha', \beta + \beta')$. Now the mapping

$$\phi : K \to \mathbf{H}_1 : (\alpha, c, \beta) \mapsto (\alpha - \beta, c + \frac{1}{2}(\alpha^2 - \beta^2), \alpha + \beta)$$

can easily be seen to be an isomorphism. We conclude that the GQ $\mathcal{P}(\mathbf{W}(q), r)$, q odd, admits a Singer group isomorphic to the 3-dimensional Heisenberg group over $\mathbb{F}_q$.

Conversely it is well-known, see for instance [17] and [21], that starting from a Heisenberg group $\mathbf{H} = \mathbf{H}_1$ of dimension 3 over $\mathbb{F}_q$ with q odd, an EGQ $(\mathbf{Q}^x, \mathbf{H})$ of order q can be constructed using a Kantor family. As a specific example it is possible to obtain the classical GQ $\mathbf{W}(q)$ in this way when q is odd.

Remark 4.3.1 In [29] various properties of Heisenberg groups are investigated related to GQs.

4.4 The other GQs (of order s) with a regular point

Only one class of GQs of order s is known which wasn't already described. Let $\mathcal{S}$ be a TGQ of order s with s even which arises from a translation generalized oval [25, 26] (or, equivalently, for which the point-line dual is also a TGQ [25, 26]). Then there is a line L of regular points through the (regular) translation point (∞) of $\mathcal{S}$. Each of the points x of $L\setminus\{(\infty)\}$ gives rise to a GQ $\mathcal{P}(\mathcal{S},x)$; we will show that a GQ of this type only admits a Singer group if $\mathcal{S}$ is classical. (If $\mathcal{S}\cong\mathbf{Q}(4,s)$ is classical, each point is a translation point.) Since no generalized ovals are known which do not arise from "ordinary" ovals, we will restrict ourselves to TGQs $\mathcal{S}$ arising from translation ovals. Let K be a hypothetical Singer group of $\mathcal{P}(\mathcal{S},x)$; it is clear that K cannot be naturally induced by $\mathrm{Aut}(\mathcal{S})$ unless $\mathcal{S}\cong\mathbf{Q}(4,s)$. (It would follow that (∞) is not fixed by K, so that $\mathcal{S}$ contains distinct translation points. By, e.g., [27] we then would have that $\mathcal{S}\cong\mathbf{Q}(4,s)$.) One now easily shows that $\mathcal{S}$ contains $(s+1)\times(s+1)$-grids not containing (∞) (use, e.g., [27, Chapter 5]). By [23, 3.3.3], we conclude that $\mathcal{S}\cong\mathbf{Q}(4,s)$.

Motivated by the observations made in this chapter and Section 7.4 (cf. Chapter 7), we pose the following conjecture.

CONJECTURE 4.4.1 *If a finite thick GQ* $\mathbf{Q}$ *admits a Singer group* G*, then either* $\mathbf{Q}$ *is the GQ of order* $(5,3)$*, or* G *is* (1) *an elementary abelian* 2*-group, or* (2) *an odd order Heisenberg group, and in* (1)*-*(2) $\mathbf{Q}$ *is a Payne-derived GQ arising in the usual way from an EGQ with elation group isomorphic to* G*.*

One could also replace "Heisenberg" by "special" in Conjecture 4.4.1.

Chapter 5

Abelian and Heisenberg Singer Groups

In this chapter we will discuss what is known about Singer groups for thick finite GQs. From the previous chapter we know that conjecturally the only such groups should be either elementary abelian groups of even order, or Heisenberg groups of odd order. Two questions are of great importance here:

> (1) Given a group G, can it act as a Singer group on a GQ?
> (2) If a group G *can* act as a Singer group, on which GQs can it act as such?

In the first section we will show that an abelian Singer group necessarily is the Singer group of a Payne-derived GQ. In the second section we look at odd order Heisenberg groups. These results are taken from [7] and [9].

5.1 Abelian Singer groups

For the rest of this section let G be an abelian group acting sharply transitively on a thick finite GQ $\mathcal{Q}$ of order (s, t). By e.g. Section 3.2 we immediately obtain that the stabilizer in G of any line of $\mathcal{Q}$ has order $s + 1$. We now easily see that the following lemma holds.

Lemma 5.1.1 *Let L be any line of* **Q***, then L^G is a spread of symmetry of* **Q**. ■

This allows one to prove that **Q** is a Payne-derived GQ.

Theorem 5.1.2 *The GQ* **Q** *can be obtained by Payne-derivation.*

Proof. We claim that **Q** has parameters $(s, s+2)$. As before we identify the points of **Q** with the elements of G. Let L_1, L_2 and L_3 be three distinct lines through id. Furthermore denote by S_i the stabilizer in G of the line L_i, $i = 1, 2, 3$. Clearly $S_1S_2 = \langle S_1, S_2 \rangle$ is a group of size $(s+1)^2$. Also $S_3 \cap S_1S_2 = \{id\}$, since the existence of any non-trivial element $s_1s_2 \in S_3$, with $s_1 \in S_1$ and $s_2 \in S_2$, implies that the point $s_1s_2 \neq id$ on L_3 would be collinear with the point $s_1 \neq id$ on L_1, yielding a triangle in **Q**. Hence $S_1S_2S_3$ is a group of order $(s+1)^3$, and $(s+1)^3$ divides $|G| = (s+1)(st+1)$. Consequently $s+1$ divides $\frac{t-1}{s+1} - 1$. So either $\frac{t-1}{s+1} - 1 = 0$, or $s^2 + 3s + 3 \leq t$, contradicting Higman's inequality $t \leq s^2$. Our claim is proved. The theorem now follows using Theorem 1.6.2. ■

It is possible to give a more explicit description of **Q** in this case.

Identify the points of **Q** with the elements of G. Denote the lines through id by $L_0, L_1, \ldots, L_{s+2}$ and the respective stabilizers in G by $S_0, S_1, \ldots, S_{s+2}$. Define $\mathbb{K}$ to be the set of all endomorphisms β of G with the property that $S_i^\beta \subseteq S_i$ for all $i \in \{0, 1, \ldots, s+2\}$. Then we have the following lemma.

Lemma 5.1.3 *The ring $\mathbb{K}, +, .$ (where the operations "+" and "." are obvious) is a field.*

Proof. It is sufficient to show that every element of $\mathbb{K} \setminus \{0\}$ is a bijection from G to G, and hence by the finiteness of G we only need to show injectivity. Suppose that $\beta \in \mathbb{K}$ is such that $s_0^\beta = id$ for some $s_0 \in S_0 \setminus \{id\}$; then we must show that $\beta = 0$. (The choice of S_0 is arbitrary. Further, if there is an element of the kernel of β in $\bigcup S_i$, then there is an element of the kernel in each $S_i \setminus \{id\}$ as well.) Assume the contrary. Choose any element $s_i \in S_i \setminus \{id\}$, with $i \neq 0$. Then the point s_0s_i is at distance two from id in the collinearity graph of **Q**. Since **Q** is thick there exist elements $s_l \in S_l \setminus \{id\}$ and $s_k \in S_k \setminus \{id\}$, $l, k \notin \{0, i\}$ and $l \neq k$, such that $s_0 s_i = s_l s_k$. Note that $\left|\{y, z\}^\perp\right|$, $y \not\sim z$, must be even since G is abelian (if $y \sim y^\theta \sim z$, with $y^{\theta\gamma} = z$, then $y \sim y^\gamma \sim z$, with $\theta, \gamma \in G$). Letting β act yields $s_i^\beta = s_l^\beta s_k^\beta$. First suppose that $s_l^\beta = id$; then $s_i^\beta = s_k^\beta$. Since $S_i \cap S_k = \{id\}$ we obtain that $s_i^\beta = id$. Analogously $s_k^\beta = id$ implies that $s_i^\beta = id$. Next suppose that neither s_l^β nor s_k^β equals id. In this case the line $S_l s_k^\beta$ of **Q** intersects the line S_k in $s_k^\beta \neq id$ and intersects the line S_i in $s_i^\beta \neq id$. Hence we have found a triangle in **Q**, a contradiction. We conclude that $s_i^\beta = id$, and henceforth that $S_j^\beta = id$, for all $j \in \{0, 1, \ldots, s+2\}$. By the connectedness of **Q** we know that $G = \langle S_0, S_1, \ldots S_{s+2} \rangle$, and hence it follows that $G^\beta = id$, that is, $\beta = 0$. ∎

Consequently G can be seen as a $\mathbb{K}$-vector space of dimension $\log_{|\mathbb{K}|}(|G|)$, and the S_i's as vector subspaces of dimension $\log_{|\mathbb{K}|}(s+1)$. It is clear that the line set of **Q** is exactly the set of all translates of these vector subspaces. Hence **Q** has a (generalized) linear representation in the affine space constructed from the $\mathbb{K}$-vector space G. We obtain the following theorem.

Theorem 5.1.4 *If G is an abelian group acting as a Singer group on the points of a thick finite GQ* **Q***, then G is elementary abelian of even order,* **Q** *has order $(s, s+2)$ and arises from a generalized hyperoval.*

Proof. Immediate. ∎

This completely answers both questions from the introduction for abelian groups.

5.2 The Heisenberg case

We first prove the following general lemma for Singer p-groups.

