Rend. Sem. Mat. Univ. Padova, Vol. 136 (2016), 61–68
DOI 10.4171/RSMUP/136-6

Automorphisms of finite order of nilpotent groups IV

B. A. F. Wehrfritz (∗)

Abstract – Let ϕ be an automorphism of finite order of the nilpotent group G of class c and m and r positive integers with $\phi^m = 1$. Consider the two (not usually homomorphic) maps ψ and γ of G given by

$$\psi\colon g \longmapsto g \cdot g\phi \cdot g\phi^2 \cdot \ldots \cdot g\phi^{m-1} \quad \text{and} \quad \gamma\colon g \longmapsto g^{-1} \cdot g\phi \quad \text{for } g \in G.$$

We prove that the subgroups

$$X = \langle x\alpha\colon x \in \ker\psi, \alpha \in \operatorname{Aut} G, x^r \in \textstyle\bigcup_{s\geq 0}(G\gamma)^s\rangle,$$

$$Y = \langle g\gamma\alpha\colon g \in G, \alpha \in \operatorname{Aut} G, (g\gamma)^r \in \ker\gamma\rangle,$$

$$X^* = \langle x^r\alpha\colon x \in \ker\psi, \in \alpha \in \operatorname{Aut} G, x^r \in \textstyle\bigcup_{s\geq 0}(G\psi)^s\rangle,$$

$$Y^* = \langle (g\gamma)^r\alpha\colon g \in G, \alpha \in \operatorname{Aut} G, (g\gamma)^r \in \ker\gamma\rangle = \langle ((G\gamma)^r \cap \ker\gamma) \operatorname{Aut} G\rangle$$

of G all have finite exponent bounded in terms of c, m and r only. This yields alternative proofs of the theorem of [4] and its related bounds.

Mathematics Subject Classification (2010). 20F18, 20F28, 20E36.

Keywords. Nilpotent group, automorphism of finite order.

Let ϕ be an automorphism of finite order of the group G and m a positive integer with $\phi^m = 1$. There are certain maps η (not usually homomorphisms) of G into itself that one frequently needs to consider (so in particular $G\eta$ and $\ker\eta = \{g \in G\colon g\eta = 1\}$ are not usually subgroups of G). There are just two maps η that interest us here, namely the maps

$$\psi\colon g \longmapsto g \cdot g\phi \cdot g\phi^2 \cdot \ldots \cdot g\phi^{m-1} \quad \text{and} \quad \gamma\colon g \longmapsto g^{-1} \cdot g\phi \quad \text{for } g \in G.$$

(∗) *Indirizzo dell'A.*: School of Mathematical Sciences, Queen Mary University of London, Mile End Road, London E1 4NS, England
E-mail: b.a.f.wehrfritz@qmul.ac.uk

In a series of papers we have discussed in some detail these two maps for nilpotent FAR groups. – Soluble FAR (short for "finite abelian ranks") groups are defined and discussed in the book [1]. An equivalent definition, more convenient for our purposes, is given by the following. A soluble group is an FAR group if and only if it has finite Hirsch number and satisfies min-q, the minimal condition on q-subgroups, for every prime q. A group has finite Hirsch number if it has a series of finite length whose factors are infinite cyclic or locally finite, the number of infinite cyclic factors in such a series being its Hirsch number.

Let G be a nilpotent FAR group. In [3] we proved that $G\psi \cdot \ker\psi$ and $G\gamma \cdot \ker\gamma$ are both very large subsets of G in that they contain characteristic subgroups of G of finite index. In [4] we proved that $\langle G\psi \cap \ker\psi\rangle$ and $\langle G\gamma \cap \ker\gamma\rangle$ are both very small; they are finite π-groups, where π is the set of prime divisors of m. Firstly our proofs in [3] require us to study $G\gamma \cdot (\ker\gamma)^m$ and not just $G\gamma \cdot \ker\gamma$. Secondly in [3] we have a version of the theorem that requires no rank restrictions. Specifically if G is just nilpotent of class c and if m, r and s are positive integers and if ϕ is an automorphism of G with $\phi^m = 1$, then there is a positive integer f such that

$$\langle G^f\rangle \subseteq (G\gamma)^r(\ker\gamma)^s \cap (\ker\psi)^r(\ker\gamma)^s \cap (\ker\psi)^r(G\psi)^s \cap (G\gamma)^r(G\psi)^s.$$

