



ELSEVIER

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Non-PORC behaviour in groups of order p^7

Michael Vaughan-Lee

Christ Church, Oxford, OX1 1DP, United Kingdom

ARTICLE INFO

Article history:

Received 29 June 2016

Available online xxxx

Communicated by

N. Andruskiewitsch, A. Elduque,
E. Khukhro and I. Shestakov*MSC:*

20D15

Keywords: p -Group

PORC

ABSTRACT

We investigate a family of 3-generator groups $G_{(p,x,y)}$ indexed by a prime $p > 3$ and integers x, y . The groups all have order p^7 and class 3. If x and y are coprime to p , then the order of the automorphism group of $G_{(p,x,y)}$ is one of four polynomials in p , where the choice of polynomial depends on the number of roots in $\text{GF}(p)$ of the polynomial $g(t)$, where $g(t) = t^3 - xt - y$. If x and y are integers such that the Galois group of $g(t)$ over the rationals is S_3 , then the number of roots of $g(t)$ over $\text{GF}(p)$ is not a PORC function. So for most pairs of integers x, y the order of the automorphism group of $G_{(p,x,y)}$ is not a PORC function. Nevertheless, the frequency with which the different orders of automorphism group arise over all x, y is describable in terms of PORC functions.

Crown Copyright © 2016 Published by Elsevier Inc. All rights reserved.

1. Introduction

If $p > 3$ is prime then we define the group $G_{(p,x,y)}$ to be the class 3 group of order p^7 and exponent p with generators a, b, c satisfying the following relations:

$$[b, a, b] = [b, a, c] = [c, a, a] = [c, a, b] = 1, \quad [c, a, c] = [b, a, a],$$

$$[c, b, b] = [b, a, a]^y, \quad [c, b, c] = [b, a, a]^x.$$

E-mail address: michael.vaughan-lee@chch.ox.ac.uk.

<http://dx.doi.org/10.1016/j.jalgebra.2016.07.042>

0021-8693/Crown Copyright © 2016 Published by Elsevier Inc. All rights reserved.

The quotient group $G/\gamma_3(G)$ is the free class two group of exponent p of rank 3, and has order p^6 . The subgroup $\gamma_3(G)$ is cyclic of order p , generated by $[b, a, a]$. Our main result is the following theorem.

Theorem 1. *Let x, y be integers which are coprime to p , and let g be the polynomial $t^3 - xt - y$. The order of the automorphism group of $G_{(p,x,y)}$ is one of four polynomials in p , with the choice of polynomial depending on the number of roots of g in $\text{GF}(p)$. Specifically, the automorphism group of $G_{(p,x,y)}$ has order $(p^3 - 1)p^{12}$, $(p - 1)(p^2 - 1)p^{12}$, $p(p - 1)^2p^{12}$ or $(p - 1)^3p^{12}$ when g has 0, 1, 2, or 3 roots in $\text{GF}(p)$.*

There is a deep theorem in Number Theory that asserts that if $g(t)$ is a polynomial in t with integer coefficients, and if the Galois group of $g(t)$ over the rationals is abelian, then the number of roots of $g(t)$ over $\text{GF}(p)$ is a PORC function of p , whereas if the Galois group is not abelian, then the number of roots is not a PORC function of p . (A function $f(p)$ is said to be PORC, **P**olynomial **O**n **R**esidue **C**lasses, if there is a finite set of polynomials in p , $g_1(p), g_2(p), \dots, g_k(p)$, and a fixed integer M , such that for each prime p , $f(p) = g_i(p)$ for some i ($1 \leq i \leq k$), with the choice of i depending on the residue class of $p \bmod M$.) If g is quadratic, then the Galois group is always abelian, and so the number of roots of g over $\text{GF}(p)$ is PORC. Of course you can see this directly from quadratic reciprocity. For example the polynomial $t^2 + 3$ has two roots in $\text{GF}(p)$ if $p \equiv 1 \pmod{3}$, and no roots if $p \equiv 2 \pmod{3}$. But if g is a cubic with Galois group S_3 , then the number of roots of g over $\text{GF}(p)$ is not PORC. So this theorem in Number Theory immediately gives us:

Theorem 2. *If x, y are non-zero integers such that the Galois group of the polynomial $t^3 - xt - y$ over the rationals is S_3 then the order of the automorphism group of $G_{(p,x,y)}$ is not a PORC function of p .*

Note that if we have a fixed pair of non-zero integers x, y , then x and y will be coprime to p for all but finitely many primes. Note also that the Galois group of $t^3 - xt - y$ is S_3 if the cubic is irreducible, and if its discriminant $4x^3 - 27y^2$ is not a square. So the Galois group is S_3 for “most” pairs of integers x, y . See Section 2 below for a short note about this theorem from Number Theory.

On the other hand the non-PORC behaviour of individual groups $G_{(p,x,y)}$ disappears if we average over the whole family:

Theorem 3. *For any given prime $p > 3$ there are (up to isomorphism) $p + 2 + \gcd(p - 1, 3)$ different groups $G_{(p,x,y)}$. Let*

$$f(p) = \sum_G |\text{Aut}(G)|,$$

where $\text{Aut}(G)$ is the automorphism group of G , and where the sum is taken over a set of representatives for the isomorphism classes of the groups $G_{(p,x,y)}$. Then $f(p)$ is PORC.

I would like to thank Roger Heath-Brown for all the help he has given me with the number theory in this paper.