Lemma 5.2.1 *Let G be a p-group acting sharply transitively on the point set of a thick GQ of order (s, t). Then $t = s + 2$.*

Proof. From $|G| = (s+1)(st+1) = p^k$, for the natural number k, it follows that $s+1 = p^l$, for some natural number l. Furthermore, as $st+1 > s+1$, we see that $s+1$ divides $st+1$, and hence $s+1$ divides $t-1$. If $s+1 = t-1$, we obtain the desired result. So assume by way of contradiction that $t-1 > s+1$. Then $t = p^l f + 1$, for some natural number $f > 1$, and consequently $|G| = (s+1)(st+1) = p^{2l}(p^l f - f + 1)$. It follows that f is at least $1 + p^l$, that is, $f > s+1$, and $t > (s+1)^2$, contradicting Higman's inequality $t \leq s^2$. ■

Theorem 5.2.2 *Let* $\mathbf{Q}$ *be a GQ of order* (s,t) *admitting a Singer group* G*, where* G *is a* p*-group and* p *is odd. Suppose* $|Z(G)| \geq \sqrt[3]{|G|}$*. Then the following properties hold.*

(1) *We have* $t = s+2$*, and there is a GQ* $\mathbf{Q}'$ *of order* $s+1$ *with a regular point* x*, such that* $\mathbf{Q}$ *is the Payne derivative of* $\mathbf{Q}'$ *with respect to* x*. The GQ* $\mathbf{Q}'$ *is an STGQ of type* $(\mathbf{Q}'^x, K)$*, with* K *isomorphic to* G*.*

(2) *We have* $|Z(G)| = \sqrt[3]{|G|}$*, that is,* $|Z(G)| = s+1$*.*

From Theorem 5.2.2 the next result follows.

Corollary 5.2.3 *Let* $\mathbf{Q}$ *be a GQ of order* (s,t) *admitting a Singer group* G*, where* G *is a Heisenberg group of dimension* 3 *over the field* $\mathbb{F}_q$ *with* q *odd. Then we have the conclusion of* Theorem 5.2.2. ■

We now prove Theorem 5.2.2.

First of all, we note that $t = s+2$ by Lemma 5.2.1, so that $(s+1)(st+1) = (s+1)^3$.

Let α be any element of G. Suppose that no point of $\mathbf{Q}$ is mapped by α onto a point collinear with it. Then applying Theorem 1.1.7, we obtain

$$(s+1)^2 \equiv 0 \mod 2(s+1),$$

a contradiction as $s+1$ is odd (as $s+1$ divides the order of G). So there are points x for which $x^\alpha \sim x$. We now consider elements of $Z(G)$ and repeat the argument of Section 3.2. Take $\alpha \in Z(G)^\times$, and let x be a point for which $x^\alpha \sim x$. Put $L = xx^\alpha$. Let y be a point incident with L

and different from x, x^α. Let $\beta \in G$ be the element that maps x onto y. Then we have

$$x \sim x^\beta \Longrightarrow x^\alpha \sim x^{\beta\alpha} = x^{\alpha\beta}; x \sim x^\alpha \Longrightarrow x^\beta \sim x^{\alpha\beta}.$$

Hence $x, x^\alpha, x^\beta, x^{\alpha\beta}$ are all on the same line, and $\{x, x^\beta\}^\alpha = \{x^\alpha, x^{\alpha\beta}\}$ implies that L is fixed by α. Since G acts transitively on the point set of $\mathbf{Q}$, one concludes that each point is incident with a unique line that is fixed by α, that is, α fixes a spread $T(\alpha)$ linewise.

Suppose $\alpha' \in Z(G)^\times$ for which $T(\alpha') \neq T(\alpha)$. Then there exists a line $M \in T(\alpha)$ such that each point of M is incident with a line of $T(\alpha')$ different from M. Take any point $z \mathrm{~I~} M$. Then $z \sim z^\alpha \mathrm{~I~} M$, $z^\alpha \sim z^{\alpha\alpha'} \not\mathrm{I} M$, so that $z \not\sim z^{\alpha\alpha'}$. On the other hand, $\alpha\alpha' \in Z(G)$, while each element of $Z(G)$ maps a point onto a collinear point, contradiction. So $T(\alpha) = T(\alpha')$ and hence each element of $Z(G)$ fixes $T(\alpha)$ linewise. By the regularity of G this implies that $|Z(G)| \leq s + 1$. Consequently $|Z(G)| = s + 1$, and $T(\alpha)$ is a spread of symmetry.

Now (2) follows.

By Theorem 1.6.2 it follows that $\mathbf{Q}$ can be constructed by Payne deriving a GQ $\mathbf{Q}'$ with respect to a center of symmetry x. Further it is not hard to see that G induces a group of automorphisms $K \cong G$ of $\mathbf{Q}'$ fixing all lines on x and acting regularly on the points not collinear with x.

Now also (1) follows. ■

Chapter 6

The Results of Ghinelli and Yoshiara

Both D. Ghinelli and S. Yoshiara were concerned with excluding possible parameters for a finite GQ with a Singer group. Below we describe their results. Especially Yoshiara's main theorem is important in our study of possible Singer groups for the known GQs, as it shows (in a more general form) that $\mathbf{H}(3, q^2)$ cannot admit a Singer group.

6.1 Ghinelli's results

In 1992 D. Ghinelli was the first to study GQs with a Singer group. Because she approached the problem using difference sets, she was forced to restrict herself to GQs of order s. We describe how one can associate with each GQ $\mathcal{Q}$ of order s that admits a Singer group G, a difference set Δ of G with multiplier -1. Recall that a (v, k, λ)-*difference set* in a group G of order v is a subset Δ of order k of G, such that every non-identity element of G can be written in exactly λ ways as a difference of two elements of Δ. An integer m is said to be a *multiplier* of a difference set Δ provided that $\Delta = \Delta^m := \{d^m \parallel d \in \Delta\}$. Now choose any point p of $\mathcal{Q}$. Define

$$\Delta := \{g \in G \parallel p^g \sim p\}.$$

One easily checks that Δ is a $(s^3 + s^2 + s + 1, s^2 + s + 1, s + 1)$-difference set with multiplier -1, that is $\Delta^{-1} = \Delta$. Ghinelli first generalizes a result on abelian difference sets with multiplier -1 to the nonabelian case, and then starts to apply this to the case of GQs of order s with a Singer group. A first result is that each conjugacy class of G meets Δ, yielding that G cannot be abelian (for the complete solution of "abelian Singer GQs" see the previous chapter). She then obtains the following result.

Lemma 6.1.1 (Ghinelli [13]) *Let G be a group acting regularly on the points of a GQ of order s. If N is an elementary abelian normal p-subgroup, $p \neq 2$, of G, then $|N| = p^a$ divides $1 + s^2$.*

Proof. See Theorem 3.5 of [13]. ■

In order to have the conclusion of Lemma 6.1.1 for every elementary abelian normal subgroup of G, Ghinelli then specializes to GQs of even order s, obtaining the following lemma.

Lemma 6.1.2 (Ghinelli [13]) *The difference set Δ cannot contain a non-trivial normal abelian subgroup.*

Proof. See Lemma 4.1 of [13]. ■

This yields

Theorem 6.1.3 (Ghinelli [13]) *A GQ of even order s does not admit a Singer group with non-trivial center.*

Proof. See Theorem 4.3 of [13]. ■

As a further application of Lemma 6.1.1, Ghinelli proves a restriction on the Fitting subgroup of G (as s is even, G is solvable). She then obtains

Theorem 6.1.4 (Ghinelli [13]) *A GQ of even order s does not admit a Singer group that is a Frobenius group.*

Proof. See Theorem 4.5 of [13]. ■

Finally, the latter theorem is used to prove

Theorem 6.1.5 (Ghinelli [13]) *If $1 + s^2$ is square free, a GQ of even order s does not admit a Singer group.*

Proof. See Theorem 4.6 of [13]. ∎

6.2 Yoshiara's results

Let $\mathcal{Q}$ be a GQ of order (s, t) with a Singer group G. Because Yoshiara does not use the theory of difference sets, he does not need to require any severe restrictions on the parameters s and t. Let p be an arbitrary but fixed point of $\mathcal{Q}$, and let Δ be defined as in the previous section (note that Δ is not necessarily a difference set in G). Yoshiara starts by generalizing several results from Ghinelli's paper (giving simpler proofs). We mention the following lemmas.

Lemma 6.2.1 (Yoshiara [35]) *Let H be a non-trivial subgroup of G which is entirely contained in Δ. Then there is a unique line L through p stabilized by H. Furthermore, if H is normal, then $|G_L| = s + 1$, and so the G-orbit of L forms a spread.*

Proof. See the proofs of Lemmas 4 and 9 of [35]. ∎

Lemma 6.2.2 (Yoshiara [35]) *Let a be a non-trivial element of G, and let d equal $\gcd(s, t)$. Then the following hold.*

- *If $d > 1$, we have $a^G \cap \Delta \neq \emptyset$.*
- *$\left|a^G \cap \Delta^c\right|$ is a multiple of d (possibly 0), where Δ^c is the complement of Δ in G.*

Proof. See the proof of Lemma 6 in [35]. ∎

Corollary 6.2.3 *If $\gcd(s, t) > 1$ then Property (C) is satisfied.* ∎

Lemma 6.2.4 (Yoshiara [35]) *Assume $d = \gcd(s,t) > 1$, and let $r = 2$ or 3. Then the following conditions are equivalent:*

- *$|G|$ is divisible by r;*
- *there is an element of order r of G which fixes a line L through p;*
- *$s+1$ is divisible by r.*

Proof. See the proof of Lemma 7 in [35]. ■

Finally the following lemma, that exploits the fact that the Suzuki groups are characterized among the nonabelian finite simple groups as those that are $3'$-groups, plays a key role in the proof of Yoshiara's main result.

