COSETS OF SYLOW $p$-SUBGROUPS AND A QUESTION OF RICHARD TAYLOR

DANIEL GOLDSTEIN AND ROBERT GURALNICK

For John Thompson on the occasion of his 80th birthday

Abstract. We prove that for any odd prime $p$, there exist infinitely many finite simple groups $S$ containing a Sylow $p$-subgroup $P$ of $S$ such that some coset $gP$ of $P$ in $S$ consists of elements whose order is divisible by $p$. This allows us to answer a question of Richard Taylor related to whether certain Galois representations are automorphic.

1. Introduction

In 1967, answering a question of Lowell Paige, John Thompson [6] proved the following result:

**Theorem 1.1.** Let $G = \text{PSL}_2(53)$. Let $Q$ be a Sylow 2-subgroup of $G$ (of order 4). There exists $g \in G$ such that every element in $gQ$ has even order.

Thompson actually worked in $\text{SL}_2(q)$. He wrote down a system of equations over $\mathbb{F}_q$ with $q \equiv \pm 3 \mod 8$ and observed that the existence of a coset of a Sylow 2-subgroup consisting of elements of even order amounted to finding a solution to this system of equations. He then observed that for $q = 53$, there was a solution. Now this can easily be checked in MAGMA [1] and indeed 53 can be replaced by 27 and also by any $q \geq 53$ with $q \equiv \pm 3 \mod 8$ (by showing that the variety defined by Thompson always has points for $q \geq 53$). We have no knowledge of Paige’s motivation.

Here we prove an analog for $p$ odd. Our motivation for considering this problem was a question posed by Richard Taylor regarding what are called adequate groups. See [3, 4, 7] for more about this question and its relation to Galois representations which are automorphic.

We actually prove the following theorem:

**Theorem 1.2.** Let $p$ be an odd prime. Let $D$ be the dihedral group of order $2p$. Let $q$ be a prime power with $p$ dividing $q - 1$ and $p^2$ not dividing $q - 1$. View $D$ as a subgroup of $G := \text{PSL}_2(q)$. If $q$ is sufficiently large, there exists $g \in G$ such that every element of $gD$ has order divisible by $p$.

2010 Mathematics Subject Classification. Primary 20D20, 20D06; Secondary 11F80, 11R34.

Guralnick was partially supported by the NSF grant DMS-1001962 and Simons Foundation fellowship 224965.
Our method is similar to the one used by Thompson. The idea of the proof is to write down a variety parametrizing a family of solutions to the condition that every element of $gD$ has order a multiple of $p$. We then prove that this variety is irreducible and defined over $\mathbb{F}_q$ (indeed, defined over $\mathbb{Z}[\theta]$ where $\theta$ is a $p$th root of 1). We can then apply Lang-Weil [5] to conclude that there are solutions as long as $q$ is sufficiently large.

In fact, there should be many more examples. While $gD$ is far from being a random subset of $G$, if one assumes that this is the case, a straightforward computation of probabilities shows that there should be many elements $g \in G$ with $gD$ consisting of elements of order a multiple of $p$. On the other hand, one does need to be a bit careful. If $G$ is a $p$-solvable group and $P$ is a Sylow $p$-subgroup of $G$, then every coset $gP$ contains some $p'$-element (let $H$ be a $p$-complement in $G$, then $|H \cap gP| = 1$ for all $g \in G$). Our phenomenon may be related to the degree of the smallest nontrivial character of $G$ (and the relative size of the subset being considered). See [2] for some results of this nature.

We also note that a straightforward computation using MAGMA shows that:

**Theorem 1.3.** Let $G = \text{PSL}_2(139)$. Let $Q$ be a Sylow 2-subgroup of $G$ and let $N := N_G(Q)$. Then $N \cong A_4$. There exists a coset of $N$ in $G$ in which all elements have even order.

The consequence of the above theorems is the following result in [3] which answers the question of Taylor.

**Corollary 1.4.** Let $p$ be prime. Let $k$ be an algebraically closed field of characteristic $p$. There exists a finite group $G$ and an absolutely irreducible faithful $kG$-module $V$ such that

1. $H^1(G, k) = 0$;
2. $p$ does not divide $\dim V$;
3. $H^1(G, V \otimes V^*) = 0$; and
4. $\text{End}(V)$ is not spanned by the images of the $p'$-elements of $G$.

It is worth noting that all such examples constructed in [3] have the property that $V$ is an induced module. It is also shown in [3] that if $G$ is $p$-solvable, then (2) implies that the $p'$-elements do span $\text{End}(V)$. In [4], it was shown that if $p \geq 2 \dim V + 2$, then (1)-(4) hold.

## 2. Field Extensions

We first recall a standard consequence of Kummer theory.