2. Roots of polynomials

If $f(t)$ is a polynomial in t with integer coefficients, then we can define the function $N_f(p)$ to be the number of roots of f over $\text{GF}(p)$. As mentioned in the introduction, N_f is PORC if and only if the Galois group of f over the rationals is abelian. Of course $N_f(p) \leq \deg f$, and so N_f is PORC if and only if there is an integer M such that

$$p \bmod M = q \bmod M \text{ implies that } N_f(p) = N_f(q).$$

Wyman [11] gives the following theorem:

Theorem 4 (*Abelian polynomial theorem*). *The set $\text{Spl}(f)$ can be described by congruences with respect to a modulus depending only on f if and only if f is an abelian polynomial.*

Here, f is abelian if the Galois group of f is abelian, and $\text{Spl}(f)$ is the set of primes over which f splits. See [2], Theorem 2.1 and Corollary 5.11 for the history of this result and some proofs. If $\text{Spl}(f)$ is not describable by congruences, then of course neither is N_f , whatever the degree of f . It is easy to see that the converse holds for degree 3. If f is an irreducible polynomial of degree 3, with discriminant d , then $N_f(p) = 1$ if d is not a square in $\text{GF}(p)$ and $N_f(p) = 0$ or 3 when d is a non-zero square in $\text{GF}(p)$. Quadratic reciprocity takes care of when d is a square in $\text{GF}(p)$, and so if $\text{Spl}(f)$ is describable by congruences then so is N_f .

The beauty of the Abelian Polynomial Theorem is that it shows that cubic polynomials with $N_f(p)$ not PORC are ubiquitous. But it is relatively easy to find specific cubic polynomials f where there is a direct proof that N_f is not PORC, and this shows that there are at least some groups $G_{(p,x,y)}$ such that the orders of their automorphism groups are not PORC functions of p . For example it is well known that the polynomial $t^3 - 2$ splits over $\text{GF}(p)$ if and only if $p \equiv 1 \pmod{3}$ and $p \equiv a^2 + 27b^2 \pmod{27}$ for some a, b . And this is enough to show that N_{t^3-2} is not PORC. (See for example [3], page 179.) The polynomial $t^3 - 2$ is not suitable for our purposes, since we need cubic polynomials of the form $t^3 - xt - y$ where $x, y \neq 0$. But it is easy to show that $t^3 - 2$ has the same number of roots as $t^3 + 6t - 2$ in any field.

3. Connections with Graham Higman's PORC conjecture

My interest in the non-PORC behaviour of the groups $G_{(p,x,y)}$ arises from its connection with Graham Higman's PORC conjecture [5,6]. Higman conjectured that if we set

$f(p, n)$ equal to the number of p -groups of order p^n , then $f(p, n)$ is a PORC function of p for each positive integer n . He proved that the number of p -class two groups of order p^n is a PORC function of p for each n . At the time Higman made his conjecture it was known to hold true for $n \leq 5$, and it has since been proved correct for $n \leq 7$ (see [8,9]). For example, for $p \geq 5$ the number of groups of order p^6 is

$$3p^2 + 39p + 344 + 24 \gcd(p-1, 3) + 11 \gcd(p-1, 4) + 2 \gcd(p-1, 5).$$

The number of groups of order p^8 with exponent p has also been shown to be PORC (see [10]), as has the number of class three groups of order p^9 with exponent p .

Higman's conjecture has stimulated interest in finding p -groups exhibiting non-PORC behaviour of various sorts. For example du Sautoy and Vaughan-Lee [4] give an example of a class two group G with exponent p and order p^9 with the following properties:

1. The number of conjugacy classes of G is not PORC.
2. The order of the automorphism group of G is not PORC.
3. The number of immediate descendants of G with exponent p and order p^{10} is not PORC.

(A p -group H is said to be an immediate descendant of a p -group G if $G \cong H/N$, where N is the last non-trivial term of the lower p -central series of H . See [8] for details.) The relevance of property (3) of G to Higman's PORC conjecture is that the classification of the groups of order p^6 in [8] was obtained by classifying the immediate descendants of order p^6 of all the groups of order less than p^6 . In each case the number of descendants was PORC, and the PORC formula for the total number of groups of order p^6 was obtained by summing all these individual PORC functions. The same considerations apply to the classification of groups of order p^7 in [9]. If we were to use the same method to compute the number of groups of order p^{10} then we would need to draw up a complete and irredundant list of the groups with order dividing p^9 , and compute the number of descendants of order p^{10} of each group in the list. Our example shows that at least one group of order p^9 has a non-PORC number of descendants of order p^{10} . However there are likely to be other groups of order p^9 with a non-PORC number of descendants of order p^{10} , so the grand total of groups of order p^{10} could be PORC, with individual non-PORC summands cancelling out. Nevertheless du Sautoy and Vaughan-Lee [4] confidently asserted: "*It seems likely that there are other groups of order p^9 with a non-PORC number of immediate descendants of order p^{10} , and so it is possible that the grand total is PORC, even though not all of the summands are PORC. The authors' own view is that this is extremely unlikely.*"

It is still an open question whether the number of groups of order p^{10} is PORC, but nevertheless this assertion is now looking rather foolish! Lee [7] has recently found a class two group H with exponent p and order p^8 with the following properties:

1. The number of conjugacy classes of H is not PORC.
2. The order of the automorphism group of H is not PORC.
3. The number of immediate descendants of H with exponent p and order p^9 is not PORC.

However, in this case we now know that the total number of class three groups of order p^9 with exponent p is PORC. In fact, in apparent contradiction to Lee's result, I have a complete list of the 70 class two groups of exponent p with order dividing p^8 . For every single group G in my list

1. The number of conjugacy classes of G is a polynomial in p .
2. The order of the automorphism group of G is a polynomial in p .
3. The number of class 3 descendants of G with order p^9 and exponent p is PORC.