Lemma 6.2.5 (Yoshiara [35]) *Assume $d = \gcd(s,t) > 1$, and that 3 does not divide $s+1$. If G has a nonabelian minimal normal subgroup N, then $N = S_1 \times S_2 \times \cdots \times S_m$ with each S_i ($i = 1, 2, \ldots, m$) isomorphic to the Suzuki group ${}^2\mathbf{B}_2(q)$ for some $q = 2^{2e+1} \geq 8$, not depending on i.*

Proof. See the proof of Theorem 8 in [35]. ■

Yoshiara then turns his attention to GQs of order (t^2, t). Note that the numerical conditions of the previous lemma are naturally satisfied in this case. He obtains the following nice result, the long proof of which is based on a clever use of the above lemmas, together with some non-trivial group theory.

Theorem 6.2.6 (Yoshiara [35]) *A GQ of order (t^2, t) cannot admit a Singer group on its points.*

Proof. See Section 3 in [35]. ■

Corollary 6.2.7 *The GQ $\mathbf{H}(3, q^2)$ does not admit a Singer group.* ■

Chapter 7

Non-Classical Singer Quadrangles

In this chapter, which is taken from [10], we classify the known non-classical GQs that admit a Singer group.

7.1 Singer groups for the known GQs

All known GQs have one of the following properties (see [29], or [27]):

(i) There is an elation point.

(ii) There is an elation line.

(iii) Up to duality, it is a Payne-derived GQ of order $(s, s+2)$ for some natural number s (where $s = p^h - 1$, p a prime).

The Cases (i)-(ii) can be reduced essentially simultaneously to the "classical case", as follows. Suppose $\mathcal{S}$ satisfies (i). Then since $\mathcal{S}$ admits a Singer group each point of $\mathcal{S}$ is an elation point. In Case (ii), there clearly are two non-collinear elation lines, so each line is an elation line.

We now invoke the next result.

Theorem 7.1.1 (K. Thas and Van Maldeghem [30]) *A finite thick GQ for which either each point is an elation point or each line is an elation line, is classical or dual classical.*

Proof. See the proof of Main Result (Geometric Version) of [30]. ■

We will have to carry through a case-by-case analysis in order to obtain the desired result that among the classical GQs only $\mathbf{Q}(5,2)$ admits a Singer group. This will be the core of Chapter 8.

7.2 Payne-derived quadrangles and duals

Suppose $\mathcal{P}$ is a known GQ of order $(s, s+2)$, $s \neq 1$, admitting a Singer group. Then $\mathcal{P}$ is (isomorphic to) a Payne-derived quadrangle $\mathcal{P} = \mathcal{P}(\mathbf{Q}, x)$, and $\mathbf{Q}$ can be shown to be an EGQ $(\mathbf{Q}^x, G)$ with regular elation point x. Here the elation group G induces a Singer group on the points of $\mathcal{P}$. In all known cases this group is either elementary abelian of even order, or a Heisenberg group of dimension 3 over the field $\mathbb{F}_q$ with q odd.

Next we look at the known GQs of order $(s+2, s)$. Suppose $\mathcal{S}$ is a known GQ of order $(s+2, s)$, $s \neq 1$, admitting a hypothetical Singer group on its points. Then $\mathcal{S}^D$ is (isomorphic to) a known Payne-derived quadrangle $\mathcal{P} = \mathcal{P}(\mathbf{Q}, x)$, and $\mathbf{Q}$ can be shown to be an EGQ of order $s+1$ with regular elation point x. So $\mathcal{P}$ admits a Singer group on lines (besides a Singer group on points) if $\mathcal{S}$ admits a Singer group on points.

First suppose that the number of points of $\mathcal{P}$ is odd, and that $s > 3$. Then by De Winter and K. Thas [8], the automorphism group of $\mathcal{P}$ is induced by the stabilizer of x in the automorphism group of $\mathbf{Q}$. So $\mathrm{Aut}(\mathcal{P})$ cannot act transitively on the lines of $\mathcal{P}$ (since there are two types of lines, and they cannot be interchanged by such automorphisms).

Now suppose that the number of points of $\mathcal{P}$ is even.
Then $\mathcal{P}$ can be respresented as follows *if it is known*. Suppose $\mathcal{H}$ is a hyperoval of $\mathbf{PG}(2,q)$, so q is even. Embed $\mathbf{PG}(2,q)$ as a hyperplane in $\mathbf{PG}(3,q)$. The points of the GQ $\mathbf{T}(\mathcal{H})$ are the affine points, and the

lines are the lines which are not contained in $\mathbf{PG}(2,q)$ but meet $\mathcal{H}$ in a point. The translation group of $\mathbf{AG}(3,q) = \mathbf{PG}(3,q) \setminus \mathbf{PG}(2,q)$ induces an elementary abelian Singer group on the points of the GQ. In [8] it is shown that $\mathrm{Aut}(\mathcal{P})$ is induced by $\mathbf{P\Gamma L}_4(q)_{\mathcal{H}}$. Since $\mathrm{Aut}(\mathcal{P})$ is assumed to be line transitive, $\mathcal{H}$ is a transitive hyperoval. By [3, 18], there are only three possibilities:

- $\mathcal{H}$ is the unique hyperoval of $\mathbf{PG}(2,2)$. In this case the obtained GQ is thin.
- $s = 3$ and $\mathcal{P}$ has order $(3,5)$ (see also [20]), cf. Section 7.4.
- $\mathcal{H}$ is the Lunelli-Sce hyperoval. We will have a closer look at this case in the next subsection.

7.3 The Lunelli-Sce quadrangle

The Lunelli-Sce hyperoval is of particular interest to our study, because it has a transitive automorphism group. A corollary of this property is that the GQ of order $(15,17)$ arising from it admits a flag-transitive automorphism group, and together with the aforementioned GQ of order $(3,5)$ it is, up to duality, the only non-classical example known that has such an automorphism group. The occurence of a flag-transitive group thus makes us wonder whether there is a Singer group *on the lines* around. There are two reasons which would make a positive answer fundamental: its dual would be an example with more points on a line than lines through a point admitting a Singer group (on points), and secondly, its Singer group would not be a p-group.

THE LUNELLI-SCE HYPEROVAL. Let $\mathcal{H}$ be a hyperoval in $\mathbf{PG}(2,2^h)$, $h > 1$. Without loss of generality, we may suppose that $\mathcal{H}$ contains the points $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,1)$. The affine points of $\mathcal{H}$ are of the form $(x, f(x), 1)$, where f is a permutation polynomial which one usually calls *o-polynomial*. The Lunelly-Sce hyperoval, defined in $\mathbf{PG}(2,16)$, is (up to projective equivalence) given by

$$f(x) = x^{12} + x^{10} + \eta^{11}x^8 + x^6 + \eta^2 x^4 + \eta^9 x^2,$$

η being a primitive element of $\mathbb{F}_{16}$ satisfying $\eta^4 = \eta + 1$.

In $\mathbf{PG}(3,q) \supset \mathbf{PG}(2,q)$, $q = 2^4$, construct $\mathbf{T}(\mathcal{H})$ as above. It is well-known that $|\mathbf{P\Gamma L}_3(q)_{\mathcal{H}}| = 144$, and that the automorphism group of $\mathbf{T}(\mathcal{H})$ is induced by the group of the hyperoval (that is, it is of the form $T \rtimes \mathbf{P\Gamma L}_3(q)_{\mathcal{H}}$, where T is the translation group of $\mathbf{AG}(3,q) = \mathbf{PG}(3,q) \backslash \mathbf{PG}(2,q)$). Denote the hypothetical line Singer group of $\mathbf{T}(\mathcal{H})$ by S. Then by [22], S induces a sharply transitive automorphism group of $\mathcal{H}$. Such a group does not exist by [3] (the involutions of $\mathcal{H}$ generate a subgroup of order 36).

The authors thank Tim Penttila for providing them the references [22, 3] in this context.

7.4 The GQ of order $(3,5)$

Let $\mathcal{H}$ be the regular hyperoval of size 6 in $\mathbf{PG}(2,4)$; then $\mathbf{P\Gamma L}_3(4)_{\mathcal{H}} \cong \mathbf{S}_6$. By [31], $\mathbf{T}(\mathcal{H})$ admits a Singer group S on the lines. Such a group has size 96, so is not a p-group, and $\mathbf{T}(\mathcal{H})^D$ is the only known example admitting a Singer group on points which is not a p-group. Also, $\mathbf{T}(\mathcal{H})^D$ is the only known GQ with an order which is not of type $(s, s+2)$ admitting a Singer group (on the points).

Chapter 8

Classical Singer Quadrangles

The aim of this chapter is to show that $\mathbf{Q}(5,2)$ is the only classical GQ that admits a Singer group. In order to obtain this result, we will distinguish between some cases where an elementary geometric proof can be given, and other cases where a more involved group theoretical analysis is needed.

8.1 Projective involutions

The idea is to exploit the fact that each classical GQ or its dual is naturally (by definition) embedded in some projective space and that (if the GQ is not a (dual) grid) each automorphism of the GQ is induced by an automorphism of the projective space.

We will now exploit the classification of involutions in projective space (see Theorem 3.3.1) to prove that for odd q the GQs $\mathbf{Q}(4,q)$, $\mathbf{H}(4,q^2)$ and $\mathbf{H}(4,q^2)^D$ do not admit a Singer group.

