On a Problem of Platonov and Potapchik regarding Unipotent Groups

by

Benjamin Young

Thesis in partial fulfillment of
Master of Science
School of Mathematics and Statistics

Carleton University
Ottawa, Ontario
August 19, 2002

©Copyright 2002, Benjamin Young

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-79804-6

Canada

The undersigned reccomend to
the Faculty of Graduate Studies and Research
acceptance of the thesis

“ON A PROBLEM OF PLATONOV AND POTAPCHIK REGARDING
UNIPOTENT GROUPS”

submitted by BENJAMIN YOUNG, B.Math,
in partial fulfillment of the requirements for
the degree of Master of Science.

A handwritten signature in black ink, reading "Brian Mortimer". The script is cursive and fluid.

Chair

A handwritten signature in black ink, reading "J.D. Dixon". The script is cursive and fluid.

Thesis Supervisor

Carleton University
August 17, 2002

Abstract

Platonov and Potapchik conjecture that a two-generator group $G = \langle x, y \rangle$ of matrices over $\mathbb{C}$ is unipotent provided that all words primitive in x and y are unipotent. We show that when $\mathbb{C}$ is replaced with the finite field with p elements, $GF(p)$, the conjecture is false. Moreover, we demonstrate a link between the characteristic 0 and the characteristic p situations which supports Platonov and Potapchik's conjecture.

Acknowledgment:

I would like to thank my advisor, J.D. Dixon, for his support, patience, and inspiration. He is a great mathematician and a great teacher.

Contents

1	Introduction	1
1.1	Primitive words	1
1.2	Unipotence	2
2	The Platonov-Potapchik conjecture over finite fields	3
2.1	Unipotence and p-elements	4
2.2	Property (P2) and quotient groups	5
2.3	Solvable groups	6
2.4	Reducing a solvable counterexample to a simpler form	7
2.5	An alternate formulation of property (P2)	8
2.6	P as a linear group	12
2.7	A counterexample for $p = 2$	14
2.8	Possible generators for P	16
2.9	Counterexamples for $p > 2$	22
3	Connections between characteristics 0 and p	27
3.1	Transcendence bases	27
3.2	A Platonov group over F	29
3.3	A Platonov group over a local ring R	30
3.4	A Platonov group over $GF(p)$	33

4	Conclusions	35
4.1	Future work	35
	Bibliography	38

Chapter 1

Introduction

1.1 Primitive words

Let $F(x, y)$ be the free group on two generators. A word $w_1 \in F(x, y)$ is called *primitive in x and y* if there exists $w_2 \in F(x, y)$ such that $F(x, y) = \langle w_1, w_2 \rangle$. It can be shown (see [5], Proposition I.4.1, p.23) that $F(x, y) = \langle w_1, w_2 \rangle$ if and only if the pair (x, y) may be transformed into (w_1, w_2) with a finite sequence of the following transformations:

$$(N1) \ (u, v) \mapsto (v, u)$$

$$(N2) \ (u, v) \mapsto (u^{-1}, v)$$

$$(N3) \ (u, v) \mapsto (uv, v)$$

These transformations are called *elementary Nielsen transformations*. Note that each of the elementary Nielsen transformations can be inverted using a sequence of elementary Nielsen transformations, and that these transformations induce an equivalence relation on the set of ordered pairs of elements of $F(x, y)$. In particular, all of the generators of $F(x, y)$ form one equivalence class.

If $G = \langle x, y \rangle$ is any two-generator group (not necessarily free), we can define primitive words in x and y using the elementary Nielsen transformations: $w_1 \in G$ is

primitive if there exists a $w_2 \in G$ such that (x, y) may be transformed into (w_1, w_2) by a finite sequence of Nielsen transformations.

Not all generators of G need be primitive words, if G is not free. For example, let S be the set of ordered pairs of generators of the dihedral group with 20 elements, D_{20} . One can verify with a computer algebra package that the elementary Nielsen transformations induce two orbits on S . Call these orbits Ω_1 and Ω_2 . Suppose $D_{20} = \langle x, y \rangle$, with $(x, y) \in \Omega_1$. Then Ω_1 is the set of primitive words in x and y . Ω_2 is the set of all generators which are not primitive in x and y .

1.2 Unipotence

Let G be a linear group of degree n over a field $\mathbf{F}$: that is, a subgroup of the general linear group $\mathrm{GL}(n, \mathbf{F})$. Let x be an element of G . We say that x is *unipotent* if all of the eigenvalues of x are 1, and that G is unipotent if all of its elements are unipotent.

Much is known about unipotent groups. In particular, a unipotent group G is conjugate to a group of upper triangular matrices, implying that G is a solvable group (see [8]). For this reason, it is desirable to find necessary conditions under which a group is unipotent.

In [8], the authors make the following conjecture: If $G = \langle x, y \rangle$ is a linear group of degree n over the complex numbers, and all primitive words in x and y are unipotent, then G is itself unipotent. (In fact, the authors formulate their conjecture for an n -generator group, but we shall only treat the 2-generator case here.)

In this thesis, we present some results related to this conjecture. Our main result is that the conjecture is false when we replace the complex numbers with some finite field. Also, we shall explain a method by which the complex case may be reduced to the finite field case.

Chapter 2

The Platonov-Potapchik conjecture over finite fields

Platonov and Potapchik [8] conjecture that a matrix group over the complex numbers must be unipotent if all of its primitive words are unipotent. To simplify our terminology, we make the following definition:

Definition 2.0.1 *A two-generator linear group G is said to be a Platonov group if G is not unipotent, but G has a pair of generators x, y such that all primitive words in x and y are unipotent.*

Then the conjecture of Platonov and Potapchik states that Platonov groups over the complex numbers do not exist.

In this chapter, we shall replace the complex numbers with a finite field of characteristic p , and demonstrate that in this context, the conjecture is false. In fact, for any prime p , we shall construct a Platonov group over the finite field $GF(p)$ with p elements.

2.1 Unipotence and p -elements

For the rest of this chapter we fix a prime p . Let $\mathbb{F}$ be the finite field with p elements. Because the characteristic of $\mathbb{F}$ is p , we shall see that the unipotent matrices over $\mathbb{F}$ are precisely the matrices whose multiplicative order is a power of p .

Proposition 2.1.1 *Let x be a square matrix over $\mathbb{F}$. Then x is unipotent if and only if $|x| = p^k$ for some $k \geq 0$.*

Proof: First, suppose that x is unipotent. Then the minimal polynomial of x is $(\lambda - 1)^t \in \mathbb{F}[\lambda]$ for some $t \geq 0$. Let k be such that $p^k \geq t$. Then x also is a root of the polynomial $(\lambda - 1)^{p^k} \in \mathbb{F}[\lambda]$, which is identical to $\lambda^{p^k} - 1$ as the characteristic of $\mathbb{F}$ is p . This in turn means that $x^{p^k} = 1$.

Now, suppose that $x^{p^k} = 1$ for some k . Then x is a root of the polynomial $\lambda^{p^k} - 1 = (\lambda - 1)^{p^k}$. Therefore, as the minimal polynomial of x must divide the latter, all eigenvalues of x are equal to one, and x is a unipotent matrix. $\square$

We now make the following definition:

Definition 2.1.1 *Let G be a 2-generator group. Then $x \in G$ is said to be a 2-generator of G if there exists an element y such that $G = \langle x, y \rangle$.*

Let $G = \langle x, y \rangle$ be a 2-generator group. We consider the following properties (which may or may not hold for G):

- (P1) Every primitive word in x and y is a p -element in G .
- (P2) Every 2-generator of G is a p -element.

Note that a primitive word is a 2-generator, so property (P2) implies property (P1). Also, recall that every finite group may be faithfully represented as a linear group over any field (for example, by permutation matrices). Because of Proposition 2.1.1, if we can construct a group G on two generators which satisfies property

(P2) but is not a p -group, a suitable faithful representation of G will be a counterexample to Platonov and Potapchik's hypothesis for characteristic p .