Moreover f can be chosen only to depend on c, m and the least common multiple of r and s and to be divisible only by primes dividing cmrs. (If S is a subset of some group and if n is a positive integer, then here S^n denotes the subset $\{s^n : s \in S\}$ and not the more usual $\langle s^n : s \in S\rangle$.) We did not consider this more general situation in [4], if only because the obvious analogue is false (example below). However a very slight weakening does hold and this is the main content of this current paper. Moreover it turns out still to be strong enough that the results of [4] can be recovered from it and thus it gives an alternative, and I feel a better, approach to those results. The following is the main theorem of this paper. (Note that whenever we have a group G, $m \geq 1$ and $\phi \in \operatorname{Aut} G$ with $\phi^m = 1$, the maps ψ and γ are always defined as above.)

Theorem. *Let G be a nilpotent group of class c, m and r positive integers and ϕ an automorphism of G with $\phi^m = 1$. With ψ and γ defined from ϕ and m as usual, set*

$$X = \langle x\alpha : x \in \ker\psi, \alpha \in \operatorname{Aut} G, x^r \in \textstyle\bigcup_{s\geq 0}(G\gamma)^s\rangle,$$

$$Y = \langle g\gamma\alpha : g \in G, \alpha \in \operatorname{Aut} G, (g\gamma)^r \in \ker\gamma\rangle,$$

$$X^* = \langle x^r\alpha \colon x \in \ker\psi, \in \alpha \in \operatorname{Aut} G, x^r \in \textstyle\bigcup_{s\geq 0}(G\psi)^s\rangle,$$
$$Y^* = \langle (g\gamma)^r\alpha \colon g \in G, \alpha \in \operatorname{Aut} G, (g\gamma)^r \in \ker\gamma\rangle = \langle ((G\gamma)^r \cap \ker\gamma) \operatorname{Aut} G\rangle$$

Then X and Y have exponents dividing $(mr)^c$ and X^* and Y^* have exponents dividing $m(mr)^{c-1}$ (meaning 1 *if $G = \langle 1\rangle$).*

Trivially $\bigcup_{s\geq 0}(\ker\gamma)^s = \ker\gamma$. The point of this theorem is that $\langle(\ker\psi)^r \cap (G\psi)^s\rangle \subseteq X^*$ and $\langle(G\gamma)^r \cap (\ker\gamma)^s\rangle \subseteq Y^*$. Further below we will see that if G is abelian, then $\exp X$ (= the exponent of X) and $\exp Y$ divide m, if $m = 2$, then $\exp X^*$ and $\exp Y^*$ divide 2^c, if X is abelian, then $\exp X^*$ divides m^c and $\exp X$ divides $m^c r$, and if Y is abelian then $\exp Y^*$ divides m and $\exp Y$ divides mr.

With the hypotheses of the theorem above, assume that π is a finite set of primes such that G satisfies min-q for all primes q in π and that m and r are π-numbers (meaning that all the prime divisors of mr lie in π). Then $T = O_\pi(G)$ is a Chernikov group. Let A denote the finite residual of T, d the rank of A, t the order of T/A and e the exponent of T/A. Let k be minimal such that $[A, {}_kG] = \langle 1\rangle$ (note that $k \leq c$ and $k \leq d$).