Theorem 8.1.1 *The GQ $\mathbf{Q}(4,q)$, q odd, does not admit a Singer group.*

Proof. Suppose G were a Singer group of $\mathbf{Q}(4,q)$. We consider the dual situation where G is a group acting regularly on the lines of $\mathbf{W}(q) \subset \mathbf{PG}(3,q)$. Let ι be any involution in G. Since $\mathbf{W}(q)$ satisfies Property (C), ι maps some line to a concurrent line, and hence fixes the point, say p, that is the intersection of this line and its image. If by ρ we denote the defining polarity of $\mathbf{W}(q)$, we see that ι also must fix the plane $\pi := p^\rho$. The involution ι now induces an involution (or the identity) in this plane π, and hence fixes a line L of π through p. This line, however, is a line of the GQ $\mathbf{W}(q)$, contradicting the regularity of the group G on lines of $\mathbf{W}(q)$. ■

Theorem 8.1.2 *The GQ $\mathbf{H}(4, q^2)$, q odd, does not admit a Singer group.*

Proof. Suppose G would be a Singer group of $\mathbf{H}(4, q^2) \subset \mathbf{PG}(4, q^2)$ and let ι be any involution in G. By Theorem 3.3.1 ι is either a Baer-involution or fixes the points of two complementary subspaces. Since every subspace of dimension at least 1 intersects $\mathbf{H}(4, q^2)$ non-trivially, the latter cannot occur. So suppose that ι is a Baer-involution. As $\mathbf{H}(4, q^2)$ satisfies Property (C) we know that ι fixes some line L of $\mathbf{H}(4, q^2)$. Since ι is a Baer-involution there are exactly $q^2 + q + 1$ planes through L fixed by ι. One of these planes is the image of L under ρ, the polarity defining $\mathbf{H}(4, q^2)$, which intersects $\mathbf{H}(4, q^2)$ exactly in the line L. However, the other $q^2 + q$ planes must intersect $\mathbf{H}(4, q^2)$ in a cone $p\mathbf{H}(1, q^2)$, p a point on L. Hence in each of these planes ι must fix the unique top of that cone, contradicting the regularity of ι. ■

Theorem 8.1.3 *The GQ $\mathbf{H}(4, q^2)^D$, q odd, does not admit a Singer group.*

Proof. Consider the dual situation and suppose that G would be a group acting regularly on the lines of $\mathbf{H}(4, q^2)$. Once again let ι be any involution in G. By Theorem 3.3.1 ι is either a Baer-involution or fixes the points of two complementary subspaces. First suppose ι would fix two complementary subspaces. Since every 3-space contains a line of $\mathbf{H}(4, q^2)$, the Singer involution ι must fix pointwise a plane π and a line L, disjoint from π. Clearly π must intersect $\mathbf{H}(4, q^2)$ in a Hermitian variety $\mathbf{H}(2, q^2)$. Let ρ be the polarity defining $\mathbf{H}(4, q^2)$. The line L contains at least one point p_1 of $\mathbf{H}(4, q^2)$. Similarly, the line $p_1^\rho \cap \pi$ contains at least one point p_2 of $\mathbf{H}(4, q^2)$. The line p_1p_2 is stabilized by ι, contradiction.

Next suppose that ι is a Baer-involution. Let p be any point of $\mathbf{H}(4, q^2)$ that is fixed by ι (p exists by Property (C)). Clearly also the 3-space p^ρ is fixed by ι. This 3-space then must intersect the fixed point structure of ι in a Baer subspace $\mathbf{PG}(3, q)$. Hence there is a plane π of p^ρ not containing p that is fixed by ι. This plane intersects $\mathbf{H}(4, q^2)$ in a Hermitian curve $\mathbf{H}(2, q^2)$. Furthermore, the fixed point structure of ι in π must be a Baer subplane. Since every Baer subplane intersects a Hermitian curve $\mathbf{H}(2, q^2)$ non-trivially (see for example [1]), we see that ι fixes a point $n \neq p$ of $\mathbf{H}(4, q^2)$ in p^ρ. Hence ι fixes the line pn, which is a line of $\mathbf{H}(4, q^2)$, contradicting the regularity of G. ■

8.2 Solvable Singer groups

Throughout this section we will use the celebrated Feit-Thompson theorem that states that a group G of odd order is solvable.

Theorem 8.2.1 *The GQ $\mathbf{H}(4, q^2)$, q even, does not admit a Singer group.*

Proof. Suppose G is a Singer group of $\mathbf{Q} = \mathbf{H}(4, q^2)$, q even. Then G has odd order and so is solvable. Let h be the Hermitian form associated with $\mathbf{Q}$ and let V be the vector space whose singular 1- and 2-spaces (with respect to h) represent the points and lines of $\mathbf{H}(4, q^2)$. Let $\tilde{G}$ be the subgroup of $\mathbf{\Gamma U}_5(q^2)$ representing G. Let $\hat{G}$ be $\tilde{G} \cap \mathbf{GU}_5(q^2)$. We have a normal series

$$Z(\mathbf{GL}_5(q^2)) \trianglelefteq \hat{G} \trianglelefteq \tilde{G},$$

with $\left|\tilde{G}/\hat{G}\right|$ dividing $2a$, where $q = 2^a$, $|Z(\mathbf{GL}_5(q^2))|$ dividing $q^2 - 1$, and $\tilde{G}/Z(\mathbf{GL}_5(q^2)) = G$. Consider a Z-prime r for $q^{10} - 1$. Then clearly r divides $q^5 + 1$. By Corollary 3.4.5 there exists a subgroup R of $\hat{G}$ whose order is r, and as r is a Z-prime for $q^{10} - 1$, $R \cap Z(\mathbf{GL}_5(q^2)) = \mathbf{1}$. Moreover, R acts irreducibly on V. Suppose R normalized a group $A \leq \hat{G}$ which it did not centralize. Then by Lemma 3.4.2, $r = 6$, which is impossible. If R were not in the Fitting group $\mathbf{F}(\hat{G})$ of $\hat{G}$ it would act faithfully on it (since $\hat{G}$ is solvable the Fitting group contains its own centralizer). Thus, R lies in the Fitting group of $\hat{G}$. Without loss of generality we may take R to be in the center of the $\mathbf{F}(\hat{G})$ (since a nilpotent group is the direct product of its Sylow subgroups and the center of a nilpotent subgroup contains the direct product of the centers of its Sylow subgroups). Now we see that $C_{\hat{G}}(R)$ is a cyclic group (since R acts irreducibly on V) which contains $\mathbf{F}(\hat{G})$. Thus R is the unique group of order r in $\mathbf{F}(\hat{G})$, and so is a characteristic subgroup of $\hat{G}$.

Now $\hat{G}/C_{\hat{G}}(R) \leq \mathrm{Aut}(R)$ and does not change the minimal polynomial of degree 5 exhibited by a generator of R in its action on V. Thus $\left|\hat{G}/C_{\hat{G}}(R)\right| = 1$ or 5. Now the index of $\hat{G}$ in $\tilde{G}$ is a divisor of the odd part d of $|\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_2)|$. So if $q = 2^a$, d is the odd part of a. We have the following diagram

$$\begin{array}{c} \tilde{G} \\ | \\ \text{divisor of } d \\ | \\ \hat{G} \\ | \\ 1 \text{ or } 5 \\ | \\ C_{\hat{G}}(R) \end{array}$$

where intermediate integers denote subgroup indices. Now suppose that no prime dividing q^2+1 divides $|C_{\hat{G}}(R)|$. Then clearly q^2+1 divides $\left[\tilde{G} : C_{\hat{G}}(R)\right]$ which divides $5d$. So, if $q = 2^a$ we see that $2^{2a} + 1$ divides $5a$, forcing $a = 1$. Thus $\mathbf{Q} = \mathbf{H}(4, 4)$, $\tilde{G} = \hat{G}$, $Z(\mathbf{GL}(V)) \cong \mathbb{Z}_3$ and $|C_{\hat{G}}(R)| = 99$. Now there is a subgroup A of $\hat{G}$ of order 9 containing $Z(\mathbf{GL}(V))$. This subgroup must centralize R and hence must be cyclic. So it acts homogeneously on V with modules of dimension 3. This would force 3 to divide 5, an absurdity.

Thus, there is a prime s dividing $q^2 + 1$ and $|C_{\hat{G}}(R)|$. Consider an element x of order s in $\hat{G}$. But here x acts homogeneously on V with irreducible modules of dimension 2 (the prime s is a Z-prime for $(q^2)^2 - 1$). This forces 2 to divide 5, the final contradiction. ■

Theorem 8.2.2 *The GQ $\mathbf{H}(4, q^2)^D$, q even, does not admit a Singer group.*

Proof. Suppose G were a Singer group for $\mathbf{H}(4, q^2)^D$. We consider the dual situation where G acts regularly on the lines of $\mathbf{H}(4, q^2)$. Then there is a group $\tilde{G}$ representing G in $\mathbf{\Gamma U}_5(q^2)$. As before let $\hat{G} = \tilde{G} \cap \mathbf{GU}_5(q^2)$. The kernel of the action of $\tilde{G}$ fixes every line of $\mathbf{H}(4, q^2)$, and so fixes all points, and so lies in $\tilde{Z}$, the subgroup of $\tilde{G}$ fixing all points. Now we see that $(1 + q^3)(1 + q^5)$ divides $|\tilde{G}/\tilde{Z}|$. As $\tilde{G}$ is solvable we can repeat the argument from the previous theorem to obtain a cyclic subgroup $C_{\hat{G}}(R) \leq \hat{G}$ that is the centralizer in $\hat{G}$ of the unique group $R \leq \hat{G}$ of order r, where r is a Z-prime for $q^{10}-1$. We claim that for some prime s dividing q^2-q+1, there is an element of that order in $C_{\hat{G}}(R)$. If false, q^2-q+1 must divide $\left[\tilde{G} : C_{\hat{G}}(R)\right]$ which divides $10a$, where $q = 2^a$. Now q^2-q+1 is odd. Furthermore it is easy to see that 5 does not divide q^2-q+1. If it did, $q \not\equiv 0 \pmod 5$. But $q^2 \equiv \pm 1 \pmod 5$, and if $q^2 \equiv -1 \pmod 5$, then $0 \equiv q^2-q+1 \equiv -q \pmod 5$, a contradiction. Thus $q^2 \equiv 1 \pmod 5$, so $0 \equiv -q+2 \pmod 5$. Hence $q^2 \equiv 4 \pmod 5$, which we already excluded. Consequently if q^2-q+1 divides $10a$, it divides a itself. As $p^a > a$ this is impossible. Thus $C_{\hat{G}}(R)$ contains an element x of order s. The final contradiction can now be derived — see [10] for the necessary details. ■

