

5-2023

Automorphisms of a Generalized Quadrangle of Order 6

Ryan Pesak
William & Mary

Follow this and additional works at: <https://scholarworks.wm.edu/honorstheses>



Part of the [Algebra Commons](#), [Discrete Mathematics and Combinatorics Commons](#), and the [Geometry and Topology Commons](#)

Recommended Citation

Pesak, Ryan, "Automorphisms of a Generalized Quadrangle of Order 6" (2023). *Undergraduate Honors Theses*. William & Mary. Paper 1937.
<https://scholarworks.wm.edu/honorstheses/1937>

This Honors Thesis -- Open Access is brought to you for free and open access by the Theses, Dissertations, & Master Projects at W&M ScholarWorks. It has been accepted for inclusion in Undergraduate Honors Theses by an authorized administrator of W&M ScholarWorks. For more information, please contact scholarworks@wm.edu.

Automorphisms of a Generalized Quadrangle of Order 6

A thesis submitted in partial fulfillment of the requirement
for the degree of Bachelor of Science in Mathematics from
William & Mary

by

Ryan Mitchell Pesak

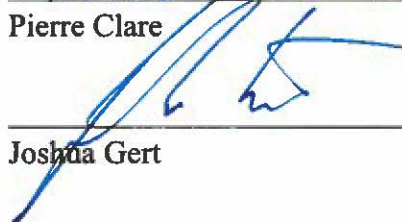
Accepted for HONORS



Eric Swartz, Director



Pierre Clare



Joshua Gert

Williamsburg, VA

May 9, 2023

Automorphisms of a Generalized Quadrangle of Order 6

Ryan Pesak

Abstract

In this thesis, we study the symmetries of the putative generalized quadrangle of order 6. Although it is unknown whether such a quadrangle \mathcal{Q} can exist, we show that if it does, that \mathcal{Q} cannot be transitive on either points or lines. We first cover the background necessary for studying this problem. Namely, the theory of groups and group actions, the theory of generalized quadrangles, and automorphisms of GQs. We then prove that a generalized quadrangle \mathcal{Q} of order 6 cannot have a point- or line-transitive automorphism group, and we also prove that if a group G acts faithfully on \mathcal{Q} such that $259 \mid |G|$, then G is not solvable. Along the way, we develop techniques for studying composite order automorphisms of a generalized quadrangle. Specifically, we deal with automorphisms of order p^k and pq , where p and q are prime.

Acknowledgment

I would like to thank Professor Clare, Professor Gert, and Professor Swartz for serving on my honors committee. I would especially like to thank Professor Swartz, who served as my advisor for this project. His expertise, time, advice, and calming attitude were all invaluable to the project, and helped me stay motivated and optimistic throughout this process. Working on this thesis was a challenging and rewarding experience for me, and I appreciate Professor Swartz for mentoring me through it. Finally, I would like to thank my family and friends for supporting me throughout this experience, and my mother in particular for encouraging me to pursue honors research to begin with.

Contents

1	Introduction	5
2	Group Actions	9
2.1	Basic Facts	9
2.2	Group Actions	14
2.3	Quasiprimitive Actions	20
3	Generalized Quadrangles	23
3.1	Basic Facts	25
3.2	Automorphisms of Generalized Quadrangles	30
3.3	Automorphisms of Prime Order	38
4	A Generalized Quadrangle of Order 6	42
4.1	Bounds on Automorphism Orders	44
4.1.1	Prime Power Automorphism Orders	44
4.1.2	Automorphisms of Order $37p$	49
4.2	Proof of Intransitivity	52
4.3	Solvability	59
A	The Finite Simple K_3-, K_4-, and K_5-Groups	63
	Bibliography	66

List of Figures

3.1	The generalized quadrangle of order 2, taken from [10].	23
3.2	The GQ of order $(2, 1)$ and its dual.	25
3.3	A strongly regular graph with parameters $(10, 3, 0, 1)$	27

Chapter 1

Introduction

A (*finite*) *generalized quadrangle* \mathcal{Q} is a finite geometric structure, similar to a finite projective plane, which consists of a set of points \mathcal{P} , a set of lines \mathcal{L} , and a symmetric point-line incidence relation I between them. In addition, \mathcal{Q} has parameters s and t , and must obey the following axioms:

- (i) There are exactly $s + 1$ points incident to each line, and for each pair of points there is at most one line which is incident to both points in the pair.
- (ii) There are exactly $t + 1$ lines incident to each point, and for each pair of lines there is at most one point which is incident to both lines in the pair.
- (iii) (The GQ Axiom) For a point $P \in \mathcal{P}$ and $\ell \in \mathcal{L}$ with P not incident to ℓ , there exists a unique point P' and a unique line ℓ' such that $P I \ell' I P' I \ell$.

If a generalized quadrangle \mathcal{Q} has $s + 1$ points incident to each line, and $t + 1$ lines incident to each point, we say that \mathcal{Q} has *order* (s, t) , and if \mathcal{Q} has order (s, s) , then we say that \mathcal{Q} has *order* s .

It has been a long-standing problem to develop restrictions on the possible orders (s, t) that a generalized quadrangle can have. The most well known restrictions are that $s + t$ must divide $st(s + 1)(t + 1)$ and that $s \leq t^2$ and $t \leq s^2$ (see Propositions

3.7 and 3.8 respectively). However, these restrictions leave many open cases. Many examples of generalized quadrangles with a variety of different orders exist. In particular, if q is a prime power, then GQs of order (q, q) , (q, q^2) , (q^2, q) , (q^2, q^3) , (q^3, q^2) , $(q + 1, q - 1)$, and $(q - 1, q + 1)$ have all been constructed [7]. The variety of possible orders indicates that the feasible orders of generalized quadrangles follow no obvious pattern, so it is difficult in general to construct or rule out a given order.

One possible GQ order whose feasibility remains open is $(6, 6)$. From the above paragraph, generalized quadrangles of order 1, 2, 3, 4, and 5 have been constructed, so $s = 6$ is the smallest order such that the existence of a GQ of order s is unknown. It is likely that the techniques used to decide the existence of the GQ of order 6 can be generalized to GQs of higher order. This problem has been recognized in [12, Appendix E, Problem 4] to be of import, and so it will be our goal in this thesis to make progress towards solving it.

In pursuit of this goal, we will use techniques relating to group actions and symmetry. Generalized quadrangles were invented by Jaques Tits [11] in order to be acted on by certain classical groups, so it is only natural that group actions play a large role in their study. An automorphism of a GQ is a bijection which maps points to points, lines to lines, and preserves incidence. Naturally, the collection of all automorphisms of a given GQ forms a group, and for the known examples of GQ, such groups are generally large enough to be interesting.

The question we ask is whether the GQ of order 6 – if it exists – admits a point-transitive or line-transitive automorphism group. In [1], Afton and Swartz developed a suite of techniques for studying prime order automorphisms of generalized quadrangles, and then applied those techniques to show that the putative GQ of order $(4, 12)$ cannot have a point- or line-transitive automorphism group. We extend their work to the putative generalized quadrangle of order $(6, 6)$, in order to prove the following result.

Theorem. *Let \mathcal{Q} be a generalized quadrangle of order $(6, 6)$. Then the full automorphism group of \mathcal{Q} is not point-transitive or line-transitive.*

Generalized quadrangles are highly regular structures – all points of a GQ tend to “look the same,” and so group actions on generalized quadrangles tend to be transitive. (That is, generalized quadrangles tend to have the property that for any points P and Q , there exists an automorphism x such that $P^x = Q$.) The fact that no GQ of order 6 has a point- or line-transitive automorphism group serves as a point against the existence of such an object (although this fact does *not* constitute a proof that no such object can exist).

Along the way to this result, we also find a useful technique for dealing with automorphisms of generalized quadrangles structure with prime power order.

Proposition. *Let Ω be a finite set and let $x \in \text{Sym}(\Omega)$ have order p^k , for $k \geq 2$ and p prime. Then if N is the size of the fixed point set of $x^{p^{k-1}}$, then $N \equiv |\Omega| \pmod{p^k}$.*

Although this proposition is phrased purely in the language of group actions, it has particular use for generalized quadrangles. We have access to many tools for studying prime order automorphisms of generalized quadrangles, and we can generally achieve a very sharp restriction on the size of the fixed point sets and fixed line sets of prime order automorphisms. This proposition lets us take automorphism x of prime power order, power it up to a prime order automorphism y , and achieve additional restrictions on the fixed point and fixed line sets of y . This proposition is likely to be applicable in other places where much is known about the prime order automorphisms of some structure.

Finally, we develop a sufficient condition to show that a group acting on a generalized quadrangle of order 6 is not solvable.

Proposition. *Let G be a group acting faithfully on the generalized quadrangle \mathcal{Q} of order 6 such that 7 and 37 divide $|G|$. Then G does not admit a Hall $\{7, 37\}$ -subgroup,*

and in particular, G is not solvable.

It is still unknown whether a GQ of order 6 necessarily has automorphisms of order 7 and 37, so it is still unknown whether or not the full automorphism group of this GQ is solvable.

The rest of this thesis is organized into three chapters and an appendix. Chapter 2 covers the notions of groups, group actions, and quasiprimitive actions, and develops much of the theory we will need to prove our results on the algebraic side. Chapter 3 covers the theory of generalized quadrangles. We prove some basic restrictions on the parameters (s, t) that are feasible for a GQ, and develop a lot of the technology relating to automorphisms of a generalized quadrangle. Chapter 4 is devoted completely to original results, as well as some of the more advanced techniques we need to prove them. We spend Section 4.1 proving the result about prime power automorphisms, and then using it to restrict the possible automorphism orders for the GQ of order 6. In Section 4.2, we prove that the GQ of order 6 is not point-transitive or line-transitive, and in Section 4.3, we prove the sufficient condition for the automorphism group of the GQ of order 6 to be nonsolvable. Finally, in Appendix A, we review the classification of simple groups whose orders have exactly n prime divisors, for $n = 3, 4, 5$.

Chapter 2

Group Actions

2.1 Basic Facts

Groups are essential to the study of any kind of symmetry, so this thesis will largely be concerned with the theory of groups. In this section, we will review many of the basic properties of groups, and state some group-theoretic theorems we will use later.

Definition 2.1. A *group* is an ordered pair (G, \cdot) such that G is a set, \cdot is a binary operation $G \times G \rightarrow G$, and the following axioms hold:

- (i) For every $x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- (ii) There exists an element $1 \in G$ such that for every $g \in G$, $g \cdot 1 = 1 \cdot g = g$.
- (iii) For every $g \in G$, there exists an element $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Example 2.2. The set \mathbb{Z} is a group under the binary operation of addition. For any set K , the set $\text{Sym}(K)$ of bijections $K \rightarrow K$ is a group under function composition.

Now, we establish some notation. Normally, we omit the binary product \cdot in favor of concatenation, i.e., we write $gh = g \cdot h$ for $g \in G$ and $h \in H$. Due to this, we also refer to a group as a set, not as an ordered pair of set and operation. (That is, we say “let G be a group” rather than “let (G, \cdot) be a group.”)

Let $g \in G$ and $n \in \mathbb{Z}$. If $n > 0$, define g^n to be the product of n copies of g . If $n < 0$, define g^n to be the product of $|n|$ copies of g^{-1} , and define $g^0 = 1$. This exponential notation obeys many of the laws one would expect of such notation. In particular for $m, n \in \mathbb{Z}$, $g^{m+n} = g^m g^n$, and $g^{mn} = (g^m)^n$. It is important to note that it does *not* hold in general that $(gh)^n = g^n h^n$ for $g, h \in G$ and $n \in \mathbb{N}$.

The *order* of a group G is the cardinality of the underlying set G . A *subgroup* of a group G is a subset $H \subseteq G$ such that H is a group under the binary operation of G . If H is a subgroup of G , we write $H \leq G$. For a group G with finite order, there is an elegant theorem relating the order G to the order of its subgroups.

Proposition 2.3 (Lagrange's Theorem). *Let G be a finite group and $H \leq G$. Then $|H|$ divides $|G|$.*

To prove this theorem, we must develop the notion of *cosets*. Let G be a group and $H \leq G$. The (*right*) *cosets* of H in G are the sets $Hg = \{hg \mid h \in H\}$ for each $g \in G$. These sets have the nice property that for any $g, g' \in G$, either $Hg = Hg'$ or $Hg \cap Hg' = \emptyset$. Suppose that Hg and Hg' have a nonempty intersection. Say $x \in Hg = Hg'$. Then there exist $h, h' \in H$ such that $hg = x = h'g'$. Since H is a subgroup, then $H = Hh = Hh'$. Thus, $Hg = Hhg = Hh'g' = Hg'$.

So the cosets of H in G are pairwise disjoint, and the coset Hg automatically contains any $g \in G$. Thus, the cosets of H partition G . Noting that the map $h \mapsto hg$ is an invertible map $H \rightarrow Hg$, we see that every coset of H is the same size as H . Since G is partitioned by sets, each of which has size $|H|$, it follows that $|H|$ must divide $|G|$. This proves Lagrange's theorem.

The set of cosets of H in G is labeled G/H . The size of this set, labeled $|G : H|$, is called the *index* of H in G . Lagrange's theorem, then, is the statement that for any group G and $H \leq G$, we have $|G| = |G : H| \cdot |H|$.

An important question to ask is when G/H can be equipped with a group structure in a "natural" way. We would want to evaluate multiplication of cosets by

multiplication of elements in G . That is, we would want $(Hx)(Hy) = Hxy$ for every $x, y \in G$. However, we can, in general have $x' \neq x$ such that $Hx = Hx'$, so this multiplication is not necessarily well defined. (Indeed, for many groups G and many subgroups $H \leq G$, the multiplication $(Hx)(Hy) = Hxy$ is *not* well defined.)

The concept of *normal subgroups* solves this problem. A subgroup $N \leq G$ is called a *normal subgroup* of G if $g^{-1}Ng = N$ for every $g \in G$. If N is a normal subgroup of G , we write $N \trianglelefteq G$.

Proposition 2.4. *Let G be a group and $N \trianglelefteq G$. Then the set G/N is a group with multiplication $(Ng)(Nh) = Ngh$ and identity N . The group G/N is called the quotient of G by N .*

Proof. First, we show that multiplication is well defined. Suppose $Ng = Ng'$ and $Nh = Nh'$. We wish to show that $Ng'h' = Ngh$. Since N is normal in G , then $Ng = gN$. Note that setwise multiplication in groups is associative. So

$$Ng'h' = (Ng')h' = (Ng)h' = (gN)h' = g(Nh') = g(Nh) = (gN)h = (Ng)h = Ngh.$$

Thus, multiplication is well defined in G/N . Associativity, identity, and inverses in G/N are all proven easily from associativity, identity, and inverses in G . \square

Another important question to ask is when two groups are “the same up to relabelling.” A small example is the multiplicative group $G = \{1, i, -1, -i\} \subseteq \mathbb{C}$, and the group $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ of integers modulo 4. In this case, swapping $\bar{0} \leftrightarrow 1$, $\bar{1} \leftrightarrow i$, $\bar{2} \leftrightarrow -1$, and $\bar{3} \leftrightarrow -i$ reveals the same group structure on two different sets. (One may write out the multiplication tables of these groups, and see that up to relabelling, they are the same.) We can identify groups that “are the same up to relabelling” more generally using the concept of *isomorphism*.

Definition 2.5. Two groups G and H are *isomorphic* if there is a bijection $\phi : G \rightarrow H$

such that $\phi(x)\phi(y) = \phi(xy)$ for every $x, y \in G$. If an isomorphism exists between G and H , we say G is *isomorphic* to H , and write $G \cong H$.

Such a map preserves the group structure and serves to identify elements of G and elements of H . Isomorphic groups can be viewed as “essentially the same” or “the same up to relabelling.” As one would expect, \cong is an equivalence relation.

Given a group G , there is an easy way to generate subgroups of G . It can be shown that the intersection of a family of subgroups of G remains a subgroup. Thus, for a subset $A \subseteq G$, we can take the group $\langle A \rangle$, which is the intersection of all subgroups of G containing A . This is particularly useful when A is a singleton. For $x, y \in G$, we abbreviate $\langle x \rangle = \langle \{x\} \rangle$. Then $\langle x \rangle$ is equal to the set $\{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}$.

If G is finite, and $x \in G$, then $\langle x \rangle$ must be finite as well. Therefore, we define the *order* of x , denoted $|x|$, to be the order of $\langle x \rangle$. Although this is a rather elementary notion, it will be of chief importance to the results of this thesis. As such, we outline some facts about group orders and groups of the form $\langle x \rangle$.

- By Lagrange’s Theorem, $|x|$ divides $|G|$ for any $x \in G$.
- If $x \neq 1$, then $|x|$ is the smallest integer n such that $x^n = 1$. This is useful for ascertaining the order of a group element.
- If $|x| = ab$ for some $a, b \in \mathbb{Z}$, then x^a has order b , since $(x^a)^b = x^{ab} = 1$.

Not only is it fruitful to study the order of x , but it is also fruitful to study the group $\langle x \rangle$ itself. Such groups, generated by a single element, are called *cyclic groups*. Cyclic groups are extremely well understood – their isomorphism type and subgroups are completely determined by their size. The following proposition codifies this relationship. The proof of (b) is taken from [4, X.6 Lemma and X.7 Corollary].

Proposition 2.6. *Let $\langle x \rangle$ be a finite cyclic group, and put $|\langle x \rangle| = n$. Then the following hold:*

(a) If \mathbb{Z}_n is the group of integers modulo n , with operation addition modulo n , then $\langle x \rangle \cong \mathbb{Z}_n$.

(b) If $d \mid n$, then there exists a unique subgroup of $\langle x \rangle$ of order d , which is cyclic.

