ISRAEL JOURNAL OF MATHEMATICS, Vol. 52, Nos. 1-2, 1985

GROUPS OF TYPE $F^{a,b,-c}$

BY

MANLEY PERKEL

Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA

ABSTRACT

For integers a, b and c, the group $F^{a,b,-c}$ is defined to be the group $\langle R, S : R^2 = RS^aRS^bRS^{-c} = 1\rangle$. In this paper we identify certain subgroups of the group of affine linear transformations of finite fields of order p^n (for certain p and n) as groups of type $F^{a,b,-c}$ for certain (not unique) choices of a, b and c.

1. Introduction

For integers a, b and c, the group $F^{a,b-c}$ is defined by

$$F^{a,b,-c} = \langle R, S : R^2 = RS^aRS^bRS^{-c} = 1\rangle.$$

These groups were first investigated in [1] and interest in them has arisen, partly, because they can be used to generate examples of trivalent Cayley graphs, in particular those whose automorphism groups are regular on their vertices (see [3]), although some with larger automorphism groups have also been found (see [2]). Also in [2] and [3] it is shown that some of these groups are not only metabelian but also metacyclic. The aim of this paper is the identification of certain subgroups of the group of affine linear transformations of finite fields of order p^n (for certain p and n), as groups of type $F^{a,b,-c}$ for certain (not unique) choices of a, b, c.

Let K be a field of order p^n, H a subgroup of the multiplicative group K^* of K, so that $|H| = (p^n - 1)/d$ for some integer d and $H = \langle \alpha^d \rangle$ where α is a generator of K^*. Let L be the smallest subfield of K containing H, and let $G(d, p^n) = \{f : K \to K \mid \text{for } x \in K, f : x \mapsto rx + s, r \in H, s \in L\}$. Thus $G(1, p^n)$ is the group of affine linear transformations of the field K and for any d dividing $p^n - 1$, $G(d, p^n)$ is a subgroup of $G(1, p^n)$. Further, $G(d, p)$ is always metacyclic.

Now suppose that $p^n \equiv 1 \pmod 4$ (so that n is even if $p \equiv -1 \pmod 4$) and

Received February 2, 1984 and in revised form January 29, 1985

choose integers a', b' and c' as follows: (i) $b' = (p^n - 1)/4$, (ii) c' is an integer with $\alpha^{c'} = 1 - \alpha^{b'}$, and (iii) $a' = b' + c'$. Let d be the g.c.d. of b' and c', and let $a = a'/d$, $b = b'/d$ and $c = c'/d$. As a first step in the identification we have the following.

THEOREM 1. (i) *For a, b, c, d as above, $G(d, p^n)$ is a homomorphic image of $F^{a,b,-c}$.*

(ii) *If $p \equiv 1 \pmod 4$ then $G(d, p^n)$ is isomorphic to a subgroup of $G(1, p)$, while if $p \equiv -1 \pmod 4$ then $G(d, p^n)$ is isomorphic to a subgroup of $G(1, p^2)$.*

Let h be the order of -2 modulo p, i.e. h is the smallest positive integer such that $(-2)^h \equiv 1 \pmod p$. Clearly, if h is even, p divides $(-2)^{h/2} + 1$. However, if $h \equiv 4 \pmod 8$, so that $h = 4k$ with k odd, we even have

$$(-2)^{h/2} + 1 = 2^{2k} + 1 = (2^k + 1 - 2^{(k+1)/2})(2^k + 1 + 2^{(k+1)/2}),$$

so that p divides one of $2^k + 1 \pm 2^{(k+1)/2}$. Now let

$$m = \begin{cases} [(-2)^h - 1]/p, & \text{if } h \equiv 1 \pmod 2, \\ [(-2)^{h/2} + 1]/p, & \text{if } h \equiv 0, 2 \text{ or } 6 \pmod 8, \\ [2^{h/4} + 1 \pm 2^{(h+4)/8}]/p, & \text{if } h \equiv 4 \pmod 8. \end{cases}$$

We now have the following.

THEOREM 2. *Let a, b, c be as in Theorem* 1.