The explanation for this “contradiction” is that Lee's group H is really a family of groups, one for each p , as are the groups in my list. For any given p , Lee's group H must lie in one of my families, but it does not have to lie in the same family for every p . It turns out that there are four (families of) groups in my list A , B , C , D . If $p = 3$ then $H \cong A$, if $p = 2 \bmod 3$ then $H \cong B$, if $p = 1 \bmod 3$ and $t^3 - 2$ has no roots in $\text{GF}(p)$ then $H \cong C$, and if $p = 1 \bmod 3$ and $t^3 - 2$ has three roots in $\text{GF}(p)$ then $H \cong D$. The non-PORC properties of Lee's group arise from the fact that the number of roots of $t^3 - 2$ over $\text{GF}(p)$ is not PORC.

The groups $G_{(p,x,y)}$ do not directly impinge on Higman's conjecture since they are all terminal (i.e. they have no descendants). Also the number of conjugacy classes of $G_{(p,x,y)}$ is “well behaved”. If y is coprime to p then $G_{(p,x,y)}$ has $p^4 + p^3 - 1$ conjugacy classes, and if $p|y$ it has $p^4 + 2p^3 - p^2 - p$ conjugacy classes. Nevertheless it is interesting to see non-PORC behaviour in groups with order as low as p^7 . And it is also interesting to see how the non-PORC behaviour of individual groups in the family $G_{(p,x,y)}$ cancels out when you look at the “grand total”.

4. The groups $G_{(p,x,y)}$ — isomorphisms and automorphisms

Clearly

$$G_{(p,x,y)} \cong G_{(p,x',y')}$$

if $x = x' \bmod p$ and $y = y' \bmod p$. More precisely, we can say that $G_{(p,x,y)}$ is isomorphic to $G_{(p,x',y')}$ if and only if

$$x' = \lambda^2 x \bmod p, \quad y' = \lambda^3 y \bmod p$$

for some λ which is coprime to p . The “if” part of this claim is straightforward. If a, b, c are the defining generators of $G_{(p,x,y)}$, and if we set $a' = a$, $b' = b^{\lambda^2}$, $c' = c^{\lambda}$, then a', b', c'

satisfy the relations of $G_{(p, \lambda^2 x, \lambda^3 y)}$. The “only if” part of the claim is far from trivial — we give a proof in Section 7.

There are $p - 1$ non-isomorphic groups $G_{(p, x, y)}$ with x and y coprime to p . There are $\gcd(p - 1, 3)$ groups $G_{(p, 0, y)}$ with y coprime to p , two groups $G_{(p, x, 0)}$ with x coprime to p , and the group $G_{(p, 0, 0)}$. So, in all we have $p + 2 + \gcd(p - 1, 3)$ groups $G_{(p, x, y)}$ for any given p . It is easy enough to write down an irredundant set of representatives for the $p + 2 + \gcd(p - 1, 3)$ isomorphism classes if we think of x and y as elements of $\text{GF}(p)$ — we can do this since up to isomorphism it is only the values of x and y modulo p which matter. We obtain a set of representatives for the $p - 1 + \gcd(p - 1, 3)$ isomorphism classes with $y \neq 0$ as follows. If $p \equiv 1 \pmod{3}$ we pick a primitive element $\omega \in \text{GF}(p)$, let y range over $\{1, \omega, \omega^2\}$ and let x range over $\{0\} \cup T$, where T is a transversal for the cube roots of unity in the multiplicative group $\text{GF}(p) \setminus \{0\}$. If $p \equiv 2 \pmod{3}$ we let $y = 1$, and let x take any value in $\text{GF}(p)$. For $y = 0$ and $x \neq 0$ we have two isomorphism classes depending on whether x is a square in $\text{GF}(p)$, or not a square. And finally, of course, we have the group $G_{(p, 0, 0)}$.

The automorphism group of any one of the groups $G_{(p, x, y)}$ is determined by its action on the Frattini quotient G/G' . If d, e, f are any three elements in the derived group then we have an automorphism mapping a, b, c to ad, be, cf , and we can compose any other automorphism of G with this automorphism. So the order of the automorphism group of G is $|A|p^{12}$, where A is the automorphism group induced on G/G' . This group A is a subgroup of $\text{GL}(3, p)$ and we show that if x and y are coprime to p it is the group $\mathcal{A}_{(x, y)}$ of all non-singular matrices in $\text{GL}(3, p)$ of the form

$$\begin{pmatrix} \alpha & \beta & \gamma \\ y\gamma & \alpha + x\beta & -y\beta \\ y\beta + x\gamma & -\gamma & \alpha \end{pmatrix}.$$

(Here α, β, γ represent general elements of $\text{GF}(p)$.) When $p|x$ but y is coprime to p then the group of automorphisms induced on G/G' depends on $p \pmod{3}$. If $p \equiv 2 \pmod{3}$ then it is $\mathcal{A}_{(0, y)}$, but when $p \equiv 1 \pmod{3}$ it is the group of all non-singular matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda^2 & 0 \\ 0 & 0 & \lambda \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ y\gamma & \alpha & -y\beta \\ y\beta & -\gamma & \alpha \end{pmatrix}$$

where $\lambda^3 = 1$. The group $\mathcal{A}_{(0, y)}$ is a subgroup of index 3 in this group.

If $y \neq 0$, it turns out that the order of $\mathcal{A}_{(x, y)}$ depends on the number of roots of the polynomial $t^3 - xt - y$. Depending on whether the number of roots is 0, 1, 2 or 3, $\mathcal{A}_{(x, y)}$ has order $p^3 - 1$, $(p - 1)(p^2 - 1)$, $p(p - 1)^2$ or $(p - 1)^3$. We give proofs of these claims in Section 6 and Section 7.