2.2 Property (P2) and quotient groups

Next, we show that property (P2) is preserved under the operation of taking quotient groups of G . For this, we will need the following theorem of W. Gaschütz, from [3]:

Theorem 2.2.1 ([3], Satz 1) *Let G be a finite group which can be generated by n elements (or fewer). Suppose G has a normal subgroup K . Then for every set of n elements $\{x_1K, \dots, x_nK\}$ which generate G/K , there exist $u_1, \dots, u_n \in K$ such that $G = \langle u_1x_1, \dots, u_nx_n \rangle$.*

Proof: Let $H = G/K$ with $\phi : G \rightarrow H$ the canonical projection. Let $L \leq G$; let $\langle x_1K, \dots, x_nK \rangle = H$, for some $S = (x_1, \dots, x_n) \in H^n$. Set

$$t_S(L) = \#\{(v_1, \dots, v_n) \in L^n : \phi(v_i) = x_iK \text{ and } L = \langle v_1, \dots, v_n \rangle\}.$$

We claim that $t_S(L)$ is independent of the choice of generators S for H . The proof is by induction on $|H|$; the base case is when L has no proper subgroups which map surjectively on H . In this case,

$$t_S(L) = \#\{(v_1, \dots, v_n) \in L^n : \phi(v_i) = x_iK\}.$$

If $(x_1K, \dots, x_nK)$ has no preimage in L^n then $\phi(L) < H$, so $t_S(L) = 0$ regardless of the choice of generating set. Otherwise, $\phi(L) = H$ so every generating set of H has a preimage in L . Moreover, each element of H has $|\ker(\phi_L)|$ preimages in L , where ϕ_L is the restriction of ϕ to L . Therefore, $t_S(L) = |\ker(\phi_L)|^n$ for any choice of S .

Now suppose the claim holds for subgroups of G of size smaller than $|L|$. Unless we are in the base case, L has a proper subgroup K with $\phi(K) = H$. Then by induction, $t_S(K)$ is independent of S .

If yK is a coset of K in L , then $\phi(yK) = \phi(y)\phi(K) = H$. Thus, if $x \in H$ has t preimages in K , x has $t|L : K|$ preimages in L , and so $t_S(L) = |L : K|^n t_S(K)$, regardless of the choice of S . The claim is proven.

Now, if $t_S(G) \neq 0$, we are done. But this is the case by construction, because H is a quotient group of G , and G can be generated by n elements. $\square$

Corollary 2.2.1 *Suppose G has property (P2), and K is a normal subgroup of G . Then G/K has property (P2).*

Proof: Let x_1K be a 2-generator of G/K . Then there exists x_2K such that $G/K = \langle x_1K, x_2K \rangle$. By Theorem 2.2.1, there exist $u_1, u_2 \in K$ such that $G = \langle x_1u_1, x_2u_2 \rangle$. As G satisfies (P2), x_1u_1 is a p -element of G , and so $x_1K = x_1u_1K$ is a p -element of G/K . $\square$

2.3 Solvable groups

The fact that property (P2) is preserved under the operation of taking quotient groups suggests that we look among the solvable groups for our counterexample. To see why, we need some elementary facts about solvable groups, which we shall state without proof.

Definition 2.3.1 ([6], Chapter 10, p. 196) *A group G is solvable if it has a normal series*

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{r-1} \supseteq G_r = 1$$

in which G_{i-1}/G_i is abelian for $1 \leq i \leq r$. If G is solvable and the shortest series of this type has length r , then G is said to be solvable of length r .

Theorem 2.3.1 ([6], Theorem 10.07, p.199) *Let G be a group with a subgroup S and a normal subgroup N . Then*

1. if G is solvable of length r then S is solvable of length $\leq r$;
2. if G is solvable of length r then G/N is solvable of length $\leq r$;
3. if $G/N, N$ are solvable of lengths s, t respectively, then G/N is solvable of length $\leq s + t$.

Theorem 2.3.2 ([6], Corollary 10.10, p. 202) *A minimal normal subgroup of a finite solvable group is an elementary abelian p -group, for some prime p .*

2.4 Reducing a solvable counterexample to a simpler form

Suppose that G is a solvable group which satisfies (P2), but is not a p -group. By forming a suitable quotient group of G , we may construct another non- p -group which satisfies (P2), and which has a very simple structure.

Proposition 2.4.1 *There is a quotient group H of G which has the following properties:*

1. H satisfies (P2),
2. H has a minimal normal subgroup A which is an elementary abelian q -group, for some prime $q \neq p$,
3. H/A is a p -group.

Proof: Let $\mathcal{S}$ be the set of all normal subgroups N of G for which G/N is not a p -group. Clearly $1 \in \mathcal{S}$, so $\mathcal{S}$ is nonempty. Partially order $\mathcal{S}$ by inclusion, and let M be a maximal element of $\mathcal{S}$. Set $H = G/M$.

Now, Corollary 2.2.1 implies (1) directly. H is solvable by Theorem 2.3.1, and so by Theorem 2.3.2, H has a minimal normal subgroup A which is an elementary

abelian q -group, for some prime q . Let $\tilde{A} \leq G$ be the normal subgroup of G such that $\tilde{A}/M = A$. Clearly $M < \tilde{A}$. If $q = p$, then there must be some prime $q_0 \neq p$ such that q_0 divides $|H|$. But then $H/A \simeq G/\tilde{A}$ is not a p -group, contradicting the maximality of M . Thus $q \neq p$, proving (2). Finally, if H/A is not a p -group, then neither is $G/\tilde{A}$, again contradicting the maximality of M . This proves (3). $\square$

For convenience, we will assume in the sequel that $G = H$, so that G has the structure described in Proposition 2.4.1. Also, for convenience, let $P = G/A$.

2.5 An alternate formulation of property (P2)

For groups with the structure given in Proposition 2.4.1, we wish to restate Property (P2) in a way which is easier to manage. In order to do this, we will need some basic properties of semidirect products of groups, which we shall state without proof.

Theorem 2.5.1 (*[2], Section 5.5, Theorem 10, p. 178*) *Let H and K be groups and let ϕ be a homomorphism from K into $\text{Aut}(H)$. Let exponentiation denote the (right) action of K on H determined by ϕ . Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G :*

$$(h_1, k_1)(h_2, k_2) = (h_1^{k_2} h_2, k_1 k_2).$$

1. *This multiplication makes G into a group of order $|G| = |H||K|$.*
2. *The sets $\{(h, 1) | h \in H\}$ and $\{(1, k) | k \in K\}$ are subgroups of G and the maps $h \mapsto (h, 1)$ and $k \mapsto (1, k)$ for $k \in K$ are isomorphisms of these subgroups with the groups H and K respectively:*

$$H \simeq \{(h, 1) | h \in H\} \quad \text{and} \quad K \simeq \{(1, k) | k \in K\}.$$

Identifying H and K with their isomorphic copies in G described in (2) we have

3. $H \trianglelefteq G$
4. $H \cap K = 1$
5. for all $h \in H$ and $k \in K$, $k^{-1}hk = h^k = \phi(k)(h)$.

Note that in [2], the authors' group actions are on the left, whereas ours are on the right.

Definition 2.5.1 ([2], Section 5.5, Page 179) Let H and K be groups and let ϕ be a homomorphism from K into $\text{Aut}(H)$. The group described in Theorem 2.5.1 is called the semidirect product of H and K with respect to ϕ and will be denoted by $H \rtimes_{\phi} K$ (when there is no danger of confusion, we shall simply write $H \rtimes K$).

Theorem 2.5.2 ([2], Section 5.5, Theorem 12, Page 182) Suppose G is a group with subgroups H and K such that

1. $H \triangleleft G$, and
2. $H \cap K = 1$.

Let $\phi : K \rightarrow \text{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H . Then $HK \simeq H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K .

Consider the groups G , P and A as defined in the previous section. Let P_0 be a Sylow p -subgroup of G . Because $\gcd(|P_0|, |A|) = \gcd(p, q) = 1$, P_0 and A intersect trivially. Therefore, $|P_0A| = |P_0||A| = |G|$, since p and q are the only primes dividing $|G|$. Thus $G = P_0A$. Moreover, $P = G/A = P_0A/A \simeq P_0/(A \cap P_0) = P_0$ by the Second Isomorphism theorem. Therefore, G is isomorphic to $A \rtimes P$, a semidirect product of A by P , since A is normal in G .

Lemma 2.5.1 *P acts irreducibly on A .*

Proof: Let $a \in A$. We wish to define $a^{xA} = a^x$, but in order to do this we must first see that all elements of xA act on a in the same way. Let $xA = \tilde{x}A \in P$, so $\tilde{x} = bx$ for some $b \in A$. Then, $a^{\tilde{x}} = \tilde{x}^{-1}a\tilde{x} = x^{-1}b^{-1}abx = x^{-1}ax = a^x$, as A is abelian. Hence, we may define $a^{xA} := a^x$. Conjugation by elements of G defines an action of G on A , as A is normal in G . Therefore, we have defined an action of P on A .