Theorem 8.2.3 *The GQ* $\mathbf{W}(3,q)$ *does not admit a solvable Singer group.*

Proof. Suppose G is a solvable Singer group of $\mathbf{W}(3,q)$. Let $\tilde{G}$, $\hat{G}$ be defined as in the previous theorem. Let r be a Z-prime for q^4-1, so r divides q^2+1. Then, by Corollary 3.4.5 there exists a group $R \leq \hat{G}$ of order r such that $R \cap Z(\mathbf{GL}_4(q)) = \mathbf{1}$. Suppose r does not divide the order of $\mathbf{F}(\hat{G})$, so $R \cap \mathbf{F}(\hat{G}) = \mathbf{1}$. Then R acts non-trivially on $\mathbf{F}(\hat{G})$ and so we can find a subgroup N of $\mathbf{F}(\hat{G})$ minimal with respect to being normalized but not centralized by R. Since $|R| = r > 4$ we see that N is an extra-special group of order p^{2a+1}, where $p^a = \dim(V) = 4$ and $r-1 = p^a$. Hence N is extra-special of order 32 and $r = 5$. Notice that by the even order of N, q is forced to be odd. If there were some other odd prime r dividing q^2+1 besides 5, then a group R of that order must centralize $\mathbf{F}(\hat{G})$ and so be contained in it and centralize the extra-special N. But that would force N to be cyclic, a contradiction. Thus, $q^2+1 = 2^a 5^b$. Now if $b > 1$, Sylow's theorem would give us a group R^2, of order 25 acting on $\mathbf{F}(\hat{G})$. If it acted faithfully, one would again obtain an elementary abelian or extra-special group faithfully supporting the action of R^2, and this would force $\dim(V) \geq 5 \cdot 4 = 20$, an absurdity. Thus 5 divides q^2+1 to the first power only, and so $q^2+1 = 2^a \cdot 5$. Now $q^2 \equiv 1 \pmod 8$ as q is odd, and so $q^2+1 \equiv 2 \pmod 8$, forcing $q^2+1 = 2 \cdot 5$, and hence $q = 3$, $\mathbf{Q} = \mathbf{W}(3,3)$ and $r = 5$. So we have already produced a subgroup of order $5 \cdot 32$ of $\hat{G}$ and hence a subgroup of order at least $5 \cdot 32/2 = 80$ of G, an absurdity as $\mathbf{W}(3,3)$ contains only 40 points.

Thus in all cases R can be taken to be in the center of an r-Sylow subgroup of $\mathbf{F}(\hat{G})$ and hence must be the unique subgroup of order r

in $\mathbf{F}(\hat{G})$. Hence R is a characteristic subgroup of $\hat{G}$ and so is normal in $\tilde{G}$. Moreover, its centralizer $\hat{C} := C_{\hat{G}}(R)$ is a normal cyclic subgroup of $\hat{G}$ whose index in $\hat{G}$ divides 4 ($= \dim(V)$).

Let $q = p^a$, p prime. Then $\tilde{G}/\hat{G}$ is cyclic of order d, where d divides a. Also $\tilde{G}/(\tilde{G} \cap Z(\mathbf{\Gamma L}(V))) \cong G$ and so has order $(q+1)(q^2+1)$. Then clearly $\left[\tilde{G} : \hat{G} \cap Z(\mathbf{GL}(V))\right]$ is a multiple of $(q+1)(q^2+1)$.

We wish to produce an element x of $C_{\hat{G}}(R)$ whose order divides $q+1$ and which acts with an irreducible submodule of dimension 2. Let q be even. If no element of order a prime divisor of $q+1$ occurs in $\hat{C}$, $q+1$ is prime to $|\hat{C}|$, so that $q+1$ divides $\left|\tilde{G}/\hat{C}\right| = 2^e \cdot d$, with $e \in \{0,1,2\}$. As r_2 is odd it divides d. Since d divides a we have that $q+1 = 2^a+1$ divides a, which is impossible.

Now suppose q is odd. If $C_{\hat{G}}(R)/(\hat{G} \cap Z(\mathbf{GL}(V)))$ has even order, then $C_{\hat{G}}(R)$ contains an element x of order a power of 2, and, because it centralizes R, it acts homogeneously on V. If the $\langle x\rangle$-modules were 1-dimensional, x would lie in $Z(\mathbf{GL}(V)) \cap \hat{G}$. Thus the $\langle x\rangle$-modules are 2-dimensional (for x^2 is a scalar matrix). Similarly, if r_2 is an odd prime divisor of $q+1$ and $|C_{\hat{G}}(R)|$, we may obtain an element x of $C_{\hat{G}}(R)$ acting with irreducible modules of dimension 2, as we were trying to prove.

Thus we may assume that any prime dividing $q+1$ is not a divisor of $|C_{\hat{G}}(R)/(Z(\mathbf{GL}(V)) \cap \hat{G})|$. Thus $q+1$ divides $\left[\tilde{G} : C_{\hat{G}}(R)\right]$, which yields that p^a+1 divides $4d$. Thus p^a+1 divides $4a$, forcing $p^a = q = 3$. Then $\tilde{G} = \hat{G}$ and $r = 5$. So $\left|C_{\hat{G}}(R)/(\hat{G} \cap Z(\mathbf{GL}(V)))\right| \in \{5, 10\}$. If it were 10, then we find an element x as desired by the argument above; if it were 5, then $\left[\hat{G} : \hat{C}\right]$ would be strictly bigger than 4, a contradiction as $\tilde{G} = \hat{G}$. Thus in all cases, there is an element x in $\hat{C}$ whose irreducible modules have dimension 2, all of which are pairwise isomorphic.

We set $R = \langle y\rangle$. Let $\mathbb{K}$ be the field obtained when all n-th roots of unity have been adjoined to $\mathbb{F}_q$. Further, let f^* be the symplectic form on $W := V \otimes \mathbb{K}$ defined by the same 4×4 Grammian matrix over $\mathbb{F}_q$ used to define f. Then f^* is a $\mathbb{K}$-bilinear symplectic form on W. Now there exists an eigenbasis u_1, u_2, u_3, u_4 for the element xy of order $o(x).o(y)$ (recall that $o(x)$ divides $q+1$, and $o(y)$ is an odd divisor of q^2+1, so the orders are relatively prime). The eigenvalues must be conjugate. Thus, if $u_1^x = \theta u_1$ and $u_1^y = \omega u_1$, we see that $\theta, \theta^q = \theta^{-1}$ are the eigenvalues of x, and that $\omega, \omega^q, \omega^{q^2} = \omega^{-1}, \omega^{q^3} = \omega^{-q}$, are the eigenvalues of y. Hence $x \to \mathrm{diag}(\theta, \theta^q, \theta, \theta^q)$ and $y \to \mathrm{diag}(\omega, \omega^q, \omega^{q^2}, \omega^{q^3})$, with respect to the above eigenbasis. Now $f^*(u_1, u_2) = f^*(u_1^y, u_2^y) = \omega.\omega^q f^*(u_1, u_2)$. So if $f^*(u_1, u_2)$ were non-zero, one would have $\omega^{q+1} = 1$, which is false. Similarly, if $f^*(u_1, u_4) \neq 0$, we deduce that $\omega^{1+q^3} = 1 = 1^q = \omega^{q+q^4} = \omega^{q+1}$, a contradiction. If $f^*(u_1, u_3)$ were non-zero, we would see $f^*(u_1, u_3) = f^*(u_1^x, u_3^x) = \theta.\theta f^*(u_1, u_3)$, so $\theta^2 = 1$ and in fact $\theta = 1$ or -1, contradicting the fact that x acts irreducibly on a 2-dimensional space. Thus $f^*(u_1, u_2) = f^*(u_1, u_3) = f^*(u_1, u_4) = 0$. So u_1 is in the radical. But f^* is non-degenerate since its Grammian matrix has independent rows. This contradiction completes the proof. ■

Theorem 8.2.4 *The GQ* $\mathbf{Q}(5, q)$*,* $q > 2$*, does not admit a solvable Singer group.*

Proof. Define the normal series $\tilde{Z}(= \tilde{G} \cap Z(\mathbf{GL}(V))) \leq \hat{G} \leq \tilde{G}$ as in the previous theorems. Thus $\tilde{G}/\tilde{Z} \cong G$, the proposed Singer group. Moreover, $\left[\tilde{G} : \hat{G}\right] = d$ which divides a, where $q = p^a$, and p is the characteristic of the 6-dimensional space V admitting the quadratic form which defines $\mathbf{Q}(5, q)$. Thus $|G| = (q+1)(q^3+1)$.

By Lemma 3.4.8, there exists primes dividing $q^2 - q + 1$ that are distinct from 3. By Corollary 3.4.5, $\hat{G}$ contains an element of order r for each such prime r. Choose such a prime r and an element y of order r in $\hat{G}$. Since r is a Z-prime for $q^6 - 1$, y must act irreducibly on V, and must preserve the quadratic form[1] on V. Now set $R = \langle y \rangle$. As before, since $\dim(V) = 6$, Lemma 3.4.2 can be exploited to show that R is in the center of the Fitting group $\mathbf{F}(\hat{G})$ of $\hat{G}$. Furthermore R is a characteristic subgroup of $\hat{G}$, being the only subgroup of its order to be found. Let $\hat{C}$ denote the centralizer $C_{\hat{G}}(R)$ of R in $\hat{G}$. Now conjugation by elements of $\hat{G}$ induces an automorphism of R that permutes the roots (in some larger field) of the minimal polynomial of degree six, with which y acts. As a result, $\hat{G}/\hat{C}$ has order dividing $6 = \dim(V)$, so $\left[\tilde{G} : \hat{C}\right]$ divides $6a$.