Proof. We leave as an exercise to the reader that the map $\phi : \mathbb{Z}_n \rightarrow \langle x \rangle$ by $n \mapsto x^n$ is well defined, injective, and surjective. We may calculate $\phi(m+n) = x^{m+n} = x^m x^n = \phi(m)\phi(n)$. Therefore, ϕ is an isomorphism. This proves (a).

Next, let $d \mid n$ and put $G_d = \langle x^{n/d} \rangle$. Then $x^{n/d}$ has order d , and so G_d is a cyclic subgroup of G of order d . In order to prove (b), it suffices to show that every subgroup of $\langle x \rangle$ is of the form G_d .

Suppose that $H \leq G$. If $|H| = 1$, then H and G_1 are both trivial and so they are isomorphic. If $|H| > 1$, let k be the smallest positive integer such that $x^k \in H$. For each $x^\ell \in H$, write $\ell = qk + r$ where $0 \leq r < k$. Then, $x^r = (x^k)^{-q} x^\ell \in H$. By minimality of k , we must have $r = 0$, and so $k \mid \ell$. Thus, every element in H is a power of x^k , and so $H = \langle x^k \rangle$. In particular $x^n = x^0 \in H$, so $k \mid n$. Thus, $H = \langle x^k \rangle = \langle x^{n/d} \rangle = G_d$, where $d = n/k$. This proves (b). \square

Let $\langle x \rangle$ be a cyclic group of prime order. Then by the above proposition, the only subgroups of $\langle x \rangle$ are $\{1\}$ and $\langle x \rangle$. Any group G must have subgroups $\{1\}$ and G , but for the case of $\langle x \rangle$, these are the only subgroups. It turns out that this property characterizes cyclic groups of prime order. It is unreasonable to expect that a group in general has no nontrivial subgroups. However, we can ask that a group has no nontrivial *quotients*, and study a broader class of groups.

Definition 2.7. Let G be a group. If the only normal subgroups of G are $\{1\}$ and G , then G is said *simple*.

Such groups have no nontrivial quotients, since a nontrivial quotient of G would imply a nontrivial normal subgroup of G .

Just as the prime numbers can be viewed as the multiplicative building blocks of integers, the simple groups can be viewed as the building blocks of groups. Although it is beyond the scope of this thesis, there is a foundational result called the Jordan-Hölder Theorem, which allows us to uniquely “factor” a group into a series of simple groups. (Two nonisomorphic groups may share the same series of factors, however two groups that have distinct factors cannot be isomorphic.) A proof of this theorem can be found in [9, Theorem 5.11 and Theorem 5.12].

Due to their chief importance in understanding the structure of all groups, it has long been a goal of mathematics to find all of the finite simple groups. Fortunately, this has been done, as a result of the work of hundreds of mathematicians. This theorem, known as the Classification of Finite Simple Groups, is often regarded as one of the crowning achievements of 20th century mathematics.

We will not need the full power of the classification. However, the full classification bears mentioning, since we will use several other classification results which are derived from this larger result. (For instance, we use the classification of simple groups whose orders have only three prime divisors.)

2.2 Group Actions

Groups often arise as the set of symmetries of some structure. Aside from the symmetric group $\text{Sym}(K)$, the famous group D_{2n} of isometries of the regular n -gon also serves as an example. Indeed, the entire field of representation theory is built on viewing groups as symmetries of vector spaces. This connection between groups and symmetry is made rigorous via the concept of *group actions*.

Definition 2.8. Let G be a group and Ω be a set. A *group action* of G on Ω if there is a map $\Phi : \Omega \times G \rightarrow \Omega$ such that

- (i) $\Phi(P, 1) = P$ for every $P \in \Omega$,

(ii) $\Phi(\Phi(P, g), h) = \Phi(P, gh)$ for every $P \in \Omega$ and $g, h \in G$.

If such a Φ exists, we say G acts on Ω .

If G acts on Ω , we abbreviate $\Phi(P, g) = P^g$. Then the two group action axioms may be written more concisely:

(i) $P^1 = P$ for every $P \in \Omega$,

(ii) $(P^g)^h = P^{gh}$ for every $P \in \Omega$ and $g, h \in G$.

Example 2.9. The group $\text{Sym}(\Omega)$ acts on the set Ω by $P^\phi = \phi^{-1}(P)$ for $P \in \Omega$ and $\phi \in \text{Sym}(\Omega)$. Moreover, if G is any group, then G acts on itself via right multiplication. That is, for $g, h \in G$, we set $g^h = gh$.

In this section, we will cover many notions and results relating to group actions and symmetry. The first of these is the orbit. If a group G acts on a set Ω , the *orbit* of $P \in \Omega$ is the set $P^G = \{P^g \mid g \in G\}$. It can be shown that for $P, Q \in \Omega$, either $P^G = Q^G$, or $P^G \cap Q^G = \emptyset$. This is because the relation \sim where $P \sim Q$ exactly when there exists $g \in G$ such that $P^g = Q$ is an equivalence relation on Ω , and the orbit of P is the class of P under this relation. As such, the orbits of all the points in Ω partition Ω .

Another important concept is that of the stabilizer. For a point $P \in \Omega$, the *stabilizer* of P is the group $G_P = \{g \in G \mid P^g = P\}$. It turns out, that the orbit of a point and its stabilizer are deeply related. Indeed, the size of one can be counted using the size of the other. This result, called the Orbit-Stabilizer Theorem, is fundamental to the study of group actions.

Theorem 2.10 (Orbit-Stabilizer). *Let G be a group acting on a set Ω . Then for any $P \in \Omega$, there is a bijection from the set G/G_P to the set P^G . In particular, if G is a finite group, then $|G|/|G_P| = |G : G_P| = |G/G_P| = |P^G|$.*

Proof. Let $\phi : G/G_P \rightarrow P^G$ be defined by $G_P h \mapsto P^h$. We first show that this map is well defined. Suppose $G_P h = G_P h'$. Then there exists $g \in G_P$ such that $gh = h'$. Then,

$$\phi(G_P h) = P^h = (P^g)^h = P^{gh} = P^{h'} = \phi(G_P h').$$

Thus, ϕ is well defined. Next, we show that ϕ is injective. Let $G_P h, G_P h' \in G/G_P$ such that $\phi(G_P h) = \phi(G_P h')$. That is, $P^h = P^{h'}$. Then $P = P^{h'h^{-1}}$, so $h'h^{-1} \in G_P$. Thus, $h' = (h'h^{-1})h \in G_P h$, and so $G_P h = G_P h'$.

Finally, we show that ϕ is surjective. Given any point $P^h \in P^G$, we have that $\phi(G_P h) = P^h$. Thus, ϕ is surjective. Therefore, ϕ is a well-defined bijection from G/G_P to P^G . The result follows. \square

Although we deal with the set G/G_P , it is not necessarily true that $G_P \trianglelefteq G$, and so it does not necessarily hold that G/G_P is a group. However, the primary power of Orbit-Stabilizer is in counting arguments, and so this issue is of little concern.

Another notion we must develop are those of *fixed points* and *invariant sets*. Let G be a group acting on a set Ω . We say that $P \in \Omega$ is a *fixed point* of G if $P^g = P$ for every $g \in G$. We say $U \subseteq \Omega$ is G -invariant if for every $P \in U$, $P^g \in U$ for each $g \in G$. An interesting property of G -invariant sets is that the action of G on Ω may be restricted to a G -action on a G -invariant subset $U \subseteq \Omega$. As such, G -invariant sets are also partitioned by G -orbits, and indeed, the G -orbit of P may be viewed as the smallest G -invariant set containing P .

An important example of a group action is a group G acting on itself via right multiplication. This action has the property that it only has one orbit. Indeed, for any $h \in G$, $h^G = \{hg \mid g \in G\} = hG = G$. This means by Orbit-Stabilizer that $|G_h| = |G|/|h^G| = |G|/|G| = 1$. Thus, the stabilizer of any point is trivial. Finally, we can note that the only $g \in G$ for which $h^g = h$ for all $h \in G$ is $g = 1$. These properties of the action of G on itself by right multiplication may be generalized,

inspiring the following definitions.

Definition 2.11. Let G act on a set Ω .

- We say G acts *transitively* on Ω if there is a unique G -orbit on Ω . That is, G acts transitively on Ω if for every $P, Q \in \Omega$ there exists $g \in G$ such that $P^g = Q$.
- We say that G acts *semiregularly* or *fixed point freely* on Ω if the stabilizer of every point P is trivial. That is, G acts fixed point freely on Ω if $P^g = P$ implies $g = 1$ for every $P \in \Omega$.
- If G acts on Ω semiregularly and transitively, we say that G acts *regularly* on Ω .
- The *kernel* of the action of G on Ω is the set $K = \{g \in G \mid P^g = P \text{ for every } P \in \Omega\}$. If $K = \{1\}$, we say G acts *faithfully* on Ω .

Remark 2.12. Upon seeing the definition of a faithful action, one may wonder in what sense faithful actions are faithful. Let G act faithfully on Ω , and consider the map $\rho : G \rightarrow \text{Sym}(\Omega)$ given by $\rho(g) : P \mapsto P^g$. Since G acts faithfully on Ω , we can show that the map ρ is injective. Note that for $g, h \in G$ and $P \in \Omega$, $P^{\rho(g)\rho(h)} = (P^{\rho(g)})^{\rho(h)} = (P^g)^h = P^{gh} = P^{\rho(gh)}$. Thus, $\rho(gh) = \rho(g)\rho(h)$. Also, we can immediately see that $\rho(g)^{-1} = \rho(g^{-1})$. Then if $g, h \in G$ such that $\rho(g) = \rho(h)$, we have

$$P^{gh^{-1}} = (P^{\rho(g)})^{h^{-1}} = (P^{\rho(g)})^{\rho(h)^{-1}} = P.$$

for every $P \in \Omega$. This means that if K is the kernel of the action of G , then $gh^{-1} \in K$. However, G acts faithfully, so $gh^{-1} = 1$. Therefore, $g = h$, and so ρ is injective.

The result of this discussion is that each $g \in G$ may be uniquely identified with a bijection on Ω . Since the map ρ is isomorphic onto its image, G is isomorphic to a subgroup of $\text{Sym}(\Omega)$. Since ρ never sends distinct elements of G to the same place, the action of G on Ω is said *faithful*.

Suppose that G acts regularly on Ω . Then, fixing a distinguished point $P \in \Omega$, the map $g \mapsto P^g$ is a bijection from G to Ω . (The map is surjective by transitivity of the action and injective, otherwise P would have a nontrivial stabilizer.) Thus, the elements of G may be identified with the elements of Ω , so it is as if G acts on itself. In this way, the regular action of G on Ω directly generalizes the right multiplication action of G on itself.

The right multiplication action of G on itself has applications in pure group theory. Specifically, it may be applied to prove a very powerful theorem providing a partial converse to Lagrange's Theorem. The proof we show is due to Wielandt, and is printed in [4, 1.7. Theorem].

Theorem 2.13 (Sylow E). *Let G be a finite group and p be a prime dividing $|G|$. If we write $|G| = p^a m$ where $p \nmid m$, then G has a subgroup X of order p^a . Such a group is called a Sylow p -subgroup of G .*

Proof. Let Ω be the set of subsets of G having cardinality p^a . Then G acts on Ω via right multiplication. Then Ω is partitioned into G -orbits. It is an exercise in combinatorics to prove that $\binom{p^a m}{p^a} \equiv m \pmod{p}$, and a proof may be seen in [4, 1.8 Lemma]. Then

$$|\Omega| = \binom{p^a m}{p^a} \equiv m \not\equiv 0 \pmod{p},$$

and so there must be an orbit \mathcal{O} with length not divisible by p . Now let $X \in \mathcal{O}$. Then by Orbit-Stabilizer, $|\mathcal{O}| = |G|/|G_X| = p^a m/|G_X|$. Thus, $p^a \mid |G_X|$, otherwise $p \mid |\mathcal{O}|$. In particular, $|G_X| \geq p^a$. Since G_X stabilizes X under multiplication, then for any $y \in X$, $yG_X \subseteq X$. Thus, $|G_X| = |yG_X| \leq |X| = p^a$. Thus, $|G_X| = p^a$, and the result follows. \square

Corollary 2.14. [4, 1.9 Corollary] Let G be a finite group and p a prime dividing $|G|$. Then G has an element of order p .

Proof. Let X be a Sylow p -subgroup of G . Since $|X|$ is the largest power of p dividing

G , then X is nontrivial. So take some nonidentity $x \in X$. Then $\langle x \rangle$ is a cyclic group. By Lagrange's Theorem, $|\langle x \rangle|$ divides $|X|$, so $|\langle x \rangle|$ is a power of p . If we put $|\langle x \rangle| = p^a$, then $|x| = p^a$. Therefore, if we put $y = x^{p^{a-1}}$, then $y^p = (x^{p^{a-1}})^p = x^{p^a} = 1$. Thus, y is order p as desired. \square

Another way G can act on itself is via conjugation. For $g, h \in G$, we set $g^h = h^{-1}gh$. It is important to note that the conjugation action of G on itself is different than the right multiplication action of G on itself. Indeed, the singleton $\{1\}$ is an orbit in the former action, whereas in the latter action it is not.

The interesting thing about the conjugation action of G on itself is that the map $x \mapsto x^g$ is an isomorphism from G to G . Since isomorphisms from a group to itself are often called *automorphisms*, then G can be said to *act via automorphisms* on itself. This concept comes into play with another useful theorem about Sylow subgroups. The proof is, again, taken from [4, 1.11 Theorem].

Theorem 2.15 (Sylow C). *Let P be an arbitrary p -subgroup of a finite group G , and let X be a Sylow p -subgroup of G . Then $P \leq X^g$ for some $g \in G$. In particular, if P is another Sylow p -subgroup of G , there exists $g \in G$ such that $P = X^g$.*

Proof. Let $\Omega = \{Xy \mid y \in G\}$. Since X is a Sylow p -subgroup of G , then $|\Omega| = |G : X|$ is not divisible by p . Since G acts by right multiplication on Ω , and $P \leq G$, then P does as well. As such, Ω is partitioned into P -orbits. Since $|\Omega|$ is not divisible by p , there must exist some P -orbit \mathcal{O} whose length is not divisible by P . By Orbit-Stabilizer, $|\mathcal{O}|$ divides $|P|$, and so $|\mathcal{O}|$ must be a power of p . The only power of p not divisible by p is 1, so $|\mathcal{O}| = 1$.

Since the members of Ω are cosets of X , and \mathcal{O} is a singleton subset of Ω , we can label Xg the unique member of \mathcal{O} . That is, Xg is a fixed point of P . So for any $u \in P$, $Xgu = Xg$. Then $gu \in Xg$, and so $u \in g^{-1}Xg$. Thus, $P \subseteq g^{-1}Xg = X^g$ as desired.

In the case that P is a Sylow p -subgroup, then since the order of P is equal to the order of X^g , then $P = X^g$. \square

Let P and X be Sylow p -subgroups of G and retrieve $g \in G$ such that $P = X^g$. Then the map $x \mapsto x^g$ is a bijection from X to P . However, this bijection is also an isomorphism, so X is isomorphic to P . We have therefore proven that all Sylow p -subgroups of G are isomorphic.

We will use Sylow C to prove a technical-sounding but surprisingly applicable lemma known as the Frattini Argument. In order to understand this lemma, we must develop the notion of normalizers.

Definition 2.16. Let G be a group and $H \leq G$. The group $N_G(H) = \{g \in G \mid g^{-1}Hg = H\}$ is called the *normalizer* of H in G .

For G a group and $H \leq G$, $N_G(H)$ is the largest subgroup of G in which H is normal. The Frattini Argument follows, and the proof is taken from [4, 1.13 Lemma].

Lemma 2.17 (The Frattini Argument). *Let G be a group, $N \trianglelefteq G$, and P a Sylow p -subgroup of N . Then $G = N_G(P)N$.*

Proof. Choose $g \in G$ arbitrarily, and note that $P^g \subseteq N^g = g^{-1}Ng = N$. Thus, P^g is a subgroup of N which is isomorphic to P . Then P^g is a Sylow p -subgroup of N . It follows by Sylow C that there exists $n \in N$ such that $P^{g^n} = P$. Since $(gn)^{-1}P(gn) = P^{g^n} = P$, it follows that $gn \in N_G(P)$. Therefore, $g \in N_G(P)n^{-1} \subseteq N_G(P)N$. Since $g \in G$ was chosen arbitrarily, it follows that $G \subseteq N_G(P)N$. \square

2.3 Quasiprimitive Actions

In this section, we briefly review the notions of primitivity and quasiprimitivity from the theory of permutation groups, as well as state a theorem restricting the types of groups that can act quasiprimitively.

Definition 2.18. Let G be a group acting transitively on a set Ω . A *block* is a subset $\Delta \subseteq \Omega$ such that for any $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. A block Δ is called *trivial* if either Δ is a singleton or $\Delta = \Omega$. If the only blocks for G on Ω are trivial, we say that G acts *primitively* on Ω , or that G is *primitive*.

Example 2.19. Let G be a group acting on itself by right multiplication. Then each subgroup $H \leq G$ is a block for G . If G is cyclic of prime order, then G acts primitively on itself.

Suppose G is a group acting faithfully and transitively on a set Ω . Suppose further that G has a nontrivial normal subgroup N which is not transitive on Ω . Then take any $P \in \Omega$ and consider the orbit P^N . We see that for any $g \in G$,

$$(P^N)^g = P^{Ng} = P^{gN} = (P^g)^N.$$

So raising the orbit P^N to the power of G gives us another N -orbit. Since the N -orbits of Ω partition Ω , then either $(P^N)^g = P^N$, or $P^N \cap (P^N)^g = \emptyset$. As such the set P^N is a block for Ω . Indeed, since we assumed N not transitive, there are multiple such blocks, and since N is a nontrivial group that acts faithfully on Ω , each N -orbit has size larger than 1. This shows that P^N is a *nontrivial* block on Ω . Thus, the action of G on Ω is not primitive.