Suppose that the action of P on A is reducible. Then P stabilizes some subgroup N of A , which is in fact normal in A as A is abelian. Because P stabilizes N , and the action of P on A coincides with conjugation in the semidirect product, $P \leq N \rtimes P$ normalizes N . This means that N is normal in G . This contradicts the minimality of A in part (3) of Proposition 2.4.1. Thus P acts irreducibly on A . $\square$

G was constructed as a two-generator group. We would now like to see that P is a two-generator group as well. For this, we will need some elementary results on cyclic groups.

Lemma 2.5.2 ([2], Section 2.3, Theorem 7, parts 1 and 3, p.59) *Let H be a cyclic group.*

1. *Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.*
2. *If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a . This subgroup is the cyclic group $\langle x^d \rangle$, where $d = n/a$. Furthermore, for every integer m , $\langle x^m \rangle = \langle x^{\gcd(n,m)} \rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n .*

Corollary 2.5.1 *If H and K are subgroups of a finite cyclic p -group C , with $|H| \leq |K|$, then $H \leq K$.*

Proof: Since C is a p -group, H and K are p -groups as well, so $|H|$ divides K . As K is cyclic, K has precisely one subgroup H_0 of order $|H|$. But then $H_0 \leq C$, and C itself is cyclic. So $H_0 = H$ is the unique subgroup of C of order $|H|$. $\square$

Lemma 2.5.3 *If G satisfies (P2), then P is a 2-generator p -group.*

Proof: G can be generated by two elements, so $P = G/A$ must be either cyclic or two-generator. Suppose P is cyclic.

Let $G = \langle x_1, x_2 \rangle$. Then $P = \langle x_1A, x_2A \rangle$. Without loss of generality, suppose $|x_1A| \leq |x_2A|$. Applying Corollary 2.5.1, we find that $\langle x_1A \rangle \leq \langle x_2A \rangle$, which implies that $x_1A = x_2^tA$ for some $t > 0$. Therefore, $x_1 = x_2^t a$ for some $a \in A$. It follows that $G = \langle x_2^t a, x_2 \rangle = \langle a, x_2 \rangle$. If $a = 1$ then G is cyclic, contradicting the choice of G ; otherwise a is a 2-generator of G , contradicting (P2). Hence, P cannot be cyclic. $\square$

As we shall see, condition (P2) can be described in terms of the action of P on A . In order to do this, we shall need some basic results on the Frattini subgroup of G .

Definition 2.5.2 ([6], Chapter 9, p. 185) *The Frattini subgroup of the group G is the intersection of all the maximal subgroups of G . We adopt the notation $\Phi(G)$ for this subgroup, and the convention that $\Phi(G) = G$ if G has no maximal subgroup.*

Theorem 2.5.3 ([9], Theorem 7.3.2, p. 159) *$\Phi(G)$ is the set of all elements x such that if $G = \langle x, S \rangle$ for some $S \subset G$, then $G = \langle S \rangle$.*

We remark that an element x such as is described in Theorem 2.5.3 is called a *non-generator* of G .

Lemma 2.5.4 ([1], problem 8.10) *If N is a normal subgroup of a group G , and $N \subseteq \Phi(G)$, then $\Phi(G/N) = \Phi(G)/N$.*

Theorem 2.5.4 ([1], problem 8.26) *If P is a finite m -generator p -group, then $P/\Phi(P)$ is an elementary abelian p -group of rank m .*

Write $A^\#$ for the set $A - \{1\}$. We define the following condition:

(P3) If there exist $a \in A^\#$ and $x \in P$ such that $a^x = a$, then $x \in \Phi(P)$.

Proposition 2.5.1 *Conditions (P2) and (P3) are equivalent.*

Proof: First, assume G satisfies (P2). Let $F = \Phi(P)$, and let $x \in P \setminus F$. By Theorem 2.5.4, P/F is elementary abelian. The only non-generator of an elementary abelian group is the identity, so xF is a 2-generator for P/F . Therefore, there exists $y \in P$ such that $P/F = \langle xF, yF \rangle$. It then follows that $P = \langle x, y, F \rangle$; applying Theorem 2.5.3, we have $P = \langle x, y \rangle$. Using Theorem 2.2.1, we may find $b \in A$ such that bx is a 2-generator for G . By (P2), bx is a p -element.

Suppose, for a contradiction, that there exists $a \in A$ such that $a^x = a$. Then we have $a = x^{-1}ax = x^{-1}b^{-1}abx$ as A is abelian, so a commutes with bx . As a result, $(abx)^t = a^t(bx)^t$ for some $t \in \mathbb{N}$. Since a is a q -element and bx is a p -element, abx is a generator of G which is not a p -element, a contradiction. Therefore, G satisfies (P3).

Now, let us assume that G does not satisfy (P2). Then there is some 2-generator x of G which is not a p -element. Suppose $|x| = p^r q^s$, and let $a = x^{p^r}$. Then $|a| = q^b$, so $a \in A$. Since x is not a p -element, $a \neq 1$, so $a \in A^\#$. Also, $a \in \langle x \rangle$, so $a^x = a$. Finally, as x is a 2-generator of G , xA is a 2-generator of P , so xA is a 2-generator of P/F . P/F is a rank 2 elementary abelian p -group by Theorem 2.5.4; the identity is the only non-2-generator in such a group. Thus $xA \in P - F$ stabilizes the element $a \in A^\#$, so G does not satisfy (P3). $\square$

2.6 P as a linear group

Let $\phi : P \rightarrow \text{Aut}(A)$, the *action* of P on A , be the function which sends $x \in P$ to the automorphism $a \mapsto a^x$ of A . If we can construct G so that ϕ is one-to-one, then $\phi(P)$ is an isomorphic copy of P in $\text{Aut}(A)$. However, A is an elementary abelian

q -group of rank n , so its automorphism group is the general linear group $GL(n, q)$. This makes P isomorphic to a linear group over $GF(q)$.

Recall that ϕ is one-to-one if and only if its kernel is trivial — that is, if the centralizer in P of A is trivial. This suggests that we should replace P by $\bar{P} := P/C_P(A)$, if the resulting semidirect product $A \rtimes \bar{P}$ still retains property (P2).

Proposition 2.6.1 *$\bar{P}$ acts irreducibly on A by conjugation. The semidirect product $A \rtimes \bar{P}$ according to this action possesses property (P2).*

Proof: Let $C = C_P(A)$. Let $a \in A$. If $x_1 C = x_2 C$, then $x_1^{-1} x_2 \in C$, so $a^{x_1^{-1} x_2} = a$. Thus $a^{x_1} = a^{x_2}$, and we may define the action of $\bar{P}$ on A by $a^{xC} = a^x$. If $\bar{P}$ acts reducibly on A , then so does P , contradicting Lemma 2.5.1.

Property (P2) is equivalent to property (P3) by Proposition 2.5.1, so we need only check (P3). Suppose $xC \in \bar{P}$ fixes the point $a \in A$. Then x fixes a , so $x \in \Phi(P)$. Therefore, $xC \in \Phi(P)/C = \Phi(\bar{P})$ by Lemma 2.5.4. $\square$

In light of Proposition 2.6.1, we shall replace P by $\bar{P}$ and G by $A \rtimes \bar{P}$. We therefore have:

Corollary 2.6.1 *P is isomorphic to an irreducible linear group over $GF(q)$.*

We may now apply a theorem of Passman [7] to see that P cannot be abelian.

Theorem 2.6.1 ([7], Corollary 14.5, page 128) *Let P act faithfully and irreducibly on an abelian group A . Suppose that $|P|$ and $|A|$ are relatively prime. Then $Z(P)$ is cyclic.*

Corollary 2.6.2 *P is not abelian.*

Proof: If P is abelian, then $P = Z(P)$ is cyclic by Theorem 2.6.1, contradicting Lemma 2.5.3. $\square$

Since P is linear over A , $G = A \rtimes P$ has a natural representation as an affine group.

Proposition 2.6.2 *If P is a linear group of degree n which acts on the vector space A , then $G = A \rtimes P$ has a faithful representation of degree $n + 1$, whose matrices are of the form*

$$\left[\begin{array}{c|c} x & 0 \\ \hline a & 1 \end{array} \right]$$

where $x \in P$ and $a \in A$.

Proof: The only thing to be verified is that the representation preserves the multiplication of G :

$$(a_1, x_1)(a_2, x_2) \mapsto \begin{bmatrix} x_1 & 0 \\ a_1 & 1 \end{bmatrix} \begin{bmatrix} x_2 & 0 \\ a_2 & 1 \end{bmatrix} = \begin{bmatrix} x_1 x_2 & 0 \\ a_1 x_2 + a_2 & 1 \end{bmatrix} \mapsto (a_1^{x_2} a_2, x_1 x_2)$$

which is the correct result. $\square$

2.7 A counterexample for $p = 2$

By Proposition 2.1.1, a Platonov group over $\text{GF}(p)$ is a 2-generator group G which is not a p -group, but which possesses property (P1). We are trying to construct a group which possesses property (P2). Such a group will be a Platonov group, as (P2) is stronger than (P1).