The group G has order divisible by $(q+1)^2$. Let $u^{e(u)}$, $e(u) \geq 1$, be the highest power of the prime u that divides $q + 1$. Suppose, for some integer m, $1 \leq m \leq e(u)$, that $u^{e(u)+m}$ divides the order of $\hat{C}/\tilde{Z}$. Then there are three cases:

[1] The proportionality class of the form has cardinality dividing $q-1$ and so is prime to r.

- $u \neq 2$ and $\hat{C}$ contains an element x of order $u^{e(u)+m}$ and $\langle x\rangle \cap \tilde{Z}$ is the identity group;
- $u = 2$, $e(2) > 1$, $q \equiv 3 \pmod 4$, and $\hat{C}$ contains an element x of order $2^{e(2)+m+1}$ and $\langle x\rangle \cap \tilde{Z} \cong Z_2$ acts on V as scalar multiplication by ± 1;
- $u = 2$, $e(2) = 1$, $q \equiv 1 \pmod 4$, and $\hat{C}$ contains an element x of order 2^{k+m+1}, where $2^k \geq 4$ is the highest power of 2 dividing $q-1$. Here $\langle x\rangle \cap \tilde{Z} \cong Z_{2^k}$ acts as a group of scalar multiplications on V.

In all cases x acts homogeneously on V with irreducible modules of dimension dividing $2u^m$. Thus $2u^m$ divides 6. This forces $u^m = 3$. Since $(q+1)^2$ divides $\left[\tilde{G} : Z(\mathbf{GL}(V))\right]$, we see that $(q+1)/3$ must divide $\left[\tilde{G} : \hat{C}\right]$. Thus

$$p^a + 1 = q + 1 \text{ divides } 18a. \tag{8.1}$$

The solutions to the inequality $p^a < 18a$ are

$$p^a = 3, 5, 7, 3^2, 5^2, 11, 13, 17, 3^3 \text{ and all powers of 2 dividing } 2^6.$$

By hypothesis $p^a = 2$ is excluded. When the exponent a is odd, we must have $q \equiv 1 \pmod 4$ or q even. This requirement excludes $q = 3, 7, 11, 3^3$. We also see that if $q = 13, 3^2$ or 5^2, then $q+1$ cannot divide 18 or $18 \cdot 2$, so Equation (8.1) fails. For q an even power of 2, $q+1$ is not divisible by 3 and so the full value of $q+1$ divides $\left[\tilde{G} : \hat{C}\right]$, and so divides $6a$. But $2^2+1=5$, $2^4+1=17$ and $2^6+1=5\cdot 13$ do not divide $6\cdot 2$, $6\cdot 4$ or $6\cdot 6$, respectively. Also $2^5+1=33$ does not divide $18\cdot 5=90$ and $2^7+1=3\cdot 43$ does not divide $18\cdot 7=126$. Thus Equation (8.1) fails for all powers of 2 except $q=2^3$.

Thus the only cases that remain are $q = 5, 8$ and 17.

We consider the case $q = 17$ first. Here $|G| = 2^2 \cdot 3^5 \cdot 7 \cdot 13$. Choose the Z-prime $r = 7$. We find as above a normal subgroup R of $\hat{C}$ of order 7. Let x be any non-identity element of R. Then the number of conjugates of x in $\hat{G}$ equals the index $\left[\hat{G} : \hat{C}\right]$. On the other hand, as R is normal, x has at most 6 conjugates. It follows that 3^4 must divide

$|C_{\hat{G}}(R)|$. However, as 3^2 is the highest power of 3 dividing $q+1=18$, Corollary 3.4.7 would force 9 to divide $\dim(V)=6$, an absurdity.

Now assume $q=8$. Here $|G|=3^5\cdot 19$. Clearly 19 is the Z-prime and we find a normal Sylow subgroup R of this order. As $\left[\tilde{G}:\hat{G}\right]\in\{1,3\}$ and $\left[\hat{G}:\hat{C}\right]\in\{1,2,3,6\}$, we see that $\left[\tilde{G}:\hat{C}\right]\leq 18$. Hence 3^3 divides the order of $\hat{C}$. As on the other hand 3^4 cannot divide the order of $\hat{C}$ we find that $\hat{C}$ has index 3 in $\hat{G}$, and that $\hat{G}$ has index 3 in $\tilde{G}$. Since $\hat{C}$ is a characteristic subgroup of $\hat{G}$, it is normal in $\tilde{G}$. Let Z be the kernel of the action of $\tilde{G}$ on $\mathbf{Q}(5,8)$. Then $|Z|\in\{1,7\}$. We have a normal series

$$\hat{C}/Z\leq\hat{G}/Z\leq G,$$

where $\hat{C}/Z$ is a cyclic group of order $3^3\cdot 19$ which is normal in G. Now the elements of $G\setminus(\hat{C}/Z)$ act as automorphisms of order 3 or 9 on $\hat{C}/Z$. Hence they act trivially on the unique cyclic subgroup C_{27} of $\hat{C}/Z$ of order 27. We conclude that C_{27} is in the center of G. This contradicts Lemma 3.2.1.

For the case $q=5$, we refer to [10]. ■

8.3 Non-solvable Singer groups

We consider the two cases in which G is a non-solvable Singer group of (i) $\mathbf{W}(3,q)$, q odd, and (ii) of $\mathbf{Q}(5,q)$, q odd. Both GQs are represented by a non-degenerate bilinear form (V,f) over $\mathbb{F}_q$, one symplectic in dimension 4, the other symmetric in dimension 6. The Singer group G is induced by a group $\tilde{G}$ of semilinear transformations which preserve the proportionality class of f; thus for every element $g\in\tilde{G}$ there exists a field automorphism $\sigma(g)$ and scalar $\gamma(g)$ such that

$$f(u^g,v^g)=\gamma(g)\cdot[f(u,v)]^{\sigma(g)},$$

for all vector pairs $(u,v)\in V\times V$. This group contains a normal subgroup $\hat{G}$ of linear transformations of V which preserve the proportionality class of the form f, and the factor group $\tilde{G}/\hat{G}$ is a subgroup of the Galois group $\mathrm{Gal}(\mathbb{F}_q)$, which is a cyclic group of order a where $q=p^a$, for a prime p. Finally, we let $\hat{G}_0$ be the group of isometries of (V,f)

— transformations of V which preserve the form f. We thus have a normal series

$$\hat{G}_0 \leq \hat{G} \leq \tilde{G}.$$

Lemma 8.3.1 *Suppose G is a Singer group of (i) $\mathbf{W}(3,q)$ or (ii) $\mathbf{Q}(5,q)$, q odd, in each case. We suppose G is non-solvable and let $\hat{E} := E(\tilde{G})$ be the layer of $\tilde{G}$ — the product (in G) of the subnormal quasisimple subgroups of $\tilde{G}$. Since $\hat{E}$ is a perfect group, and $\tilde{G}/\hat{G}_0$ is metacyclic, we must have $\hat{E} = E(\hat{G}_0)$.*

We let r be a prime which is an odd divisor of q^2+1 in Case (i), or is a prime distinct from 3 dividing q^2-q+1 in Case (ii). Then a full r-Sylow subgroup of $\hat{G}$ lies in $\hat{E}$.

As a consequence, $\hat{E}$ is itself a quasisimple subgroup. Moreover, $E := \hat{E}/(\hat{E} \cap Z(\hat{G}))$ has an order divisible by the following numbers:

Case (a) $(q^2+1)/2c$, *where c is the greatest common divisor of q^2+1 and $|\tilde{G}/\hat{G}|$, a divisor of a where $q = p^a$;*

Case (b) $(q^2-q+1)/ce$, *where c is the greatest common divisor of $(q^2-q+1)/e$ and $|\tilde{G}/\hat{G}|$, and $e = 3$ or 1 according as $q \equiv -1 \pmod 3$ or not.*

Proof. Let r be a prime chosen as in the second paragraph of the statement of the lemma. We first notice that $\hat{G}$ contains an element of this order. This follows from Corollary 3.4.5.

Now let R_0 be a subgroup of $\hat{G}$ of order r. We claim that we can choose R_0 in $\hat{E}$. So suppose, by way of contradiction, that this is false. The arithmetic conditions on r show that in both cases (i) and (ii), R_0 acts irreducibly on V. Thus the centralizer in $\hat{G}$ of R_0 is a cyclic group $\hat{C}$. Since $\dim(V) = 4$ or 6, Lemma 3.4.2 forces R_0 to centralize every subgroup of order prime to r that it normalizes. The same dimension restrictions show that the number of quasisimple components in $\hat{E}$ is $1, 2$ or 3. But r is odd and cannot be 3 in either case. Thus each quasisimple component of $\hat{E}$ is normalized by R_0. From this situation one proves that $\dim(V)$ is prime, a contradiction (see [10] for details).

It now follows that $R_0 \subseteq \hat{E}_1$. All other quasisimple components of $\hat{E}$ would then centralize R_0 and so would be cyclic and hence not quasisimple. Thus $\hat{E}_1 = \hat{E}$.