Corollary. *The groups X and Y have exponents dividing $(mr)^k te$ and orders dividing $(mr)^{dk} t^{d+1}$, the group X^* has exponent dividing $m^k te$ and order dividing $m^{dk} t^{d+1}$ and the group Y^* has exponent dividing mte and order dividing $m^d t^{d+1}$.*

The proofs

Our notation below is accumulative and reflects the notation of the theorem and its corollary.

a) *Let N be a normal subgroup of a group M such that $N^m \subseteq [N, M]$ for some positive integer m. Then $[N, {}_{i-1}M]^m \subseteq [N, {}_iM]$ for all $i \geq 1$. In particular if M is nilpotent of class c, then N has finite exponent* $\exp(N)$ *dividing m^c.*

Proof. If $g \in M$, then $x[N, M] \mapsto [x, g][N, {}_2M]$ is a homomorphism of $N/[N, M]$ into $[N, M]/[N, {}_2M]$. In particular $[x, g]^m \in [x^m, g][N, {}_2M] = [N, {}_2M]$ for all $x \in N$ and $g \in M$. Therefore $[N, M]^m \subseteq [N, {}_2M]$. A simple induction completes the proof. □

b) *Let G be a nilpotent group of class c, m and r positive integers and ϕ an automorphism of G with $\phi^m = 1$. Set*

$$X = \langle x\alpha : x \in \ker\psi, \alpha \in \operatorname{Aut} G, x^r \in \textstyle\bigcup_{s\geq 0}(G\psi)^s\rangle$$

and

$$Y = \langle g\gamma\alpha : g \in G, \alpha \in \operatorname{Aut} G, (g\gamma)^r \in \ker\gamma\rangle.$$

Then X and Y have finite exponents dividing $(mr)^c$.

Proof. Let $x \in \ker\psi$, $g \in G$ and $s \geq 1$ with $x^r = (g\psi)^s$. Of course $X/[X,G]$ is abelian and ψ induces an endomorphism on it. Thus $1 = (x\psi)^r \in (x^r\psi)[X,G]$. Also for $i \geq 1$, if $g(i) = g \cdot g\phi \cdot g\phi^2 \cdot \ldots \cdot g\phi^{i-1}$, then

$$x^r\phi^i = ((g\psi)^s)\phi^i = (g\psi\phi^i)^s = ((g\psi)^{g(i)})^s = ((g\psi)^s)^{g(i)} = (x^r)^{g(i)}.$$

Thus $x^r\psi = x^r \cdot (x^r)^{g(1)} \cdot \ldots \cdot (x^r)^{g(m-1)} \in x^{mr}[X,G]$. Hence $x^{mr} \in [X,G]$, so each $(x\alpha)^{mr} \in [X,G]$ and therefore $X^{mr} \subseteq [X,G]$. Consequently a) yields that X has exponent dividing $(mr)^l$, where l is minimal such that $[X,{}_lG] = \langle 1\rangle$ and in particular that $\exp X$ divides $(mr)^c$.

Now let $g \in G$ with $(g\gamma)^r \in \ker\gamma = C_G(\phi)$. Then $((g\gamma)^r)\psi = (g\gamma)^{mr}$. Also $Y/[Y,G]$ is abelian, so modulo $[Y,G]$ we have $(g\gamma)^r\psi \equiv (g\gamma\psi)^r = 1$. Thus $(g\gamma)^{mr} \in [Y,G]$, $(g\gamma\alpha)^{mr} = ((g\gamma)^{mr})\alpha \in [Y,G]$ and $Y^{mr} \subseteq [Y,G]$. Consequently the exponent of Y divides $(mr)^{l'}$ and hence also $(mr)^c$, where l' is minimal with $[Y,{}_{l'}G] = \langle 1\rangle$. □

c) *Continuing with the notation of* b), *set*

$$X^* = \langle x^r\alpha : x \in \ker\psi, \alpha \in \operatorname{Aut} G, x^r \in \textstyle\bigcup_{s\geq 0}(G\psi)^s\rangle$$

and

$$Y^* = \langle (g\gamma)^r\alpha : g \in G, \alpha \in \operatorname{Aut} G, (g\gamma)^r \in \ker\gamma\rangle.$$

Then X^* has exponent dividing $m(mr)^{l-1}$ (1 if $X = \langle 1\rangle$) and $m(mr)^{c-1}$ (1 if $G = \langle 1\rangle$). Also Y^* has exponent dividing $m(mr)^{l'-1}$ (1 if $Y = \langle 1\rangle$) and $m(mr)^{c-1}$ (1 if $G = \langle 1\rangle$).