Not every block of a group action can necessarily be induced from a non-transitive nontrivial normal subgroup of G . However, many of the properties of primitive actions can be attained by disallowing these types of blocks. This inspires the following definition.

Definition 2.20. Let G be a group acting faithfully and transitively on a set Ω . We say G acts *quasiprimatively* on Ω if every nontrivial normal subgroup of G is transitive.

Since the block P^N is nontrivial if and only if N is not transitive or N is trivial, then P^N must be a trivial block if G acts quasiprimatively on Ω .

If a group G acts quasiprimitively on a set Ω , we can say a lot about its structure. Praeger [8] proved a powerful restriction on the types of groups that can act quasiprimitively. However, we need a couple definitions in order to understand this restriction. Let G be a group. A *minimal normal subgroup* is a nontrivial normal subgroup $N \trianglelefteq G$ such that there is no normal subgroup $H \trianglelefteq G$ with $\{1\} < H < N$. The *socle* of G is the setwise product of all minimal normal subgroups of G . Note that the socle of G is itself a normal subgroup of G . So if G is quasiprimitive, then the socle of G must be transitive. Finally, define $\text{Aut}(G)$ to be the set of all isomorphisms $G \rightarrow G$.

Note that if T is a nonabelian simple group, then T acts on itself via conjugation. Since T acts nontrivially on itself, T must also act faithfully on itself, since the kernel of any group action is a normal subgroup. Thus, T is isomorphic to a subgroup of $\text{Sym}(T)$. However, T acts on itself via conjugation, so each $t \in T$ is sent to an automorphism of T . Thus, T is isomorphic to a subgroup of $\text{Aut}(T)$, and so we may write $T \leq \text{Aut}(T)$ by abuse of notation.

We are now ready to state Praeger's restriction on quasiprimitive groups. The theorem Praeger proves has many conclusions which are beyond the scope of this thesis, so we omit them for the sake of brevity.

Theorem 2.21. [8, Theorem 1] Let G be a finite group acting quasiprimitively on a set Ω , and let B be the socle of G . Then $B \cong T^k$ for a finite simple group T , and one of the following holds:

- (I) $T \cong \mathbb{Z}_p$, B is the unique minimal normal subgroup of G , and B acts regularly on Ω . In particular, $|\Omega| = p^k$.
- (II) $k = 1$, T is a nonabelian simple group, and $T \leq G \leq \text{Aut}(T)$.
- (III) $k \geq 2$ and T is a nonabelian simple group.

Chapter 3

Generalized Quadrangles

The primary object of study in this thesis will be finite geometric structures called *generalized quadrangles*. Similar to finite projective planes, these structures consist of a set of *points*, a set of *lines*, and an incidence relation governing which points are incident to which lines, and which lines are incident to which points. However, generalized quadrangles are subject to more axioms, which we outline in the following definition.

Definition 3.1. A *generalized quadrangle* (or GQ) of order (s, t) is an ordered trio $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, I)$ where \mathcal{P} and \mathcal{L} are disjoint nonempty sets, which we view as the set of *points* and *lines* respectively. The relation I is a symmetric incidence relation between

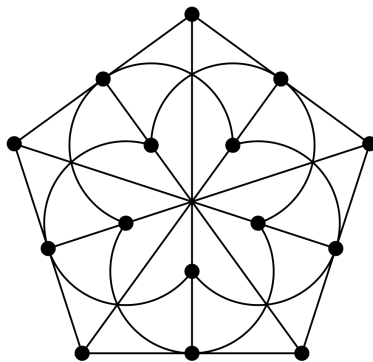


Figure 3.1: The generalized quadrangle of order 2, taken from [10].

\mathcal{P} and \mathcal{L} such that the following axioms hold:

- (i) There are exactly $s + 1$ points incident to each line, and for each pair of points there is at most one line which is incident to both points in the pair.
- (ii) There are exactly $t + 1$ lines incident to each point, and for each pair of lines there is at most one point which is incident to both lines in the pair.
- (iii) (The GQ Axiom) For a point $P \in \mathcal{P}$ and $\ell \in \mathcal{L}$ with P not incident to ℓ , there exists a unique point P' and a unique line ℓ' such that $P \text{ I } \ell' \text{ I } P' \text{ I } \ell$.

If \mathcal{Q} has order (s, s) , we say that \mathcal{Q} is a generalized quadrangle of order s .

An important observation to make is that switching the words “line” and “point” in the previous definition gives an equivalent condition. Therefore, we may switch the roles of lines and points, and the resulting structure will still be a generalized quadrangle. Also, if $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \text{I})$ is a GQ of order (s, t) , then $\mathcal{S} = (\mathcal{L}, \mathcal{P}, \text{I})$ must be a GQ of order (t, s) . This result – called *duality* – is vitally important to the study of generalized quadrangles.

Similarly to the case of groups, we can tell that two generalized quadrangles have the same structure via a map called an *isomorphism*.

Definition 3.2. Let $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \text{I})$ and $\mathcal{Q}' = (\mathcal{P}', \mathcal{L}', \text{I}')$. An *isomorphism* from \mathcal{Q} to \mathcal{Q}' is a bijection $\phi : \mathcal{P} \cup \mathcal{L} \rightarrow \mathcal{P}' \cup \mathcal{L}'$ which sends points to points, lines to lines, and preserves incidence. That is, for every $P \in \mathcal{P}$ and $\ell \in \mathcal{L}$, $\phi(P) \in \mathcal{P}'$, $\phi(\ell) \in \mathcal{L}'$, and $P \text{ I } \ell$ if and only if $\phi(P) \text{ I}' \phi(\ell)$. If there exists an isomorphism between two GQs \mathcal{Q} and \mathcal{Q}' , we say that \mathcal{Q} and \mathcal{Q}' are *isomorphic*.

Since an isomorphism preserves points, lines, and the incidence relation, it preserves all of the structure of a GQ. Like isomorphic groups, isomorphic GQs can be thought of as “the same up to relabelling.”

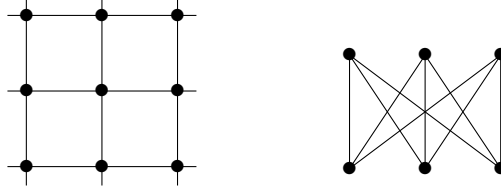


Figure 3.2: The GQ of order $(2, 1)$ and its dual.

Example 3.3. Pictured in Figure 3.1 is the generalized quadrangle \mathcal{Q} of order $(2, 2)$, often referred to as “The Doily.” This quadrangle has 3 lines incident to each point, 3 points incident to each line, 15 total lines, and 15 total points. This is the smallest example of a *thick* generalized quadrangle, i.e., a quadrangle of order (s, t) where $s > 1$ and $t > 1$. There is a unique GQ of order $(2, 2)$, so \mathcal{Q} is isomorphic to its dual.

Example 3.4. A *grid* with parameters (a, b) is an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathbf{I})$ with point set $\mathcal{P} = \{P_{ij} \mid 0 \leq i \leq a, 0 \leq j \leq b\}$ and line set $\mathcal{L} = \{\ell_0, \dots, \ell_a, m_0, \dots, m_b\}$, where $P_{ij} \mathbf{I} \ell_k$ iff $k = i$ and $P_{ij} \mathbf{I} m_k$ iff $k = j$. A *dual grid* with parameters (a, b) , as the name suggests, is a structure obtained by switching the roles of points and lines for a grid with parameters (a, b) .

A grid with parameters (a, a) is a generalized quadrangle of order $(a, 1)$, since each line would then be incident to exactly $a + 1$ points, and each point would be incident to exactly 2 lines. Similarly, a dual grid with parameters (a, a) must be a generalized quadrangle of order $(1, a)$. See Figure 3.2 for the $a = 2$ case.

If two points P_1 and P_2 of a generalized quadrangle are incident to a common line, we say they are *collinear* and write $P_1 \sim P_2$. Similarly, if two lines ℓ_1 and ℓ_2 are incident to a common point, we say that ℓ_1 is *concurrent* to ℓ_2 and write $\ell_1 \sim \ell_2$.

3.1 Basic Facts

We will now prove some basic facts about generalized quadrangles which will be of use later. First and foremost, we can calculate the number of points (or lines) in a

generalized quadrangle in terms of its order.

Proposition 3.5. [7, 1.2.1] Let $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \text{I})$ be a generalized quadrangle of order (s, t) . Then $|\mathcal{P}| = (s + 1)(st + 1)$ and $|\mathcal{L}| = (t + 1)(st + 1)$.

Proof. Let $v = |\mathcal{P}|$ and $w = |\mathcal{L}|$. First, we show that $v = (s + 1)(st + 1)$. Fix a line $\ell \in \mathcal{L}$. We will count the number N of ordered pairs $(P, m) \in \mathcal{P} \times \mathcal{L}$ with $P \not\sim \ell$, $P \text{ I } m$, and $m \sim \ell$.

First, fixing a point $P \not\sim \ell$, then by axiom (iii), there is exactly one line m such that $P \text{ I } m$ and $m \sim \ell$. Therefore, the ordered pairs (P, m) are in bijection with the number of points not on ℓ . Thus, $N = v - (s + 1)$.

Next, we count this quantity a different way. There are $s + 1$ points on ℓ , and each such point is incident to t lines $m \neq \ell$. On each line m , there are s points not incident to ℓ . This makes for $(s + 1)st$ ordered pairs (P, m) such that $m \sim \ell$, $m \text{ I } P$, and $P \not\sim \ell$. Thus $N = (s + 1)st$.

Since $v - (s + 1) = N = (s + 1)st$, then $v = (s + 1)(st + 1)$ as desired. To conclude that $w = (t + 1)(st + 1)$, we need only apply duality. We just proved that the quadrangle $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \text{I})$ of order (s, t) has $(s + 1)(st + 1)$ points. However, we may apply this same logic to show that the quadrangle $\mathcal{S} = (\mathcal{L}, \mathcal{P}, \text{I})$ of order (t, s) has $(t + 1)(st + 1)$ points. Thus, $w = |\mathcal{L}| = (t + 1)(st + 1)$ as desired. \square

A generalized quadrangle \mathcal{Q} has an underlying graph Γ associated to it, where the vertices of Γ are the points of \mathcal{Q} , and the edges of Γ are the pairs $\{P, Q\}$ such that $P \neq Q$ and $P \sim Q$. The graph Γ is called the *point graph* of \mathcal{Q} .

One may easily count that there are exactly $(t + 1)s$ points collinear with a given point P , so Γ is regular of valency $(t + 1)s$. Given a pair of collinear points P and Q , we may also count that there are exactly $s - 1$ points collinear to both, since all the point collinear to P and Q are contained on one line. Finally, we may count the number of points collinear with both P and Q when $P \not\sim Q$, of which there are $t + 1$.

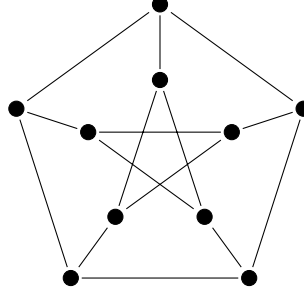


Figure 3.3: A strongly regular graph with parameters $(10, 3, 0, 1)$.

The fact that these quantities are constant motivates the following definition.

Definition 3.6. A *strongly regular graph* with parameters (v, k, λ, μ) is a graph Γ such that Γ has exactly v vertices, every vertex of Γ has exactly k neighbors, each pair of vertices with an edge between them has exactly λ mutual neighbors, and each pair of vertices with no edge between them has exactly μ mutual neighbors.

By the above discussion, it becomes clear that the point graph Γ of a generalized quadrangle \mathcal{Q} is a strongly regular graph with parameters $((s+1)(st+1), (t+1)s, s-1, t+1)$. This relation allows us to use graph theoretic techniques to study generalized quadrangles, and vice versa. The following proposition is a demonstration of this fact.

Proposition 3.7. [7, 1.2.2] Let $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \text{I})$ be a generalized quadrangle of order (s, t) . Then $s+t$ divides $st(s+1)(t+1)$.

Proof. Let $\Gamma = (\mathcal{P}, E)$ be the point graph of \mathcal{Q} , and label $v = (s+1)(st+1)$ and $\mathcal{P} = \{P_1, P_2, \dots, P_v\}$. Define a $v \times v$ matrix $A = (a_{ij})$ where $a_{ij} = 1$ if $\{P_i, P_j\} \in E$, and $a_{ij} = 0$ otherwise. That is, $a_{ij} = 1$ exactly when $i \neq j$ and $P_i \sim P_j$. Then A is called the *adjacency matrix* of Γ .

Label $A^2 = (c_{ij})$. Then the entry c_{ij} counts the number of points collinear with both P_i and P_j . Since Γ is a strongly regular graph with parameters $((s+1)(st+1), (t+1)s, s-1, t+1)$, this means $c_{ii} = (t+1)s$, $c_{ij} = s-1$ if $P_i \neq P_j \sim P_i$, and $c_{ij} = t+1$ if $P_i \not\sim P_j$. As such, $A^2 - (s-t-2)A - (t+1)(s-1)I = (t+1)J$, where

I is the $v \times v$ identity matrix, and J is the $v \times v$ matrix whose entries are constantly equal to 1.

Now, we study the eigenvalues of A . Since the valency of Γ is constantly equal to $(t+1)s$, the row sum of A is constantly equal to $(t+1)s$. Thus, if $u = [1, \dots, 1]^T$, then $Au = (t+1)su$, and so $(t+1)s$ is an eigenvalue of A . Taking the matrix J as a linear map $\mathbb{R}^v \rightarrow \mathbb{R}^v$, we see immediately that the rank of J is 1, so the nullity of J is $v-1$. Therefore, J has the eigenvalue 0 with multiplicity $v-1$. Since $Ju = vu$, then J has the eigenvalue v with multiplicity 1.

Since $((t+1)s)^2 - (s-t-2)((t+1)s) - (t+1)(s-1) = (t+1)(st+1)(s+1) = (t+1)v$, the eigenvalue $(t+1)s$ of A corresponds with the eigenvalue v of J , and so $(t+1)s$ has multiplicity 1. This entails that the other eigenvalues of A are roots of the equation $x^2 - (s-t-2)x - (t+1)(s-1) = 0$. Denote the multiplicities of these eigenvalues θ_1, θ_2 by m_1, m_2 respectively. Solving this polynomial, we have $\theta_1 = -t-1$ and $\theta_2 = s-1$, $v = 1 + m_1 + m_2$, and $s(t+1) - m_1(t+1) + m_2(s-1) = \text{tr}(A) = 0$. Solving this system, we get $m_1 = s^2(st+1)/(s+t)$ and $m_2 = st(s+1)(t+1)/(s+t)$. Since m_1 and m_2 are integers, the result follows. \square

Aside from demonstrating the effectiveness of graph theoretic techniques on the study of generalized quadrangles, this lemma provides a useful restriction on the feasible (s, t) pairs such that a GQ of order (s, t) exists. Another popular restriction on the parameters s and t exists, however, we will not use it in this thesis. As such, we merely state it without proof.

Proposition 3.8. [7, 1.2.3 and 1.2.5] Let \mathcal{Q} be a generalized quadrangle of order (s, t) . If $s > 1$ and $t > 1$, then $s \leq t^2$ and $t \leq s^2$. Furthermore, if $s \neq t^2$, then $s \leq t^2 - t$, and if $t \neq s^2$, then $t \leq s^2 - s$.

When we study any sort of mathematical structure, it is natural to look at substructures of the same type. For graphs, these are subgraphs, for vector spaces, these

are subspaces, and for groups, these are subgroups. For generalized quadrangles, we have the notion of *subquadrangles*.

Definition 3.9. If $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \mathbf{I})$ is a generalized quadrangle, then \mathcal{S} is a *subquadrangle* of \mathcal{Q} if $\mathcal{S} = (\mathcal{P}', \mathcal{L}', \mathbf{I}')$ is a generalized quadrangle such that $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{L}' \subseteq \mathcal{L}$, and \mathbf{I}' is the restriction of \mathbf{I} to \mathcal{P}' and \mathcal{Q}' . If \mathcal{P}' is a proper subset of \mathcal{P} or \mathcal{L}' is a proper subset of \mathcal{L} , we say that \mathcal{S} is a *proper subquadrangle* of \mathcal{Q} .

It is easy to see that if \mathcal{Q} is a GQ of order (s, t) , \mathcal{S} is a proper subquadrangle of \mathcal{Q} , and \mathcal{S} has order (s', t') , then either $s' < s$ or $t' < t$. For, if $s' = s$ and $t' = t$, then \mathcal{S} has $(s+1)(st+1)$ points and $(t+1)(st+1)$ lines, implying that $\mathcal{P}' = \mathcal{P}$ and $\mathcal{S}' = \mathcal{S}$.

The following proposition restricts the size of a subquadrangle of a GQ \mathcal{Q} in terms of the order of \mathcal{Q} .

Proposition 3.10. [7, 2.2.1] Let $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \mathbf{I})$ be a generalized quadrangle of order (s, t) and $\mathcal{S} = (\mathcal{P}', \mathcal{L}', \mathbf{I}')$ be a proper subquadrangle of \mathcal{Q} , with order (s', t') . If $s' < s$ and $t' < t$, then $s \geq s't'$ and $t \geq s't'$.

Proof. If P is a point in \mathcal{Q} such that P is incident to a line in \mathcal{L}' , but $P \notin \mathcal{P}'$, we say P is *tangent* to \mathcal{Q}' . We can quickly count that there are $(t'+1)(s't'+1)(s-s')$ such points in \mathcal{Q} . If P is not tangent to \mathcal{Q}' and not a point in \mathcal{Q}' , we say that P is *external* to \mathcal{Q}' . If V is the set of points external to \mathcal{Q} , we can count $|V| = (s+1)(st+1) - (s'+1)(s't'+1) - (t'+1)(s't'+1)(s-s')$.