There are three groups $G_{(p, x, y)}$ with $p|y$, $G_{(p, x, 0)}$ with $x = 0, 1, \omega$ where ω is a primitive element modulo p . Calculating the action induced on G/G' by the automorphism group of

G in these three cases is straightforward. When $x = 0$ we have the group of non-singular matrices of the form

$$\lambda \begin{pmatrix} 1 & \beta & \gamma \\ 0 & \mu^2 & 0 \\ 0 & -\gamma\mu & \mu \end{pmatrix}$$

which has order $p^2(p-1)^2$. When $x = 1, \omega$ we have the group of non-singular matrices

$$\lambda \begin{pmatrix} \alpha & \frac{1-\alpha}{x} & \gamma \\ 0 & 1 & 0 \\ \pm x\gamma & \mp \gamma & \pm \alpha \end{pmatrix}.$$

The determinant of this matrix is $\lambda^3(\alpha^2 - x\gamma^2)$, so the order of this group $2(p-1)^3$ if $x = 1$, and $2(p-1)(p^2-1)$ if $x = \omega$.

5. Proof of Theorem 3

In this section we show that Theorem 3 follows from Theorem 1.

Let

$$f_n = |\{x, y \mid x, y \in GF(p) \setminus \{0\}, t^3 - xt - y \text{ has } n \text{ roots}\}|$$

for $n = 0, 1, 2, 3$. Then the functions f_n have the following values. If $p \equiv 1 \pmod{3}$ then f_0, f_1, f_2, f_3 are

$$(p-1)\frac{p-1}{3}, (p-1)\frac{p-1}{2}, (p-1), (p-1)\frac{p-7}{6}$$

respectively, and if $p \equiv 2 \pmod{3}$ then f_0, f_1, f_2, f_3 are

$$(p-1)\frac{p+1}{3}, (p-1)\frac{p-3}{2}, (p-1), (p-1)\frac{p-5}{6}$$

respectively. This is quite easy to see. The discriminant of $t^3 - xt - y$ is $4x^3 - 27y^2$. The polynomial has one root if $4x^3 - 27y^2$ is not a square, and two roots if $4x^3 - 27y^2 = 0$. It is easy to see that there are $p-1$ pairs x, y with $x, y \neq 0$ and $4x^3 - 27y^2 = 0$. This gives the value of f_2 . When $x, y \neq 0$ we can write

$$4x^3 - 27y^2 = x^2(4x - 27\frac{y^2}{x^2})$$

so we can see that for a fixed value of $\frac{y}{x}$ there are $\frac{p-1}{2}$ non-zero values of x such that $4x^3 - 27y^2$ is not a square when $p \equiv 1 \pmod{3}$, and $\frac{p-3}{2}$ values when $p \equiv 2 \pmod{3}$. This

gives the value of f_1 . The value of f_0 comes from counting the number of irreducible polynomials of the form $t^3 - xt - y$. Finally, we have $f_3 = (p-1)^2 - f_0 - f_1 - f_2$.

Up to isomorphism there are $p-1$ groups $G_{(p,x,y)}$ with $x, y \neq 0$, each group arising $p-1$ times. As stated in Theorem 1, if $x, y \neq 0$ the order of the automorphism group of $G_{(p,x,y)}$ is one of four polynomials in p , with the choice of polynomial depending on the number of roots of $t^3 - xt - y$ in $\text{GF}(p)$. The number of times each automorphism group arises as we range over these $p-1$ groups can be obtained by dividing the functions f_n by $p-1$. So if we sum the orders of the automorphism groups over these $p-1$ groups we obtain a PORC function.

When $x = 0$ and $y \neq 0$ we have (up to isomorphism) one group with automorphism group of order $(p-1)(p^2-1)p^{12}$ when $p \equiv 2 \pmod{3}$, or three groups with automorphism groups of orders

$$3(p-1)^3 p^{12}, 3(p^3-1)p^{12}, 3(p^3-1)p^{12}$$

when $p \equiv 1 \pmod{3}$. And finally, when $y = 0$ we have three groups with automorphism groups of order

$$p^2(p-1)^2 p^{12}, 2(p-1)^3 p^{12}, 2(p-1)(p^2-1)p^{12}.$$

This proves Theorem 3.

6. The matrix group $\mathcal{A}_{(x,y)}$

In this section we investigate the group $\mathcal{A}_{(x,y)}$ of non-singular matrices in $\text{GL}(3, p)$ of the form

$$M(\alpha, \beta, \gamma) = \begin{pmatrix} \alpha & \beta & \gamma \\ y\gamma & \alpha + x\beta & -y\beta \\ y\beta + x\gamma & -\gamma & \alpha \end{pmatrix},$$

where $x, y \in \text{GF}(p)$, $y \neq 0$. The key feature of these matrices is that the second and third rows are determined by the first row. It is easy to check that the set of non-singular matrices $M(\alpha, \beta, \gamma)$ forms a group under multiplication. In fact the group is an abelian group. We show that the order of this group depends on the number of roots of $t^3 - xt - y$, and is $p^3 - 1$, $(p-1)(p^2-1)$, $p(p-1)^2$ or $(p-1)^3$ depending on whether this polynomial has 0, 1, 2 or 3 roots.

The determinant of $M(\alpha, \beta, \gamma)$ is

$$\alpha^3 + \alpha^2\beta x - 3\alpha\beta\gamma y - \alpha\gamma^2 x - \beta^3 y^2 - 2\beta^2\gamma xy - \beta\gamma^2 x^2 - \gamma^3 y,$$

and we need to determine the number of triples α, β, γ such that this determinant is zero. It turns out to be helpful to look at some special cases:

$$\begin{aligned}
\det(M(\alpha, 0, 0)) &= \alpha^3, \\
\det(M(0, \beta, 0)) &= -\beta^3 y^2, \\
\det(M(0, 0, \gamma)) &= -\gamma^3 y, \\
\det(M(0, \beta, \gamma)) &= -\beta^3 y^2 - 2\beta^2 \gamma xy - \beta \gamma^2 x^2 - \gamma^3 y, \\
\det(M(\alpha, 0, \gamma)) &= \alpha^3 - \alpha \gamma^2 x - \gamma^3 y, \\
\det(M(\alpha, \beta, 0)) &= \alpha^3 + \alpha^2 \beta x - \beta^3 y^2.
\end{aligned}$$

So if two of α, β, γ are zero and the third is non-zero then the determinant is non-zero. If two of α, β, γ are non-zero and the third is zero, then the number of matrices with zero determinant depends on the numbers of roots of the following polynomials: $y^2 t^3 - 2xyt^2 - x^2 t - y$, $t^3 - xt - y$, $t^3 + xt - y^2$. It is easy to see that these three cubics all have the same number of roots, and we can obtain expressions giving the roots of any one of these cubics in terms of the roots of any other.