(i) *If $p \equiv -1 \pmod 4$, then $|F^{a,b,-c}| = 4bm^2p^2$.*

(ii) *If $p \equiv 1 \pmod 4$, then*

$$|F^{a,b,-c}| = \begin{cases} 4bm^2p^2, & \text{if } b \equiv 2 \pmod 4, \\ 4bmp, & \text{otherwise.} \end{cases}$$

Let us call a prime p a *semi-Fermat prime* if $p = 2^k + 1 + 2^{(k+1)/2}$ or if $p = 2^k + 1 - 2^{(k+1)/2}$ for some odd integer k. (For example, $5, 13, 41, 113, 2113, \ldots$ are semi-Fermat primes.) Then we have the following.

COROLLARY. *Let a, b, c be as in Theorem* 1.

(i) *If p is a Mersenne prime, i.e. a prime of the form $2^q - 1$ (so that q is an odd prime), then $b = 2q$, $|F^{a,b,-c}| = 8qp^2$ and $F^{a,b,-c} \cong G(d, p^n)$.*

(ii) *If p is a Fermat prime, i.e. a prime of the form $2^q + 1$ (so that q is a power of 2), or if p is a semi-Fermat prime, then $|F^{a,b,-c}| = 4bp$ and $F^{a,b,-c} \cong G(d, p^n)$.*

REMARKS. (a) Note in the Corollary that if we take $n = 2$ in part (i), we have $F^{a,b,-c} \cong G(d, p^2)$, and if we take $n = 1$ in part (ii), we have $F^{a,b,-c} \cong G(d, p)$ (for

the appropriate values of d in each case; however the values of a, b, c remain the same).

(b) In [3], Chapter 12, the Cayley graph of the group $F^{3,2,-1}$ of order 72 is shown to be zero-symmetric. The above Corollary identifies this group as $G(1,9)$, the full group of affine linear transformations of the field with 9 elements. Also, using a different generator α for K^* gives $F^{7,2,-5} \cong F^{3,2,-1} \cong G(1,9)$. (The first isomorphism also follows from [1], Theorem 4.2.)

(c) From the Corollary we have for example, $F^{2,1,-1} \cong G(1,5)$ of order 20; $F^{7,6,-1} \cong G(2,7^2)$ of order $24 \cdot 49$; $F^{9,4,-5} \cong G(1,17)$ of order $16 \cdot 17$; $F^{21,10,-11} \cong G(24,31^2)$ of order $40 \cdot 31^2$; $F^{8,3,-5} \cong G(1,13)$ of order $12 \cdot 13$; $F^{9,5,-4} \cong G(2,41)$ of order $20 \cdot 41$; and $F^{23,8,-15} \cong G(8,257)$ of order $32 \cdot 257$.

The above results are proved in Section 2. In Section 3 we analyze in detail the kernel of the homomorphism promised by Theorem 1(i), leading to the following. Let N be an integer >0 and C_N denote the cyclic group of order N.

THEOREM 3. *Let E denote the kernel of the homomorphism of Theorem* 1(i) *and let m be as defined above.*

(i) *If $p \equiv -1 \pmod 4$, then $E \cong C_{|m|} \times C_{|m|}$.*

(ii) *If $p \equiv 1 \pmod 4$, then*

$$E \equiv \begin{cases} C_{|m|} \times C_{|m|p}, & \text{if } b \equiv 2 \pmod 4, \\ C_m, & \text{otherwise.} \end{cases}$$

Actually more is proven in Section 3. We obtain explicit generators for the kernel as well as describe in detail the action of the group on these generators.

2. Proofs of Theorems 1 and 2

Let K, α, a, b, c, etc. be as in the paragraphs immediately preceding the statement of Theorem 1.