Put $|V| = d$ label $V = \{P_1, \dots, P_d\}$, and let t_i be the number of points of \mathcal{P}' that are collinear with P_i . We count the number of ordered pairs (P_i, Q) such that $P_i \in V$, $Q \in \mathcal{P}'$, and $P_i \sim Q$. Naïvely, the total works out to $\sum_i t_i$, but we can count it another way. For each point $Q \in \mathcal{P}'$, there are $t - t'$ lines incident to Q which are not in \mathcal{L}' . On each such line, there are s points which are not Q , each of which is

external to \mathcal{Q}' . Every external point has such a Q and such a line, so the total also works out to $(s' + 1)(s't' + 1)(t - t')s$. Thus, $\sum_i t_i = (s' + 1)(s't' + 1)(t - t')s$.

Similarly, count the number of ordered triples (P_i, Q, Q') such that $P_i \in V$, $Q, Q' \in \mathcal{P}'$, $Q \sim P_i \sim Q'$, and $Q \neq Q'$. By a similar counting argument to the above paragraph, we obtain the equality $\sum_i t_i(t_i - 1) = (s' + 1)(s't' + 1)s'^2 t'(t - t')$. Combining this equality with the equality achieved in the previous paragraph, we obtain the identity $\sum_i t_i^2 = (s' + 1)(s't' + 1)(t - t')(s + s'^2 t')$.

Since the average of the squares of a sequence of numbers is greater than or equal to the square of the average of that sequence of numbers, we can derive the inequality $d \sum_i t_i^2 - (\sum_i t_i)^2$. Applying algebra to this, we obtain the inequality $(s' + 1)(s't' + 1)(st + s'^2 t'^2)(t - t')(s - s')(s - s't') \geq 0$. Since $t - t' > 0$ and $s - s' > 0$ by assumption, we must have $s \geq s't'$. Dually, $t \geq s't'$. \square

3.2 Automorphisms of Generalized Quadrangles

If our goal is to study symmetries of generalized quadrangles, then we must develop some notion of symmetry of a generalized quadrangle. Recall that a symmetry of a graph maps vertices to vertices and edges to edges in such a way that preserves incidence. We will define symmetries of generalized quadrangles similarly.

Definition 3.11. An *automorphism* of a generalized quadrangle $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \mathbf{I})$ is a bijection $x : \mathcal{P} \cup \mathcal{L} \rightarrow \mathcal{P} \cup \mathcal{L}$ such that $P^x \in \mathcal{P}$ for every $P \in \mathcal{P}$, $\ell^x \in \mathcal{L}$ whenever $\ell \in \mathcal{L}$, and $P^x \mathbf{I} \ell^x$ exactly when $P \mathbf{I} \ell$. Equivalently, an automorphism of \mathcal{Q} is an isomorphism from \mathcal{Q} to itself.

Since an automorphism x of \mathcal{Q} is bijective, maps points to points, lines to lines, and preserves incidence, then x preserves every relevant aspect of \mathcal{Q} . (For instance, x maps sub-GQs to sub-GQs.) The collection of automorphisms of \mathcal{Q} forms a *group*, and so is subject to group-theoretic techniques. However, more combinatorial techniques,

such as counting fixed point sets of automorphisms, are also fruitful.

In this vein is Benson's Lemma, which relates several quantities arising from an automorphism of a GQ. Let x be an automorphism of a generalized quadrangle \mathcal{Q} . Define $\alpha_0(x)$ to be the number of fixed points of x , define $\alpha_1(x)$ to be the number of points $P \in \mathcal{P}$ such that $P \neq P^x$ and $P \sim P^x$, and define $\alpha_2(x)$ to be the number of points $P \in \mathcal{P}$ such that $P \not\sim P^x$. We can similarly define the quantities $\beta_0(x)$, $\beta_1(x)$, and $\beta_2(x)$ replacing the word "point" with "line" and \mathcal{P} with \mathcal{L} in the previous definition. Naïvely, we can calculate $|\mathcal{P}| = \alpha_0(x) + \alpha_1(x) + \alpha_2(x)$, but we can achieve a more useful restriction using Benson's lemma.

Benson's lemma uses linear algebraic techniques, so we must define several matrices associated to a generalized quadrangle. All matrices will be over \mathbb{C} . Let $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \text{I})$ be a generalized quadrangle of order (s, t) with $\mathcal{P} = \{P_1, P_2, \dots, P_v\}$ and $\mathcal{L} = \{\ell_1, \ell_2, \dots, \ell_b\}$. Recall the *adjacency matrix* $A = (a_{ij})$ of the point graph of \mathcal{Q} is the $v \times v$ matrix where $a_{ij} = 1$ exactly when $P_i \sim P_j$, and $a_{ij} = 0$ when $P_i \not\sim P_j$. Also let $D = (d_{ij})$ be the $v \times b$ matrix where $d_{ij} = 1$ if $P_i \text{ I } \ell_j$ and $d_{ij} = 0$ otherwise.

Now consider the matrix $M = DD^T$. Noting that the ij -entry of M counts the number of lines incident to both P_i and P_j , we see that $M = A + (t + 1)I$. By this equality, we may retrieve the eigenvalues of M by adding $t + 1$ to the eigenvalues of A . Recalling the eigenvalues of A from Proposition 3.7, we may easily calculate that M has eigenvalues $\tau_0 = (1 + s)(1 + t)$, $\tau_1 = 0$, and $\tau_2 = s + t$, with respective multiplicities $m_0 = 1$, $m_1 = s^2(st + 1)/(s + t)$ and $m_2 = st(s + 1)(t + 1)/(s + t)$.

Now let x be an automorphism of \mathcal{Q} , and define $Q = (q_{ij})$ to be the $v \times v$ matrix such that $q_{ij} = 1$ if $P_i^x = P_j$ and 0 otherwise. Similarly, define $R = (r_{ij})$ to be the $b \times b$ matrix such that $r_{ij} = 1$ if $\ell_i^x = \ell_j$ and 0 otherwise. Then Q and R are permutation matrices, and we leave as an exercise to the reader that $QD = DR$. Since Q and R

are permutation matrices, then $Q^T = Q^{-1}$ and $R^T = R^{-1}$. Then,

$$QM = QDD^T = DRD^T = DR(Q^{-1}DR)^T = DRR^TD^T(Q^{-1})^T = DD^T(Q^{-1})^T = MQ.$$

Hence, Q and M commute. We are now ready to prove Benson's Lemma.

Theorem 3.12. [7, 1.9.1 and 1.9.2] Let \mathcal{Q} be a generalized quadrangle of order (s, t) and x an automorphism of \mathcal{Q} . Then

$$(t+1)\alpha_0(x) + \alpha_1(x) \equiv st + 1 \pmod{s+t}$$

and

$$(t+1)\alpha_0(x) + \alpha_1(x) = (s+1)\beta_0(x) + \beta_1(x).$$

Proof. Suppose that x has order n . Then $(QM)^n = Q^n M^n = M^n$. Therefore, the eigenvalues of QM are the eigenvalues of M multiplied by some root of unity. Note that the ij -entry of $M = DD^T$ counts the number of lines incident to both P_i and P_j . Let J be the $v \times v$ matrix where every entry is 1. Then the ij -entry of MJ is the sum of the i^{th} row of M . However, this is constantly equal to $(s+1)(t+1)$, so $MJ = (s+1)(t+1)J$. Then $QMJ = (s+1)(t+1)QJ = (s+1)(t+1)J$. Thus, $(s+1)(t+1)$ is an eigenvalue of QM . Since M has the eigenvalue $(s+1)(t+1)$ with multiplicity $m_0 = 1$, then so does QM .

Also recall that 0 is an eigenvalue of M with multiplicity $m_1 = s^2(st+1)/(s+t)$. Since Q is a permutation matrix, the same holds for QM .

By the discussion above, the remaining eigenvalues of QM take the form $\xi(s+t)$, where ξ is some n^{th} root of unity. Since the characteristic polynomial of QM has real coefficients, each primitive d^{th} root of unity contributes the same number of times to the eigenvalues of QM . That is, if $d \mid n$ and ξ_d and ξ'_d are primitive d^{th} roots of unity, then the multiplicity of the eigenvalue $\xi_d(s+t)$ is the same as the multiplicity of the

eigenvalue $\xi'_d(s+t)$. Call this multiplicity a_d .

For each divisor d of N , let U_d denote the sum of the primitive d^{th} roots of unity. It is left to the reader to prove (via induction) that U_d is an integer. Then we have

$$\text{tr}(QM) = (1+s)(1+t) + \sum_{d|n} a_d(s+t)U_d.$$

Thus, $\text{tr}(QM) \equiv 1 + st \pmod{s+t}$.

Note also that the ii -entry of QM counts the number of lines incident with P_i and P_i^x . Thus, $\text{tr}(QM) = (t+1)\alpha_0(x) + \alpha_1(x)$. Hence, we achieve the equivalence

$$(t+1)\alpha_0(x) + \alpha_1(x) = \text{tr}(QM) \equiv st + 1 \pmod{s+t}.$$

This proves the first part of the theorem.

Next, we prove the second part of the theorem. Let N be the number of pairs (P, ℓ) for which $P \text{ I } \ell$, $P \sim P^x \neq P$ and $\ell \sim \ell^x \neq \ell$. Now count the number M of pairs (P, ℓ) for which $P \text{ I } \ell$, $P \sim P^x$, and $\ell \sim \ell^x$. This total works out to

$$M = (t+1)\alpha_0(x) + \alpha_1(x) + N/2.$$

The $(t+1)\alpha_0(x)$ term counts the number of pairs (P, ℓ) for which $P^x = P$. Next, we account for the pairs (P, ℓ) where P is not fixed by x . Note that if (P, ℓ) is such that $P \text{ I } \ell$, $P \sim P^x \neq P$, and $\ell \sim \ell^x \neq \ell$, then either $\ell = PP^x$ or $\ell = PP^{x^{-1}}$. Otherwise, ℓ , ℓ^x , and PP^x are all distinct lines, each of which is concurrent to the others, which is disallowed by the GQ axiom. Then, the $\alpha_1(x)$ term counts the number of pairs (P, ℓ) for which $\ell^x = \ell$ or $\ell = PP^x \neq \ell$. The remaining $N/2$ term counts the number of pairs for which $\ell = PP^{x^{-1}} \neq \ell$.

Thus, the identity above holds. By duality, we also achieve the equality $M =$

$(t+1)\beta_0(x) + \beta_1(x) + N/2$. Therefore, we have the equality

$$(t+1)\alpha_0(x) + \alpha_1(x) = M - N/2 = (t+1)\beta_0(x) + \beta_1(x).$$

□

More important to the results in this thesis, however, is the classification of fixed substructures of automorphisms of \mathcal{Q} . If x is an automorphism of a GQ \mathcal{Q} , define \mathcal{Q}_x to be the collection of points and lines fixed by x . This collection maintains the geometric structure of \mathcal{Q} , since we can restrict the incidence relation I to \mathcal{Q}_x . As such, \mathcal{Q}_x is called the *fixed substructure* of x .

Theorem 3.13. [7, 2.4.1] Let x be an automorphism of a GQ \mathcal{Q} . Then the fixed substructure \mathcal{Q}_x takes one of the following forms:

- (0) The substructure \mathcal{Q}_x is empty, i.e., there are no fixed points and no fixed lines.
- (1) At least one point is fixed, there are no fixed lines, and no fixed points are collinear.
- (1') At least one point is fixed, there are no fixed points, and no fixed lines are concurrent.
- (2) There exists some fixed point P such that $P \sim P'$ for each fixed point P , there exists at least one fixed line, and every fixed line is incident to P .
- (2') There exists some fixed line ℓ such that $\ell \sim \ell'$ for each fixed line ℓ , there exists at least one fixed point, and every fixed point is incident to ℓ .
- (3) The substructure \mathcal{Q}_x is a grid with parameters (a, b) such that $a < b$.
- (3') The substructure \mathcal{Q}_x is a dual grid with parameters (a, b) such that $a < b$.
- (4) The substructure \mathcal{Q}_x is a generalized subquadrangle of order (s', t') .

Proof. For any $P, Q \in \mathcal{P}$, denote by PQ the unique line incident to both P and Q , if it exists. Similarly, for any $\ell, m \in \mathcal{L}$, denote by ℓm the unique point incident to both ℓ and m , if it exists.

Let $\mathcal{Q}_x = (\mathcal{P}_x, \mathcal{L}_x, I)$ be the fixed substructure of x , and suppose that \mathcal{Q}_x is not (0), (1), (1'), (2), (2'), (3), or (3'). We wish to show that \mathcal{Q}_x is a sub-GQ. We first show that the GQ Axiom holds for \mathcal{Q}_x . Since \mathcal{Q}_x is not (0), (1), or (1'), then \mathcal{P}_x and \mathcal{L}_x are both nonempty. Take $P \in \mathcal{P}_x$ and $\ell \in \mathcal{L}_x$ such that $P \not I \ell$. Let $Q \in \mathcal{P}$ and $m \in \mathcal{L}$ such that $PImIQI\ell$. Then $P^xIm^xIQ^xI\ell^x$, i.e., $PIm^xIQ^xI\ell$. By uniqueness, $m = m^x$ and $Q = Q^x$. So $m \in \mathcal{L}_x$ and $Q \in \mathcal{P}_x$. This proves the GQ Axiom for \mathcal{Q}_x .

Next, we prove axiom (ii), and note that axiom (i) follows by duality. For a point $P \in \mathcal{P}_x$, denote by $v(P)$ the number of lines in \mathcal{L}_x incident with P . Call this the *valency* of P . First, we show that if $P \not\sim Q$, then $v(P) = v(Q)$. Let $P \not\sim Q \in \mathcal{P}_x$ and suppose $\ell I P$. Then there exist unique R, ℓ' such that $P I \ell I R I \ell' I Q$. Performing this process for distinct lines maps different lines $\ell I P$ to different lines $\ell' I Q$, so $v(P) \leq v(Q)$. Similarly, $v(Q) \leq v(P)$, and so $v(P) = v(Q)$.

Thus, fixing a point $P \in \mathcal{P}_x$, we see that $v(Q) = v(P)$ if $Q \not\sim P$. It suffices to show that if $Q \sim P$, then $v(Q) = v(P)$. Suppose $P \sim Q \in \mathcal{P}_x$. If there exists a point $R \in \mathcal{P}_x$ such that $P \not\sim R \not\sim Q$, then $v(P) = v(R) = v(Q)$ and we are done. So, for the remainder of the proof, we may assume that every point of \mathcal{Q}_x is collinear with P or collinear with Q .

We first show that P and Q both have valency 2 or larger. If P has valency 1, then every point of \mathcal{Q}_x is collinear to Q , implying that \mathcal{Q}_x is type (2). Thus, $v(P) \geq 2$, and similarly $v(Q) \geq 2$.

Suppose a point R is collinear with P and Q . Then by the GQ axiom, P, Q , and R are mutually incident with a distinguished line ℓ . Now suppose that every point of \mathcal{Q}_x is incident to ℓ . Then \mathcal{Q}_x is type (2'), a contradiction. Thus, there must be a point $S \not I \ell$. This point must be collinear to P or Q , but not both. Assume

without loss of generality that $S \sim P$. Then, there is a line $m \text{ I } Q$ which is not equal to ℓ , so applying the GQ axiom with m and S , we retrieve a point $T \sim Q$. Then $P \not\sim T \not\sim R \not\sim S \not\sim Q$, so $v(P) = v(T) = v(R) = v(S) = v(Q)$ as desired.

Thus, for the remainder of the proof, we may assume that no point in $\mathcal{Q}_x \setminus \{P, Q\}$ is collinear with both P and Q . Since every point in \mathcal{Q}_x must be collinear with P or collinear with Q , it follows that every point $R \in \mathcal{P}_x \setminus \{P, Q\}$ is collinear with either P or Q , but not both. Our goal will be to prove that \mathcal{Q}_x is a dual grid. Relabel $P = P_0$, $Q = Q_0$, $v(P) = t' + 1$, and $v(Q) = t'' + 1$, and let $\ell_{0,0} \in \mathcal{L}_x$ be the unique line through P and Q . Label the lines incident to P but not Q $\ell_{0,j}$ for $1 \leq j \leq t'$, and similarly label the lines through Q but not P $\ell_{i,0}$ for $1 \leq i \leq t''$.

If every point of \mathcal{Q}_x is incident to $\ell_{0,0}$, then \mathcal{Q}_x is type (2'), so there must be a point R which is not incident to $\ell_{0,0}$. This point must be collinear with either P_0 or Q_0 , but not both, so assume without loss of generality that $R \sim P_0$. Then by the GQ axiom, there exist points $P_1, \dots, P_{t''}$ such that $Q_i \text{ I } \ell_{i,0}$ for each i . Applying this same logic with the point P_1 , we may construct points $Q_1, \dots, Q_{t'}$ such that $Q_j \text{ I } \ell_{0,j}$ for every j .

Suppose that \mathcal{P}_x has more points than $P_0, \dots, P_{t'}$ and $Q_0, \dots, Q_{t''}$. Say that R is one of these points. Then either $R \sim P$ or $R \sim Q$, so $R \text{ I } \ell_{0,j}$ for some j , or $R \text{ I } \ell_{i,0}$ for some i . Assume without loss of generality that $R \text{ I } \ell_{0,1}$. Then by the GQ axiom, R is incident to a point $S \text{ I } \ell_{1,0}$. Since $S \sim R$, then by the GQ axiom, $S \not\sim Q_1$. Thus, $P_0 \not\sim S \not\sim Q_1 \not\sim Q_0$, so $v(P) = v(S) = v(Q_1) = v(Q_0)$. In this case, the GQ axiom follows, so for the rest of the proof, we may deal with cases where $P_0, \dots, P_{t'}$ and $Q_0, \dots, Q_{t''}$ are all of the points of \mathcal{Q}_x .