To handle the general case, we let K be a splitting field for $t^3 - xt - y$ over $\text{GF}(p)$, and we let d, e, f be the roots of $t^3 - xt - y$ in K . Then

$$\det M(\alpha, \beta, \gamma) = (\alpha + (-d^2 + x)\beta - d\gamma)(\alpha + (-e^2 + x)\beta - e\gamma)(\alpha + (-f^2 + x)\beta - f\gamma).$$

This factorization was not so easy to find, but it is easy to verify it using a computer algebra system such as MAGMA [1]. Define P to be

$$(\alpha + (-d^2 + x)\beta - d\gamma)(\alpha + (-e^2 + x)\beta - e\gamma)(\alpha + (-f^2 + x)\beta - f\gamma) - \det M(\alpha, \beta, \gamma).$$

Then we want to prove that $P = 0$. We have $d + e + f = 0$ and $ef + fd + de + x = 0$. We use the equation $d + e + f = 0$ to eliminate d from $ef + fd + de + x$, and obtain $x - e^2 - ef - f^2 = 0$. If we use the equation $d + e + f = 0$ to eliminate d from P , and then add

$$(f^3 - fx - y)(3\alpha\beta\gamma + \beta^3 f^3 - \beta^3 fx + \beta^3 y + 2\beta^2 \gamma x + \gamma^3)$$

(which we know to be zero), then we obtain an expression which is exactly divisible by $x - e^2 - ef - f^2$. So $P = 0$.

If $t^3 - xt - y$ has no roots in $\text{GF}(p)$, then none of the factors

$$\begin{aligned}
&(\alpha + (-d^2 + x)\beta - d\gamma), \\
&(\alpha + (-e^2 + x)\beta - e\gamma), \\
&(\alpha + (-f^2 + x)\beta - f\gamma)
\end{aligned}$$

can be zero unless $\alpha = \beta = \gamma = 0$, and so $\mathcal{A}_{(x,y)}$ has order $p^3 - 1$.

If the discriminant of $t^3 - xt - y$ is zero then we have roots d, e, e in $\text{GF}(p)$, with $d \neq e$. There are p^2 triples (α, β, γ) such that $\alpha + (-d^2 + x)\beta - d\gamma = 0$, and p^2 triples such that $\alpha + (-e^2 + x)\beta - e\gamma = 0$. Also, there are p triples such that

$$\alpha + (-d^2 + x)\beta - d\gamma = \alpha + (-e^2 + x)\beta - e\gamma = 0.$$

So $\mathcal{A}_{(x,y)}$ has order $p^3 - 2p^2 + p = p(p-1)^2$.

If $t^3 - xt - y$ has three distinct roots $d, e, f \in \text{GF}(p)$ then the three simultaneous equations

$$\alpha + (-d^2 + x)\beta - d\gamma = 0,$$

$$\alpha + (-e^2 + x)\beta - e\gamma = 0,$$

$$\alpha + (-f^2 + x)\beta - f\gamma = 0$$

are independent since

$$\det \begin{pmatrix} 1 & -d^2 + x & -d \\ 1 & -e^2 + x & -e \\ 1 & -f^2 + x & -f \end{pmatrix} = (d-f)(d-e)(e-f).$$

So the order of the group $\mathcal{A}_{(x,y)}$ is $p^3 - 3p^2 + 3p - 1 = (p-1)^3$.

Finally suppose that $t^3 - xt - y$ has a single root $d \in \text{GF}(p)$. Then

$$t^3 - xt - y = (t-d)(t^2 + dt + d^2 - x),$$

and so if we pick $u \in \text{GF}(p^2)$ such that $u^2 = 4x - 3d^2$ then the other two roots e, f of $t^3 - xt - y$ can be expressed in the form

$$\frac{-d \pm u}{2}.$$

Note that since $e, f \notin \text{GF}(p)$, $u \notin \text{GF}(p)$. Using this expression for e , the factor $\alpha + (-e^2 + x)\beta - e\gamma$ can be expressed in the form

$$\alpha + \frac{1}{2}\beta d^2 + \frac{1}{2}\gamma d - \frac{1}{2}\gamma u + \frac{1}{2}\beta du$$

Since $u \notin \text{GF}(p)$ this factor can only be zero if $\gamma = \beta d$, and then it equals $\beta d^2 + \alpha$. So this factor can only be zero if $\alpha = -\beta d^2$ and $\gamma = \beta d$. The same applies to the factor $\alpha + (-f^2 + x)\beta - f\gamma$. So in this case there are p^2 solutions to $\alpha + (-d^2 + x)\beta - d\gamma = 0$ and p solutions to

$$(\alpha + (-e^2 + x)\beta - e\gamma)(\alpha + (-f^2 + x)\beta - f\gamma) = 0.$$

Note that if $\alpha = -\beta d^2$ and $\gamma = \beta d$ then the factor $\alpha + (-d^2 + x)\beta - d\gamma$ is equal to $\beta(x - 3d^2)$ which can only be zero if $\beta = 0$. (If $x = 3d^2$ then $u^2 = 9d^2$ and $u \in \text{GF}(p)$.) It follows that $\mathcal{A}_{(x,y)}$ has order $p^3 - p^2 - p + 1 = (p-1)(p^2-1)$.