If $G = A \rtimes P$ is in the form of Proposition 2.4.1, we have just seen that property (P2) is equivalent to property (P3), which states that only elements outside of $\Phi(P)$ can fix nontrivial elements of A . In this section, let us impose a stronger condition: that *no* nontrivial element of P fixes any nontrivial element of A . This condition makes G a *Frobenius group*, a well-studied class of groups.

Definition 2.7.1 ([4], 7.1, p. 99) Let $H \leq G$, with $1 < H < G$. Assume that $H \cap H^g = 1$ whenever $g \in G \setminus H$. Then H is a Frobenius complement in G . A group which contains a Frobenius complement is called a Frobenius group.

Theorem 2.7.1 ([4], 7.2, p. 100) Let G be a Frobenius group with complement H . Then there exists $N \triangleleft G$ with $HN = G$ and $H \cap N = 1$ (H is called a Frobenius kernel).

Theorem 2.7.2 ([4], Problem 7.1, p. 121) Let $N \triangleleft G$, $H \leq G$, with $NH = G$ and $N \cap H = 1$. Then H is a Frobenius complement in G if and only if $C_H(n) = 1$ for all $n \neq 1$ in N .

In Theorem 2.7.2, G is a semidirect product of N by H , and so H acts on N by conjugation (see Theorem 2.5.2). If $C_H(n) = 1$ for all $n \neq 1$ in N , then we say that the action is *fixed-point free*. This is slightly inaccurate, since the identity is always a fixed point, but the terminology is conventional.

If G is a Frobenius group with Frobenius complement P and Frobenius kernel A , then P acts fixed-point free on A , so G certainly satisfies (P3). However, part (iv) of Theorem 18.1 (p.194) of Passman [7] severely restricts the possible structures of G .

Theorem 2.7.3 ([7] Theorem 18.1, Part 4) Let P be a Frobenius complement; let p be a prime. If $p > 2$ then the Sylow p -subgroups of P are cyclic; if $p = 2$ then the Sylow p -subgroups of P are cyclic or generalized quaternion.

Suppose G is a Frobenius group. By Lemma 2.5.3, P cannot be cyclic. Hence P must be a generalized quaternion group, and $p = 2$. The simplest such P is the quaternion group of order 8:

$$Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, i^{-1}ji = j^{-1} \rangle.$$

The group Q_8 has a faithful, irreducible representation R of degree 2 over $\mathbb{C}$ given by

$$R(i) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad R(j) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

It is straightforward to check that $|Q_8| = 8$, and

$$R(Q_8) = \left\{ \pm I, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\}$$

Of these matrices, only the matrix I has 1 as an eigenvalue. $-I$ has the single eigenvalue -1 ; the other matrices have complex eigenvalues. If we select a finite field with a primitive fourth root of unity, say $GF(5)$, then we may replace i with this root (in this case, 2) and take A to be the additive group of $GF(5)^2$. Then Q_8 acts fixed-point free on A , so $G = GF(5)^2 \rtimes Q_8$ is a Frobenius group. Thus G is a counterexample for the prime 2 – that is, a faithful representation of G over $GF(2)$ is a Platonov group.

Unfortunately, however, this method can only yield counterexamples when $p = 2$. In the remainder of this chapter, we will assume $p > 2$ and construct a group $G = A \rtimes P$ satisfying (P3), for which $\phi(P)$ is not trivial.

2.8 Possible generators for P

Using the following theorem of Vol'vačev [10], we may impose some restrictions on the degree n of P . In order to state the theorem, we make the following definitions: Let $\mathbb{F}$ be a field of characteristic q , which contains a primitive p th root of unity. For $a \geq 1$, we define N_a to be a Sylow p -subgroup of the group of all permutation matrices of degree p^a (so N_a is isomorphic to a Sylow p -subgroup of S_{p^a} , the symmetric group on p^a elements). Define D_a to be the group of diagonal matrices of degree p^a with entries from a Sylow p -subgroup of $\mathbb{F}^*$, the multiplicative group of $\mathbb{F}$.

The product $N_a D_a$ is a group of *monomial matrices* in $GL(n, \mathbb{F})$, where a monomial matrix is a matrix with precisely one nonzero entry in each row and column. Observe also that D_1 is a normal subgroup of $N_1 D_1$.

Theorem 2.8.1 ([10], Theorem 2) *If $n \neq p^a$ for some a , then $GL(n, \mathbb{F})$ contains no irreducible p -subgroups; for $n = p^a$, every irreducible p -subgroup of $GL(n, \mathbb{F})$ is conjugate in $GL(n, \mathbb{F})$ to a subgroup of $N_a D_a$.*

In other words, for our groups, the only possible values for the degree n of P are powers of p ; in these cases, an appropriate choice of basis will make P a certain monomial p -group.

We shall attempt to find a group P of degree $n=p$, where $F = GF(q)$ is a field containing a primitive p th root of unity (in fact, we shall require at least a p^2 th root of unity for our construction). In this case, Theorem 2.8.1 states that we may take P to be a subgroup of $N_1 D_1$. N_1 , in this case, is isomorphic to a Sylow p -subgroup of S_p . The Sylow p -subgroups of S_p are cyclic of order p ; hence, we may take N_1 to be the group generated by the cyclic permutation matrix

$$u = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{bmatrix}. \quad (2.1)$$

One of the generators of P is not diagonal (otherwise, P would be abelian, contradicting Corollary 2.6.2). Suppose this generator is du^s , for some $d \in D_1$ and some integer s . As D_1 is a normal subgroup of $N_1 D_1$, we have that $(du^s)^t = d_0 u^{st}$ for all integers t , where d_0 is some diagonal matrix. In particular, for a suitable choice of t we have $(du^s)^t = d_0 u$, a matrix whose nonzero entries lie in the same positions as those of u .

Lemma 2.8.1 *Let x be the monomial matrix*

$$\begin{bmatrix} & \alpha_1 & & \\ & & \ddots & \\ & & & \alpha_{p-1} \\ \alpha_p & & & \end{bmatrix}.$$

for some p -elements $\alpha_i \in \mathbb{F}$. Then there exists a diagonal matrix d with diagonal entries $d_1, \dots, d_p$ such that

$$d^{-1}xd = \begin{bmatrix} & \alpha & & \\ & & 1 & \\ & & & \ddots \\ 1 & & & & 1 \end{bmatrix},$$

where α is a p -element of $\mathbb{F}^$.*

Proof: Taking determinants of the above equation yields $\alpha = \det x = \alpha_1 \alpha_2 \cdots \alpha_p$, as the determinant is preserved under conjugation. Then, by multiplying out the left side of the equation in the lemma and comparing the entries of the two matrices, we obtain the system of equations

$$\begin{aligned} d_1^{-1} \alpha_1 d_2 &= \alpha \\ d_2^{-1} \alpha_2 d_3 &= 1 \\ &\vdots \\ d_{p-1}^{-1} \alpha_{p-1} d_p &= 1 \\ d_p^{-1} \alpha_p d_1 &= 1 \end{aligned}$$

Let $d_1 = 1$. We may then solve for $d_2, \dots, d_{p-1}$, using the equations in reverse order.

In particular,

$$\begin{aligned} d_p &= \alpha_p, \\ d_{p-1} &= \alpha_{p-1} d_p = \alpha_p \alpha_{p-1}, \\ &\vdots \\ d_2 &= \alpha_p \alpha_{p-1} \cdots \alpha_2. \end{aligned}$$

Then the first equation says that $\alpha_1\alpha_2\ldots\alpha_p = \alpha$, so the system is consistent. $\square$

Now we can replace P by $d^{-1}Pd$, an equivalent representation of P , and so assume that

$$x = \begin{bmatrix} & \alpha & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}$$

is one of our generators.

Let the second generator of P be y . For some t , the matrix x^ty is diagonal and $P = \langle x, x^ty \rangle$. Replace y with x^ty , so that $P = \langle x, y \rangle$ where

$$y = \begin{bmatrix} \beta_1 & & & & \\ & \beta_2 & & & \\ & & \ddots & & \\ & & & & \beta_p \end{bmatrix},$$

for some $\beta_1, \dots, \beta_p$ which are p -elements of $\mathbb{F}^*$.

At this point, we need a standard result about the structure of the Frattini subgroup of a p -group.