In this case, each line $\ell_{i,0}$ and $\ell_{0,j}$ is incident to exactly two points. Applying the GQ axiom, we may construct lines $\ell_{i,j} \in \mathcal{L}_x$ such that $P_i \text{ I } \ell_{i,j}$ and $Q_j \text{ I } \ell_{i,j}$ for all $0 \leq i \leq t'$ and $0 \leq j \leq t''$. Since $P_i \not\sim P_0$ for $i > 1$, then $v(P_i) = v(P_0) = t' + 1$ for all i . Similarly, $v(Q_j) = t'' + 1$ for all j . Each point P_i is incident with the lines $\ell_{i,0}, \dots, \ell_{i,t''}$

so no other lines can be incident with P_i . Similarly, each point Q_j is incident with all the lines $\ell_{0,j}, \dots, \ell_{t'',j}$. Since each line of \mathcal{Q}_x must be incident to a point, by the GQ axiom, so there are no other lines in \mathcal{Q}_x . Since the P_i 's and Q_j 's are the only points, and the $\ell_{i,j}$'s are the only lines, then \mathcal{Q}_x must be a dual grid with parameters (t', t'') . Since \mathcal{Q}_x is not (3') we must have $t' = t''$, and so $v(P) = v(Q)$. Thus, in all cases $v(P) = v(Q)$, and so axiom (ii) follows. \square

Finally, we prove a useful lemma about abelian groups acting regularly on points of a GQ \mathcal{Q} . Recall that a group G is *abelian* if for any $g, h \in G$, $gh = hg$. Many famous groups are abelian, such as the group \mathbb{Z} of integers, taken additively, and the group \mathbb{Q}^\times of nonzero rational numbers taken multiplicatively. More relevant to our purposes, all cyclic groups are abelian.

Lemma 3.14. [2, Lemma 2.1] Let $\mathcal{Q} = (\mathcal{P}, \mathcal{L}, \mathbf{I})$ be a generalized quadrangle of order (s, t) and let $G \leq \text{Aut}(\mathcal{Q})$ be an abelian group acting regularly on \mathcal{P} . Then for any line $\ell \in \mathcal{L}$, the stabilizer G_ℓ is size $s + 1$. In particular, an abelian group G cannot act regularly on both points and lines.

Proof. Let ℓ be a line in \mathcal{Q} and fix a point $P \mathbf{I} \ell$. Since G acts regularly on \mathcal{P} , there is a bijection $\mathcal{P} \rightarrow G$ mapping $Q \in \mathcal{P}$ to the unique $g \in G$ such that $P^g = Q$. If $T = \{P = P_0, P_1, \dots, P_s\}$ is the set of points incident to ℓ , then let $S = \{g_0 = 1, g_1, \dots, g_s\}$ be the image of T under this bijection. We show that S is a subgroup of G stabilizing ℓ .

Consider elements $g_i, g_j \in S$ such that $i \neq 0 \neq j$. Then $P \sim P^{g_i}$ implies $P^{g_i} \sim P^{g_i g_j}$ and $P \sim P^{g_j}$ implies $P^{g_j} \sim P^{g_j g_i} = P^{g_i g_j}$. Thus, $P^{g_i g_j}$ is collinear to two distinct points incident to ℓ , and so $P^{g_i g_j}$ is incident to ℓ as well. It follows that $\ell^{g_i} = (PP^{g_j})^{g_i} = P^{g_i} P^{g_i g_j} = \ell$. Thus S stabilizes ℓ , so $S \subseteq G_\ell$.

Note that any $g \in G_\ell$ must map P to another point incident to ℓ . Since there are at most $s + 1$ points of ℓ , there are at most $s + 1$ points to which G_ℓ can move

P . Since G_ℓ acts semiregularly on \mathcal{P} , this means $|G_\ell| \leq s + 1$. From the inclusion $S \subseteq G_\ell$, we can conclude $S = G_\ell$, and so $|G_\ell| = s + 1$. \square

3.3 Automorphisms of Prime Order

The restrictions above hold for automorphisms of any order. However, if x is an automorphism of prime order, we can say much more. Specifically, we can narrow down the type of \mathcal{Q}_x by the classes of $s + 1$ and $t + 1$ modulo p . This is a powerful technique utilized in [1], so all of the results in this section are taken from that paper. Here, we reproduce several lemmas helpful to the study of the GQ of order 6, although more results are available in [1].

Lemma 3.15. [1, Lemma 3.2] Let x be an order p automorphism of a GQ \mathcal{Q} , where p is prime. If \mathcal{Q}_x has type (0), then either $t + 1 \equiv s + 1 \equiv 0 \pmod{p}$, or $st + 1 \equiv 0 \pmod{p}$. Furthermore, if p is an odd prime, then $s + 1 \equiv t + 1 \equiv 0 \pmod{p}$ if and only if $st + 1 \not\equiv 0 \pmod{p}$.

Proof. Since \mathcal{Q}_x is type (0), it follows that $\alpha_0(x) = \beta_0(x) = 0$, which implies that $p \mid (s + 1)(st + 1)$ and $p \mid (t + 1)(st + 1)$. If $p \nmid st + 1$, then by Euclid's lemma, $p \mid s + 1$ and $p \mid t + 1$. Finally, if p is an odd prime, and $s + 1 \equiv t + 1 \equiv 0 \pmod{p}$, then

$$st + 1 \equiv (-1)(-1) + 1 \equiv 2 \not\equiv 0 \pmod{p}.$$

\square

Lemma 3.16. [1, Lemma 3.3] Let x be an order p automorphism of a GQ \mathcal{Q} , where p is prime. If \mathcal{Q}_x has type (1), then $t + 1 \equiv 0 \pmod{p}$. If \mathcal{Q}_x has type (1'), then $s + 1 \equiv 0 \pmod{p}$.

Proof. Suppose \mathcal{Q}_x is type (1). Then there are no fixed lines, but at least one fixed point. Let P be such a point, and let S be the set of lines incident with P . Then

$|S| = t + 1$. Also note that S is invariant under x , since $\ell \text{ I } P$ implies $\ell^x \text{ I } P^x = P$. Then S may be partitioned into $\langle x \rangle$ -orbits. Since x does not fix any lines, then these orbits are all size p . and so $p \mid |S| = t + 1$. The analogous result if \mathcal{Q}_x is type (1') follows by duality. \square

Lemma 3.17. [1, Lemma 3.4] Let x be an order p automorphism of a GQ \mathcal{Q} , where p is prime.

- (i) If \mathcal{Q}_x has type (2) and $\alpha_0(x) = 1$, then $s + 1 \equiv 1 \pmod{p}$.
- (ii) If \mathcal{Q}_x has type (2) and $\alpha_0(x) > 1$, then $t + 1 \equiv 1 \pmod{p}$.
- (iii) If \mathcal{Q}_x has type (2') and $\beta_0(x) = 1$, then $t + 1 \equiv 1 \pmod{p}$.
- (iv) If \mathcal{Q}_x has type (2') and $\beta_0(x) > 1$, then $s + 1 \equiv 1 \pmod{p}$.

Proof. We will prove (i) and (ii), since (iii) and (iv) then follow by duality. Suppose \mathcal{Q}_x is type (2) and assume that $\alpha_0(x) = 1$. Then there is a unique fixed point P which is incident with a fixed line ℓ . The remaining s points incident to ℓ form an $\langle x \rangle$ -invariant set. Since all of these points are moved by x , then $p \mid s$ showing that $s + 1 \equiv 1 \pmod{p}$, and so (i) follows.

Next, assume that $\alpha_0(x) > 1$. Let P and Q be two fixed points, and assume by hypothesis that $P' \sim P$ for every fixed point P' . Hence, $Q \sim P$, and so x also fixes the unique line ℓ such that $P \text{ I } \ell \text{ I } Q$. None of the other t lines incident with Q are fixed by x , so they must be partitioned into $\langle x \rangle$ -orbits of size p . Thus, $t + 1 \equiv 1 \pmod{p}$, and so (ii) follows. \square

Lemma 3.18. [1, Lemma 3.6] Let x be an order p automorphism of a GQ \mathcal{Q} , where p is prime. If \mathcal{Q}_x has type (3), then $t + 1 \equiv 2 \pmod{p}$, and $a \equiv b \equiv s \pmod{p}$. If \mathcal{Q}_x has type (3'), then $s + 1 \equiv 2 \pmod{p}$, and $a \equiv b \equiv t \pmod{p}$.

Proof. Assume \mathcal{Q}_x is type (3), and let P be a fixed point of the grid. Then there are exactly two fixed lines incident with P , and so the remaining $t - 1$ lines incident

with P are partitioned into $\langle p \rangle$ -orbits of size p . Thus, $t + 1 \equiv 2 \pmod{p}$. Now, there are two types of lines in the grid, one of which contains $a + 1$ fixed points, and the other which contains $b + 1$ fixed points. If ℓ contains $a + 1$ fixed points, the remaining $(s + 1) - (a + 1)$ fixed points are partitioned into $\langle p \rangle$ -orbits of size p . Thus, $s - a \equiv 0 \pmod{p}$, so $s \equiv a \pmod{p}$. Similarly, $s \equiv b \pmod{p}$. If \mathcal{Q}_x is type (3'), the result follows by duality. \square

Lemma 3.19. [1, Lemma 3.8] Let x be an order p automorphism of a GQ \mathcal{Q} , where p is prime. If \mathcal{Q}_x has type (4) such that \mathcal{Q}_x is a subquadrangle of order (s', t') , then $s' \equiv s \pmod{p}$ and $t' \equiv t \pmod{p}$.

Proof. Let ℓ be a fixed line. Then exactly $s' + 1$ points on ℓ are fixed, so the other $s + 1 - (s' + 1) = s - s'$ are partitioned into $\langle x \rangle$ -orbits of size p . Therefore, $s - s' \equiv 0 \pmod{p}$, and so $s \equiv s' \pmod{p}$. Dually, $t' \equiv t \pmod{p}$. \square

Lemma 3.20. [1, Lemma 3.9 and 3.10] Let x be an order p automorphism of a generalized quadrangle \mathcal{Q} of order (s, t) , where p is prime. If \mathcal{Q}_x is a subquadrangle of order (s, t') , then $\alpha_1(x) = 0$ and $s + t$ divides $st'(st + 1)$.

Proof. First, we show that $\alpha_1(x) = 0$. Let P be a point not fixed by x . If ℓ is a line fixed by x , since \mathcal{Q}_x is a subquadrangle of order (s, t') , then all points incident with ℓ are fixed by x . This means P is not incident with ℓ , so by the GQ axiom, there must be a unique point Q incident with ℓ such that $P \sim Q$. Let ℓ' be the line incident with both P and Q . Since Q is fixed, $(\ell')^x$ is also incident with Q . However, we cannot have $P \sim P^x$, otherwise P , P' , and Q are a triangle. Thus, $P \not\sim P^x$, for every $P \in \mathcal{P}$, and so $\alpha_1(x) = 0$.

Next, we show that $s + t$ divides $st'(st + 1)$. Note that $\alpha_0(x) = (s + 1)(st' + 1)$. By Benson's lemma,

$$(t + 1)(s + 1)(st' + 1) = (t + 1)\alpha_0(x) + \alpha_1(x) \equiv st + 1 \pmod{s + t}.$$

Then,

$$\begin{aligned} st'(st+1) &= (st'+1)(st+1) - (st+1) \equiv (st'+1)(st+s+t+1) - (st+1) \\ &= (st'+1)(t+1)(s+1) - (st+1) \equiv 0 \pmod{s+t}. \end{aligned}$$

The result follows. \square

The results so far in this section help narrow down the fixed substructure of an automorphism, which are useful for establishing properties of a specific automorphism. However, these results also have use in a more general context, as they establish a strong restriction on the types of primes that can divide the automorphism group of a GQ of order (s, t) .

Lemma 3.21. [1, Lemma 3.13] Let p be a prime that divides the automorphism group of a generalized quadrangle \mathcal{Q} of order (s, t) . Then either $p \mid st+1$ or $p \leq \max\{s+1, t+1\}$.

Proof. Assume $p \nmid st+1$. If $t=1$, then \mathcal{Q} is a grid with symmetry group $S_{s+1} \wr 2$. Then $p \leq s+1$. Dually, if $s=1$, then $p \leq t+1$. Therefore, we may assume that \mathcal{Q} is a thick generalized quadrangle.

Assume for contradiction $p > s+1$ and $p > t+1$, and let x be an automorphism of \mathcal{Q} of order p . Since \mathcal{Q} is thick, we have $s+1 \not\equiv 0, 1, 2 \pmod{p}$ and $t+1 \not\equiv 0, 1, 2 \pmod{p}$. Applying Lemmas 3.16, 3.17, and 3.18, we may conclude that \mathcal{Q}_x is not type (1), (1'), (2), (2'), (3), or (3'). Since $p > s+1 \geq 2$, then p must be an odd prime. Since $s+1 \not\equiv 0 \pmod{p}$, $t+1 \not\equiv 0 \pmod{p}$, and $st+1 \not\equiv 0 \pmod{p}$, then by Lemma 3.15, we conclude that \mathcal{Q}_x is not type (0). Therefore, \mathcal{Q}_x must be type (4).

Assume \mathcal{Q}_x is a subquadrangle of order (s', t') . Then by Lemma 3.19, $s' \equiv s \pmod{p}$. However, $p > s \geq s'$, and so $s' = s$. A similar argument shows that $t' = t$. Therefore, $\mathcal{Q}_x = \mathcal{Q}$, and so x is the identity automorphism, which in particular is not order p . The result follows via contradiction. \square

Chapter 4

A Generalized Quadrangle of Order 6

We now turn our attention to a generalized quadrangle of order 6. The parameters $(6, 6)$ are not immediately ruled out by Proposition 3.7, so the existence of a GQ with these parameters is still an open question. If such an object \mathcal{Q} exists, we know immediately that it must have 7 points incident to each line, 7 lines incident to each point, and its point set and line set must both be size $7 \cdot 37 = 259$. Lemma 3.21 tells us that the only primes that may divide the automorphism group of \mathcal{Q} are 2, 3, 5, 7, and 37. We can also apply the theory developed in the previous section to restrict the fixed substructures of automorphisms of \mathcal{Q} .

Lemma 4.1. *Let x be a prime-order automorphism of \mathcal{Q} . Then $|x| = 2, 3, 5, 7$, or 37. Furthermore, if \mathcal{Q}_x is the fixed substructure of x , then the following hold:*

- (a) *If $|x| = 2$, then \mathcal{Q}_x is type (2), (2'), or (4). In the last case, the sub-GQ must have order $(2, 2)$.*
- (b) *If $|x| = 3$, then \mathcal{Q}_x is type (2) or (2').*
- (c) *If $|x| = 5$, then \mathcal{Q}_x is type (3), (3'), or (4). In the case of (3) (resp., (3')),*

the grid (resp., dual grid) must have parameters $(1, 6)$. In the case of (4), the sub-GQ must have order $(1, 1)$.

(d) *If $|x| = 7$, then \mathcal{Q}_x is type (0) , (1) , or $(1')$.*

(e) *If $|x| = 37$, then \mathcal{Q}_x is type (0) .*

Proof. The constraint on the possible orders of x follows from Lemma 3.21.

(a) First, assume $|x| = 2$. By Lemma 3.15, \mathcal{Q}_x does not have type (0) and by Lemma 3.16, \mathcal{Q}_x does not have type (1) or $(1')$. By Lemma 3.18, \mathcal{Q}_x does not have type (3) . So \mathcal{Q}_x must be type (2) or (4) . If \mathcal{Q}_x is type (4) , then \mathcal{Q}_x is a sub-GQ of order (s', t') , and by Lemma 3.19, $s' \equiv 6 \equiv 0 \pmod{2}$ and $t' \equiv 6 \equiv 0 \pmod{2}$. The orders $(4, 2)$ and $(4, 4)$, and $(4, 6)$ are ruled out by Proposition 3.10. The order $(6, 2)$ is ruled out by Proposition 3.7. Therefore, \mathcal{Q}_x must be a GQ of order $(2, 2)$. Thus (a) holds.

(b) Next, assume $|x| = 3$. By Lemma 3.15, \mathcal{Q}_x does not have type (0) and by Lemma 3.16, \mathcal{Q}_x does not have type (1) or $(1')$. By Lemma 3.18, \mathcal{Q}_x does not have type (3) . If \mathcal{Q}_x is type (4) , then \mathcal{Q}_x is a sub-GQ of order (s', t') , and by Lemma 3.19, $s' \equiv 6 \equiv 0 \pmod{3}$ and $t' \equiv 6 \equiv 0 \pmod{3}$. The order $(3, 6)$ was ruled out by Dixmier and Zara, a proof of which can be seen in [7, 6.2.2]. The order $(3, 3)$ is ruled out by Proposition 3.10, so type (4) is impossible. Therefore, \mathcal{Q}_x must be type (2) or $(2')$, and so (b) holds.

(c) Now, assume $|x| = 5$. By Lemma 3.15, \mathcal{Q}_x is not type (0) , and by Lemma 3.16, \mathcal{Q}_x is not type (1) or $(1')$. By Lemma 3.17, \mathcal{Q}_x is not type (2) or $(2')$. If \mathcal{Q}_x is type (4) , then \mathcal{Q}_x is a sub-GQ of order (s', t') , and by Lemma 3.19, $s' \equiv 6 \equiv 1 \pmod{5}$ and $t' \equiv 6 \equiv 1 \pmod{5}$. The order $(6, 1)$ is ruled out by Lemma 3.20, and so \mathcal{Q}_x must have order $(1, 1)$.

If \mathcal{Q}_x is type (3) , then \mathcal{Q}_x must be a grid with parameters (a, b) with $a < b$ and by Lemma 3.18, $a \equiv b \equiv 6 \equiv 1 \pmod{5}$. Thus, \mathcal{Q}_x is a grid with parameters $(1, 6)$.

Dually, if \mathcal{Q}_x is type (3'), then \mathcal{Q}_x is a dual grid with parameters (1, 6). Thus, \mathcal{Q}_x is either a grid with parameters (1, 6), a dual grid with parameters (1, 6), or a sub-GQ of order (1, 1). Thus, (c) holds.

