CONFORMALITY AND p-ISOMORPHISM IN FINITE NILPOTENT GROUPS

C. D. H. COOPER

(Received 16 December 1964, revised 8 August 1965)

1. Introduction

This paper discusses the relationship between two equivalence relations on the class of finite nilpotent groups. Two finite groups are *conformal* if they have the same number of elements of all orders. (Notation: $G \approx H$.) This relation is discussed in [4] pp 107—109 where it is shown that conformality does not necessarily imply isomorphism, even if one of the groups is abelian. However, if both groups are abelian the position is much simpler. Finite conformal abelian groups are isomorphic.

The other equivalence relation to be discussed is that of p-isomorphism (for prime p). Two finite groups G, H are *p-isomorphic* if there is a 1—1 correspondence between them which preserves p-th powers. (Notation: $G \underset{p}{\sim} H$.)

Before stating the theorems proved in this paper we define a relation ρ on the set of primes by $p \rho q$ if and only if there is a positive integer u such that $q \mid p^u - 1$ and $q^2 \nmid p^u - 1$.

THEOREM A. *Suppose* $m = \prod_{i=1}^{r} q_i^{a_i}$ *where* $q_1, \cdots, q_r$ *are distinct primes and* $a_1, \cdots, a_r$ *are positive integers. A necessary and sufficient condition that all pairs of p-isomorphic nilpotent groups of order m are conformal is that for each i in $\{1, \cdots, r\}$ at least one of the following conditions holds*:

(1) $a_i = 1$

(2) $q_i^{a_i} = 4$ *and* $p \rho q_i$

(3) $q_i \neq 2$ *and* $p \rho q_i$

(4) $q_i = p$

THEOREM B. *Let G, H be two conformal groups at least one of which is nilpotent. If for some prime p the Sylow p-subgroups of G, H are regular, then G and H are p-isomorphic.*

These main theorems sum up fairly completely the conditions under which p-isomorphism and conformality imply each other for finite nilpotent groups. Two other theorems for p-groups which will be proved are:

THEOREM C. *A regular finite p-group is p-isomorphic with an abelian group.*

THEOREM D. *Lattice isomorphic finite p-groups are p-isomorphic.*

The author wishes to acknowledge the assistance of Professor G. E. Wall, Dr D. W. Barnes and the referee in the simplification and presentation of some of the proofs.

2. Conditions under which conformality implies p-isomorphism

We first prove a lemma proving that conformality and p-isomorphism of finite nilpotent groups are equivalent to the same relation between corresponding Sylow subgroups. For the proof of this lemma we need the notation $N_{p,d}(G)$ for the number of elements of order dividing p^d-1. Two groups G, H of the same order prime to p are p-isomorphic if and only if:

$$N_{p,d}(G) = N_{p,d}(H) \text{ for } d = 1, 2, \cdots$$

In this case, conformality implies p-isomorphism.

LEMMA 1. *Let G, H be finite nilpotent groups of the same order $m = \prod_{i=1}^{s} p_i^{a_i}$ and let G_i, H_i, be the Sylow p_i-subgroups of G, H respectively for all i in $\{1, \cdots, s\}$. Then*

$$G_i \approx H_i \text{ for all } i \text{ if and only if } G \approx H$$

and

$$G_i \underset{p}{\sim} H_i \text{ for all } i \text{ if and only if } G \underset{p}{\sim} H.$$

PROOF. The only result needing proof here is that $G \underset{p}{\sim} H$ implies $G_i \underset{p}{\sim} H_i$ for all i.

Case 1 : $p \mid m$

Suppose $p = p_j$.

Let $G' = \otimes_{i \neq j} G_i$ and $H' = \otimes_{i \neq j} H_i$

Then $G = G_j \otimes G'$ and $H = H_j \otimes H'$.

Suppose $G \underset{p}{\sim} H$ and let $f : G \to H$ be a p-isomorphism. Clearly f maps elements of G of order prime to p to elements of H or order prime to p, and elements of G of p-power order to elements of H of p-power order. Thus $f(G_j) = H_j$ and $F(G') = H'$, whence $G_j \underset{p}{\sim} H_j$ and $G' \underset{p}{\sim} H'$ under the p-isomorphisms $f \mid G_j$ and $f \mid G'$ respectively. We now apply Case 2 to the groups G', H'.