Theorem 2.8.2 ([6], Theorem 9.26, p.187) *If P is a p -group, then*

$$\Phi(P) = \langle [a, b], c^p \mid a, b, c \in P \rangle$$

Observe that the commutator of any two matrices in N_1D_1 is a diagonal matrix; likewise, the p^{th} power of any matrix in N_1D_1 is a diagonal matrix. Hence $\Phi(P)$ consists of diagonal matrices.

We would now like to identify which matrices of N_1D_1 fix a point of A . In the language of linear algebra, we need to identify the matrices in N_1D_1 which have 1 as an eigenvalue.

Lemma 2.8.2 *Let $m \in D_1$. Then m has 1 as an eigenvalue if and only if m has 1 as a diagonal entry.*

Proof: This is clear.

Lemma 2.8.3 *Let $m \in N_1 D_1$ be non-diagonal. Then m has 1 as an eigenvalue if and only if $\det m = 1$.*

Proof: Suppose m has nonzero entries $\gamma_1, \gamma_2, \dots, \gamma_p$ where the γ_i are p -elements of $\mathbb{F}^*$. Write $m = ud$ where $u \in N_1$ and $d \in D_1$. Observe that

$$m^p = udud \cdots ud = (udu^{-1})(u^2du^{-2}) \cdots (u^{p-1}du^{1-p})(d),$$

where the bracketed terms are diagonal matrices whose nonzero entries are the p different cyclic shifts of the diagonal entries of d . This means that m^p is equal to the scalar matrix $\gamma_1 \gamma_2 \cdots \gamma_p I = (\det m)I$. Therefore, m is a root of the polynomial $\lambda^p - \det m$, so the minimal polynomial $g(\lambda)$ of m must divide $\lambda^p - \det m$. This polynomial has 1 as a root if and only if $\det m = 1$. Finally, it is a basic fact from linear algebra that 1 is an eigenvalue of m if and only if 1 is a root of $g(\lambda)$. $\square$

An immediate application of Lemma 2.8.3 is that $\alpha \neq 1$, for if this is not the case, x is a generator which fixes a point in A , contradicting Property (P3).

We now prove a series of technical facts involving the orders of the entries of x and y , and the determinants of x and y . Note first that $x^p = \text{diag}(\alpha, \alpha, \dots, \alpha) \in \Phi(P)$. If $|\alpha| \geq |\beta_i|$ for some i , then $\alpha^t = \beta_i^{-1}$ for some t , and hence $(x^p)^t y$ is a diagonal matrix with a 1 in the i th diagonal entry. Thus by Lemma 2.8.2, $(x^p)^t y$ fixes a point in A , but it does not lie in the Frattini subgroup of P (since $x^p \in \Phi(P)$ but $y \notin \Phi(P)$), contradicting property (P3). Hence $|\alpha| < |\beta_i|$ for all i .

Next, observe that if $|\det y| \geq |\alpha|$, then $\det y^t = \alpha^{-1}$ for some t , and thus $y^t x$ has determinant 1. Also, $y^t x$ is not diagonal, so it lies outside of $\Phi(P)$ but (by Lemma 2.8.3) fixes a point in A , again contradicting (P3). Hence $|\det y| < |\alpha|$, so $|\det y| \leq |\alpha|^p = |\det x^p|$. Therefore, $|\det y|^{-1} = |\det x^{pe}|$ for some e , and by replacing y with yx^{pe} (which together with x still generates P), we may take $\det y = 1$.

Thirdly, observe that

$$x^{-t}yx^t = \begin{bmatrix} \beta_{1-t} & & & \\ & \beta_{2-t} & & \\ & & \ddots & \\ & & & \beta_{p-t} \end{bmatrix}. \quad (2.2)$$

where the subscripts of the β_i are taken modulo p . Suppose that $|\beta_i| < |\beta_j|$ for some i, j . Then $|\beta_i| \leq |\beta_j^p|$, so $\beta_i^{-1} = \beta_j^{pe}$ for some e . Let $t = i - j$. Then $(x^{-t}y^{pe}x^t)y$ has a 1 in the j th diagonal entry, so it fixes a point in A by Lemma 2.8.2. However, $y^{pe} \in \Phi(P)$; as $\Phi(P)$ is a characteristic subgroup of G , $x^{-t}y^{pe}x^t \in \Phi(P)$ as well. Thus $(x^{-t}y^{pe}x^t)y$ lies outside of $\Phi(P)$, in contradiction to Property (P3). Therefore, *all* of the β_i have the same order. Let $|\beta_i| = p^s$.

Finally, observe that

$$[x^t, y] = x^{-t}y^{-1}x^ty = \begin{bmatrix} \beta_1\beta_{1-t}^{-1} & & & \\ & \beta_2\beta_{2-t}^{-1} & & \\ & & \ddots & \\ & & & \beta_p\beta_{p-t}^{-1} \end{bmatrix}. \quad (2.3)$$

where the subscripts of the β_i are again taken modulo p . If any of the elements $\beta_i\beta_{i-t}$ has order p^s , then there exists e such that $\beta_i^{-1} = (\beta_i\beta_{i-t})^e$. Thus $[x^t, y]^e y$ has a 1 in the i th diagonal position, making it fix a point by Lemma 2.8.3. But $[x^t, y]^e y$ lies outside $\Phi(G)$, which contradicts property (P3). Therefore, $|\beta_i\beta_j| < p^s$ for all $i \neq j$. That is, for all i , $\beta_i = \gamma\delta_i$, where $|\gamma| = p^s$ and $|\delta_i| < p^s$.

For convenience, we summarize these results in a lemma:

Lemma 2.8.4 *If there exists an irreducible matrix group of degree p over $\mathbb{F}$ which satisfies Property (P3), then there exists an irreducible matrix group $P = \langle x, y \rangle \leq GL(p, \mathbb{F})$ satisfying the same property, where*

$$x = \begin{bmatrix} & \alpha & & \\ & & 1 & \\ & & & \ddots \\ 1 & & & & 1 \end{bmatrix}, \quad y = \begin{bmatrix} \beta_1 & & & \\ & \beta_2 & & \\ & & \ddots & \\ & & & \beta_p \end{bmatrix},$$

with $\alpha, \beta_1, \dots, \beta_p \in \mathbb{F}^*$ satisfying the following:

1. $|\beta_i| = p^s$ for all i ;
2. $1 < |\alpha| < p^s$;
3. $\det y = \prod_{i=1}^p \beta_i = 1$;
4. $\beta_i = \gamma \delta_i$, where $|\gamma| = p^s$ and $|\delta_i| < p^s$.

Note that part (2) of the lemma implies that $s \geq 2$, so $\mathbb{F}$ must in fact have a primitive p^2 th root of unity, as mentioned earlier.

2.9 Counterexamples for $p > 2$

In light of Lemma 2.8.4, we are now ready to construct a counterexample to the Platonov/Potapchik conjecture over finite fields of odd characteristic. Let p be any odd prime; let q be a prime such that p^2 divides $q - 1$. We know that such a prime number q exists; in fact, Dirichlet's theorem on prime numbers in arithmetical progressions guarantees the existence of infinitely many primes q in the sequence $\{1 + kp^2\}_{k=1}^\infty$. Let $\mathbb{F} = GF(q)$. Then the multiplicative group of $\mathbb{F}$ has order divisible by p^2 , so $\mathbb{F}$ has a primitive p^2 th root of unity, α .

Define $P = \langle x, y \rangle$, where

$$x = \begin{bmatrix} & \alpha^p & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}, \quad y = \begin{bmatrix} \alpha & & & & \\ & \alpha & & & \\ & & \ddots & & \\ & & & \alpha & \\ & & & & \alpha^{1-p} \end{bmatrix} \in GL(p, q).$$

and let $F = \Phi(P)$. As before, elements of F are diagonal matrices. Note that any word in x and y is a monomial matrix whose entries are p -elements; hence, P is in

fact a p -group. Observe also that $\det(x) = \alpha^p$ and $\det(y) = \alpha^{p-1}\alpha^{1-p} = 1$. We now give two descriptions of the elements of P , which will be used to find $\Phi(P)$.

Proposition 2.9.1 *If $z \in P$, then $z = \alpha^t m$, where $0 \leq t < p$ and m is a monomial matrix whose entries have order at most p .*

Proof: The nonzero entries of x have order 1 or p . Similarly,

$$y = \alpha \cdot \text{diag}(1, 1, \dots, 1, \alpha^{-p}),$$

so both x and y are in the above form, as are x^{-1} and y^{-1} .