(d) Now, assume $|x| = 7$. By Lemma 3.17, \mathcal{Q}_x is not type (2) or (2'), and by Lemma 3.18, \mathcal{Q}_x is not (3) or (3'). If \mathcal{Q}_x is type (4), then \mathcal{Q}_x is a sub-GQ of order (s', t') , and by Lemma 3.19, $s' \equiv t' \equiv 6 \pmod{7}$. Then $s' = t' = 6$, which is a contradiction. Thus, \mathcal{Q}_x is type (0), (1), or (1'). Thus, (d) holds.

(e) Now, assume $|x| = 37$. By Lemma 3.16, \mathcal{Q}_x is not type (1) or (1'), by Lemma 3.17, \mathcal{Q}_x is not type (2) or (2'), and by Lemma 3.18, \mathcal{Q}_x is not (3) or (3'). If \mathcal{Q}_x is type (4), then \mathcal{Q}_x is a sub-GQ of order (s', t') , and by Lemma 3.19, $s' \equiv t' \equiv 6 \pmod{37}$. Then $s' = t' = 6$, which is a contradiction. Thus, \mathcal{Q}_x is type (0), and so (e) holds. \square

With these restrictions established, we are now able to study the symmetries of the GQ of order 6 in earnest.

4.1 Bounds on Automorphism Orders

4.1.1 Prime Power Automorphism Orders

We begin by establishing some limits on the orders of prime-power order automorphisms of \mathcal{Q} . For $p = 37, 7, 5$, we prove that an automorphism of order p^k must have $k = 1$. In addition, we prove that for $p = 2, 3$, an automorphism of order p^k must have $k \leq 2$.

Since no automorphism of order 37 may fix any points or lines, we can say something much stronger about 37 – that a Sylow 37-subgroup of $\text{Aut}(\mathcal{Q})$ must be trivial or cyclic of order 37. A very similar situation occurs for a hypothesized GQ of order (4, 12), so we may adapt Lemma 6.5 of [1] almost directly.

Lemma 4.2. *Let G be the group of automorphisms of \mathcal{Q} . Then, a Sylow 37-subgroup of G must have order at most 37. In particular, there is no automorphism of \mathcal{Q} of order 37^2 .*

Proof. Let X be a Sylow 37-subgroup of G and $x \in X$ a non-identity element. Then, $x^{|x|/37}$ is an element of order 37 in X . By Lemma 4.1, $x^{|x|/37}$ does not have any fixed points. If x had a fixed point, then $x^{|x|/37}$ would fix it as well, so x cannot have any fixed points. This implies that X acts semiregularly on \mathcal{P} , and so $|X|$ divides $|\mathcal{P}| = 259$. Thus, $|X| = 37$. \square

For $p = 2, 3, 5, 7$, we cannot say as much about the Sylow p -subgroup, however, we can bound the maximal k such that \mathcal{Q} has an automorphism of order p^k . In general, the presence of an automorphism x of order p^k imposes restrictions on the fixed point set of $y = x^{p^{k-1}}$. Therefore, the existence of x imposes restrictions on $\alpha_0(y)$ and $\beta_0(y)$. However, for $k \geq 2$, y is a prime order automorphism of \mathcal{Q} , so we may employ Lemma 4.1 to achieve other restrictions on $\alpha_0(y)$ and $\beta_0(y)$. Playing these restrictions against each other results in a contradiction in every case.

In pursuit of this goal, the following technical proposition helps us count in general the size of $\alpha_0(x^{p^{k-1}})$ given an automorphism x of order p^k .

Proposition 4.3. *Let Ω be a finite set and let $x \in \text{Sym}(\Omega)$ have order p^k , for $k \geq 2$ and p prime. Then if N is the size of the fixed point set of $x^{p^{k-1}}$, then $N \equiv |\Omega| \pmod{p^k}$.*

Proof. For convenience of notation, label $y = x^{p^{k-1}}$ and let $G = \langle x \rangle$. Let $\text{fix}_\Omega(y)$ be the set of y -fixed points and consider $K = \Omega \setminus \text{fix}_\Omega(y)$. Then $G = \langle x \rangle$ is invariant on $\text{fix}_\Omega(y)$, and so x is also invariant on its complement K . Thus, G acts on K .

By Orbit-Stabilizer, the possible lengths of G -orbits on K are p^j for $0 \leq j \leq k$, so we may write

$$|K| = \sum_{j=1}^k p^j n_j,$$

where each n_j counts the number of length p^j orbits on K . We will show that $n_j = 0$ for each $j < k$.

If we let $j < k$ and assume for contradiction that $n_j > 0$, then there must be some $P \in K$ such that $|P^G| = p^j$. Then by Orbit-Stabilizer, $|G_P| = |G|/|P^G| = p^k/p^j = p^{k-j} \geq p$. Note that since G is a cyclic group, G has a unique order p subgroup H . Since G_P is a subgroup of G with order larger than p , then G_P must also contain H as a subgroup. However, $\langle y \rangle$ is an order p subgroup of G , since $|y| = |x^{p^{k-1}}| = p$. By uniqueness, $\langle y \rangle = H$, and so $y \in H \leq G_P$. Therefore, y fixes P , and so $P \in \text{fix}_\Omega(y)$. However, P cannot be in $\text{fix}_\Omega(y)$ and its complement K at the same time, so this is a contradiction. Therefore, $n_j = 0$.

Since $n_j = 0$ for every $j < k$, the sum $|K| = \sum_{j=1}^k p^j n_j$ becomes the equality $|K| = p^k n_k$. In particular p^k divides $|K|$. However, since $K = |\Omega| \setminus \text{fix}_\Omega(y)$, then $|K| = |\Omega| - \alpha_0(y)$. Therefore, p^k divides $|\Omega| - \alpha_0(y)$, and so $\alpha_0(y) \equiv |\Omega| \pmod{p^k}$ as desired. \square

For the case of generalized quadrangles, we have the following corollary:

Corollary 4.4. *Let \mathcal{Q} be a generalized quadrangle of order (s, t) and let x be an automorphism of \mathcal{Q} with order p^k , for $k \geq 2$ and p prime. Then $\alpha_0(x^{p^{k-1}}) \equiv (s + 1)(st + 1) \pmod{p^k}$ and $\beta_0(x^{p^{k-1}}) \equiv (t + 1)(st + 1) \pmod{p^k}$.*

This result allows us to study automorphisms with prime power order using the techniques developed for prime order automorphisms. The existence of an automorphism x of order p^k imposes restrictions on the fixed substructure of the automorphism y of order p that we get by powering up x the appropriate number of times. This result is likely to be applicable to other contexts in which much is known about prime order automorphisms of some structure, say in the case of strongly regular graphs, or other generalized quadrangles.

For the case of a generalized quadrangle \mathcal{Q} of order $(6, 6)$, and x an automor-

phism of order p^k , Corollary 4.4 gives us the congruence $\alpha_0(x^{p^{k-1}}) \equiv \beta_0(x^{p^{k-1}}) \equiv 259 \pmod{p^k}$. With this group-theoretic counting tool, we may apply the GQ-theoretic Lemma 4.1 to prove the desired restrictions on prime-power automorphism orders.

Corollary 4.5. *There is no automorphism of \mathcal{Q} of order 49.*

Proof. Suppose for contradiction that x is an automorphism of order $49 = 7^2$. Then x^7 is an automorphism of order 7, so by Lemma 4.1, \mathcal{Q}_{x^7} must be type (0), (1), or (1'). In particular, either $\alpha_0(x^7) = 0$ or $\beta_0(x^7) = 0$. However, Corollary 4.4 tells us that $\alpha_0(x^7) \equiv \beta_0(x^7) \equiv 259 \equiv 14 \pmod{49}$. In particular, this means that $\alpha_0(x^7)$ and $\beta_0(x^7)$ are both positive, a contradiction. \square

Corollary 4.6. *There is no automorphism of \mathcal{Q} of order 25.*

Proof. Suppose for contradiction that x is an order 25 automorphism of \mathcal{Q} . Then Corollary 4.4 tells us that $\alpha_0(x^5) \equiv \beta_0(x^5) \equiv 259 \equiv 9 \pmod{25}$. Since $|x^5| = 5$, Lemma 4.1 tells us that \mathcal{Q}_{x^5} is either a grid with parameters (1, 6), a dual grid with parameters (1, 6), or a GQ of order (1, 1). In the first case, \mathcal{Q}_{x^5} has 14 points, and so $\alpha_0(x^5) = 14$, contradicting $\alpha_0(x^5) \equiv 9 \pmod{25}$. In the second case, \mathcal{Q}_{x^5} has 14 lines, and so $\beta_0(x^5) = 14$, contradicting $\beta_0(x^5) \equiv 9 \pmod{25}$. In the third case, \mathcal{Q}_{x^5} has exactly 4 points, and so $\alpha_0(x^5) = 4$, contradicting $\alpha_0(x^5) \equiv 9 \pmod{25}$. \square

Corollary 4.7. *There is no automorphism of \mathcal{Q} of order 27.*

Proof. Suppose for contradiction that x is an automorphism of order $27 = 3^3$. Then Corollary 4.4 tells us that $\alpha_0(x^9) \equiv \beta_0(x^9) \equiv 259 \equiv 16 \pmod{27}$. Since x^9 is an order 3 automorphism of \mathcal{Q} , then \mathcal{Q}_{x^9} is either type (2) or (2') by Lemma 4.1. In particular, this means that every fixed line of x^9 is contained on one point, or that every fixed point of x^9 is contained on one line. Since there are exactly 7 lines on each point and exactly 7 points through each line, this means that $\alpha_0(x^9) \leq 7$ or $\beta_0(x^9) \leq 7$. This contradicts $\alpha_0(x^9) \equiv \beta_0(x^9) \equiv 16 \pmod{27}$. Therefore, there can be no automorphism of order 27. \square

Corollary 4.8. *There is no automorphism of \mathcal{Q} order 8.*

Proof. Suppose x is an automorphism of \mathcal{Q} with order $8 = 2^3$ and put $G = \langle x \rangle$. Then x must fix some point P otherwise $2 \mid |\mathcal{P}| = 259$. Consider the set A of lines incident to P . Since x fixes P , then A must be a G -invariant subset of \mathcal{L} . There are exactly 7 lines in A , so any G -orbit inside A has size at most 4. Therefore, x^4 fixes every line in A . Thus, $\beta_0(x^4) \geq 7$. Similarly, $\alpha_0(x) \geq 7$.

Now, we employ Lemma 4.1 to see that \mathcal{Q}_{x^4} is either type (2), type (2'), or a GQ of order $(2, 2)$, since $|x^4| = 2$. The last possibility is ruled out by the fact that the x^4 -fixed point P has all seven lines incident to it fixed. Thus, \mathcal{Q}_{x^4} is either type (2) or (2'). In particular, this means that every fixed line of x^4 is incident with one distinguished point, or that every fixed point of x^4 is incident with one distinguished line. Since there are exactly 7 lines on each point and exactly 7 points through each line, this means that $\alpha_0(x^4) \leq 7$ or $\beta_0(x^4) \leq 7$. Since we showed earlier that $\alpha_0(x^4) \geq 7$ and $\beta_0(x^4) \geq 7$, this means that either $\alpha_0(x^4) = 7$ or $\beta_0(x^4) = 7$.

Finally, we apply Corollary 4.4 to see that $\alpha_0(x^4) \equiv \beta_0(x^4) \equiv 259 \equiv 3 \pmod{8}$. This contradicts the fact that either $\alpha_0(x^4) = 7$ or $\beta_0(x^4) = 7$. Therefore, no automorphism of order 8 may exist. \square

Finally, we can use Corollary 4.5 to find a useful restriction on the size of a Sylow 7-subgroup of $G = \text{Aut}(\mathcal{Q})$.

Lemma 4.9. *Let $G = \text{Aut}(\mathcal{Q})$, where \mathcal{Q} is the GQ of order 6. Then a Sylow 7-subgroup of G must have order at most 7^3 .*

Proof. Assume for contradiction that X is a Sylow 7-subgroup of G with $|X| \geq 7^4$, and let $P \in \mathcal{P}$. Then let X_P be the stabilizer of P in X . Since any X -orbit must have length smaller than 259, the possible sizes of X -orbits are $\{1, 7, 49\}$. Since any orbit of X is size 7^2 or smaller, then by Orbit-Stabilizer, $|X_P| = |X|/|P^G| \geq 7^4/7^2 = 7^2$.

Now consider the incidence graph Γ of \mathcal{Q} , whose vertices are the lines and points of \mathcal{Q} , and where there is an edge from $\ell \in \mathcal{L}$ to $R \in \mathcal{P}$ exactly when ℓ is incident with R . Since G acts faithfully on \mathcal{Q} , it must act faithfully on Γ as well. Since X_P is a subgroup of G , it must also act faithfully on Γ .

Let $\Gamma(P)$ be a neighborhood of our distinguished point P , i.e., the subgraph induced by the point P along with its neighbors ℓ_1, \dots, ℓ_7 . The action of X_P on Γ induces an action of X_P on Γ_P , which has kernel K . I contend that no non-identity automorphism of X_P is in this kernel. Let $x \in X_P \setminus \{1\}$. Then by Corollary 4.5, $|x| = 7$, and so by Lemma 4.1, \mathcal{Q}_x is either type (0), (1), or (1'). However, x fixes P , and so \mathcal{Q}_x must be type (1). Therefore, x fixes no lines, so x acts nontrivially on $\Gamma(P)$. Thus, $x \notin K$. Since no nonidentity x is in K , we conclude $K = \{1\}$.

Therefore, X_P acts faithfully on $\Gamma(P)$. However, this entails that $X_P \lesssim S_7$, since any $x \in X_P$ can only permute the lines ℓ_1, \dots, ℓ_7 . This is a contradiction, since $|X_P| \geq 7^2$. Therefore, $|X| \leq 7^3$. \square

4.1.2 Automorphisms of Order $37p$

Next, we show that for p prime, there can be no automorphism of \mathcal{Q} with order $37p$. This is desirable, since ruling out automorphisms of order $37p$ naturally rules out even more automorphism orders. Indeed, if suppose that for some $n \geq 2$ that \mathcal{Q} has an automorphism x of order $37n$, consider the cyclic group $G = \langle x \rangle$. Since for some prime p , $37p$ divides $37n$, then G must have a cyclic subgroup H of order $37p$. This cyclic subgroup H must contain an automorphism of order $37p$, which results in contradiction. So just by ruling out automorphisms of order $37p$ for p prime, we have also ruled out the much broader class of automorphisms of order $37n$ for $n \geq 2$.

In order to achieve this result, Lemma 4.1 tells us that we may restrict our attention to the primes 2, 3, 5, 7, and 37. Lemma 4.2 already tells us that \mathcal{Q} has no automorphism of order $37 \cdot 37$, otherwise the Sylow 37-subgroup of $\text{Aut}(\mathcal{Q})$ would be

too large. The case of $7 \cdot 37$ is also a special case, which we will handle below.

Lemma 4.10. *There is no automorphism of \mathcal{Q} of order $7 \cdot 37$.*

Proof. Suppose for contradiction that z is an automorphism of order $7 \cdot 37$. Then it may be written as the product $z = xy = yx$ of an automorphism x of order 7 and an automorphism y of order 37. Since x and y commute, then $\langle z \rangle = \langle xy \rangle = \langle x, y \rangle$. Thus, z fixes a point P exactly when both x and y fix that point P .

Employing duality and Lemma 4.1, we may assume without loss of generality that \mathcal{Q}_x is either type (0) or (1') so that x fixes no points. Lemma 4.1 also tells us that \mathcal{Q}_y is type (0), so y does not fix any points either. Therefore, z does not fix any points. Since $|z| = 259 = |\mathcal{P}|$, this means that $\langle z \rangle$ acts regularly on \mathcal{P} . However, this contradicts Lemma 3.14. Therefore, no automorphism of order $7 \cdot 37$ may exist. \square

Luckily, in order to rule out $5 \cdot 37$, $3 \cdot 37$, and $2 \cdot 37$, we can use many of the same methods. The general structure of the proofs is start with an automorphism of order $37p$ (for $p \in \{2, 3, 5\}$) and decompose it into two automorphisms x and y such that x and y commute, x is order p , and y is order 37. We can then restrict the size of $\alpha_0(x)$ and $\beta_0(x)$ using elementary group-theoretic methods. However, since x is a prime-order automorphism, we can also restrict the size of $\alpha_0(x)$ and $\beta_0(x)$ using Lemma 4.1. Playing these two restrictions against each other results in a contradiction for each $p \in \{2, 3, 5\}$.

Lemma 4.11. *Let p be prime and suppose x and y are automorphisms of \mathcal{Q} with $|x| = p$, $|y| = 37$, and $xy = yx$. Then $\alpha_0(x) \equiv \beta_0(x) \equiv 0 \pmod{37}$.*

Proof. Let \mathcal{P}_x be the fixed point set of x . Since x and y commute, y is invariant on \mathcal{P}_x . By Lemma 4.1, \mathcal{Q}_y is type (0), and so y fixes no points. Therefore, y acts fixed point freely on \mathcal{P}_x , and so $37 \mid |\mathcal{P}_x|$. Thus, $\alpha_0(x) \equiv 0 \pmod{37}$. A dual argument shows that $\beta_0(x) \equiv 0 \pmod{37}$. \square

Corollary 4.12. *There is no automorphism of \mathcal{Q} of order $5 \cdot 37$.*

Proof. Suppose for contradiction that there exists an automorphism z of order $5 \cdot 37$. Then we may write $z = xy = yx$ for some automorphisms x and y with $|x| = 5$ and $|y| = 37$. Then by Lemma 4.11, $\alpha_0(x) \equiv 0 \pmod{37}$.

