# On automorphisms of a group of prime exponent

Gunnar Traustason
Department of mathematical sciences
University of Bath
Bath BA2 7AY, England
email:masgt@maths.bath.ac.uk

March 1, 2011

The work in this article was motivated by a question about Fibonacci sequences in groups. Let $a, b$ be arbitrary elements of a group $G$. We define a Fibonacci sequence in $G$ as for the integers. Let $x_0 = a, x_1 = b$ and $x_{n+1} = x_{n-1}x_n$. In [3], Wall investigated the length of the fundamental period of the Fibonacci sequence in a finite cyclic group. Aydin and Smith [1] looked more generally at finite nilpotent groups. The study quickly reduces to finite p-groups. Denote by $k(G)$, the length of the fundamental period of the Fibonacci sequence in $G$. Aydin and Smith proved the following theorem that generalises a result that Wall obtained in the cyclic case.

**Theorem (Aydin, Smith [1])** *If $G$ is a finite p-group, then $k(G)$ divides $k(\mathbb{Z}/p\mathbb{Z})p^{c-1}$ where $c$ denotes the p-class of $G$.*

Although this result seems to be optimal for the general case, the behaviour of the Fibonacci sequence turns out to depend on the group. Aydin and Smith for example observed that $k(R(2,5)) = k(\mathbb{Z}/5Z) = 20$, where $R(2,5)$ is the largest finite 2-generator group of exponent 5. This looks quite mysterious when one compares with the theorem above. The theorem only tells us that $k(R(2,5))$ divides $20 \cdot 5^{11}$.

We will prove a quite general result about certain automorphisms on groups

of prime exponent that will clarify the above mystery. Let $G$ be a finite 2-generator group of exponent $p$, where $p$ is a prime number and let $\phi \in \mathrm{Aut}(G)$. Let $\tilde{\phi}$ be the induced vector space isomorphism on $G/[G,G]$. We ask ourselves the following question. How are the exponents of $\phi$ and $\tilde{\phi}$ related? Our main result is the following.

**Theorem** *Let $G$ be a finite 2-generator group of exponent $p$, for some prime number $p$ and let $\phi \in Aut(G)$. Let $\tilde{\phi}$ be the induced automorphism on $G/[G,G]$. Suppose*

*(a) The minimal polynomial of $\tilde{\phi}$ is of the form $(x-\lambda)^2$, where $\lambda$ has order $p-1$ in $\mathbb{Z}_p^*$.*
*(b) $G$ has class at most $r(p-1)$ where $r \geq 2$.*

*Then $\phi^{p^{r-1}(p-1)} = 1$.*

Note that the $p(p-1)$ is also the order of $\tilde{\phi}$. So letting $r = 2$, the theorem tells us that the order does not increase until the class goes beyond $2(p-1)$. The bound $2(p-1)$ is probably sharp. We will see that this is true when $p = 5$. We will see later that it follows from this theorem that $k(R(2,5))$ should be at most $100 = 20 \cdot 5$. We will also see that the reason why the length turns out to be 20 rather than 100 seems to be an accident and we construct an automorphism of $R(2,5)$ that reduces to the Fibonacci recurrence on the largest abelian quotient but has order 100.

We now begin the proof of the theorem. Let $G$ be a 2 generator group of exponent $p$, where $p$ is a prime, and let $\phi \in \mathrm{Aut}(G)$. Let $\tilde{\phi}$ be the induced automorphism on $G/[G,G]$. Suppose the minimal polynomial of $\tilde{\phi}$ is $(x-\lambda)^2$ where $\lambda$ has order $p-1$ in $\mathbb{Z}_p^*$. We can then choose the generators $u, v$ for $G$ such that

$$\phi(v) = v^\lambda u \quad \text{and} \quad \phi(u) = u^\lambda \tag{1}$$

modulo $[G,G]$. Let $H = \langle u \rangle^G$, the normal closure of $u$ in $G$. From (1) it is clear that $H$ is a $\phi$-invariant subgroup of $G$. We start with an elementary well known lemma.