Proof. Assume $X \neq \langle 1\rangle$. Now a) and the proof of b) yields that $[X,G]$ has exponent dividing $(mr)^{l-1}$ and also that $x^{mr} \in [X,G]$ for all x as in the definition of X^*. It follows that $(X^*)^m \subseteq [X,G]$. Therefore the exponent of X^* divides $m(mr)^{l-1}$. The proof for Y^* is similar. □

d) Corollary. *If G is abelian, then the exponents of X^* and Y^* divide m.*

e) *If $m = 2$, then the exponents of X^* and Y^* divide 2^c.*

Proof. Let $x \in \ker\psi$. Then $x{\cdot}x\phi = 1, x\phi = x^{-1}, x^r\phi = x^{-r}$ and $x^r \in \ker\psi$. Thus

$$X^* \leq \langle x\alpha : x \in \ker\psi, \alpha \in \operatorname{Aut} G, x \in \textstyle\bigcup_{s\geq 0}(G\psi)^s\rangle$$

and the latter has exponent dividing $m^c = 2^c$ by b).

If $g \in G$, then $g\gamma\phi = g^{-1}\phi \cdot g\phi^2 = g^{-1}\phi \cdot g = (g\gamma)^{-1}$. Hence $(g\gamma)^r\phi = (g\gamma)^{-r}$. If also $(g\gamma)^r \in \ker\gamma$, then $(g\gamma)^r\phi = (g\gamma)^r, (g\gamma)^{-r} = (g\gamma)^r$ and $(g\gamma)^{2r} = 1$. Consequently Y^* is generated by involutions and therefore Y^* has exponent dividing $2l'$ and hence also 2^c. □

f) *If X is abelian then $(X^*)^m \subseteq [X^*, G]$,* $\exp X^*$ *divides m^c and* $\exp X$ *divides $m^c r$. Also if Y is abelian, then $(Y^*)^m = \langle 1\rangle$ and* $\exp Y$ *divides mr.*

Proof. Let $x \in \ker\psi$, $g \in G$ and $s \geq 0$ with $x^r = (g\psi)^s$. Since X is abelian ψ induces an endomorphism on X. Thus $x^r\psi = (x\psi)^r = 1$. Also, as in the proof of b) we have that

$$x^r\psi = x^r \cdot (x^r)^{g(1)} \cdot \ldots \cdot (x^r)^{g(m-1)} \in x^{mr}[X^*, G].$$

Therefore $x^{mr} \in [X^*, G]$. It follows easily that $(X^*)^m \subseteq [X^*, G]$. Now apply a).

Now let $g \in G$ with $(g\gamma)^r \in \ker\gamma$. Since Y is abelian, so $\psi|_Y$ is an endomorphism of Y and $(g\gamma)^r\psi = (g\gamma\psi)^r = 1$. Also $(g\gamma)^r \in C_G(\phi)$, so $(g\gamma)^r\psi = (g\gamma)^{mr}$. It follows that $(g\gamma)^{mr} = 1$ and that $(Y^*)^m = \langle 1\rangle$. The conclusions for X and Y are now immediate. □

Again continuing with the notation of b) let π denote the (finite) set of prime divisors of mr. Suppose G satisfies min-q for each q in π. Then $T = O_\pi(G)$ is a Chernikov group. Let A denote the finite residual of T, d the rank of A, t the order of T/A and e the exponent of T/A. Let k be minimal such that $[A, {}_kG] = \langle 1\rangle$. Then $k \leq c$ and also (by [4], Lemma 4) $k \leq d$. By b) both X and Y are contained in T. Then with this notation and hypotheses we have the following.

g) *The groups X and Y have exponents dividing $(mr)^k te$ and $(mr)^d te$ resp. and orders dividing $(mr)^{dk}t^{d+1}$. The group X^* has exponent dividing $m^k te$ and order dividing $m^{dk}t^{d+1}$. The group Y^* has exponent dividing mte and order dividing $m^d t^{d+1}$.*

These bounds depend only on m and the structure constants of $O_\pi(G)$ and not for example on the class c of G.