**Lemma 2.1.** Let $p$ be a prime. Let $E/F$ be an extension of fields with characteristic not $p$. Assume that $E/F$ is Galois with elementary abelian Galois group $G$ of order $p^n$ and that $F$ contains the $p$th roots of unity. Then $(E^*/F^*)[p]$ has order $p^n$. 

Theorem 2.2. Let $D$ be a UFD with quotient field $F$ of characteristic not dividing $2p$ for some odd prime $p$. Assume that $D$ contains $\theta$, a primitive $p$th root of 1. Let $f_1, \ldots, f_m \in D$ with the $f_i$ square free non-units and pairwise having no common irreducible factors. Fix an algebraic closure $L$ of $F$. Let $q_i \in L$ with $q_i^2 = f_i$. Let $c_i \in L$ with $c_i^p \in D[q_i]$ and $c_i$ not in $D[q_i]$. Let $\Omega$ be the subset of $F[c_1, \ldots, c_m]$ consisting of elements of the form $\prod_i q_i^{e_i} \prod_i c_i^{\ell_i}$ where $e_i \in \{0, 1\}$ and $\ell_i \in \{0, 1, \ldots, p-1\}$.

1. $[F[c_1, \ldots, c_m] : F] = (2p)^m$;
2. $D[c_1, \ldots, c_m]$ is a free $D$-module of rank $(2p)^m$ with basis $\Omega$.

Proof. To prove (1), we may invert all irreducible elements of $D$ other than those dividing $f := f_1 \ldots f_m$ and so assume that $D$ has only finitely many height 1 prime ideals. This implies that $D$ is a semilocal PID (to see this, it suffices to reduce to the case that $D$ is a local UFD with a single irreducible element where the result is obvious). Indeed, by inverting some further prime elements, we may assume that the $f_i$ are distinct primes. Let $v_i$ be the $f_i$ valuation on $D$.

Let $Q = F[q_1, \ldots, q_m]$. By Lemma [2.1], $Q$ is Galois of degree $2^m$. So it suffices to show that $L := F[c_1, \ldots, c_m]$ has degree $p^m$ over $Q$. Let $c = c_i$. Since $c_i^p \in Q$ and $Q$ contains the $p$th roots of 1, for any field $L'$ containing $Q$, either $c \in L'$ or the minimal polynomial of $c$ over $L'$ is $x^p - c^p$.

This implies that $L/Q$ is Galois of degree $p^s$ for some $s \leq m$ and moreover, the Galois group is an elementary abelian $p$-group.

Let $0 \leq e_i < p$ be integers for $i = 1, \ldots, m$. Extend each valuation $v_i$ to a valuation $w_i$ on $L$. Note that $w_j(\prod_i c_i^{e_i}) > 0$ for some $j$ unless $e_i = 0$ for all $i$. Thus, the elements $\prod_i c_i^{e_i}$ are all distinct modulo $F^*$.

Thus, the $p$-torsion subgroup of $L^*/Q^*$ has order at least $p^m$. Now apply the previous lemma. This shows that $[F[c_1, \ldots, c_m] : F] = (2p)^m$. Clearly, $\Omega$ is a spanning set and therefore a basis for $F[c_1, \ldots, c_m]/F$. Thus $D[c_1, \ldots, c_m] = D[\Omega]$ is free over $D$ with basis $\Omega$. □

Theorem 2.3. Let $p$ be a prime. Let $F$ be a field of characteristic not dividing $2p$ containing a nontrivial $p$th root of unity $\theta$. Let $I$ be the ideal of $R := F[a, b, c_1, \ldots, c_p]$ generated by

$$(c_i^p \theta)^2 - (a \theta^i + b \theta^{-i})(c_i^p \theta) + 1,$$

for $i = 1, \ldots, p$. Then $I$ is a prime ideal of $R$.

Proof. Set $d_i = \theta c_i^p$. Thus, $d_i^2 - (a \theta^i + b \theta^{-i})d_i + 1 \in I$.

Note that the discriminant of this quadratic is

$$f_i := (a \theta^i + b \theta^{-i})^2 - 4 = (a \theta^i + b \theta^{-i} + 2)(a \theta^i + b \theta^{-i} - 2).$$

Note that $f_i$ are pairwise relative prime in $D := F[a, b]$. Let $\Omega$ be the set of elements of the form $\prod_i d_i^{e_i} \prod_i c_i^{\ell_i}$ where $e_i \in \{0, 1\}$ and $\ell_i \in \{0, 1, \ldots, p-1\}$. Applying the previous result shows that $\Omega$ is a basis for $R/I$ over $D$ since they are linearly independent in a homomorphic image.
Now \((R/I \otimes_D Q(D))\) surjects onto the field described in the previous theorem. Comparing ranks show that \(R/I \otimes_D Q(D)\) is a field and \(R/I\) injects into this field, whence \(I\) is a prime ideal as required. \(\square\)

3. COSETS OF SUBGROUPS

We can now prove an analog of Thompson’s theorem for odd primes.