PROOF OF THEOREM 1. (i) Let $R, S \in G(1,p^n)$ be defined by $R : x \mapsto -x$ and $S : x \mapsto \alpha^d x + k$ (for $x \in K$) where $k = (p-1)/2$. Then $S^{-1} : x \mapsto \alpha^{-d}x - \alpha^{-d}k$, so that if we define $Q = S^{-1}RSR$ (products from left to right) then $Q : x \mapsto x + 1$. Let $P = SQ^{-k}$. Then $P : x \mapsto \alpha^d x$. Since L is the smallest subfield of K containing $H = \langle \alpha^d \rangle$, we see that $G(d,p^n) = \langle P, Q \rangle$, whence $G(d,p^n) \leqq \langle R, S \rangle$. Now clearly d divides $b' = (p^n - 1)/4$, so $2d$ divides $p^n - 1$, and

$$(\alpha^d)^{(p^n-1)/2d} = \alpha^{(p^n-1)/2} = -1.$$

Hence $P^{(p^n-1)/2d} = R$, whence from $S = PQ^k$ we conclude that $G(d,p^n) = \langle R, S \rangle$.

Now certainly $R^2 = 1$. The following can easily be verified:

$$RS^a : x \mapsto -\alpha^{ad}x + k(1-\alpha^{ad})/(1-\alpha^d),$$

$$RS^aRS^b : x \mapsto \alpha^{(a+b)d}x - [\alpha^{bd}k(1-\alpha^{ad}) - k(1-\alpha bd)]/(1-\alpha^d)$$

$$= \alpha^{(a+b)d}x + k[1-2\alpha^{bd} + \alpha^{(a+b)d}]/(1-\alpha^d),$$

$$RS^aRS^bRS^{-c} : x \mapsto -\alpha^{(a+b-c)d}x - \alpha^{-cd}k[2-2\alpha^{bd} + \alpha^{(a+b)d} - \alpha^{cd}]/(1-\alpha^d).$$

Now, $(a+b-c)d = 2b' = (p^n-1)/2$, so $\alpha^{(a+b-c)d} = -1$. Also, $(a+b)d = a'+b' = 2b'+c'$, so $\alpha^{(a+b)d} = \alpha^{2b'}\alpha^{c'}$. Thus $2-2\alpha^{bd}+\alpha^{(a+b)d}-\alpha^{cd} = 2-2\alpha^{b'}-2\alpha^{c'} = 2(1-\alpha^{b'}-\alpha^{c'}) = 0$. Hence, $RS^aRS^bRS^{-c} = 1$. The completes the proof of (i).

(ii) Let $f \in G(d,p^n)$ and consider $f|_L$, the restriction of f to L. Since H is a subset of L, $f|_L$ has range in L, so that $f|_L$ is an affine linear transformation of L. Further, for $f, g \in G(d,p^n)$, if $f|_L = g|_L$, then $f = g$. Thus $G(d,p^n)$ is isomorphic to a subgroup of the group of affine linear transformations of L.

Now $\alpha^{2b'} = -1$ so that if -1 is a square in the field Z_p of integers modulo p, $\alpha^{b'}$, and hence $\alpha^{c'}$ too, will be in Z_p, and thus so will α^d. Thus $L = Z_p$ in this case. If -1 is not a square in Z_p, then $\alpha^{b'}$ will lie in an extension of degree 2 of Z_p in K, so that $|L| = p^2$. This finishes the proof of Theorem 1.

REMARK. It can also be shown, as in the proof of Theorem 1, that $G(1,p^n)$ is a homomorphic image of $F^{a',b',-c'}$; however, except when $d = 1$, these latter groups are infinite, whereas the finiteness of the groups $F^{a,b,-c}$ follows from Theorem 2. [For $n \geq 2$, $d = 1$ only for $p^n = 3^2$.]

PROOF OF THEOREM 2. First consider the group

$$F^{a,b,-c} = \langle R, S : R^2 = RS^aRS^bRS^{-c} = 1\rangle$$

with $a = b + c$. By Lemma 2.1 of [1], $F^{a,b,-c} \cong F^{a,-c,b}$ and $b = a + (-c)$, so that by Lemma 7.1 of [1], $S^{4b} = 1$ and $F^{a,b,-c}$ is a group of type $H^{a,b,-c}$. Thus, with a, b, c as in the hypotheses of Theorem 2, by Theorem 7.2 of [1], $F^{a,b,-c}$ has order $4b(2^b + 1 - 2^{1+b/2}\cos[(b+2c)\pi/4])$.