**Lemma 1** $[u,_{p-1} v] \in [H,H]$.

**Proof** Since $G$ is of exponent $p$, we have (modulo $[H,H]$)

$$\begin{aligned} 1 &= (vu)^p \\ &= v^p u^{v^{p-1}+\cdots+v+1} \\ &= u[u,v^{p-1}]u[u,v^{p-2}]\cdots u[u,v]\cdot u \\ &= u^p[u,v]^{\binom{p}{2}}[u,_2\, v]^{\binom{p}{3}}\cdots[u,_{p-2}\, v]^{\binom{p}{p-1}}[u,_{p-1}\, v] \\ &= [u,_{p-1}\, v] \quad \square \end{aligned}$$

It follows that $H$ is generated modulo $[H,H]$ by $u, [u,v], [u,_2\, v], \ldots [u,_{p-2}\, v]$. By (1), the induced linear map on $H/[H,H]$ has a lower triangular matrix (with respect to these generators) of the form

$$A = \begin{pmatrix} \lambda & & & & & \\ * & \lambda^2 & & & & \\ \cdot & * & \cdot & & & \\ \cdot & \cdot & * & \cdot & & \\ \cdot & \cdot & \cdot & * & \cdot & \\ \cdot & \cdot & \cdot & \cdot & * & \lambda^{p-1} \end{pmatrix}$$

Since the eigenvalues are distinct, the matrix is diagonalisable and thus $A^{p-1} = I$. In other words $[H, \langle\phi^{p-1}\rangle] \leq [H,H]$. The first identity in (1) also gives $[G, \langle\phi^{p-1}\rangle] \leq H$. By an induction using the three subgroups lemma, it follows that

$$[\gamma_i(H), \langle\phi^{p-1}\rangle] \leq \gamma_{i+1}(H)$$

for all integers $i \geq 0$. Let $F$ be the free group of rank two generated by $x$ and $y$. Using standard techniques involving Hall's commutator collection process (see for example [2], chapter 3) one can see that

$$[x,y^p] = [x,y]^p c_2^{\binom{p}{2}} \cdots c_{p-1}^{\binom{p}{p-1}} c_p$$

where $c_i \in \gamma_i(y^F)$. Let $g \in G$. Since $G$ is of exponent $p$ it follows that $[g, \phi^{p-1}]$ is a product of commutators in $g$ and $\phi^{p-1}$ with at least $p$ occurrences of $\phi^{p-1}$. Repeated application of the inclusion $[\gamma_i(H), \langle\phi^{p-1}\rangle] \leq \gamma_{i+1}(H) \leq \gamma_{i+2}(G)$, gives $[g, \phi^{p(p-1}] \in \gamma_{p+1}(G)$. Hence

$$[G, \phi^{p(p-1)}] \leq \gamma_{p+1}(G).$$

We have therefore proved the following.

**Proposition 2** *If $G$ has class at most $p$ then $\phi^{p(p-1)} = 1$.*

As a step towards larger nilpotency class, we introduce the notion of a $\lambda$-automorphism. We say that an automorphism $\psi$ on a finite $p$-group is a $\lambda$-automorphism if the generators can be chosen in such a way that $\psi(x) = x^\lambda$ for each generator $x$.

**Lemma 3** *Let $H$ be a 2-generator group of exponent $p$ and class $m \geq 2$. Let $\psi \in Aut(H)$ such that the induced homomorphism $\tilde{\psi}$ on $H/\gamma_m(H)$ is a $\lambda$-automorphism. Then*

*(a) $\psi^p$ is a $\lambda$-automorphism.*
*(b) If $m \not\equiv 1$ modulo $p-1$ then $\psi$ is a $\lambda$-automorphism.*