Now let R_{00} be the full r-Sylow subgroup of $\hat{E} \cap \hat{C}$, and let R be the full r-Sylow subgroup of $\hat{C}$. Note that R_{00} is an r-Sylow subgroup of $\hat{E}$ and that R is an r-Sylow subgroup of $\hat{G}$. Now $\hat{E}$ is a perfect group. Thus the cyclic r-Sylow R_{00} of $\hat{E}$ is acted on non-trivially by an element x in its normalizer in $\hat{E}$, for otherwise the Burnside Transfer Theorem (Theorem 2.2.1) would provide a non-trivial abelian factor of $\hat{E}$. In fact $[x, R_{00}] = R_{00}$ for the same reason.

We claim that $R = R_{00}$ — that is, the full r-Sylow of $\hat{G}$ lies in $\hat{E}$. Now R lies in $\hat{C}$ which is cyclic, and normalizes $N := N_{\hat{E}}(R_{00})$, as well as $C := \hat{C} \cap \hat{E}$. Thus R acts on the section N/C which has order dividing $r - 1$ (the r' part of the automorphism group of R_{00}). It follows that the action of this r-group is trivial. This means that if y is a generator of R, then $x^{-1}yx = yc$ where $c \in \hat{C}$ and so commutes with y. Since the order of the element on the left hand side of this last equation is a power of r, c must have order an r-power and so must lie in R_{00} since the latter is the unique r-Sylow subgroup of $\hat{E} \cap \hat{C}$. Thus $[x, y] \in R$ and so x normalizes R. Now, since x has order prime to r, and centralizes the section R/R_{00}, we see that $R = R_{00} \times C_R(x)$. As R is cyclic, the equality $R = R_{00} \times C_R(x)$ forces $C_R(x) = \mathbf{1}$, namely $R = R_{00}$.

We now see that except for the powers of r which might divide the exponent a, all the rest of the r-part of G must divide the order of $\hat{E}$. Noting in passing that 4 cannot divide $q^2 + 1$ and that 9 cannot divide $q^2 - q + 1$, we see that except for the divisors 2, 3 and the divisors of these polynomials that can divide the group index $b = [\tilde{G} : \hat{G}]$, which divides a, all other divisors of these polynomials divide $|\hat{E}|$. This proves the lemma. ■

Theorem 8.3.2 *The generalized quadrangles* $\mathbf{W}(3, q)$ *and* $\mathbf{Q}(5, q)$*, for* q *odd, do not admit a non-solvable Singer group.*

Proof. We continue with the same notation as before: (V, f) is the supporting form, the Singer group G is induced by the group of semilinear transformations $\tilde{G}$; $\hat{G}$ is its subgroup of linear transformations preserving the proportionality class of f so that the factor group $\tilde{G}/\hat{G}$ is cyclic of order b, a subgroup of the Galois group of order a, where $q = p^a$.

The previous lemma imposes the following arithmetic constraint on the order of the layer $\hat{E}$. If r is a Z-prime for $q^4 - 1$ or $q^6 - 1$ in the respective Cases (i) and (ii) above, then an r-Sylow subgroup of $\hat{G}$ lies in $\hat{E}$. Since the index $\left[\tilde{G} : \hat{G}\right]$ divides the exponent a, we must have:

$$(q^2+1)/2 \quad \text{divides} \quad \left|\hat{E}\right| \cdot a \text{ (Case (i))}$$
$$(q^2-q+1)/e \quad \text{divides} \quad \left|\hat{E}\right| \cdot a \text{ (Case (ii))}$$

where, in Case (ii), $e = 3$ or 1 according as q is congruent to -1 mod 3 or not.

Now suppose $\hat{E}$ contained an involution t that was not in the center $Z(\mathbf{GL}(V))$. Since q is odd, t acts with eigenvalues ± 1. In Case (i), t must stabilize an isotropic 1-space of V, while not being a scalar transformation — i.e. while inducing a non-trivial action on the $\mathbf{W}(3, q)$. That contradicts the regularity of G. In Case (ii), t stabilizes every 1-space in each of its two eigenspaces, neither of which is trivial (as t is non-central) and one of which has vector space dimension at least three. Then t must stabilize a singular 1-space in the larger eigenspace. That again contradicts the regularity of G.

Thus we must conclude that every involution in $\hat{E}$ lies in the center. But since $\hat{E}$ acts irreducibly (it contains R_0 of the previous lemma) a central involution acts homogeneously — that is, it is scalar multiplication by -1. It is thus clear that $\hat{E}$ contains just one involution t. It follows that a 2-Sylow subgroup of $\hat{E}$ is a generalized quaternion group[2], and so the simple central factor E of $\hat{E}$ has a dihedral 2-Sylow subgroup. We now invoke the theorem of Gorenstein and Walter [14] (see Theorem 2.2.3) to conclude that E is $\mathbf{PSL}_2(k)$, for k odd, or $\mathbf{A}_7$, and that a central extension of it possesses a coprime representation of degree $\dim V = 4$ or 6. The possible central extensions are

$$\mathbf{SL}_2(k),\ 2 \cdot \mathbf{A}_6 = 2 \cdot \mathbf{PSL}_2(9),\ 6 \cdot \mathbf{A}_6 = 6 \cdot \mathbf{PSL}_2(9),$$
$$2 \cdot \mathbf{A}_7 \text{ and } 6 \cdot \mathbf{A}_7.$$

Case (i): Here the degree of the representation of $\hat{E}$ is 4, so we can ignore the $6 \cdot \mathbf{A}_6$ and $6 \cdot \mathbf{A}_7$ where the minimal degrees are 6. The group $\mathbf{SL}_2(k)$ contains a Frobenius group of order $k(k-1)/2$ whose representation has degree $(k-1)/2$ which must be bounded by 4, so $k \leq 9$.

[2]This 2-Sylow subgroup cannot be cyclic since the perfect group $\hat{E}$ possesses a normal 2-complement.

Now by the previous lemma, elements of $\hat{G}$ of odd prime order r, where r divides $(q^2+1)/2$, lie in $\hat{E}$ and act irreducibly on V, while elements of $\mathbf{SL}_2(k)$ of order dividing $k-1$ do not act irreducibly on V. Thus such an r divides the odd part of $k(k+1)$. Assembling such prime power elements in $\hat{G}$ we conclude that $(q^2+1)/2c$ divides the odd part of $k(k+1)$. So we have

$$p^{2a}+1 \text{ divides } k(k+1)^{\text{odd}} \cdot 2a, \tag{8.2}$$

where the symbol n^{odd} always denotes the odd part of the integer n.

Now $k \neq 3$, for then $\hat{E}$ would be solvable. So we have just $k = 5, 7$ and 9, where the rightmost factor in (8.2) is $30a, 14a$ and $90a$, respectively.

If $k = 5$, the prime p cannot be 2, or 5, and so $p = 3$ or $p \geq 7$. We leave the case $p = 3$ as an exercise, but it can also be found in [10]. If $a > 1$, then $q = p^a \geq 7^a > 24a$, and so we have

$$(24a)^2 + 1 < 7^{2a} + 1 \leq p^{2a} + 1 \leq 30a.$$

Comparing the extremes provides an immediate contradiction. Thus we have $a = 1$, and so p^2+1 divides 30, where p is at least 7. This is clearly impossible.

Using (2) and noting that p cannot divide $|E|$, the cases $k = 7, 9$ are excluded analogously.

If $\hat{E} = 2{\cdot}\mathbf{A}_6$, respectively $\hat{E} = 2{\cdot}\mathbf{A}_7$, then $p^{2a}+1$ divides $90a$, respectively $630a$. In the first case the prime p is at least 7, in the second case at least 11, unless, in both cases, $p = 3$ and $a = 1$. (For the latter case, see [10].) One obtains an impossibility as before.

Case (ii): Here the cases $2 \cdot \mathbf{A}_6$ and $2 \cdot \mathbf{A}_7$ are impossible as these have smallest degrees 4 and 8, respectively 4 and 14. First we handle the case that $\hat{E}$ is $\mathbf{SL}_2(k), k$ odd. This time $(k-1)/2 \leq 6$ so $k \leq 13$. We must have

$$q^2 - q + 1 \text{ divides } k(k+1)^{\text{odd}} ae, \tag{8.3}$$

where $e = 3$ if $q \equiv -1 \bmod 3$, and is 1, otherwise. As usual $q = p^a$. With $k \leq 13$, all numbers on the right end of (8.3) are bounded by $273a$. We have $p \geq 5$ which must be coprime to $|\hat{E}|$. If $a > 1$, then $5^a > 12a$. So

$$(12a-1)^2 < (5^a-1)^2 \leq (p^a-1)^2 \leq p^{2a}-p^a+1 < 273a.$$

The extremes of this chain of inequalities yield a contradiction, unless $a = 2$. But in that case $p^4 - p^2 + 1 > 546$, with $p \geq 5$, which yields a contradiction. So we must assume $a = 1$ in all cases. In the cases $k = 13, 11, 9, 7$ and 5, the factor on the right hand side of (8.3) now assumes the respective values $91e, 33e, 45e, 7e$, and $15e$. Since e is one or three, none of the latter numbers is divisible by $49 - 7 + 1 = 43$, $81-9+1 = 73$, $121-11+1 = 111$, $169-13+1 = 157$, or $125-5+1 = 121$. Thus $q \geq 17$ and now $q^2 - q + 1$ surpasses the over-all limit of 273.

This leaves the case that $\hat{E} = 6 \cdot \mathbf{A}_6$ or $6 \cdot \mathbf{A}_7$. In the first case $\hat{E}$ would be a $\{2, 3, 5\}$-group, and there is no prime r for which an element $\hat{E}$ of that prime order could act irreducibly on the 6-dimensional space V. In the second case we find as before that $a = 1$. Hence $p^2 - p + 1$ divides $945e$. One checks that it is impossible to find a prime $p \geq 11$ satisfying this condition.