Now since $S^{4b} = 1$ and since the g.c.d. of b' and c' equals the g.c.d. of b' and $c' + t(p^n-1)$ for any integer t, we may choose c' with $1 \leq c' \leq p^n - 1$ in defining our group $F^{a,b,-c}$. Since $\alpha^{c'} = 1 - \alpha^{b'}$ we have $\alpha^{2c'} = (1-\alpha^{b'})^2 = -2\alpha^{b'}$. Since the order of -2 modulo p is h we have

$$-2 = \alpha^{e(p^n-1)/h} \qquad \text{for some integer } e, \quad 1 \leq e < h,$$

with e relatively prime to h. Thus

$$2c' \equiv e(p^n - 1)/h + b' \bmod (p^n - 1),$$

whence

$$2c' = (p^n - 1)(4e + h + 4hg)/4h, \qquad \text{where } g = 0 \text{ or } 1.$$

Now suppose that $p \equiv -1 \pmod 4$. Then either $h \equiv 1 \pmod 2$ or $h \equiv 2 \pmod 4$, since h divides $p - 1$. Since e and h are relatively prime, in the former case, $4e + h + 4hg$ has no factors in common with $2h$, so that $d = (p^n - 1)/8h$, while in the latter case, $2e + h/2 + 2hg$ has no factors in common with h, so that $d = (p^n - 1)/4h$. Thus we have

$$b = \begin{cases} h, & \text{if } h \equiv 2 \pmod 4 \\ 2h, & \text{if } h \equiv 1 \pmod 2 \end{cases}$$

and

$$c = \begin{cases} 2e + h/2 + 2gh & \text{if } h \equiv 2 \pmod 4 \\ 4e + h + 4gh & \text{if } h \equiv 1 \pmod 2. \end{cases}$$

Now when $h \equiv 2 \pmod 4$, $e \equiv 1 \pmod 2$, so that $b + 2c = 4e + 2h + 4gh \equiv 0 \pmod 8$, so that

$$|F^{a,b,-c}| = 4b(2^h + 1 - 2^{1+h/2}) = 4b[(-2)^{h/2} + 1]^2 = 4bm^2p^2.$$

When $h \equiv 1 \pmod 2$, $b + 2c = 8e + 4h + 8gh \equiv 4 \pmod 8$, so that

$$|F^{a,b,-c}| = 4b(2^{2h} + 1 + 2^{1+h}) = 4b[(-2)^h - 1]^2 = 4bm^2p^2,$$

so we are done when $p \equiv -1 \pmod 4$.

Now suppose that $p \equiv 1 \pmod 4$. If $h \equiv 1 \pmod 2$ or $h \equiv 2 \pmod 4$, then, as in the previous case, we get that $|F^{a,b,-c}| = 4bm^2p^2$. So suppose that either $h \equiv 0 \pmod 8$ or $h \equiv 4 \pmod 8$. Then, since now e is odd, we have in the former case that $e + h/4 + hg$ has no factors in common with h, so that $d = (p^n - 1)/2h$, while in the latter case, $e + h/4$ is even and so $d = (p^n - 1)/h$. Thus now we have

$$b = \begin{cases} h/2, & \text{if } h \equiv 0 \pmod 8 \\ h/4, & \text{if } h \equiv 4 \pmod 8 \end{cases}$$

and

$$c = \begin{cases} e + h/4 + hg, & \text{if } h \equiv 0 \pmod 8 \\ (4e + h)/8 + hg/2, & \text{if } h \equiv 4 \pmod 8. \end{cases}$$

Now, when $h \equiv 0 \pmod 8$, $b + 2c = 2e + h + 2gh \equiv 2$ or $6 \pmod 8$ so that $|F^{a,b,-c}| = 4b(2^{h/2} + 1) = 4bmp$, while if $h \equiv 4 \pmod 8$, $b + 2c = e + h/2 + hg$ is odd, so that

$$|F^{a,b,-c}| = 4b(2^{h/4} + 1 \pm 2^{(h+4)/8}) = 4bmp,$$

since by Theorem 1 we know that p divides $|F^{a,b,-c}|$. This completes the proof of Theorem 2.