**Proof** Let $u_1, u_2$ be generators of $H$ such that $\tilde{\psi}(\bar{u}_i) = \bar{u}_i{}^\lambda$, where $\bar{u}_i = u_i\gamma_m(H)$. Then

$$\psi(u_i) = u_i^\lambda x_i$$

for some $x_i \in \gamma_m(G)$. Since $\psi([u_{i_1}, \ldots, u_{i_m}]) = [u_{i_1}^\lambda, \ldots, u_{i_m}^\lambda] = [u_{i_1}, \ldots, u_{i_m}]^{\lambda^m}$, we have that $\psi(u) = u^{\lambda^m}$ for all $u \in \gamma_m(G)$. If $x_1 = x_2 = 1$, then there is nothing to prove. So suppose $x_i \neq 1$. The restriction of $\psi$ of $\langle u_i, x\rangle$ has matrix

$$\begin{pmatrix} \lambda & 0 \\ 1 & \lambda^m \end{pmatrix}$$

with respect to $u_i, x_i$. If $m \not\equiv 1$ modulo $p-1$, then $\lambda^m \neq \lambda$ and the matrix is diagonalisable. This means that we can choose $l$ such that $\psi(u_i x_i^l) = (u_i x^l)^\lambda$. This shows that $\psi$ is a $\lambda$-automorphism when $m \not\equiv 1$ modulo $p-1$. If $m \equiv 1$ modulo $p-1$, then the $p$th power of the matrix is $\lambda I$ and therefore $\psi^p(u_i) = u_i^\lambda$. □

We can now easily finish the proof of the theorem.

**Lemma 4** *The induced automorphism $\bar{\phi}$ on $G/\gamma_{p+1}(G)$ has the property that $\bar{\phi}^p$ is a $\lambda$-automorphism.*

**Proof** By (1), $\phi^p$ is a $\lambda$-automorphism modulo $[G, G]$. Applying Lemma 3 repeatedly, we see that $\phi^p$ is a $\lambda$-automorphism modulo $\gamma_p(G)$. This implies that there are generators $u_1, u_2$ for $G$ such that

$$\bar{\phi}^p(\bar{u}_i) = \bar{u}_i{}^\lambda x_i$$

for some $x_i \in \gamma_p(G)$. We want to show that $x_i$ must then be 1. If this were not the case then the matrix for the restriction of $\bar{\phi}^p$ on $\langle \bar{u}_i, x_i \rangle$ would be

$$\begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}$$

with respect to $\bar{u}_i, x_i$. But from Proposition 2 we know that $\bar{\phi}^{p(p-1)} = 1$. This contradicts the fact that the matrix above does not have order dividing $p-1$. Hence we must have that $x_1 = x_2 = 1$ and $\bar{\phi}^p$ is a $\lambda$-automorphism. □

**Proof of the theorem** By Lemma 4, $\phi^p$ is a $\lambda$-automorphism modulo $\gamma_{p+1}(G)$. By Lemma 3, the order of $\phi$ can only increase by factor of $p$ when the class reaches some $m \equiv 1$ modulo $p-1$. Hence $\phi^{p^{r-1}(p-1)} = 1$. □

Let us now return to the Fibonacci sequence in groups of exponent 5. The length of the sequence is the order of the automorphism $\phi$ on $R(2,5) = \langle x, y \rangle$ given by

$$\phi(x) = y, \quad \phi(y) = xy.$$

One easily calculates that the induced vector space automorphism $\tilde{\phi}$ on $R/[R,R]$ has minimal polynomial $(x-3)^2$. Also, 3 has order 4 in $\mathbb{Z}_5$. It is well known that $R$ has class $12 = 3(5-1)$. Our theorem thus tells us that the order of $\phi$ divides $5^2(5-1) = 100$. If we replace $\phi$ by the automorphism $\psi$ given by

$$\psi(x) = y[y,x,y,y,x,y,x,y,y], \quad \psi(y) = xy$$

then one can see that $\psi$ has order 100. This is also true modulo $\gamma_{10}(R)$. Now $\tilde{\psi} = \tilde{\phi}$ so this tells us that $2(5-1) = 8$ is the best upper bound for the class in the main theorem when $p = 5$.

*Acknowledgement* The Author is most grateful to Dr Geoff Smith for having stimulated the research carried out in this paper.

# References

[1] H. Aydin and G. C. Smith. Finite $p$-quotients of some cyclically presented groups. *J. London Math. Soc. (2)* **49** (1994), 83-92.

[2] B. Huppert. *Endliche Gruppen I* (Springer-Verlag, Berlin, 1967).

[3] D. D. Wall. Fibonacci series modulo $m$. *Amer. Math. Monthly* **67** (1960), 525-532.