Proof. Suppose $T = A$. Since $X \subseteq A$ by b), we have $l \leq k$. The proof of b) yields that $\exp X$ divides $(mr)^k$. In general there is a characteristic subgroup K of G with $KA = T$, with $\exp K$ dividing te and with $|K|$ dividing t^{d+1}, see [4], Lemma 2. Applying the '$T = A$' case to G/K yields that in general $\exp X$ divides $(mr)^k te$ and $|X|$ divides $(mr)^{dk} t^{d+1}$. The proof for Y is similar.

For X^* and Y^* apply f) and a) to G/K. Then X^*K/K has exponent dividing m^k and Y^*K/K has exponent dividing m. The remaining claims of g) follow from the properties of K. □

The theorem of [4] and the various bounds computed in connection with it (in [4] see the introduction, the proof of the theorem and the remarks following that proof) all follow from the above. Further the above applied to the ϕ-invariant finitely generated subgroups of the group under consideration yields the following generalization and strengthening of Lemma 3 of [4].

h) *Let G be a locally nilpotent group, m a positive integer and ϕ an automorphism of G with $\phi^m = 1$. With ψ and γ defined from ϕ and m in the usual way, then the subgroups*

$$\langle x \colon x \in \ker\psi \text{ and } x^r \in \textstyle\bigcup_{s \geq 0} (G\psi)^s \text{ for some } r \geq 1 \rangle$$

and

$$\langle g\gamma \colon g \in G \text{ and } (g\gamma)^r \in \ker\gamma \text{ for some } r \geq 1 \rangle$$

are periodic. Further if $x \in \ker\psi$ and $g \in G$ are such that $x^r = (g\psi)^s$ for some positive integers r and s, then x has order dividing some power of mr and if $m = 2$, then x^r is a 2-element. If $g \in G$ with $(g\gamma)^r \in \ker\gamma$ for some positive integer r, then $g\gamma$ also has order dividing some power of mr and if $m = 2$, then also $(g\gamma)^r$ is a 2-element.

Examples. In general $(\ker\psi)^r \cap G\psi$ need not have exponent dividing some power of m and nor need $(G_\gamma)^r \cap \ker\gamma$, even if the group G is finite and even though they do have exponents dividing some power of mr and their exponents do divide some power of m if $m = 2$ or if G is abelian. Of course $\ker\psi \cap G\psi$ and $G\gamma \cap \ker\gamma$ do have exponents dividing some power of m.

Proof. The smallest examples will have to have class at least 2 and m at least 3. Let $D = \langle a, b \rangle$ be dihedral of order 8, where $a^b = a^{-1}$. Let $x \mapsto x_i$ be an isomorphism of D onto D_i for $i = 1, 2, 3$ and let P be the central product of D_1, D_2 and D_3 where the a_i^2 are amalgamated to z, $\langle z \rangle$ being the centre of P.

Let $\phi \in \operatorname{Aut} P$ permute the D_i cyclically; specifically let $x_i\phi = x_{i+1}$ for each $x \in D$ and each i, where $x_4 = x_1$. Trivially ϕ has order 3, so set $m = 3$. Consider $x = b_1 a_2 b_3 a_3^{-1}$. Simple calculations show that $x\psi = 1$, $x^2 = z$ and $z\psi = z \neq 1$. Thus $x^2 \in (\ker\psi)^2 \cap P\psi$ and x^2 has order 2, so $(\ker\psi)^2 \cap P\psi$ cannot have exponent dividing a power of $m = 3$.

Let $Q = \langle i, j\rangle$ be the quaternion group of order 8 in its usual representation in the real quaternion algebra. Then Q has an automorphism ϕ of of order 3 given by $i\phi = j$, $j\phi = ij$ (and $(ij)\phi = i$ and $(-1)\phi = -1$). Set $m = 3$. Then $i\gamma = -ij$, $(i\gamma)^2 = -1$ and $(-1)\gamma = 1$. Thus $-1 \in (Q\gamma)^2 \cap \ker\gamma$, so the exponent of $(Q\gamma)^2 \cap \ker\gamma$ does not divide any power of $m = 3$. □

Remarks. Obviously in the example P above $\ker\psi$ is not a union of subgroups, although G is a 2-group and even although quite generally $\ker\psi$ always is a union of subgroups if $m = 2$ (since if $m = 2$ then $\ker\psi = \{g \in G : g\phi = g^{-1}\}$). This is not just because $3 = m$ and the exponent 4 of G are coprime.