PROOF OF THE COROLLARY. Part (i) follows directly from Theorem 2(i) and its proof. If p is either a Fermat or a semi-Fermat prime, then it is easy to see that the order of -2 modulo p is congruent to 0 or 4 (mod 8), so that, by the proof of Theorem 2, $b \equiv 0, 1$ or $3 \pmod 4$, whence part (ii) follows from Theorem 2(ii).

REMARKS. (a) In case (ii) of the Corollary, if $p = 2^q + 1$ is a Fermat prime, with $q = 2^t$, then if $t = 1$, $b = 1$, so that $p = 5$ and $|F^{2,1,-1}| = 2^2 \cdot 5$, while if $t \geqq 2$, $b = 2^t$, so that $|F^{a,b,-c}| = 2^{t+2}p$. If $p = 2^k + 1 \pm 2^{(k+1)/2}$ is a semi-Fermat prime, with k odd, then $b = k$, so that $|F^{a,b,-c}| = 4kp$.

(b) It has already been noted that for $n \geqq 2$, $d = 1$ only for $p^n = 3^2$, so that $F^{3,2,-1}$ is isomorphic to the full group of affine linear transformations over the field of order 9. For $p \equiv 1 \pmod 4$, $F^{a,b,-c} \cong G(1, p)$ only if one of the following is true: (i) $p \equiv 1 \pmod{16}$ and $h = (p-1)/2$, or (ii) $p \equiv 5 \pmod 8$ and $h = p - 1$, so that -2 is a primitive root modulo p. An example in case (i) is given by $F^{9,4,-5} \cong G(1, 17)$, and in case (ii) $F^{2,1,-1} \cong G(1, 5)$ and $F^{8,3,-5} \cong G(1, 13)$. Other examples in case (ii) are given by primes $p = 4q + 1$ for q a prime, since for such p, -2 is a primitive root modulo p (see, for example, [4], page 185).

(c) Because of the term involving g ($= 0$ or 1) in the value of c computed in Theorem 2, we get two sets of parameters a, b, c for each of the groups $F^{a,b,-c}$, giving non-trivial isomorphisms between them.

(d) For computational purposes in finding a, b and c, it is easiest (and by Theorem 1(ii), sufficient) to let $n = 1$ when $p \equiv 1 \pmod 4$ and $n = 2$ when $p \equiv -1 \pmod 4$. Even in the latter case, the computations are greatly simplified by the following observation. If β is a primitive root modulo p, we may suppose we have chosen the generator α of the field K of order p^2 so that $\alpha^{p+1} = \beta$. Then, if we know the value of t such that $\beta^t = -2$, h and e can easily be obtained, from which b and c can be found using the computations in the proof of Theorem 2, and finally $a = b + c$.

(e) It is known as well (see [2]) that $F^{3,2,-2} \cong G(1, 7)$ and $F^{4,3,-2} \cong F^{4,2,-1} \cong G(1, 11)$.

3. The kernel of the homomorphism and the proof of Theorem 3

We conclude this paper with an investigation of the kernel of the homomorphism from $F^{a,b,-c}$ to $G(d,p^n)$ of Theorem 1. Let

$$F^{a,b,-c} = \langle R, S : R^2 = RS^aRS^bRS^{-c} = 1\rangle$$

where $a = b + c$ and let $E = E^{a,b,-c}$ denote the kernel of the above-mentioned homomorphism. Let

$$X_1 = RS^{2b} \in F^{a,b,-c} \quad \text{and} \quad X_2 = S^{-a}RS^{2b+a} = S^{-a}X_1S^a \in F^{a,b,-c}.$$

By Lemma 3.1, Lemma 3.3 and the proof of Theorem 7.2 of [1], we know that if $K^{a,b,-c}$ denotes the derived group of $F^{a,b,-c}$, then

(i) $F^{a,b,-c} = K^{a,b,-c} \cdot \langle S\rangle$, a split extension, and

(ii) $K^{a,b,-c}$ is abelian and generated by X_1 and X_2.