By Lemma 4.1, \mathcal{Q}_x is either a grid with parameters $(1, 6)$, a dual grid with parameters $(1, 6)$, or a GQ of order $(1, 1)$. In the first, case $\alpha_0(x) = 14$, in the second case, $\alpha_0(x) = 9$, and in the third case, $\alpha_0(x) = 4$. Each case contradicts $\alpha_0(x) \equiv 0 \pmod{37}$, and so there is no automorphism of order $5 \cdot 37$. \square

Corollary 4.13. *There is no automorphism of \mathcal{Q} of order $3 \cdot 37$.*

Proof. Suppose for contradiction that there exists an automorphism z of order $3 \cdot 37$. Then we may write $z = xy = yx$ for some automorphisms x and y with $|x| = 3$ and $|y| = 37$. By Lemma 4.1, \mathcal{Q}_x is either type (2) or (2'). Using duality, we may assume without loss of generality that \mathcal{Q}_x is type (2'). Then, x has a fixed point, and all fixed points of x are incident to a single line. Thus, $1 \leq \alpha_0(x) \leq 7$. However, by Lemma 4.11, $\alpha_0(x) \equiv 0 \pmod{37}$. This contradicts $1 \leq \alpha_0(x) \leq 7$, and so there can be no automorphism of order $3 \cdot 37$. \square

Corollary 4.14. *There is no automorphism of \mathcal{Q} of order $2 \cdot 37$.*

Proof. Suppose for contradiction that there exists an automorphism z of order $2 \cdot 37$. Then we may write $z = xy = yx$ for some automorphisms x and y with $|x| = 2$ and $|y| = 37$. By Lemma 4.1, \mathcal{Q}_x is either type (2) or (2'), or is a GQ of order $(2, 2)$. Using duality, we may assume without loss of generality that \mathcal{Q}_x is type (2') or a GQ of order $(2, 2)$. In the former case, x has a fixed point, and all fixed points of x are incident to a single line. Thus, $1 \leq \alpha_0(x) \leq 7$. In the latter case, $\alpha_0(x) = 15$. By Lemma 4.11, $\alpha_0(x) \equiv 0 \pmod{37}$, which contradicts both of these cases. Therefore, there can be no automorphism of order $2 \cdot 37$. \square

Since we have ruled out automorphisms of order $37p$ for every $p \in \{2, 3, 5, 7, 37\}$, we conclude that \mathcal{Q} has no automorphisms of order $37p$ for any prime p .

4.2 Proof of Intransitivity

In this section, we prove the following:

Theorem 4.15. *Let \mathcal{Q} be the generalized quadrangle of order 6 and G its full automorphism group. Then G does not act transitively on either points or lines of \mathcal{Q} .*

Let G be the automorphism group of \mathcal{Q} . Our first objective is to prove that if G is transitive, then it must also be quasiprimitive. This allows us use Theorem 2.21, and narrow down the types of groups that may act on \mathcal{Q} .

Lemma 4.16. *Suppose that $G = \text{Aut}(\mathcal{Q})$ is transitive on points. Then G must act quasiprimitively on points. Dually, if G is transitive on lines, then G must act quasiprimitively on lines.*

Proof. It suffices to show that if G is point-transitive, then it is quasiprimitive on points, since the corresponding statement for lines follows by duality. Suppose for contradiction that the action of G on \mathcal{P} is not quasiprimitive, i.e., there exists a normal subgroup $N \trianglelefteq G$ which is not transitive on \mathcal{P} . Let P be a Sylow p -subgroup of N for some prime p . By the Frattini Argument, $G = N_G(P)N$. Thus, $|G|$ divides $|N_G(P)| \cdot |N|$.

The group N is a normal subgroup of a transitive group G , so all the stabilizer subgroups of N must be the same size. (If $Q^x = Q'$, then $N_Q = xN_{Q'}x^{-1} = N_{Q'}.$) Therefore, all the orbits have got to be the same size. Since N acts intransitively and nontrivially on \mathcal{P} , there are two possibilities:

- (1) There are 7 distinct N -orbits of \mathcal{P} with size 37
- (2) There are 37 distinct N -orbits of \mathcal{P} with size 7.

Suppose first that (1) holds. Let 7^k be the largest power of 7 which divides $|G|$. Since N acts transitively on a set of size 37, then $37 \mid |N|$. Let P be a Sylow 37-subgroup of N which has size 37. Since G is transitive on the 7 N -orbits, $7 \mid |G : N|$. Since G is not divisible by 7^{k+1} and $|G| = |G : N| \cdot |N|$, then $7^k \nmid |N|$.

Note that 7^k divides $|G|$ which in turn divides $|N_G(P)| \cdot |N|$. If, for contradiction, we assume that $7 \nmid |N_G(P)|$, then by Euclid's Lemma, $7^k \mid |N|$, a contradiction. Therefore, $7 \mid |N_G(P)|$. The automorphism of order 7 must act trivially on the Sylow 37-subgroup of order 37, and so we retrieve an element of order $7 \cdot 37$, a contradiction.

Suppose next that (2) holds. Since N acts transitively on a set of size 7, then $7 \mid |N|$. Let P be a Sylow 7-subgroup of N which has size at most 7^3 by Lemma 4.9. Since G is transitive on the 37 N -orbits, $37 \mid |G : N|$. Since G is not divisible by 37^2 , this implies that $37 \nmid |N|$. Since 37 divides $|G|$ which in turn divides $|N_G(P)| \cdot |N|$, then by Euclid's Lemma, $37 \mid |N_G(P)|$. A computer search over all groups of order 7^k for $1 \leq k \leq 3$ reveals that the automorphism of order 37 must act trivially on N . Therefore, we retrieve an element of order $37 \cdot 7$, a contradiction.

In both (1) and (2) we arrive at a contradiction, so therefore the action of G on \mathcal{P} must be quasiprimitive. \square

Since G is quasiprimitive on points (assuming it must be transitive on points), we may employ Theorem 2.21. This theorem states that the socle of G must be of the form T^k for T a simple group. Since the set \mathcal{P} on which G acts does not have prime power size, the theorem further implies that T must be a *nonabelian* simple group.

We can further narrow down the structure of this socle. Let $H = T^k$ be the socle of G . Then H is a normal subgroup of G , being the product of normal subgroups of G . Since G acts on \mathcal{P} quasiprimitively, then its normal subgroup H must act transitively on G . Then 37 must divide the order of H , and so 37 divides $|T^k| = |T|^k$. Thus, $37 \mid |T|$. However, if $k \geq 2$, then $37^2 \mid |H| \mid |G|$, contradicting Lemma 4.2. Therefore, $k = 1$, and $H = T$ is a nonabelian simple group, which acts transitively

on \mathcal{P} .

In this light, it makes sense to narrow down the finite simple groups which can act transitively on \mathcal{P} . By Lemma 4.1, the only primes which may divide the order of a group G which acts faithfully on \mathcal{Q} are 2, 3, 5, 7, and 37. This motivates us to consider groups whose orders are divisible by a small number of primes.

Definition 4.17. A group G is a K_n -group if the order of G is divisible by exactly n primes.

For example, the linear group $\text{PSL}(2, 7)$ is a K_3 -group, since its order is $2^3 \cdot 3 \cdot 7$. The classification of simple K_n -groups is solved for $n \leq 6$. For $n = 1$, it is well known that the simple K_1 -groups are abelian of prime order. For $n = 2$, it is the precise statement of Burnside's theorem that every K_2 -group is solvable. Since such groups are solvable and divisible by multiple primes, they cannot be simple.

The case of $n = 3, 4$ is handled in [3], and the case of $n = 5, 6$ is handled in [5]. For the convenience of the reader, we reproduce the statements of these results for $n = 3, 4, 5$ in Appendix A as Theorems A.1, A.2 and A.3 respectively.

Our goal will be to rule out any simple K_3 -group, K_4 -group, or K_5 -group acting transitively on \mathcal{P} . This will result in a contradiction since by the above discussion, a simple K_3 -, K_4 -, or K_5 -group must act transitively on \mathcal{P} . To do this, we will use two facts:

- (1) If T acts transitively on \mathcal{P} , then \mathcal{P} is a single T -orbit, and so $|\mathcal{P}|$ divides $|T|$.
In particular, this entails that 7 and 37 divide $|T|$.
- (2) If T acts faithfully on \mathcal{P} , then the elements of T may be identified with automorphisms of \mathcal{Q} . Thus, the only prime order automorphisms of T must have order 2, 3, 5, 7, or 37, and so the only primes which may divide $|T|$ are 2, 3, 5, 7, or 37.

- (3) If T is a simple group acting on a set Ω , then T acts faithfully on Ω if and only if T acts nontrivially on Ω . This is because the kernel K of the action of T on Ω is a normal subgroup of T . If T acts faithfully on Ω , then T obviously acts nontrivially on Ω . However, if T acts nontrivially on Ω , then $K \neq T$, so $K = 1$ by simplicity of T , and so T acts faithfully on Ω .

We may use the first of these facts to immediately rule out every simple K_3 -group. Theorem A.1 states that there are only finitely many simple K_3 -groups, and that they may all be found (up to isomorphism) on Table A.1. An inspection of this table reveals that none of these groups have order divisible by 37, and so by fact (1), none of them may act point-transitively on \mathcal{Q} . Therefore, we have ruled out K_3 -groups acting point-transitively on \mathcal{Q} .

Next, we turn our attention to the simple K_4 -groups. Theorem A.2 states that if T is a simple K_4 -group, then T must either be isomorphic to $\text{PSL}(2, q)$ for some prime power q , or T is isomorphic to one of the groups listed on Table A.2. This requires that we rule out our first infinite family of simple groups, a task for which we must use some higher technology.

For G a group, define $P(G)$ to be the smallest $n \geq 0$ such that G acts nontrivially on a set of size n . If $P(G)$ is greater than 259 for some group G , then G must act trivially – and therefore intransitively – on points of \mathcal{Q} . Thus, a good bound on $P(\text{PSL}(2, q))$ can limit the number of groups that may act nontrivially on \mathcal{Q} . Fortunately, an explicit calculation of $P(\text{PSL}(2, q))$ is given in [6, Theorem 5.2.2], as well as calculations of $P(T)$ for many other families of simple groups. We can now rule out $\text{PSL}(2, q)$ acting transitively on \mathcal{P} for any prime power q :

Lemma 4.18. *No group of the form $\text{PSL}(2, q)$ acts transitively and faithfully on \mathcal{Q} .*

Proof. Suppose $\text{PSL}(2, q)$ acts transitively on \mathcal{Q} . Then it acts nontrivially on \mathcal{P} . By [6, Theorem 5.2.2], if $\text{PSL}(2, q)$ acts nontrivially on a set of size 259, we must have

$q + 1 = (q^2 - 1)/(q - 1) \leq 259$. This means that $q \leq 258$. However, recall for odd q , that $|\text{PSL}(2, q)| = q(q^2 - 1)/2$, and so $q \mid |\text{PSL}(2, q)|$. By Lemma 4.1, it follows that an odd q must be a power of 3, 5, 7, or 37. Combining these constraints, we glean that q is one of the following:

$$2, 4, 8, 16, 32, 64, 128, 256, 3, 9, 27, 81, 243, 5, 25, 125, 7, 49, 37.$$

The only q among the above list for which $37 \mid |\text{PSL}(2, q)|$ is $q = 37$. However, 7 does not divide $|\text{PSL}(2, 37)|$, so $q = 37$ is ruled out as well. Therefore, no group of the form $\text{PSL}(2, q)$ acts faithfully and point-transitively on \mathcal{Q} . \square

From here, a simple inspection reveals that no group listed on Table A.2 has order divisible by 37, and so no group on this table may act point-transitively on \mathcal{Q} . Since we also know that no group of the form $\text{PSL}(2, q)$ may act point-transitively on \mathcal{Q} , then by Theorem A.2, we know that no K_4 -group may act point-transitively on \mathcal{Q} .

Finally, we rule out every K_5 -group. Theorem A.3 states that if T is a simple K_5 -group, then there are seven possibilities:

- (1) $T \cong \text{PSL}(2, q)$ for some prime power q ;
- (2) $T \cong \text{PSL}(3, q)$ for some prime power q ;
- (3) $T \cong U_3(q)$ for some prime power q ;
- (4) $T \cong \text{PSp}_4(q)$ for some prime power q ;
- (5) $T \cong \text{Sz}(2^{2m+1})$ for some $m \geq 1$;
- (6) $T \cong R(3^{2n+1})$ for some $n \geq 1$;
- (7) T is isomorphic to a group listed on Table A.3.

We have already ruled out the first infinite family of K_5 -groups, so this leaves us five more to rule out. We can again use [6, Theorem 5.2.2] for possibilities (2), (3), and (4). However, for possibilities (5) and (6), more elementary methods suffice.

Lemma 4.19. *No group of the form $\text{PSL}(3, q)$ acts transitively on \mathcal{Q} .*

Proof. Suppose $\text{PSL}(3, q)$ acts transitively on \mathcal{Q} . Then it acts nontrivially on \mathcal{P} . By [6, Theorem 5.2.2], if $\text{PSL}(3, q)$ acts nontrivially on a set of size 259, we must have $q^2 + q + 1 = (q^3 - 1)/(q - 1) \leq 259$. This means that $q \leq 15$. Since q is a prime power, this means $q \in \{2, 4, 8, 3, 9, 5, 7, 11, 13\}$. We may then manually check that $37 \nmid |\text{PSL}(3, q)|$ for each $q \in \{2, 4, 8, 3, 9, 5, 7, 11, 13\}$. Thus, $\text{PSL}(3, q)$ can never be transitive on \mathcal{Q} . \square

Lemma 4.20. *No group of the form $U_3(q)$ acts transitively on \mathcal{Q} .*

Proof. Suppose that $U_3(q)$ acts transitively on \mathcal{Q} . Then it acts nontrivially on \mathcal{P} . By [6, Theorem 5.2.2], if $U_3(q)$ acts nontrivially on a set of size 259, we must have $q^3 + 1 \leq 259$. Therefore, $q \leq 6$. Since q is a prime power, our only four possibilities are $q = 2, 4, 3, 5$. We can manually check that $37 \nmid |U_3(q)|$ for all such q , and the result follows. \square

Lemma 4.21. *No group of the form $\text{PSp}_4(q)$ acts transitively on \mathcal{Q} .*

Proof. Suppose that $\text{PSp}_4(q)$ acts transitively on \mathcal{Q} . If $q = 2, 3$, then $37 \nmid |\text{PSp}_4(2)|$, a contradiction. Thus, $q > 3$.

Since $\text{PSp}_4(q)$ acts transitively on \mathcal{Q} , it acts nontrivially on \mathcal{P} . By [6, Theorem 5.2.2], if $\text{PSp}_4(q)$ acts nontrivially on a set of size 259 and $q > 3$, we must have $q^3 + q^2 + q + 1 = (q^4 - 1)/(q - 1) \leq 259$. Thus, $q \leq 6$. Since q is a prime power, and $q > 3$, this means $q = 4, 5$. However, we can manually check that $37 \nmid |\text{PSp}_4(q)|$, for $q \in \{4, 5\}$, a contradiction. Therefore, no group of the form $\text{PSp}_4(q)$ can act transitively on \mathcal{Q} . \square

For the case of the Suzuki and Ree groups, their orders are much more controlled. In particular, it is well known that Suzuki groups are $3'$ -groups, and that Ree groups are $5'$ -groups. However, if a K_5 -group T acts faithfully on \mathcal{Q} , then its prime divisors must be exactly 2, 3, 5, 7, and 37, otherwise G is not a K_5 -group, or some prime $p \notin \{2, 3, 5, 7, 37\}$ divides $|G|$, which is not allowed by Lemma 4.1. Since K_5 Suzuki groups do not have 3 as a prime divisor, and K_5 Ree groups do not have 5 as a prime divisor, they cannot act faithfully on \mathcal{Q} . Since there are no K_4 Ree groups, and neither of the two K_4 Suzuki groups, $Sz(2)$ and $Sz(8)$, have order not divisible by 37, (see Table A.2), we have eliminated possibilities (5) and (6).

Finally, an inspection of Table A.3 reveals that none of the groups on that table have order divisible by 37, and so none of those groups can act transitively on points of \mathcal{Q} . Therefore, we have ruled out possibility (7). Since we ruled out the preceding six possibilities above, then we may invoke Theorem A.3 to say that no simple K_5 -group may act point-transitively on \mathcal{Q} .

In the discussion above, we have proven that no simple K_3 -, K_4 -, or K_5 -group may act point-transitively on \mathcal{Q} . However, simple K_3 -, K_4 -, or K_5 -groups are the only nonabelian simple groups which may act transitively on \mathcal{Q} , since the full automorphism group G of \mathcal{Q} has at most five prime divisors. This means that no nonabelian simple group can act point-transitively on \mathcal{Q} . However, the discussion after Lemma 4.16 tells us that if G is transitive, then G must have a normal, nonabelian, simple subgroup which is also point-transitive. Since no nonabelian simple group may act point-transitively on \mathcal{Q} , we may conclude that G cannot be point-transitive. A dual argument shows that G cannot be line-transitive either, and so we have proven Theorem 4.15.

4.3 Solvability

Let \mathcal{Q} be the putative generalized quadrangle of order 6. In this section, we detail a sufficient condition to show that $G = \text{Aut}(\mathcal{Q})$ is not solvable. This condition also serves to rule out a prime dividing $|G|$ in the case that G is solvable.

Recall that for every finite group G , there exists a series of subgroups $N_0 = \{1\}, N_1, \dots, N_k = G$ such that $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is simple. Such a series is called a *composition series*, and the simple groups N_{i+1}/N_i are called the *composition factors* of G . It is the precise statement of the Jordan-Hölder Theorem that the isomorphism types and multiplicities of the composition factors of G are the same for every composition series of G . A *solvable* group, then, is a group whose composition factors are all cyclic of prime order. Solvable groups are very well-studied. Indeed, by a theorem of Burnside, every group whose order is $p^m q^n$, for p, q prime, must be solvable. (See [4, 7.8. Theorem].)