Theorem 3.1. Let \(p\) be an odd prime. Let \(q\) be a prime power such that:

1. \(q \equiv 1 \pmod{p}\);
2. \(p^2\) does not divide \(q - 1\).

Let \(G = \text{PSL}_2(q)\). Let \(P\) be a Sylow \(p\)-subgroup of \(G\) (of order \(p\)). Let \(P \leq D\) be a dihedral group of order \(2p\) in \(G\). If \(q\) is sufficiently large, there exists \(g \in \text{PGL}_2(q)\) such that every element in \(gD\) has order divisible by \(p\).

Proof. It suffices to work in \(H = \text{SL}_2(q)\). Let \(\theta\) be a nontrivial \(p\)th root of 1 \(\in \mathbb{F}_q\). We may assume that \(P\) is generated by the diagonal matrix \(\text{diag}(\theta, \theta^{-1})\) and that \(D = \langle P, x \rangle\) where

\[
x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.
\]

Let \(g \in H\) where

\[
g = \begin{pmatrix} a & -c \\ d & b \end{pmatrix}.
\]

Note that an element of \(G\) has order a multiple of \(p\) if and only if its trace can be written as \(e^{p\theta^j} + (e^{p\theta^j})^{-1}\) for some nonzero \(e \in \mathbb{F}_q\) and some \(j, 0 < j < p\) (an element of order a multiple of \(p\) can be conjugated so that it commutes with \(P\); i.e. it is contained in the subgroup of diagonal matrices – this subgroup is of the form \(P \times Q\) where \(Q\) has order prime to \(p\) – in particular, every element in \(Q\) is a \(p\)th power).

Consider the following \(2p\) equations:

\[
a\theta^i + b\theta^{-i} = (c^p_i\theta) + (c^p_i\theta)^{-1}
\]

\[
c\theta^i + d\theta^{-i} = (d^p_i\theta) + (d^p_i\theta)^{-1}
\]

for \(i = 1, \ldots, p\). Then

\[
g = \begin{pmatrix} a & -c \\ d & b \end{pmatrix}
\]

has the property every element of \(gD\) has order a multiple of \(p\).

By the previous result, these equations define a variety which is a direct product of two 2-dimensional irreducible varieties defined over any field containing the \(p\)th roots of 1. Thus, by Lang-Weil [5], for \(q\) sufficiently large, there are solutions (with \(ab + cd \neq 0\)). \(\square\)

Since \(\text{PGL}_2(q) \leq \text{PSL}_2(q^2)\), replacing \(q\) by \(q^2\) (which still satisfies the various hypotheses), and so we can in fact take \(g \in \text{PSL}_2(q)\) if we wish. Alternatively, we can take our two varieties which we will denote \(X(a, b)\) and \(X(c, d)\). Let \(Y\) be the subvariety of \(X(a, b) \times X(c, d) \times \mathbb{A}^1\) defined by
ab + cd = w^2 (where w is the parameter on A^1). It is easy to see that (since
X(a, b) and X(c, d) are irreducible), so is Y and so Lang-Weil applies to
Y as well. Thus, we can choose our g above to have square determinant,
whence reducing modulo the center of GL_2(q), the image of g is in PSL_2(q).

REFERENCES
[1] W. Bosma, J. Cannon and C. Palyoust, The Magma Algebra system. I. The user
language, J. Symbolic Comput. 24 (1997), 235–265.
[2] W. T. Gowers, Quasirandom groups, Combin. Probab. Comput. 17 (2008), 363–
387.
[3] R. Guralnick, Adequate Subgroups II, Bull. Math. Sci. 2 (2012), 193–203.
[4] R. Guralnick, F. Herzig, R. Taylor and J. Thorne, Adequate subgroups, J. Institute
Math. Jussieu, to appear (arXiv:1107.5993).
[5] S. Lang and A. Weil, Numbers of points of varieties in finite fields, Amer. J. Math.
76 (1954), 819–827.
[6] J. Thompson, On a question of L. J. Paige, Math. Zeitschr. 99 (1967), 26–27.
[7] J. Thorne, On the automorphy of ℓ-adic representations with small residual image,
J. Institute Math. Jussieu, to appear (arXiv:1107.5989).

CENTER FOR COMMUNICATIONS RESEARCH, SAN DIEGO, CA 92121
E-mail address: danielgolds@gmail.com

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-2532, USA
E-mail address: guralnic@usc.edu