7. Automorphism groups and isomorphisms revisited

We still need to prove our claims made in Section 4 about the automorphism groups of the groups $G_{(p,x,y)}$ when y is coprime to p . We also want to prove the “only if” part of the claim made in Section 4 that $G_{(p,x,y)}$ is isomorphic to $G_{(p,x',y')}$ if and only if

$$x' = \lambda^2 x \bmod p, y' = \lambda^3 y \bmod p \quad (1)$$

for some λ which is coprime to p .

It makes the exposition easier, and the notation clearer, if we switch to Lie algebra notation. The Lazard correspondence gives a correspondence between groups of exponent p and nilpotent Lie algebras over $\text{GF}(p)$. Under this correspondence the group $G_{(p,x,y)}$ corresponds to the Lie algebra $L_{(p,x,y)}$ over $\text{GF}(p)$ with presentation

$$\langle a, b, c \mid bab, bac, caa, cab, cac - baa, cbb - ybaa, cbc - xbaa, \text{ class } 3 \rangle.$$

The automorphism group of $L_{(p,x,y)}$ is the same as the automorphism group of $G_{(p,x,y)}$, and just as in the group case it is determined by its action on L/L^2 . If A is a matrix in $\text{GL}(3, p)$ and if we let

$$\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = A \begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

then a', b', c' generate L . We want to prove that the map sending a, b, c to a', b', c' extends to an automorphism of L if $A \in \mathcal{A}_{(x,y)}$. We also want to prove that if $x, y \neq 0$ then the map extends to an automorphism if and only if $A \in \mathcal{A}_{(x,y)}$.

It is straightforward to show that matrices $A \in \mathcal{A}_{(x,y)}$ define automorphisms. Let

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in \text{GL}(3, p).$$

Then A gives an automorphism of $L_{(p,x,y)}$ if the 7 polynomials below evaluate to zero.

$$f_1 = xbf^2 - xcef + ybef - yce^2 + ade + af^2 - bd^2 - cdf$$

$$f_2 = xbf i - xce i + ybf h - yce h + aeg + af i - bdg - cdi$$

$$f_3 = xbc i - xc^2 h + yb^2 i - ybch + a^2 h - abg + aci - c^2 g$$

$$\begin{aligned}
f_4 &= xbf_i - xcf_h + ybei - yce_h + adh + af_i - bdg - cfg \\
f_5 &= -xbcf + xbi^2 + xc^2e - xchi - yb^2f + ybce + ybhi - ych^2 - a^2e + abd \\
&\quad - acf + agh + ai^2 - bg^2 + c^2d - cgi \\
f_6 &= -xybcf + xyc^2e + xef_i - xf^2h - y^2b^2f + y^2bce - ya^2e + yabd \\
&\quad - yacf + yc^2d + ye^2i - yefh + d^2h - deg + df_i - f^2g \\
f_7 &= -x^2bcf + x^2c^2e - xyb^2f + xybce - xa^2e + xabd - xacf + xc^2d + xei^2 \\
&\quad - xfhi + yehi - yfh^2 + dgh + di^2 - eg^2 - fgi.
\end{aligned}$$

Define a', b', c' as above and then $b'a'b' = 0$ if and only if f_1 evaluates to zero, $b'a'c' = 0$ if and only if f_2 evaluates to zero, and so on.

We assume that $y \neq 0$, and let $\mathcal{H}$ be the set of matrices $A \in \text{GL}(3, p)$ such that if we define a', b', c' as above then a', b', c' satisfy the first five defining relations of $L_{(p, x, y)}$:

$$b'a'b' = b'a'c' = c'a'a' = c'a'b' = c'a'c' - b'a'a' = 0. \quad (2)$$

At this stage we place no restriction on x . We show that $\mathcal{H}$ is the set of non-singular matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda^2 & 0 \\ 0 & 0 & \lambda \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ y\gamma & \alpha + x\beta & -y\beta \\ y\beta + x\gamma & -\gamma & \alpha \end{pmatrix}. \quad (3)$$

In other words, if we set

$$J(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda^2 & 0 \\ 0 & 0 & \lambda \end{pmatrix},$$

then $\mathcal{H}$ is the set of non-singular matrices of the form $J(\lambda)M(\alpha, \beta, \gamma)$. It is easy to check that if a', b', c' do correspond to a matrix of this form, then a', b', c' do satisfy the relations (2) — just substitute the entries in a matrix of this form into the polynomials $f_1, f_2, \dots, f_5$ corresponding to these relations, and check that the polynomial evaluate to zero.

It turns out to be a straightforward calculation using a computer algebra program to show that any matrix in $\mathcal{H}$ with first row $(\alpha, \beta, 0)$ must equal $J(\lambda)M(\alpha, \beta, 0)$ for some λ . If we set $c = 0$ in $f_1, f_2, \dots, f_5$, then we obtain 5 polynomial equations in a, b, d, e, f, g, h, i , and it turns out that you can solve for d, e, f, g, h, i in terms of a, b . Similarly, any matrix in $\mathcal{H}$ with first row $(\alpha, 0, \gamma)$ must equal $J(\lambda)M(\alpha, 0, \gamma)$ for some λ , and any matrix in $\mathcal{H}$ with first row $(0, \beta, \gamma)$ must equal $J(\lambda)M(0, \beta, \gamma)$ for some λ .