If $w = \prod w_i$ where $w_i \in \{x, y, x^{-1}, y^{-1}\}$ is a general element of P , and $w_i = \alpha^{t_i} m_i$ is the expression of w_i in the above form, then $w = \prod \alpha^{t_i} m_i = \alpha^{\sum t_i} \prod m_i$, which is the desired form. $\square$

Proposition 2.9.2 *If $z \in P$, then $z = x^r y^s f$, where $0 \leq r, s < p$ and $f \in F$.*

Proof: Since $P = \langle x, y \rangle$, $P/F = \langle xF, yF \rangle$. By Theorem 2.5.4, P/F is elementary abelian of rank 2. Therefore, $|xF| = |yF| = p$ and $P/F = \{x^r y^s F \mid 0 \leq r, s < p\}$. The result follows immediately. $\square$

We can now deduce the following facts:

Proposition 2.9.3 *The elements of F all have determinant 1.*

Proof: It is enough to check that the theorem holds on the generators of the Frattini subgroup, because the determinant is a homomorphism from P to $\mathbb{F}^*$. By Theorem 2.8.2, F is generated by the commutators and the p th powers of elements of P . Because $\det(u^{-1}) = \det(u)^{-1}$, $\det([a, b]) = 1$ for all $a, b \in P$. Let w be an arbitrary word in x and y . Because $\det(x) = \alpha^p$ and $\det(y) = 1$, $\det w = \alpha^{kp}$ for some k . Therefore, $\det w^p = \alpha^{kp^2} = 1$. $\square$

Corollary 2.9.1 *Only the diagonal elements of P have determinant 1.*

Proof: From Proposition 2.9.2, elements of P have the form $x^r y^s f$, where $0 \leq r, s < p$ and $f \in F$. The matrices y and f are both diagonal, whereas the matrix x^r is only diagonal when $r = 0$. This means that the diagonal elements of P are the elements of the form $y^s f$, for $0 \leq s < p$ and $f \in F$, whereas the non-diagonal elements of P are the elements of the form $x^r y^s f$, where $0 < r < p$ and $0 \leq s < p$.

Consider a diagonal element $y^s f$ of P . By Proposition 2.9.3, $\det f = 1$. Also, $\det y = 1$ as mentioned before. Therefore, $\det y^s f = (\det y)^s (\det f) = 1$, so the diagonal elements of P have determinant 1.

Now, consider a non-diagonal element $x^r y^s f$ of P (so $0 < r < p$). As $\det x = \alpha^p$, we have $\det x^r y^s f = \det x^r = \alpha^{rp} \neq 1$. $\square$

Proposition 2.9.4 *No element of F has any entries of order p^2 .*

Proof: Again, it is adequate to prove the result for a generating set of F , which is given by Theorem 2.8.2. If $a \in P$ then $a = \alpha^t m$ where m has no entries of order p^2 . Thus $a^p = \alpha^{pt} m^p$. As $|\alpha^{pt}| = p$, all entries of a^p must have order 1 or p .

If $\alpha^{t_1} m_1$ and $\alpha^{t_2} m_2$ are in P , then $[\alpha^{t_1} m_1, \alpha^{t_2} m_2] = [m_1, m_2]$ since the scalars α^{t_1} and α^{t_2} commute with m_1 and m_2 . Clearly $[m_1, m_2]$ has entries of order less than p^2 , so we are done. $\square$.

Proposition 2.9.5 *No element of $P \setminus F$ has 1 as an eigenvalue.*

Proof: By Proposition 2.9.2, let $w = x^r y^s f$ be a general element of P , where $0 \leq r, s < p$ and $f \in F$. Suppose w has the eigenvalue 1.

If $r > 0$ then w is not diagonal; hence, by Lemma 2.8.3, $\det w = 1$. However, this is impossible by Corollary 2.9.1. Therefore, $r = 0$ and $w = y^s f$ is a diagonal matrix. By Lemma 2.8.3, w has a 1 as a diagonal entry. Note, however, that

$$[y^s]_{i,i} = \begin{cases} \alpha^s & \text{if } i \neq p \\ \alpha^{(1-p)s} & \text{if } i = p. \end{cases}$$

If $0 < s < p$, then $|\alpha^s| = |\alpha^{(1-p)s}| = p^2$. By Proposition 2.9.4, f has only entries of order 1 or p . This means that $w = y^s f$ has only entries of order p^2 , a contradiction. Thus $s = 0$, and $w = f \in F$. $\square$

We are essentially done, The only thing which remains to be shown is that G itself is a two generator group. In fact, if we treat G as an affine group as in Proposition 2.6.2, G may be generated by the matrices

$$x_0 = \left[\begin{array}{c|c} x & 0 \\ \hline 0 & 1 \end{array} \right], \quad y_0 = \left[\begin{array}{c|c} y & 0 \\ \hline 0 & 1 \end{array} \right]$$

To see that these two matrices generate the entire group, observe that

$$x_0^p = \left[\begin{array}{c|c} \alpha^p & 0 \\ \hline 1 & 1 \end{array} \right]$$

Consider $[x_0^p, y_0]$. Certainly x^p is diagonal, so it commutes with y ; thus $[x_0^p, y_0] \in A$. However, x_0^p does not commute with y_0 , so $[x_0^p, y_0] \in A^\#$.

If P were reducible, then P would reduce completely by Mashke's Theorem (see [4], Theorem 1.9, p. 4), as $p \nmid q = \text{char}(\mathbb{F})$. But then the irreducible components of P would be of degree 1 (that being the only possible degree less than p , by Theorem 2.8.1) and P would be abelian, contradicting Corollary 2.6.2. Hence P acts irreducibly on A , so P does not stabilize any proper subspace of A .

Next, observe that for $z \in P$ and $a, b \in A$,

$$\begin{bmatrix} z & 0 \\ a & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} \begin{bmatrix} z & 0 \\ a & 1 \end{bmatrix} = \begin{bmatrix} z^{-1} & 0 \\ -az^{-1} & 1 \end{bmatrix}^{-1} \begin{bmatrix} z & 0 \\ bz + a & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ bz & 1 \end{bmatrix}$$

Therefore, given any element of $A^\#$ (such as $[x_0^p, y_0]$), the irreducibility of P guarantees that we may produce a basis for A by repeatedly conjugating by x_0 and

y_0 . Taking suitable linear combinations of these basis vectors then gives the entirety of A . Hence $A \leq \langle x_0, y_0 \rangle$. Since $G/A \simeq P = \langle x, y \rangle$, we know also that x_0 and y_0 generate G modulo A . Thus $G = \langle x_0, y_0 \rangle$.

Theorem 2.9.1 *For all primes p , there exists a counterexample to the conjecture of Platonov and Potapchik over a finite field of characteristic p .*

Proof: If $p = 2$, we have already constructed the counterexample in Section 2.7. Otherwise, take $G = GF(q)^p \rtimes P$, where P and q are as defined above. This G satisfies Property (P3), so a faithful representation of G over $GF(p)$ is a Platonov group. $\square$

Chapter 3

Connections between characteristics 0 and p

In this chapter, we outline some of the connections between our work and the original conjecture of Platonov and Potapchik [8], which states that a matrix group over $\mathbb{C}$ which has all of its primitive words unipotent must itself be a unipotent group. Suppose that the conjecture is false, so there exists a group G which is not unipotent, but which has all of its primitive words unipotent. Such a group is called a *Platonov group* (see Definition 2.0.1).

If any Platonov group over $\mathbb{C}$ exists, we shall show that there exists an integer m such that there exist Platonov groups of degree m over $GF(p)$, for infinitely many primes p .

3.1 Transcendence bases

We first state some basic definitions and a theorem from field theory, taken from [2]. Let E/F be an extension of fields.

Definition 3.1.1 ([2], Chapter 14.9, page 626) *A subset $\{a_1, a_2, \dots, a_n\}$ of E is*

called algebraically independent over F if there does not exist a nonzero polynomial $f(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$ such that $f(a_1, a_2, \dots, a_n) = 0$. An arbitrary subset S of E is called algebraically independent over F if every finite subset of S is algebraically independent. The elements of S are called independent transcendentals over F .

Definition 3.1.2 ([2], Chapter 14.9, page 626) A transcendence base for E/F is a maximal subset (with respect to inclusion) of E which is algebraically independent over F .

Proposition 3.1.1 ([2], Chapter 14.9, page 626) S is a transcendence base for E/F if and only if S is a set of algebraically independent transcendentals over F and E is algebraic over $F(S)$.

Theorem 3.1.1 ([2], Chapter 14.9, page 626) The extension E/F has a transcendence base and any two transcendence bases of E/F have the same cardinality.