Case 2 : $p \nmid m$

Suppose $G \underset{p}{\sim} H$. This is equivalent to saying

$$N_{p,d}(G) = N_{p,d}(H) \text{ for } d = 1, 2, \cdots$$

Since the groups are nilpotent,

$$\prod_{i=1}^{s} N_{p,d}(G_i) = \prod_{i=1}^{s} N_{p,d}(H_i) \text{ for all } d. \tag{1}$$

From this we will deduce:

$$N_{p,d}(G_i) \equiv N_{p,d}(H_i) \text{ for all } i, d. \tag{2}$$

Let $p_1 > p_2 > \cdots$. It will suffice to prove (2) for $i = 1$. Now the largest power of p_j $(j > 1)$ to divide $p^d - 1$ is the largest power to divide $p^{dp_1 - 1}$. For if $p^d - 1 = p_j^r k$, $p \nmid k$ and $r > 0$ then

$$p^{dp_1} = 1 + p_1 p_j^r k \pmod{p_j^{r+1}}$$

and if $r = 0$ then

$$p^{dp_1} \not\equiv 1 \pmod{p_j}$$

otherwise $p_1 | p_j - 1$ which is impossible as $p_1 > p_j$.

Thus

$$N_{p,dp_1}(G_j) = N_{p,d}(G_j) \quad \text{for } j = 2, 3, \cdots, s.$$

Combining this with (1),

$$\frac{N_{p,dp_1}(G_1)}{N_{p,d}(G_1)} = \frac{N_{p,dp_1}(H_1)}{N_{p,d}(H_1)}.$$

Continuing this process we get:

$$\frac{N_{p,dp_1^r}(G_1)}{N_{p,dp_1^r}(H_1)} = \frac{N_{p,d}(G_1)}{N_{p,d}(H_1)} \quad \text{for all } r. \tag{3}$$

If $p^d - 1 \not\equiv 0 \pmod{p_1}$ then $N_{p,d}(G_1) = N_{p,d}(H_1) = 1$. If $p^d - 1 \equiv 0 \pmod{p_1}$ then for large enough r, the left hand side of (3) becomes $|G_1|/|H_1| = 1$. Thus

$$N_{p,d}(G_1) = N_{p,d}(H_1) \quad \text{for all } d. \tag{4}$$

Dividing (1) by (4) we have that

$$\prod_{i=2}^{s} N_{p,d}(G_i) = \prod_{i=2}^{s} N_{p,d}(H_i) \text{ for all } d$$

and continuing the process we deduce (2) which is equivalent to the statement: $G_i \underset{p}{\sim} H_i$, $i = 1, 2, \cdots, s$.

Proof of Theorem A. *Necessity*: To prove the necessity we suppose that for some i none of the conditions hold. Then $p \neq q_i$, $a_i \neq 1$ and either (i) $p \rho q_i$ is false or (ii) $q_i = 2$ and $a_i = 3$ or (iii) $q_i = 2$ and $a_i > 3$. In each case we exhibit two p-isomorphic, non conformal groups of order m. They

https://doi.org/10.1017/S1446788700005541 Published online by Cambridge University Press

are the direct products of the cyclic group of order $m/q_i^{a_i}$ with each of the following groups:

Case (*i*) The abelian groups of order $q_i^{a_i}$ and types $(q_i, q_i, \cdots, q_i)$ and $(q_i^2, q_i, \cdots, q_i)$.

Case (*ii*) The cyclic group of order 2^3 and the Quaternion group.

Case (*iii*) The abelian groups of order 2^{a_i} and types $(2^2, 2^2, 2, \cdots, 2)$ and $(2^3, 2, \cdots, 2)$.

Sufficiency: Suppose that $G \underset{p}{\sim} H$

Case I $r = 1$. Write $q = q_i$, $a = a_i$.

(i) If $a = 1$ the theorem is obvious.