I have been unable to find a similar straightforward calculation to deal with the case when α, β, γ are all non-zero, so I approached the problem in a different way. As above, we let $\mathcal{A} = \mathcal{A}_{(x,y)}$ be the set of non-singular matrices $M(\alpha, \beta, \gamma)$. The set $\mathcal{H}$ is not closed under multiplication, but $\mathcal{H}\mathcal{A} = \mathcal{H}$. To see this let $A \in \mathcal{H}$, and let $B \in \mathcal{A}$. We want to show that $AB \in \mathcal{H}$. Let

$$\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = B \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \quad \begin{pmatrix} a'' \\ b'' \\ c'' \end{pmatrix} = A \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix}.$$

We want to show that a'', b'', c'' satisfy the relations (2), and this follows from the fact that a', b', c' satisfy all the relations of L , and from the fact that $A \in \mathcal{H}$.

An independent proof that $\mathcal{H}\mathcal{A} = \mathcal{H}$ can be obtained as follows. If we let A be a general 3×3 matrix with symbolic entries, then we have 5 polynomials $f_1, f_2, \dots, f_5$ in the entries from A corresponding to the relations (2). If the polynomials evaluate to 0 for a particular matrix A then $A \in \mathcal{H}$. Now let $B = M(\alpha, \beta, \gamma)$, where the entries α, β, γ are symbolic. If we evaluate the polynomials $f_1, f_2, \dots, f_5$ at the entries in AB then we obtain five polynomials $g_1, g_2, \dots, g_5$, and we can verify that $f_i | g_i$ for $i = 1, 2, \dots, 5$.

Now let $A \in \mathcal{H}$ have first row (α, β, γ) . The case when $\det M(\alpha, \beta, \gamma) \neq 0$ is straightforward. If we let $B = M(\alpha, \beta, \gamma)$ then $AB^{-1} \in \mathcal{H}$ and AB^{-1} has first row $(1, 0, 0)$. But we know that the only matrices in $\mathcal{H}$ with first row $(1, 0, 0)$ are the matrices $J(\lambda)$. (This follows from the remarks above about matrices with $\alpha = 0$, or $\beta = 0$, or $\gamma = 0$.) So $AB^{-1} = J(\lambda)$ and

$$A = J(\lambda)B = J(\lambda)M(\alpha, \beta, \gamma).$$

The problem is that in the case when $\det M(\alpha, \beta, \gamma) = 0$ then we need to show there is *no* matrix in $\mathcal{H}$ with first row (α, β, γ) .

Now we know from Section 6 that if $\det M(\alpha, \beta, \gamma) = 0$ then either

$$\alpha = (d^2 - x)\beta + d\gamma$$

for some d satisfying $d^3 - xd - y = 0$, or $\alpha = -\beta d^2$ and $\gamma = \beta d$ for some d satisfying $d^3 - xd - y = 0$.

First consider the case when $\alpha = -\beta d^2$ and $\gamma = \beta d$ for some d satisfying

$$d^3 - xd - y = 0.$$

Then the row (α, β, γ) corresponds to the element

$$a' = -\beta d^2 a + \beta b + \beta dc \in L,$$

and it is straightforward to show that $la'a' = 0$ for all $l \in L$. In particular, if a', b', c' were generators of L satisfying the relations (2), then we would have $b'a'a' = 0$, which

would imply that $c'a'$ was in the centre of L . But when $y \neq 0$ then the centre of L is L^3 . So no element of $\mathcal{H}$ can have first row $(-\beta d^2, \beta, \beta d)$.

Next consider the case when $\alpha = (d^2 - x)\beta + d\gamma$, and suppose that

$$A = \begin{pmatrix} (d^2 - x)\beta + d\gamma & \beta & \gamma \\ \delta & \varepsilon & \zeta \\ \lambda & \mu & \nu \end{pmatrix} \in \mathcal{H}.$$

We know that if $\beta = 0$ or $\gamma = 0$ then A must lie in $J(\lambda)\mathcal{A}$ for some λ , so we assume that β and γ are non-zero.

Let

$$B = M((d^2 - x)\beta + d\gamma, 0, \gamma).$$

Then $AB = C$, where the last entry in the first row of C is zero. If $\det B \neq 0$ then $B \in \mathcal{A}$ and $C = AB \in \mathcal{H}$. But C has a first row with a zero in it, so $C \in J(\lambda)\mathcal{A}$ for some λ , and it follows that $A = CB^{-1} \in J(\lambda)\mathcal{A}$.

Similarly, if we let

$$D = M(\beta y, \gamma, 0)$$

then $AD = E$ where the last entry in the first row of E is zero, so that provided $\det D \neq 0$ we see that $A = ED^{-1} \in J(\lambda)\mathcal{A}$ for some λ .

We complete the proof of (3) by showing that if

$$\det B = \det D = d^3 - xd - y = 0$$

then the element $a' = ((d^2 - x)\beta + d\gamma)a + \beta b + \gamma c$ has the property that $la'a' = 0$ for all $l \in L$. As above this shows that a' cannot be part of a generating set a', b', c' satisfying the relations (2). We have $aa'a' = fbaa$ and $ba'a' = gbaa$, where

$$\begin{aligned} f &= x\beta^2 - d^2\beta^2 - d\beta\gamma - \gamma^2, \\ g &= x^2\beta^2 - 2xd^2\beta^2 - 2xd\beta\gamma - x\gamma^2 - y\beta\gamma + d^4\beta^2 + 2d^3\beta\gamma + d^2\gamma^2. \end{aligned}$$

Using the fact that $\gamma \neq 0$, $la'a' = 0$ for all $l \in L$ if and only if $f = g = 0$. However if we subtract $\beta\gamma(d^3 - xd - y)$ from g (hence eliminating y), then the result is divisible by f . So we only need to show that if

$$\det B = \det D = d^3 - xd - y = 0$$

then $f = 0$. Now $\det D = y^2(-\gamma^3 + y\beta^3 + x\beta^2\gamma)$ and $y \neq 0$, so if $\det D = 0$ we have

$$\begin{aligned} 0 &= (-\gamma^3 + y\beta^3 + x\beta^2\gamma) + \beta^3(d^3 - xd - y) \\ &= (\gamma - d\beta)f. \end{aligned}$$

So provided $\gamma \neq d\beta$ we have $f = 0$. On the other hand, if $\gamma = d\beta$ then $f = \beta^2(x - 3d^2)$, and

$$\beta^3 \det B - \frac{\gamma^3}{y^2} \det D = -\beta^6 (x - d^2) (x - 3d^2)^2.$$

We cannot have $x = d^2$ since $d^3 - xd - y = 0$ and $y \neq 0$, and so if

$$\gamma - d\beta = \det B = \det D = 0$$

then $f = 0$ as required.