Another fact about solvable groups is that a stronger form of Sylow E applies to them. If G is a group, and π is a set of primes dividing $|G|$, a *Hall π -subgroup* of G is a subgroup $H \leq G$ such that $p \nmid |G : H|$ for every $p \in \pi$. It can be easily seen that if $\pi = \{p\}$, then a Hall π -subgroup of G is just a Sylow p -subgroup of G . However, Hall π -subgroups are not guaranteed to exist if π has two or more elements. For instance, the alternating group A_5 has a Hall $\{2, 3\}$ -subgroup, but no Hall $\{2, 5\}$ -subgroup or Hall $\{3, 5\}$ -subgroup. However, for solvable groups, things are much nicer.

Proposition 4.22. [4, 3.19 Corollary and 3.20 Theorem] Let G be a solvable group, and π a set of primes, each of which divides $|G|$. Then G has a Hall π -subgroup.

Let \mathcal{Q} be the putative generalized quadrangle of order 6, and $G = \text{Aut}(\mathcal{Q})$. It will be our goal in this section to prove that G cannot have a Hall $\{7, 37\}$ -subgroup. In order to do this, we must narrow down the structure of such a group. This necessitates the following definitions.

Definition 4.23. Let G be a group, and suppose that $G = NH$, where N is a normal subgroup of G and H is merely a subgroup of G , and N and H are nontrivial. Then H acts on N via conjugation. If the only H -fixed point of N is the identity $1 \in N$, we say that G is a *Frobenius* group.

If G has normal subgroups N_1 and N_2 such that $N_1 \leq N_2$, G/N_1 is a Frobenius group, and N_2 is a Frobenius group, we say that G is a 2-Frobenius group.

Note that if $G = NH$ is a Frobenius group, then N is partitioned by H -orbits, all of which are size $|H|$ except for the singleton $\{1\}$. As such, if $G = NH$ is a Frobenius group, then $|N| \equiv 1 \pmod{|H|}$. In particular, the orders of N and H are coprime.

The second piece we will incorporate is the notion of *prime graphs*. If G is a finite group, the *prime graph* of G , denoted $\Gamma(G)$, is the graph whose vertices are the primes dividing $|G|$ such that there is an edge between p and q if there is an element of order pq in G . However, the complement of the prime graph of G , denoted $\bar{\Gamma}(G)$ is more often studied, since it tells us about the structure of the Hall $\{p, q\}$ -subgroups of G .

Lemma 4.24. *Let G be a group, and suppose that $\{p, q\}$ is an edge in $\bar{\Gamma}(G)$. Then the Hall $\{p, q\}$ -subgroup of G , if it exists, is either Frobenius or 2-Frobenius.*

Proof. Suppose that $\{p, q\}$ is an edge in $\bar{\Gamma}(G)$ and that H is a Hall $\{p, q\}$ -subgroup of G . By Burnside's famous pq Theorem, H must be solvable. Since G contains no element of order pq , then neither does H , so $\{p, q\}$ is still an edge in $\bar{\Gamma}(H)$. Thus, the prime graph of G consists of the disconnected vertices p and q . By [13, Theorem A and Corollary], this entails that H is Frobenius or 2-Frobenius. \square

If G is the automorphism group of the GQ of order 6, we showed in Subsection 4.1.2 that $\{37, p\}$ must be an edge in $\bar{\Gamma}(G)$ if $37 \mid |G|$ and $p \mid |G|$. In particular, this means that if $259 \mid |G|$, then the Hall $\{7, 37\}$ -subgroup of G – if it exists – must be Frobenius or 2-Frobenius. In either case, a Frobenius $\{7, 37\}$ -group acts on \mathcal{Q} . Therefore, it is of interest to us to investigate whether such a situation can occur.

Suppose $G = NH$ be a Frobenius $\{7, 37\}$ -group acting faithfully on \mathcal{Q} . Then $|N| \equiv 1 \pmod{|H|}$, so $|N|$ and $|H|$ must be coprime. In particular, either N is a 37-group and H is a 7-group, or N is a 7-group and H is a 37-group. Consider the former case. By Lemma 4.2, N must have order exactly 37. If $|H| = 7^k$, this means that H must satisfy

$$37 \equiv 1 \pmod{7^k}.$$

However, for $k = 1$ this fails, and for $k \geq 2$, this also fails. So N cannot be a 37-group.

This means that H must be a 37-group, and N must be a 7-group. If $|N| = 7^k$, then N must satisfy

$$7^k \equiv 1 \pmod{37}.$$

By the laws of modular arithmetic, this is eventually satisfied, however the smallest positive k which satisfies this equation is $k = 9$. We know that any 7-group acting faithfully on \mathcal{Q} has order not exceeding 7^3 , by Lemma 4.9, so therefore, N cannot be a 7-group either. Therefore, N is trivial, and so G is not a Frobenius group. This contradiction shows that no Frobenius $\{7, 37\}$ -group can act faithfully on \mathcal{Q} . We may combine this result, along with all the notions previously discussed in the section, into the following proposition.

Proposition 4.25. *Let G be a group acting faithfully on the generalized quadrangle \mathcal{Q} of order 6 such that 7 and 37 divide $|G|$. Then G does not admit a Hall $\{7, 37\}$ -subgroup. In particular, G is not solvable.*

Proof. Since G acts faithfully on \mathcal{Q} , we may take G without loss of generality to be a subgroup of $\text{Aut}(\mathcal{Q})$. Then by Lemma 4.10, $\{7, 37\}$ is an edge in the prime graph complement of G . This entails that any Hall $\{7, 37\}$ -subgroup of G – if any exist – must be Frobenius or 2-Frobenius. Suppose for contradiction that H is such a group. In either case, H has a subgroup K which is a Frobenius $\{7, 37\}$ -subgroup. However, no such group can exist. Therefore, G has no Hall $\{7, 37\}$ -subgroup. If G

were solvable, G would have a Hall $\{7, 37\}$ -subgroup, so G cannot be solvable. \square

This proposition provides a sufficient condition for a group G acting faithfully on \mathcal{Q} to be non-solvable (when 7 and 37 divide $|G|$), and it also provides sufficient conditions to rule out either an automorphism of order 7, or an automorphism of order 37 (when $G = \text{Aut}(\mathcal{Q})$ is solvable).

Appendix A

The Finite Simple K_3 -, K_4 -, and K_5 -Groups

In this appendix, we list the classification results for simple K_3 -, K_4 -, and K_5 -groups. For each $n \in \{3, 4, 5\}$, we state the classification of K_n -groups, and provide a table listing every K_n -group which does not fall into some infinite family of K_n -groups.

The classification of K_3 - and K_4 -groups is originally given as one theorem in [3, Theorem I], however, it is more convenient to split it up into two separate theorems.

Theorem A.1. *Let T be a simple K_3 -group. Then T is isomorphic to one of the groups listed on Table A.1.*

Theorem A.2. *Let T be a simple K_4 -group. Then either T is isomorphic to $\text{PSL}(2, q)$ for some prime power q , or T is isomorphic to one of the groups on Table A.2.*

Table A.1 is a reproduction of [3, TABLE 1] and Table A.2 is a reproduction of [3, TABLE 2].

Next, we deal with the case of K_5 -groups. The classification result was originally proven in [5, Theorem A], however an error was made in the statement of this result. Therefore, we also cite [14, Lemma 2.6], in which a corrected version of the theorem is given. The theorem follows:

T	$ T $
A_5	$2^2 \cdot 3 \cdot 5$
A_6	$2^3 \cdot 3^2 \cdot 5$
$U_4(2)$	$2^6 \cdot 3^4 \cdot 5$
$\text{PSL}(2, 7)$	$2^3 \cdot 3 \cdot 7$
$\text{PSL}(2, 8)$	$2^3 \cdot 3^2 \cdot 7$
$U_3(3)$	$2^5 \cdot 3^3 \cdot 7$
$\text{PSL}(3, 3)$	$2^4 \cdot 3^3 \cdot 13$
$\text{PSL}(2, 17)$	$2^4 \cdot 3^2 \cdot 17$

Table A.1: The simple K_3 -groups

Theorem A.3. *Let T be a simple K_5 -group. Then one of the following holds:*

- (1) T is isomorphic to $\text{PSL}(2, q)$ for some prime power q .
- (2) T is isomorphic to $\text{PSL}(3, q)$ for some prime power q .
- (3) T is isomorphic to $U_3(q)$ for some prime power q .
- (4) T is isomorphic to $\text{PSp}_4(q) \cong O_5(q)$ for some prime power q .
- (5) T is isomorphic to $\text{Sz}(2^{2m+1})$ for some $m \geq 1$.
- (6) T is isomorphic to $R(3^{2n+1})$ for some $n \geq 1$.
- (7) T is isomorphic to one of the groups on table A.3.

Table A.3 is a reproduction of the table immediately following Lemma 2.12 in [14].

T	$ T $		T	$ T $
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$		$Sp_4(4)$	$2^8 \cdot 3^2 \cdot 5 \cdot 17$
A_7	$2^3 \cdot 3^2 \cdot 5 \cdot 7$		$PSL(3, 5)$	$2^5 \cdot 3 \cdot 5^3 \cdot 31$
A_8	$2^6 \cdot 3^2 \cdot 5 \cdot 7$		$PSp_4(9)$	$2^8 \cdot 3^8 \cdot 5^2 \cdot 41$
$A_9 \cong PSL(4, 2)$	$2^6 \cdot 3^4 \cdot 5 \cdot 7$		$U_3(9)$	$2^5 \cdot 3^6 \cdot 5^2 \cdot 73$
A_{10}	$2^7 \cdot 3^4 \cdot 5^2 \cdot 7$		$G_2(3)$	$2^6 \cdot 3^6 \cdot 7 \cdot 13$
$PSL(3, 4)$	$2^6 \cdot 3^2 \cdot 5 \cdot 7$		${}^3D_4(2)$	$2^{12} \cdot 3^4 \cdot 7^2 \cdot 13$
$U_3(5)$	$2^4 \cdot 3^2 \cdot 5^3 \cdot 7$		$PSL(3, 7)$	$2^5 \cdot 3^2 \cdot 7^3 \cdot 19$
$U_4(3)$	$2^7 \cdot 3^6 \cdot 5 \cdot 7$		$U_3(8)$	$2^9 \cdot 3^4 \cdot 7 \cdot 19$
$PSp_4(7)$	$2^8 \cdot 3^2 \cdot 5^2 \cdot 7^4$		$U_3(8)$	$2^9 \cdot 3^4 \cdot 7 \cdot 19$
$Sp_6(2) \cong O_7(2)$	$2^9 \cdot 3^4 \cdot 5 \cdot 7$		$U_3(8)$	$2^9 \cdot 3^4 \cdot 7 \cdot 19$
$O_8^+(2)$	$2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$		$U_3(7)$	$2^7 \cdot 3 \cdot 7^3 \cdot 43$
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$		$PSL(3, 8)$	$2^9 \cdot 3^2 \cdot 17^3 \cdot 307$
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$		$Sz(8)$	$2^6 \cdot 5 \cdot 7 \cdot 13$
$U_5(2)$	$2^{10} \cdot 3^5 \cdot 5 \cdot 11$		$Sz(32)$	$2^{10} \cdot 5^2 \cdot 31 \cdot 41$
$PSL(4, 3)$	$2^7 \cdot 3^6 \cdot 5 \cdot 13$			
$U_3(4)$	$2^6 \cdot 3 \cdot 5^2 \cdot 13$			
$PSp_4(5)$	$2^6 \cdot 3^2 \cdot 5^4 \cdot 13$			
${}^2F_4(2)'$	$2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$			

Table A.2: Simple K_4 -groups not isomorphic to $PSL(2, q)$

T	$ T $		T	$ T $
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$		J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$		He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$		A_{11}	$2^7 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$
A_{12}	$2^9 \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$		$PSL(4, 5)$	$2^7 \cdot 3^2 \cdot 5^6 \cdot 13 \cdot 31$
$PSL(4, 7)$	$2^9 \cdot 3^4 \cdot 5^2 \cdot 7^6 \cdot 19$		$PSL(5, 2)$	$2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$
$PSL(6, 2)$	$2^{15} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$		$U_4(5)$	$2^5 \cdot 3^4 \cdot 5^4 \cdot 7 \cdot 13$
$U_4(7)$	$2^{10} \cdot 3^2 \cdot 5^2 \cdot 7^6 \cdot 43$		${}^3D_4(3)$	$2^6 \cdot 3^{12} \cdot 7^2 \cdot 13^2 \cdot 73$
$G_2(4)$	$2^{12} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13$		$G_2(5)$	$2^6 \cdot 3^3 \cdot 5^6 \cdot 7 \cdot 31$
$G_2(7)$	$2^8 \cdot 2^3 \cdot 7^6 \cdot 19 \cdot 43$		$G_2(8)$	$2^{18} \cdot 3^5 \cdot 7^2 \cdot 19 \cdot 73$
$S_8(2)$	$2^{16} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17$		$U_5(3)$	$2^{11} \cdot 3^{10} \cdot 5 \cdot 7 \cdot 61$
$PSL(5, 3)$	$2^9 \cdot 3^{10} \cdot 5 \cdot 11^2 \cdot 13$		$O_8^+(3)$	$2^{12} \cdot 3^{12} \cdot 5^2 \cdot 7 \cdot 13$
$O_8^-(2)$	$2^{12} \cdot 3^4 \cdot 5 \cdot 7 \cdot 17$		$U_6(2)$	$2^{15} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11$
$PSL(4, 4)$	$2^{12} \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 17$		$U_4(4)$	$2^{12} \cdot 3^2 \cdot 5^3 \cdot 13 \cdot 17$
$U_4(9)$	$2^9 \cdot 3^{12} \cdot 5^3 \cdot 41 \cdot 73$		$PSL(3, 9)$	$2^7 \cdot 3^6 \cdot 5 \cdot 7 \cdot 13$
$U_3(17)$	$2^6 \cdot 3^4 \cdot 5 \cdot 17^4 \cdot 29$		$S_4(8)$	$2^{12} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13$
$S_4(17)$	$2^{10} \cdot 3^4 \cdot 5 \cdot 17^4 \cdot 29$		$O_7(3)$	$2^9 \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$
$S_6(3)$	$2^9 \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$			

Table A.3: Simple K_5 -groups not isomorphic to $PSL(2, q)$, $PSL(3, q)$, $U_3(q)$, $S_4(q)$, $Sz(2^{2m+1})$, or $R(q)$.

Bibliography

- [1] Santana F. Afton and Eric Swartz. “On prime order automorphisms of generalized quadrangles”. In: *Algebraic Combinatorics* 3.1 (2020), pp. 143–160. DOI: 10.5802/alco.89. URL: <https://alco.centre-mersenne.org/articles/10.5802/alco.89/>.
- [2] S. De Winter and K. Thas. “Generalized quadrangles with an abelian singer group”. eng. In: *Designs, codes, and cryptography* 39.1 (2006), pp. 81–87. ISSN: 0925-1022.
- [3] B. Huppert and W. Lempken. “Simple groups of order divisible by at most four primes”. In: *Izvestiya Gomel’skogo Gosudarstvennogo Universiteta Im. F. Skoriny* 16 (Jan. 2000).
- [4] I. M. Isaacs. *Finite Group Theory*. American Mathematical Society, 2008.
- [5] A. Jafarzadeh and A. Iranmanesh. “On simple K_n -groups for $n = 5, 6$ ”. In: *Groups St Andrews 2005*. Ed. by C. M. Campbell, M. R. Quick, E. F. Robertson, and G. C. Editors Smith. Vol. 2. London Mathematical Society Lecture Note Series. Cambridge University Press, 2007, pp. 517–526. DOI: 10.1017/CB09780511721205.016.
- [6] Peter B. Kleidman and Martin W. Liebeck. *The Subgroup Structure of the Finite Classical Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1990. DOI: 10.1017/CB09780511629235.

- [7] Stanley E. Payne and Joseph A. Thas. “Finite Generalized Quadrangles”. In: 2009.
- [8] Cheryl Praeger. “An O’Nan-Scott Theorem for Finite Quasiprimitive Permutation Groups and an Application to 2-Arc Transitive Graphs”. In: *Journal of the London Mathematical Society. Second Series* 47 (Apr. 1993). DOI: 10.1112/jlms/s2-47.2.227.
- [9] Joseph J. Rotman. *An Introduction to the Theory of Groups*. eng. 4th ed. Graduate Texts in Mathematics Series ; v.148. New York, NY: Springer New York, 1999. ISBN: 9781461241768.
- [10] Parcly Taxel. *GQ(2,2), the Doily.svg*. [Online; accessed April 21, 2023]. 2017. URL: [https://commons.wikimedia.org/wiki/File:GQ\(2,2\),_the_Doily.svg](https://commons.wikimedia.org/wiki/File:GQ(2,2),_the_Doily.svg).
- [11] Jacques Tits. “Sur la trialité et certains groupes qui s’en déduisent”. In: *Publications Mathématiques de l’Institut des Hautes Études Scientifiques* 2 (1959), pp. 14–60.
- [12] Henrik Van Maldeghem. *Generalized Polygons*. Birkhäuser, 1998.
- [13] J.S Williams. “Prime graph components of finite groups”. In: *Journal of Algebra* 69.2 (1981), pp. 487–513. ISSN: 0021-8693. DOI: [https://doi.org/10.1016/0021-8693\(81\)90218-0](https://doi.org/10.1016/0021-8693(81)90218-0). URL: <https://www.sciencedirect.com/science/article/pii/0021869381902180>.
- [14] Dapeng Yu, Jinbao Li, Guiyun Chen, Liangcai Zhang, and Wujie Shi. “A new characterization of simple K_5 -groups of type $L_3(p)$ ”. In: *Bulletin of the Iranian Mathematical Society* 45 (2018), pp. 771–781.