Recall as well that $S^{4b} = 1$ so that the index of $K^{a,b,-c}$ in $F^{a,b,-c}$ is $4b$. (Note that in applying the proof of Theorem 7.2 of [1], we are using the fact that $F^{a,b,-c} \cong F^{a,-c,b}$ via the isomorphism $R \mapsto R$ and $S \mapsto S^{-1}$.)

LEMMA 1. *For $i = 1$ and 2, $RX_iR = X_i^{-1}$.*

PROOF. Since $X_1 = RS^{2b}$, we have $RX_1R = S^{2b}R = X_1^{-1}$. Now $X_2 = S^{-a}RS^{2b+a} = RS^bRS^{-c+2b+a} = RS^bRS^{-b} = [R, S^{-b}]$. (Here $[x,y]$ denotes the commutator $x^{-1}y^{-1}xy$.) Thus $RX_2R = S^bRS^{-b}R = [S^{-b}, R] = X_2^{-1}$ and we are done.

LEMMA 2. *For $i = 1$ and 2, $S^{-2b}X_iS^{2b} = X_i^{-1}$ and $S^{-(a+c)}X_iS^{(a+c)} = X_i^2$. Further, $X_1^2 = S^{-c}X_2S^c$ and $X_2 = S^{-b}X_1S^bX_1$.*

PROOF. The first equalities follow from the definitions of X_1 and X_2. For the second, note that $X_1 = RS^{2b} = RS^{a+b-c} = S^cRS^{-b}RS^{b-c} = S^c[R, S^b]S^{-c}$. Also $X_1^2 = RS^{2b}RS^{2b} = (RS^bR)^2S^{2b} = (S^{-a}RS^c)^2S^{2b} = S^{-a}[R, S^b]S^a$, since $a = b + c$. Thus $S^{-a-c}X_1S^{a+c} = X_1^2$. Since $X_2 = S^{-a}X_1S^a$, it follows as well that $S^{-a-c}X_2S^{a+c} = X_2^2$.

Now from above, $X_1^2 = S^{-c}S^{-a}X_1S^aS^c = S^{-c}X_2S^c$. Also, $X_2X_1^{-1} = S^{-a}RS^aR = S^{-a}S^cRS^{-b} = S^{-b}RS^{-b} = S^{-b}X_1S^b$, using $S^{4b} = 1$. Thus $X_2 = S^{-b}X_1S^bX_1$, concluding the proof of the lemma.

For the remainder of this section, a, b, c, d, e and g will be as in the proof of Theorem 2. We consider various cases.

Case (i). $p \equiv -1 \pmod 4$

As pointed out in the proof of part (ii) of Theorem 1, $H = \langle \alpha^d\rangle$ lies in an

extension of degree 2 of Z_p, so $|L| = p^2$. Thus $|G(d,p^n)| = |H||L| = p^2(p^n-1)/d$. Using the values of d and b found in Theorem 2, we have that $|E| = m^2$ and $|K^{a,b,-c}| = m^2p^2$.

Now if $h \equiv 1 \pmod 2$ then $b = 2h \equiv 2 \pmod 4$, so that $h(a+c) = b^2 + 4eb + 2gb^2 \equiv 2b \pmod{4b}$. Thus $S^{h(a+c)} = S^{2b}$ so that by Lemma 1, $X_i^{-1} = S^{-2b}X_iS^{2b} = S^{-h(a+c)}X_iS^{h(a+c)} = X_i^{2^h}$. Thus the order of X_i divides $2^h + 1 = -[(-2)^h - 1] = -mp = |m|p$. Hence, since $K^{a,b,-c}$ is abelian, generated by X_1 and X_2, and has order m^2p^2, we have that

$$K^{a,b,-c} = \langle X_1\rangle \times \langle X_2\rangle \cong C_{|m|p} \times C_{|m|p},$$

where for $N > 0$ an integer, C_N denotes the cyclic group of order N. Thus $E = \langle X_1^p\rangle \times \langle X_2^p\rangle \cong C_{|m|} \times C_{|m|}$.