Suppose $G = \langle x, y \rangle$ is a Platonov group over $\mathbb{C}$. In fact, we may say that $G \leq GL(n, E)$ where E is the field obtained by adjoining to $\mathbb{Q}$ all of the entries of x and y . Since E is finitely generated over $\mathbb{Q}$, there is a finite transcendence basis, say $\{t_1, t_2, \dots, t_r\}$, for $E/\mathbb{Q}$. set $F = \mathbb{Q}(\{t_1, t_2, \dots, t_r\})$. Since E is a finitely generated algebraic extension of F , E/F is a finite extension.

We shall now construct from G a Platonov group over $GF(p)$, for infinitely many primes p . This construction will proceed in three stages:

1. Construct a Platonov group over F ;
2. Construct a Platonov group over R , a local ring over Z ;
3. Construct a Platonov group over $GF(p)$.

3.2 A Platonov group over F

By Proposition 3.1.1, the extension E/F is finite of degree d , say. We shall use a matrix representation of E/F to embed G in $GL(nd, F)$ in such a way that unipotent elements of G have unipotent images, and vice versa.

For each $x \in E$, define $\tau_x : E \rightarrow E$ by $\tau_x(a) = xa$. Observe that $\tau_x(a)$ is both a linear transformation over F and a ring automorphism of E . Fix a basis $\beta = \{b_1, \dots, b_d\}$ of E/F , and let $R : E \mapsto GL(d, F)$ be the map $R(x) = [\tau_x]_\beta$, the matrix of τ_x with respect to the basis β .

Proposition 3.2.1 *R is a faithful representation of E over F .*

Proof: For all $v \in F^d$ and $x, y \in E$,

$$R(x - y)v = [\tau_{x-y}]_\beta v = [\tau_x]_\beta v - [\tau_y]_\beta v = (R(x) - R(y))v,$$

and

$$R(xy)v = [\tau_{xy}]_\beta v = [\tau_x]_\beta [\tau_y]_\beta v = R(x)R(y)v$$

so R is a representation of E . If $R(x) = R(y)$, then $\tau_x a = \tau_y a$ for all $a \in e$, so $xa = ya$ and $x = y$. Thus R is faithful. $\square$

If $x = [a_{ij}] \in GL(n, E)$, we may define an element $\hat{x} = [R(a_{ij})] \in \text{Mat}(nd, F)$. It is a routine computation to check that $\hat{x}$ is invertible with inverse $\widehat{x^{-1}}$, and that $\widehat{xy} = \hat{x}\hat{y}$. Let $\hat{G} = \{\hat{x} | x \in G\}$. Then $\hat{G}$ is isomorphic to G .

Proposition 3.2.2 *$x \in G$ is unipotent if and only if $\hat{x} \in \hat{G}$ is unipotent.*

Proof: A matrix is unipotent if and only if 1 is the only root of its minimal polynomial. Suppose $x \in G$ has minimal polynomial $(\lambda - 1)^t$. Then $(x - I_n)^t = 0$, and so $(\widehat{x - I_n})^t = (\hat{x} - I_{nd})^t = 0$. As a result, the minimal polynomial of $\hat{x}$ must divide $(\lambda - 1)^t$, making $\hat{x}$ unipotent.

Suppose now that $\hat{x} \in \hat{G}$ has minimal polynomial $(\lambda - 1)^t$. Then $(\hat{x} - I_{nd})^t = (\widehat{x - I_n})^t = 0$, and so $(x - I_n)^t = 0$. As a result, the minimal polynomial of x must divide $(\lambda - 1)^t$, so x is unipotent. $\square$

Because of Proposition 3.2.2, non-unipotent elements of G get mapped onto non-unipotent elements of $\hat{G}$. Moreover, the primitive words w of G correspond to the primitive words $\hat{w}$ of $\hat{G}$. This makes $\hat{G}$ a Platonov group, as desired.

3.3 A Platonov group over a local ring R

We have shown in the previous section that, given a Platonov group G , we may construct a Platonov group $\hat{G} \in GL(nd, F)$. The reason for doing this is that now the entries in the matrices of $\hat{G}$ lie in a field F which is purely transcendental over the rational numbers.

Suppose now that G is a Platonov group over F . Through a technique called *specialization*, we shall assign a rational number to each of the elements t_i of the transcendence basis, mapping F into $\mathbb{Q}$. Applying this map to all of the entries of G will yield a homomorphic image of G in $GL(nd, R)$, where R is a ring with $\mathbb{Z} \subseteq R \subset \mathbb{Q}$. In order for this process to be useful, we shall have to ensure that the group we get is also a Platonov group. In fact, we shall see that unipotent matrices are mapped onto unipotent matrices, and we shall be able to ensure that at least one non-unipotent matrix in G has a non-unipotent image.

To see that this can be done, we shall need the following result:

Lemma 3.3.1 *Let D be an infinite integral domain. Let*

$$\left\{ \begin{array}{l} f_1(x_1, \dots, x_k) \neq 0 \\ f_2(x_1, \dots, x_k) \neq 0 \\ \vdots \\ f_n(x_1, \dots, x_k) \neq 0 \end{array} \right.$$

be a system of n nontrivial polynomial inequalities over D in k unknowns. Then there exists a vector $(a_1, \dots, a_k) \in D^k$ satisfying each of the inequalities in the system.

Proof: Write $\bar{x}$ for $(x_1, \dots, x_n)$. First, let

$$g(x_1, \dots, x_n) = \prod_{i=1}^n f_i(x_1, \dots, x_n).$$

Observe that $g(\bar{x}) = 0$ if and only if $f_i(\bar{x}) = 0$ for some i . Hence it is enough to show that we can always find $\bar{x}$ such that $g(\bar{x})$ is nonzero.

We shall prove the theorem by induction on k . The base case is $k = 1$; here, we have a polynomial $g(x) \in D[x]$. We may consider g to be a polynomial over the quotient field Q of D , and hence over its algebraic closure $\overline{Q}$. It is known that g has $\deg(g)$ roots in $\overline{Q}$, up to multiplicity, so g can have at most finitely many roots in D . As D is infinite, there are elements of D which are not roots of g .

Next, suppose that any polynomial in the k variables $x_1, \dots, x_{k-1}$ has a non-root. Let $g(x_1, \dots, x_k) \in D[x_1, \dots, x_k]$; Let d be the highest power of x_k present in g . By collecting the terms which contain x_k^i for each i , we may write

$$g(x_1, \dots, x_k) = \sum_{i=0}^d g_i(x_1, \dots, x_{k-1})x_k^i.$$

for some $g_i \in D[x_1, \dots, x_{k-1}]$. By induction, there exists $(a_1, \dots, a_{k-1}) \in D^{k-1}$ such that $g_d(a_1, \dots, a_{k-1}) \neq 0$. Hence

$$g(a_1, \dots, a_{k-1}, x_k) = \sum_{i=0}^d g_i(a_1, \dots, a_{k-1})x_k^i$$

is a nontrivial polynomial in x_k , which has a non-root a_k as before. It then follows that $g(a_1, \dots, a_k) \neq 0$, and we are done. $\square$

Note that this theorem is false if D is any finite integral domain. In fact, any finite integral domain is a finite field, and every element of $GF(p^n)$ is a root of the polynomial $f(x) = x^{p^n} - x$.

Now, let us return to the matrix group $G = \langle x, y \rangle \leq GL(nd, F)$, where $F = \mathbb{Q}(t_1, \dots, t_n)$. Observe that F is the quotient field of the ring $\mathbb{Z}[t_1, \dots, t_n]$, so if x_{ij} is an entry of x and y_{ij} is an entry of y , we may write

$$x_{ij} = \frac{a_{ij}(t_1, \dots, t_n)}{b_{ij}(t_1, \dots, t_n)}, \quad y_{ij} = \frac{c_{ij}(t_1, \dots, t_n)}{d_{ij}(t_1, \dots, t_n)}.$$

for some $a_{ij}, b_{ij}, c_{ij}, d_{ij} \in D[t_1, \dots, t_n]$.