Let G be the wreath product of a cyclic group of order 9 and a cyclic group of order 3. Specifically let $G = \langle a_1, a_2, a_3, b\rangle$, where the a_i commute and have order 9, b has order 3 and conjugation by b permutes the a_i cyclically. Let ϕ denote conjugation by b, so ϕ has order 3, and set $m = 3$. Then $\ker\psi$ is not a union of subgroups. For let $x = b^2 a_1^{-1} a_2$. Then simple calculations show that $x\psi = 1$, $x^2 = b a_2 a_3^{-1}$ and $(x^2)\psi = a_1^3 a_2^{-3} \neq 1$. Hence x^2 lies in $(\ker\psi)^2$, does not lie in $\ker\psi$ and x but not $\langle x\rangle$ is contained in $\ker\psi$.

Also $G\psi$ and $G\gamma$ need not be unions of subgroups. For consider a dihedral group $G = \langle a, b\rangle$, where $a^b = a^{-1}$. First suppose a has order 4. Now G has an automorphism ϕ of order 2 given by $a\phi = a^{-1}$ and $b\phi = ba$. Set $m = 2$. Then $\langle a\rangle\psi = \{1\}$ and $(ba^i)\psi = a^{1-2i}$, so $b\psi = a$ and $(b\psi)^2 = a^2 \notin G\psi$. Therefore $G\psi$ is not a union of subgroups.

Continue with $G = \langle a, b\rangle$ as above, but now assume that a has order 8. Let ϕ denote conjugation by a, so $|\phi| = 4$. Set $m = 4$. Then $\langle a\rangle\gamma = \{1\}$ and $(ba^i)\gamma = a^2$. Thus here $G\gamma = \{1, a^2\}$, which clearly cannot be a union of subgroups.

Now consider the quaternion group Q and its automorphism ϕ of order $3 = m$ as in the example above. Then ϕ permutes cyclically the three involutions of $Q/\langle -1\rangle$ and hence $-1 \notin (Q\backslash\langle -1\rangle)\gamma$. Also $\langle -1\rangle\gamma = \{1\}$. Thus $-1 \notin Q\gamma$, so clearly $Q\gamma$ is not a union of subgroups. So far for $G\gamma$ we have not considered the case where $m = 2$. In this case quite generally $G\gamma$ is always a union of subgroups. This follows at once from the following formulae.

If n is a positive integer, G is any group and ϕ is an automorphism of G with $\phi^2 = 1$, then for each $g \in G$ the following hold:

$$(g\gamma)^{2n+1} = (g(g\phi\gamma)^n)\gamma, \quad (g\gamma)^{2n} = ((g\phi\gamma)^n)\gamma, \quad (g\gamma)^{-1} = g\phi\gamma.$$

The third formula here is the case $n = 1$ of the following more general result:

$$g\phi\gamma^n = (g\gamma)^h \quad \text{for } h = (-1)^n 2^{n-1}.$$

References

[1] J. C. Lennox – D. J. S. Robinson, *The theory of infinite soluble groups,* Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, Oxford, 2004.

[2] B. A. F. Wehrfritz, *Automorphisms of finite order of nilpotent groups,* Ric. Mat. **63** (2014), no. 2, pp. 261–272.

[3] B. A. F. Wehrfritz, *Automorphisms of finite order of nilpotent groups* II, Studia Sci. Math. Hungar. **51** (2014), no. 4, pp. 547–555.

[4] B. A. F. Wehrfritz, *Automorphisms of finite order of nilpotent groups* III, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM **109** (2015), no. 2, pp. 295–301.

Manoscritto pervenuto in redazione il 30 luglio 2014.