Since e and h are relatively prime, we can choose a positive integer f so that $ef \equiv 1 \pmod h$. Then from $h = b/2$ we get $8ef \equiv 8 \pmod{4b}$. Now $a + c = 2b + 8e + 4gb$ so that $S^{a+c} = S^{2b+8e}$ whence from Lemma 2, for $i = 1$ and 2, $S^{8e}X_iS^{8e} = X_i^{\pm 2}$, so that

$$S^{-8}X_iS^8 = S^{-8ef}X_iS^{8ef} = X_i^{(\pm 2)^f}.$$

Further, $c = 4e + h + 4gh \equiv h \pmod 4$ and $a = b + c \equiv 3h \pmod 4$ from which we get that either $a \equiv \pm 1 \pmod 8$ or $c \equiv \pm 1 \pmod 8$. From this we can determine the action of S on X_i (by conjugation). For example, if $c \equiv 1 \pmod 8$, then by Lemma 2,

$$X_1^2 = S^{-c}X_2S^c = S^{-1}S^{-8k}X_2S^{8k}S, \qquad \text{where } k = (c-1)/8,$$

so that $X_1^2 = S^{-1}X_2^{(-2)^{fk}}S$. Thus $SX_1^2S^{-1} = X_1^{(-2)^{fk}}$ from which we can get $SX_1S^{-1} = X_2^{-(-2)^{fk}-1}$, since $|X_1| = |X_2|$ is odd. If $a \equiv 1 \pmod 8$ then using $X_2 = S^{-a}X_1S^a$ we get $SX_2S^{-1} = X_1^{(-2)^{fk}}$ where here $k = (a-1)/8$. We get similar results when $c \equiv -1 \pmod 8$ or $a \equiv -1 \pmod 8$. This completes the analysis for $h \equiv 1 \pmod 2$.

If $h \equiv 2 \pmod 4$, then $b = h \equiv 2 \pmod 4$, so that $(a+c)h/2 = b^2 + 2eb + 2gb^2 \equiv 0 \pmod{4b}$ since here e is odd. Thus by Lemma 1,

$$X_i = S^{-(a+c)h/2}X_iS^{(a+c)h/2} = X_i^{2^{h/2}}.$$

Hence the order of X_i divides $2^{h/2} - 1 = -[(-2)^{h/2} + 1] = -mp = |m|p$, so that again we have $K^{a,b,-c} = \langle X_1\rangle \times \langle X_2\rangle$ and $E = \langle X_1^p\rangle \times \langle X_2^p\rangle \cong C_{|m|} \times C_{|m|}$, as before.

Choosing f as before, we now have that $4ef \equiv 4 \pmod{4b}$, so that from $a + c = 2b + 4e + 4gb$ we have $S^{-4}X_iS^4 = X_i^{(-2)^f}$, for $i = 1, 2$. In this case $a \equiv 1 \pmod 4$ so that, using $X_2 = S^{-a}X_1S^a$, we get $SX_2S^{-1} = X_1^{(-2)^{fk}}$ where now $k = (a-1)/4$. This completes Case (i).

Case (ii). $p \equiv 1 \pmod 4$

As pointed out in the proof of part (ii) of Theorem 1, $H = \langle \alpha^d \rangle$ lies in Z_p, so $|L| = p$. Thus $|G(d, p^n)| = p(p^n - 1)/d$. Using the values of d and b found in Theorem 2, we now have that

$$|E| = \begin{cases} m^2 p, & \text{if } b \equiv 2 \pmod 4, \\ m, & \text{otherwise.} \end{cases}$$

Also

$$|K^{a,b,-c}| = \begin{cases} m^2 p^2, & \text{if } b \equiv 2 \pmod 4, \\ mp, & \text{otherwise.} \end{cases}$$

Now $b \equiv 2 \pmod 4$ precisely when $h \equiv 1 \pmod 2$ or $h \equiv 2 \pmod 4$, so that, as in Case (i), we obtain $K^{a,b,-c} = \langle X_1 \rangle \times \langle X_2 \rangle$. Also, the action of S by conjugation on X_1 and X_2 is as found in Case (i). However E is different, as we shall now see.