(ii) If $q^a = 4$ and $q \rho p$, then for some u, $q | p^u - 1$ but $q^2 \nmid p^u - 1$. Elements of G of order 2 and the identity are fixed under the operation of raising to exponent p^u while elements of order 4 are not. This property carries over to H and hence $G \approx H$.

(iii) If $q \neq 2$ and $q \rho p$ then for some u, $q | p^u - 1$ but $q^2 \nmid p^u - 1$. This implies that $q^{i+1} | p^{uq^i} - 1$ but $q^{i+2} \nmid p^{uq^i} - 1$ for all positive integers i (see [3] p. 114).

But $N_{p, uq^i}(G) = N_{p, uq^i}(H)$ for all positive integers i and so G and H are conformal.

(iv) If $q = p$, then suppose that f is a p-isomorphism from G onto H. It follows that

$$x^{p^r} = 1 \Leftrightarrow f(x^{p^r}) = f(1) \Leftrightarrow [f(x)]^{p^r} = 1.$$

Case II $r > 1$.

By the lemma, $G \underset{p}{\sim} H$ implies $G_i \underset{p}{\sim} H_i$ for $i = 1, 2, \cdots,$. We may apply Case I to each of the corresponding pairs of Sylow subgroups and obtain $G_i \approx H_i$ for $1, 2, \cdots,$. Again by the lemma we have that $G \approx H$.

If $p = 2$ in Theorem A then condition (2) may be dropped as (2) $\Rightarrow$ (4). The conditions may be written as:

$$2 \rho p_i \text{ or } a_i = 1 \text{ for } i = 1, 2, \cdots, r.$$

Empirically it has been found that $2 \rho p$ for all primes p less than 100. Thus 2-isomorphism implies conformality for all nilpotent groups of order less than or equal to 10, 200. There are, however, 2-isomorphic non conformal finite nilpotent groups since $2 \rho 1093$ is false (see [2] p. 72—73).

3. Conditions under which p-isomorphism implies conformality

LEMMA 2. *Finite groups which are conformal with a nilpotent group are themselves nilpotent.*

https://doi.org/10.1017/S1446788700005541 Published online by Cambridge University Press

PROOF. Let G, H be conformal and suppose H is nilpotent. For any prime p dividing the common group order, G has the same number of elements of p-power order as H. Since H is nilpotent the number of elements of p-power order is equal to the order of the Sylow p-subgroups of G, H. Thus G contains only one Sylow p-subgroup for each prime dividing the group order and hence G is nilpotent (see [1] page 155).

PROOF OF THEOREM B. By the lemma we may assume that both G, H are nilpotent. Let the Sylow subgroups of G be $G_1, G_2, \cdots, G_n$ and of H be $H_1, H_2, \cdots, H_n$ where G_i, H_i are the Sylow p_i subgroups of G, H respectively. Moreover suppose that $p = p_1$. Since $G \approx H$ we have that $G_i \approx H_i$ for all $i = 1, 2, \cdots,$. If $i > 1$, G_i, H_i have order prime to p and hence $G_i \underset{p}{\sim} H_i$. We now prove that conformal regular p groups are p-isomorphic.

Let G, H be two conformal regular p groups.

Write

$$G^{p^r} = \{g \mid g = x^{p^r}, x \in G\}$$

and for $g \in G^p$ write

$$R_p(g) = \{x \mid x^p = g\}$$

and

$$R_p^*(g) = R_p(g) \cap (G - G^p),$$

with similar notation in H. Finally denote the number of elements of G (or of H) with order at most p^a by r_a.

Since G, H are regular they have the property P where M has the property P means that for each $r = 0, 1, 2, \cdots$, M^{p^r} is a subgroup of M such that every element has either no p-th roots in M^{p^r} or exactly as many p-th roots as there are elements of order p in M^{p^r}. (See [1] p. 186).