This completes the proof. ■

As a conclusion of this section we have obtained

Theorem 8.3.3 *If* $\mathbf{Q}$ *is a finite thick classical GQ admitting a Singer group, then* $\mathbf{Q} \cong \mathbf{Q}(5, 2)$. ■

Combining the above theorem and the results of Chapter 7 gives us the conclusion of the main theorem of [10].

Theorem 8.3.4 *Let* $\mathbf{Q}$ *be a known finite thick GQ, and suppose that* $\mathbf{Q}$ *admits a Singer group. Then* $\mathbf{Q}$ *is a Payne-derived GQ.* ■

Chapter 9

Nilpotent Singer Groups

From the moment one knows that one is dealing with a Payne-derived quadrangle admitting a nilpotent Singer group *of class* 2, as when (C) is satisfied, it is possible to say much more about the group. We first need a lemma.

9.1 A lemma

Lemma 9.1.1 *Let G be a nilpotent group of class 2, and let $a, b, c \in G$.*

(i) *For any natural number m, we have that $[a^m, b] = [a, b]^m$.*

(ii) *For any natural number m, we have that*

$$(acb)^m = a^m c^m b^m [b, a]^{m(m-1)/2} [c, a]^{m(m-1)/2} [b, c]^{m(m-1)/2}.$$

Proof. The first part is easy. The second part follows by (i) and induction. ■

9.2 Two theorems

Theorem 9.2.1 *Let $\mathbf{Q} = \mathcal{P}(\mathcal{S}, (\infty))$ be a Payne-derived quadrangle of order $(s-1, s+1)$ admitting a nilpotent Singer group G of class 2. Suppose furthermore that G is induced by an elation group of $\mathcal{S}$ w.r.t. (∞).*

(i) *If* $|G|$ *is odd,* G *is special of exponent* p*,* p *being the prime dividing* $|G|$.

(ii) *If* $|G|$ *is even,* G *is elementary abelian.*

Proof. By [12], s is the power of some prime p. We keep using the same notation if we consider G as an automorphism group of $\mathcal{S}$. Also, remark that the hyperbolic lines on (∞) induce a spread of symmetry of **Q** for which the associated group is contained in G. Note that we can construct a projective plane π of order s from it, as follows:

- the point set is $(\infty)^\perp$;
- the line set is the set of spans $\{q, r\}^{\perp\perp}$, where q and r are different points of $(\infty)^\perp \setminus \{(\infty)\}$, and
- incidence is the natural one.

Then the dual π^D of π defines a translation plane with line at infinity $(\infty)^D$, on which G induces the translation group. So if C is the group of (s) symmetries about (∞), G/C is an elementary abelian p-group. Whence, if $\mathcal{J}$ is the Kantor family corresponding to $(\mathcal{S}^{(\infty)}, G)$ and $A \in \mathcal{J}$,

$$AC/C \cong A$$

is elementary abelian. Also, $[G, G]$ clearly acts trivially on the plane, and so is contained in C. Since $Z(G) \cap [G, G] \neq \{\mathbf{1}\}$, there is some non-trivial element of $Z(G)$ fixing the spread of symmetry of **Q** induced by the hyperbolic lines on (∞) linewise, so each element of $Z(G)$ has this property. Whence

$$Z(G) \leq C.$$

Let A, B, D be distinct elements of $\mathcal{J}$. Then for any $\mathbf{1} \neq z \in Z(G) \leq C$, we can find a, b, d respectively in A, B, D, such that

$$azb = d.$$

Note that d is non-trivial here. By Lemma 9.1.1,

$$(azb)^p = z^p = d^p = \mathbf{1}.$$

So $Z(G)$ is elementary abelian, and $[G, G]$ also is. Now doing the same trick on any element of C, we find that C is elementary abelian. The theorem then follows from [28]. ■

This can be reformulated in terms of skew translation generalized quadrangles:

Theorem 9.2.2 *Let $\mathcal{S}$ be an STGQ of order s with a nilpotent elation group G of class 2.*

(i) *If $|G|$ is odd, G is special of exponent p, p being the prime dividing $|G|$.*

(ii) *If $|G|$ is even, G is elementary abelian, hence $\mathcal{S}$ is a TGQ.* ■

Bibliography

[1] S. G. BARWICK, C. M. O'KEEFE AND L. STORME. Unitals which met Baer subplanesin 1 modulo q points, *J. Geom.* **68** (2000), 16–22.

[2] C. T. BENSON. On the structure of generalized quadrangles, *J. Algebra* **15** (1970), 443–454.

[3] M. BILIOTTI AND G. KORCHMÁROS. Hyperovals with a transitive collineation group, *Geom. Dedicata* **24** (1987), 269–281.

[4] A. H. CLIFFORD. Representations induced in an invariant subgroup, *Ann. Math.* **38** (1937), 533–550.

[5] C.W. CURTIS AND I. REINER. *Methods of representation theory. Vol. I. With applications to finite groups and orders*, Pure and Applied Mathematics, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1981.

[6] M. DE SOETE AND J. A. THAS. A coordinatization of generalized quadrangles of order $(s, s+2)$, *J. Combin. Theory Ser. A* **48** (1988), 1–11.

[7] S. DE WINTER AND K. THAS. Generalized quadrangles with an abelian Singer group, *Des. Codes Cryptogr.* **39** (2006), 81–87.

[8] S. DE WINTER AND K. THAS. The automorphism group of Payne derived quadrangles, *Adv. Math.* **214** (2007), 146–156.

[9] S. DE WINTER AND K. THAS. Generalized quadrangles admitting a sharply transitive Heisenberg group, *Des. Codes Cryptogr.* **47** (2008), 237–242.

[10] S. DE WINTER, E. E. SHULT AND K. THAS. The Singer quadrangles amongst the known finite generalized quadrangles, Submitted.

[11] W. FEIT AND G. HIGMAN. The nonexistence of certain generalized polygons, *J. Algebra* **1** (1964), 114–131.

[12] D. FROHARDT. Groups which produce generalized quadrangles, *J. Combin. Theory Ser. A* **48** (1988), 139–145.

[13] D. GHINELLI. Regular groups on generalized quadrangles and nonabelian difference sets with multiplier -1. *Geom. Dedicata 41* (1992), 165–174.

[14] D. GORENSTEIN AND J.H. WALTER. The characterization of finite groups with dihedral Sylow 2-subgroups. III, *J. Algebra* **2** (1965) 354–393.

[15] M. HALL JR. *The Theory of Groups*, Macmillan, New York, 1959.

[16] W. M. KANTOR. Generalized quadrangles associated with $G_2(q)$, *J. Combin. Theory Ser. A* **29** (1980), 212–219.

[17] W. M. KANTOR. Some generalized quadrangles with parameters q^2, q, *Math. Z.* **192** (1986), 45–50.

[18] G. KORCHMÁROS. Collineation groups transitive on the points of an oval $[(q+2)$-arc] of $S_{2,q}$ for q even, *Atti Sem. Mat. Fis. Univ. Modena* **27** (1978/1979), 89–105.

[19] S. E. PAYNE. Nonisomorphic generalized quadrangles, *J. Algebra* **18** (1971), 201–212.

[20] S. E. PAYNE. The generalized quadrangle with $(s,t) = (3,5)$, *Proceedings of the Twenty-first Southeastern Conference on Combinatorics, Graph Theory, and Computing* (Boca Raton, FL, 1990), *Congr. Numer.* **77** (1990), 5–29.

[21] S. E. PAYNE. Finite groups that admit Kantor families. *Finite Geometries, Groups, and Computation*, 191–202, Walter de Gruyter GmbH & Co. KG, Berlin, 2006.

[22] S. E. PAYNE AND J. E. CONKLIN. An unusual generalized quadrangle of order sixteen, *J. Combin. Theory Ser. A* **24** (1978), 50–74.

[23] S. E. PAYNE AND J. A. THAS. *Finite Generalized Quadrangles*, Research Notes in Mathematics, Pitman Advanced Publishing Program, Boston/London/Melbourne, 1984.

[24] J. A. THAS. Translation 4-gonal configurations, *Rend. Accad. Naz. Lincei* **56** (1974), 303–314.

[25] J. A. THAS AND K. THAS. Translation generalized quadrangles in even characteristic, *Combinatorica* **26** (2006), 709–732.

[26] J. A. THAS, K. THAS AND H. VAN MALDEGHEM. *Translation Generalized Quadrangles*, Series in Pure Mathematics **26**, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2006.

[27] K. THAS. *Symmetry in Finite Generalized Quadrangles*, Frontiers in Mathematics **1**, Birkhäuser Verlag, Basel, 2004.

[28] K. THAS. The elation group of a central skew translation quadrangle is essentially known, Submitted.

[29] K. THAS. *Lectures on Elation Quadrangles*, 100 pp., Submitted.

[30] K. THAS AND H. VAN MALDEGHEM. Geometrical characterizations of Chevalley groups of Type $\mathbf{B}_2$, *Trans. Amer. Math. Soc.* **360** (2008), 2327–2357.

[31] K. THAS AND S. YOSHIARA. Translation generalized ovals and Singer quadrangles, Preprint.

[32] J. TITS. *Buildings of Spherical Type and Finite BN-Pairs*, Lecture Notes in Mathematics **386**, Springer-Verlag, Berlin-New York, 1974.

[33] H. VAN MALDEGHEM. *Generalized Polygons*, Monographs in Mathematics **93**, Birkhäuser Verlag, Basel, 1998

[34] A. WAGNER. Involutions of projective spaces, *Math. Z.* **112** (1969), 37–51.

[35] S. YOSHIARA. A generalized quadrangle with an automorphism group acting regularly on the points, *European J. Combin.* **28** (2008), 653–664.

[36] K. ZSIGMONDY. Zur Theorie der Potenzreste, *Journal Monatshefte für Mathematik* **3** (1892), 265-284.

Index