We are at last in a position to justify our various claims about the automorphism group of $L_{(p,x,y)}$ and $G_{(p,x,y)}$ and about the isomorphism classes of the groups $G_{(p,x,y)}$.

Let $L = L_{(p,x,y)}$ with $y \neq 0$. Let $A \in \mathrm{GL}(3, p)$, and assume that the map $\theta(A)$ sending a, b, c to a', b', c' extends to an automorphism of L , where

$$\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = A \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Then certainly $A \in \mathcal{H}$, and so $A = J(\lambda)M(\alpha, \beta, \gamma)$ for some $\lambda, \alpha, \beta, \gamma$. Let

$$\begin{pmatrix} a'' \\ b'' \\ c'' \end{pmatrix} = M(\alpha, \beta, \gamma) \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

We know $M(\alpha, \beta, \gamma)$ does give an automorphism of L , so that a'', b'', c'' satisfy all the defining relations of L . We have $a' = a''$, $b' = \lambda^2 b''$, $c' = \lambda c''$. We also know that a', b', c' satisfy the relations (2). We then have

$$\begin{aligned} c'b'b' &= \lambda^5 c''b''b'' = \lambda^5 yb''a''a'' = \lambda^3 yb'a'a', \\ c'b'c' &= \lambda^4 c''b''c'' = \lambda^4 xb''a''a'' = \lambda^2 xb'a'a'. \end{aligned} \tag{4}$$

So for $\theta(A)$ to be an automorphism we require $\lambda^3 = 1$, $\lambda^2 x = x$. If $x \neq 0$ we must $\lambda = 1$, and if $x = 0$ then λ can be any cube root of unity. This establishes our claims about the automorphism groups of $L_{(p,x,y)}$ and $G_{(p,x,y)}$ when $y \neq 0$.

Finally, assume that $y \neq 0$, and let $\varphi : L_{(p,x,y)} \rightarrow L_{(p,x',y')}$ be an isomorphism. Pick generators a', b', c' for $L_{(p,x,y)}$ such that $\varphi(a'), \varphi(b'), \varphi(c')$ are the defining generators of $L_{(p,x',y')}$. Then a', b', c' satisfy the relations (2), and

$$\begin{aligned} c'b'b' &= y'b'a'a', \\ c'b'c' &= x'b'a'a'. \end{aligned}$$

Since a', b', c' satisfy the relations (2), we must have

$$\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = J(\lambda)M(\alpha, \beta, \gamma) \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

for some $\lambda, \alpha, \beta, \gamma$, where a, b, c are the defining generators of $L_{(p,x,y)}$. So, as in (4) we have

$$\begin{aligned} c'b'b' &= \lambda^3 y b' a' a', \\ c'b'c' &= \lambda^2 x b' a' a'. \end{aligned}$$

So $x' = \lambda^2 x$, and $y' = \lambda^3 y$, as claimed in (1). In particular, the fact that $y \neq 0$ implies that $y' \neq 0$.

To complete the proof of our claim (1) about when two groups $G_{(p,x,y)}$ and $G_{(p,x',y')}$ can be isomorphic we need to prove that $G_{(p,x,0)} \cong G_{(p,x',0)}$ if and only if $x' = \lambda^2 x$ for some λ . Now we know from considering generating sets for $G_{(p,x,y)}$ of the form $a, b^{\lambda^2}, c^\lambda$ that there are at most 3 isomorphism classes of groups $G_{(p,x,0)}$ for any given p — one class when $x = 0$, one class when x is a non-zero square, and one class when x is not a square in $\text{GF}(p)$. But the groups in these three classes have different automorphism groups, so we have exactly three isomorphism classes.

References

- [1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, *J. Symbolic Comput.* 24 (1997) 235–265.
- [2] K. Conrad, History of class field theory, <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf>, 2014.
- [3] D. Cox, *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, Inc., Hoboken, NJ, 2013.
- [4] M. du Sautoy, M. Vaughan-Lee, Non-PORC behaviour of a class of descendant p -groups, *J. Algebra* 361 (2012) 287–312.
- [5] G. Higman, Enumerating p -groups. I: inequalities, *Proc. Lond. Math. Soc.* (3) 10 (1960) 24–30.
- [6] G. Higman, Enumerating p -groups. II: problems whose solution is PORC, *Proc. Lond. Math. Soc.* (3) 10 (1960) 566–582.
- [7] S. Lee, A class of descendant p -groups of order p^9 and Higman's PORC conjecture, 2015, in preparation.
- [8] M. Newman, E. O'Brien, M. Vaughan-Lee, Groups and nilpotent Lie rings whose order is the sixth power of a prime, *J. Algebra* 278 (2004) 383–401.
- [9] E. O'Brien, M. Vaughan-Lee, The groups with order p^7 for odd prime p , *J. Algebra* 292 (2005) 243–358.
- [10] M. Vaughan-Lee, Groups of order p^8 and exponent p , *Int. J. Group Theory* 4 (2015) 25–42.
- [11] B. Wyman, What is a reciprocity law?, *Amer. Math. Monthly* 79 (1972) 571–586.