We prove that $G \underset{p}{\sim} H$ by induction on the group order. It is clearly true if the group order is 1. Suppose now that G, H have order greater than 1. Then G^p and H^p each have r_{a+1}/r_1 elements of order p^a. Thus $G^p \approx H^p$. Also G^p and H^p are subgroups of G, H (proper subgroups since $|G| = |H| > 1$) themselves having property P. By the induction hypothesis $G^p \underset{p}{\sim} H^p$. Let $\phi : G^p \to H^p$ be a p-isomorphism. Every element $g \in G^p$ has as many p-th roots in G^p as $\phi(g)$ in H^p. But g, $\phi(g)$ each have r_1 p-th roots in G, H respectively. Hence by subtraction,

$$|R_p^*(g)| = |R_p^*(\phi(g))| \text{ for all } g \in G^p.$$

We may now define in a number of ways a mapping $f : G \to H$ satisfying the conditions:

(a) $f \mid G^p = \phi$

(b) for each $g \in G^p$, f maps $R_p^*(g)$ 1—1 onto $R_p^*(\phi(g))$.

https://doi.org/10.1017/S1446788700005541 Published online by Cambridge University Press

It is clear that such a map is a p-isomorphism. Thus $G \underset{p}{\sim} H$. Applying this result to the Sylow p_1 subgroups of G, H we have that $G_1 \underset{p}{\sim} H_1$. But $G_i \underset{p}{\sim} H_i$ for $i = 2, 3, \cdots, n$. Thus by Lemma 1, $G \underset{p}{\sim} H$.

The assumption that the Sylow p-subgroups be regular can be weakened to the requirement that they each satisfy the condition P which is actually used in the proof of the theorem. There are in fact non regular p-groups which have this property. An example of such a p-group is the group of order 2^4 with generators a, b and defining relations $a^8 = b^2 = 1, bab^{-1} = a^5$.

4. p-isomorphisms in p-groups

Proof of Theorem C. We prove that a regular p-group G is conformal with an abelian group by induction on the group order. The p-isomorphism between the groups follows from Theorem B. If $|G| = 1$, G is clearly conformal with an abelian group viz. itself. Suppose now that $|G| > 1$ and that G^p is conformal with an abelian group, say with the group of type $(p^{e_1}, p^{e_2}, \cdots, p^{e_r})$. Since G is regular, G^p is a subgroup of G and $|G : G^p|$ is equal to the number of p-th roots of 1 in G. It follows that p^r, which is the number of p-th roots of 1 in G^p is less than or equal to $|G : G^p|$. Thus there exists an abelian group of order $|G|$ and of type $(p^{e_1+1}, p^{e_2+1}, \cdots, p^{e_r+1}, p, \cdots, p)$. This group will clearly be conformal with G.

As in Theorem B we do not require G to be regular. It is sufficient if G satisfies property P in Theorem B. We can however extend the first part of Theorem C (that G is conformal with an abelian group) to groups G such that for $r = 1, 2, \cdots, G^{p^r}$ is a subgroup of G such that the number of elements of G^{p^r} with order p is greater than or equal to the index of G^{p^r} in $G^{p^{r-1}}$.

Proof of Theorem D. Let G, H be finite lattice isomorphic p-groups. Let ϕ be an isomorphism of the lattice of subgroups of G onto the lattice of subgroups of H. Let $C_1 = (= \{1\}), C_2, \cdots, C_s$ be the cyclic subgroups of G arranged so that $|C_i| \leqq |C_{i-1}|$ for all i. We define a mapping $f : G \to H$ by the rules:

(i) $f(1) = 1$,

(ii) if $f | C_i$ has been defined for $i = 1, \cdots, k-1$, then $f | C_k$ is any isomorphism of C_k onto $\phi(C_k)$ which extends the already defined isomorphism $f | C_k^p$ onto $\phi(C_k^p) = \phi(C_k)^p$.

Then f is a well defined mapping such that $f | C$ maps C isomorphically onto $\phi(C)$ for every cyclic subgroup C of G. Clearly f is a p-isomorphism.

References

[1] Marshall Hall, *The theory of groups* (Macmillan, 1959).
[2] G. H. Hardy and E. M. Wright, *The theory of numbers* (Oxford, 1959).
[3] B. W. Jones, *The theory of numbers* (Constable, 1955).
[4] G. A. Miller, H. F. Blichfeldt and L. E. Dickson, *Theory and applications of finite groups* (Wiley, 1916).

Queen Mary College
London