Let w be a non-unipotent matrix in G . Then the characteristic polynomial $f(\lambda)$ of w is of degree nd , such that

$$f(\lambda) \neq (\lambda - 1)^{nd} = \sum_{k=0}^{nd} \binom{nd}{k} (-1)^k \lambda^{nd-k}.$$

Let the coefficient of λ^k in $f(\lambda)$ be

$$\frac{e_k(t_1, \dots, t_n)}{f_k(t_1, \dots, t_n)}.$$

Then for some k_0 , we must have

$$\frac{e_{k_0}(t_1, \dots, t_n)}{f_{k_0}(t_1, \dots, t_n)} \neq (-1)^{k_0} \binom{nd}{k_0}$$

Consider the system of inequalities

$$b_{ij}(t_1, \dots, t_n) \neq 0, \quad 1 \leq i, j \leq nd \quad (3.1)$$

$$d_{ij}(t_1, \dots, t_n) \neq 0, \quad 1 \leq i, j \leq nd \quad (3.2)$$

$$f_{k_0}(t_1, \dots, t_n) \neq 0, \quad (3.3)$$

$$\frac{e_{k_0}(t_1, \dots, t_n)}{f_{k_0}(t_1, \dots, t_n)} \neq (-1)^{k_0} \binom{nd}{k_0} \quad (3.4)$$

By Lemma 3.3.1, this system has a solution $(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n$.

Let $\phi : \mathbb{Z}[t_1, \dots, t_n] \rightarrow \mathbb{Z}$ be the evaluation homomorphism at $(a_1, \dots, a_n)$. ϕ extends to a partial to a map $\tilde{\phi} : F \dashrightarrow \mathbb{Q}$, by setting

$$\tilde{\phi} \left(\frac{a(t_1, \dots, t_n)}{b(t_1, \dots, t_n)} \right) = \frac{\phi(a(t_1, \dots, t_n))}{\phi(b(t_1, \dots, t_n))}.$$

Of course, this is undefined where the polynomials $b(t_1, \dots, t_n)$ have a root at $(a_1, \dots, a_n)$, but we know by (3.1) and (3.2) that $\tilde{\phi}$ is defined for all of the entries of x and y . Let $\psi : G \rightarrow GL(nd, \mathbb{Q})$ be the map obtained by applying $\tilde{\phi}$ to each of the entries of the matrices in G . Because $\tilde{\phi}$ preserves addition and multiplication, ψ is a homomorphism. Let $R = \mathbb{Z}[b_{ij}(a_1, \dots, a_n)^{-1}, d_{ij}(a_1, \dots, a_n)^{-1}]$. Then every matrix in $\psi(G)$ has entries in R .

If a matrix $v \in G$ is unipotent, then w has the characteristic polynomial

$$\det(v - \lambda I) = (\lambda - 1)^{nd} \in \mathbb{Q}[\lambda].$$

Because $\tilde{\phi}$ fixes $\mathbb{Q}$, $\psi(v)$ has the same characteristic polynomial and is therefore unipotent. Thus ψ sends unipotent matrices to unipotent matrices.

On the other hand, if $\psi(w)$ were unipotent, it would have characteristic polynomial

$$f(\lambda) = (\lambda - 1)^{nd} = \sum_{k=0}^{nd} \binom{nd}{k} (-1)^k \lambda^{nd-k}.$$

and (3.4) prevents this from occurring. Hence $\psi(w)$ is not unipotent, so G is not unipotent. As before, the primitive words in $\phi(x), \phi(y)$ are images under ψ of primitive words in x and y . So, $\psi(G)$ is a Platonov group.

3.4 A Platonov group over $GF(p)$

We have constructed a Platonov group over the ring

$$R = \mathbb{Z}[b_{ij}(a_1, \dots, a_n)^{-1}, d_{ij}(a_1, \dots, a_n)^{-1}] \subseteq \mathbb{Q}.$$

Observe that R contains the multiplicative inverses of only finitely many prime numbers. Suppose now that G is a Platonov group over R . Let p be a prime number which does not have an inverse in R .

Each element in R can be written in the form a/b , where $a, b \in \mathbb{Z}$ and $p \nmid b$. Therefore, b has a multiplicative inverse in $\mathbb{Z}_p$, the integers modulo p . We define a map $\pi : R \rightarrow \mathbb{Z}_p$ such that $\pi(a/b) = ab^{-1} \in \mathbb{Z}_p$.

It is clear that π is well defined. Also,

$$\pi(a/b + c/d) = \pi((ad + bc)/bd) = ab^{-1} + cd^{-1} = \pi(a/b) + \pi(c/d)$$

and

$$\pi((a/b)(c/d)) = \pi(ac/bd) = acd^{-1}b^{-1} = \pi(a/b)\pi(c/d)$$

making π a ring homomorphism. If $x \in GL(nd, R)$, define $\Pi(x)$ to be the matrix obtained by applying π to each of the entries of x . As before, Π is a homomorphism of groups, because π preserves addition and multiplication. Let $\overline{G} = \Pi(G)$.

If $x \in GL(nd, R)$ is a unipotent matrix, then its characteristic polynomial is $(\lambda - 1)^{nd}$. Therefore, the characteristic polynomial of $\Pi(x)$ is $(\lambda - 1)^{nd} \in GF(p)[x]$, making x unipotent. On the other hand, suppose $w \in GL(nd, R)$ is not a unipotent matrix, and that w has characteristic polynomial $f(\lambda) \neq (\lambda - 1)^{nd}$. Then the characteristic polynomial of $\Pi(w)$ is

$$\overline{f}(\lambda) = \sum_{i=0}^t a_i \lambda^i$$

where $\overline{f}(\lambda) = f(\lambda) \pmod{p}$. It is possible that $\overline{f}(\lambda) = (\lambda - 1)^{nd}$, but for this to occur, we must have

$$a_k \equiv \binom{nd}{k} (-1)^k \pmod{p}$$

for all $0 \leq k \leq t$. This can be true for only a finite number of primes p . Hence there are infinitely many primes p such that $\overline{f}(\lambda) \neq (\lambda - 1)^{nd}$ and p is not invertible in R . If we use any of these primes, $\Pi(w)$ is not a unipotent matrix, making $\overline{G}$ a Platonov group in $GL(nd, p)$.

Chapter 4

Conclusions

We have been investigating a conjecture of Platonov and Potapchik [8], in which they postulate that a matrix group over $\mathbb{C}$ in which all primitive words are unipotent must itself be unipotent. We have defined a *Platonov group* to be a non-unipotent group which has unipotent primitive words, and we have constructed Platonov groups over the finite field $GF(p)$ for any p .

We have also shown that if Platonov groups over the complex numbers exist, then for some fixed degree, we may construct Platonov groups over the field $GF(p)$ for infinitely many prime numbers p .

4.1 Future work

We suspect that Platonov groups over the complex numbers do not exist. Although Platonov groups over $GF(p)$ exist, the ones we have constructed are minimal in a sense, and their degrees seem to increase. It seems unlikely that one can construct infinitely many Platonov groups over various finite fields if the degree must be fixed.

Let G_p be the group constructed in the preceding chapter, which has property (P2) for the prime p . Recall that G_p was constructed as a matrix group of degree

$p + 1$ over $GF(q)$, for $q \neq p$. G_p is a minimal solvable example of a group which has property (P2). In light of these observations, we make the following conjectures:

1. If a faithful representation of G_p over $GF(p)$ has minimum degree d_p , then d_p increases with p .
2. No Platonov groups over $GF(p)$ have smaller degree than G_p .

One might approach these problems by looking for non-solvable Platonov groups over finite fields (we suspect that there are none). Then, one might try to look for Platonov groups over finite fields which possess property (P1), but not (P2), although it is unclear how such a group might be constructed. Thirdly, one could investigate the degrees of faithful representations of G_p over $GF(p)$ to verify that they increase with p .

Note that these conjectures would imply that Platonov groups over the complex numbers do not exist, since it would be impossible to perform the reduction outlined in the previous sections.

Bibliography

- [1] John D. Dixon, *Problems in group theory*, Dover Publications, Inc., New York, New York, 1973.
- [2] David S. Dummit and Richard M. Foote, *Abstract algebra*, Prentice Hall, Englewood Cliffs, N.J., 1991.
- [3] W. Gaschütz, *Zu einem von B.H. Neumann gestellten problem*, Math. Nachr. **14** (1956), 249–252.
- [4] I. Martin Isaacs, *Character theory of finite groups*, Dover Publications, Inc., New York, New York, 1994.
- [5] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin, 1977.
- [6] Ian D. Macdonald, *The theory of groups*, Robert E. Krieger Publishing Company, Malabar, Florida, 1988.
- [7] Donald Passman, *Permutation groups*, W. A. Benjamin, Inc., New York, New York, 1968.
- [8] Vladimir P. Platonov and Alexander Potapchik, *New combinatorial properties of linear groups*, Journal of Algebra **235** (2001), 399–415.
- [9] W. R. Scott, *Group theory*, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1964.

- [10] R. T. Vol'vačev, *Sylow p -subgroups of the general linear group (Transl.)*, Nine Papers on Logic and Group Theory, 2, vol. 64, American Mathematical Society, 1967, pp. 216–243.