Since $p \equiv 1 \pmod 4$, we have observed in Theorem 1(ii) that $\alpha^{ad} = \alpha^{a'}$ is in Z_p. So choose an integer t, $1 \leqq t < p$, so that $\alpha^{ad} \equiv t \pmod p$. Under the homomorphism of Theorem 1(i), X_1 gets mapped to $x \mapsto x - (1 - \alpha^d)^{-1}$ and X_2 gets mapped to $x \mapsto x - \alpha^{ad}(1 - \alpha^d)^{-1}$ in $G(d, p^n)$. Thus $X_1^{-t}X_2$ gets mapped to the identity in $G(d, p^n)$, whence $X_1^{-t}X_2$ is in E and has order $|m|p$. Thus

$$E = \langle X_1^p \rangle \times \langle X_1^{-t}X_2 \rangle \cong C_{|m|} \times C_{|m|p}.$$

This completes the analysis of E when $h \equiv 1 \pmod 2$ or $h \equiv 2 \pmod 4$ (i.e. $b \equiv 2 \pmod 4$).

Suppose b is odd, so that $h = 4b \equiv 4 \pmod 8$. Then again choose a positive integer f so that $ef \equiv 1 \pmod h$. Now $a + c = 2b + e + 4gb$, so that $S^{a+c} = S^{2b+e}$, whence by Lemma 2, for $i = 1$ and 2, $S^{-e}X_iS^e = X_i^{-2}$, so that $S^{-1}X_iS = X_i^{(-2)^f}$. Now, again by Lemma 2, $X_2 = S^{-b}X_1S^bX_1$, so that $X_2 = X_1^{(-2)^{fb}+1}$. Since f is odd, and since $|X_1|$ divides mp, which divides $(-2)^{h/2} + 1$, we have $X_2 = X_1^{1 \pm 2^{h/4}}$, where the sign in the exponent is chosen according as $f \equiv -1 \pmod 4$ or $f \equiv +1 \pmod 4$, respectively. Thus X_2 is in $\langle X_1 \rangle$ and hence $K^{a,b,-c} = \langle X_1 \rangle \cong C_{mp}$ and $E = \langle X_1^p \rangle \cong C_m$.

Finally, suppose $b \equiv 0 \pmod 4$, so that $h = 2b \equiv 0 \pmod 8$. Again choose f as before, so that $2ef \equiv 2 \pmod{4b}$. Now $a + c = 2b + 2e + 4gb$ so that we now have $S^{-2}X_iS^2 = X_i^{(-2)^f}$, for $i = 1, 2$. By Lemma 2, $X_2 = S^{-b}X_1S^bX_1$, whence

$$X_2 = X_1^{1+2^{fh/4}} = X_1^{1 \pm 2^{h/4}},$$

since $|X_1|$ divides $mp = 2^{h/2} + 1$, where the sign in the exponent is chosen

according as $f \equiv \pm 1 \pmod 4$. In any event, X_2 is in $\langle X_1 \rangle$ and hence $K^{a,b,-c} = \langle X_1 \rangle \cong C_{mp}$ and $E = \langle X_1^p \rangle \cong C_m$. This completes Case (ii) and the analysis of the kernel.

Acknowledgement

The author wishes to thank the referee for suggesting he include the material of Section 3 of this paper.

References

1. C. M. Campbell, H. S. M. Coxeter and E. F. Robertson, *Some families of finite groups having two generators and two relations*, Proc. Soc. London, A **357** (1977), 423–438.

2. H. S. M. Coxeter and R. W. Frucht, *A new trivalent symmetrical graph with* 110 *vertices*, Ann. N.Y. Acad. Sci. **319** (1979), 141–152.

3. H. S. M. Coxeter, R. W. Frucht and D. L. Powers, *Zero-Symmetric Graphs*, Academic Press, New York, 1981.

4. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea Publishing Co., New York, 1971.