Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Algebra 300 (2006) 10–15
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

An arithmetic theorem related to groups of bounded nilpotency class

Thomas W. Müller

School of Mathematical Sciences, Queen Mary & Westfield College, University of London, Mile End Road, E1 4NS London, United Kingdom

Received 7 June 2005

Available online 16 November 2005

Communicated by Eamonn O'Brien

Dedicated to Charles Leedham-Green on the occasion of his 65th birthday

Abstract

We characterize the set of positive integers m having the property that every group of order m is nilpotent of class at most c, where c is a fixed positive integer or infinity. This generalizes and relates results of Dickson and Pazderski. The special case where $c = 1$ (all groups of order m are abelian) is used to construct a substantial class of finite Schreier systems S in free groups such that S is not a right transversal for any normal subgroup.

1. Introduction and main result

Let $\mathbb{N}$ be the set of positive integers, and define a multiplicative function $\psi : \mathbb{N} \to \mathbb{N}$ via

$$\psi(1) = 1$$
$$\psi(p^\nu) = (p^\nu - 1)\big(p^{\nu-1} - 1\big)\cdots(p - 1) \quad (p \text{ prime},\ \nu \geqslant 1).$$

E-mail address: t.w.muller@qmul.ac.uk.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2005.10.013

Denote by (a, b) the greatest common divisor of integers a, b. The following result, which generalizes and relates theorems of Dickson and Pazderski, appears to have escaped notice.

Theorem 1. *Fix $c \in \mathbb{N} \cup \{\infty\}$, and let m be a positive integer. Then the following two assertions are equivalent*:

(a) *m satisfies $(m, \psi(m)) = 1$ and is $(c+2)$-power free.*
(b) *Every group of order m is nilpotent of class at most c.*

If $m > 1$, then condition (a) can be rephrased in terms of the prime decomposition $m = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$ of m as follows:

(i) $\nu_i \leqslant c + 1,\ 1 \leqslant i \leqslant r$,
(ii) $p_i \nmid (p_j^{\nu_j} - 1)(p_j^{\nu_j - 1} - 1) \cdots (p_j - 1),\ 1 \leqslant i, j \leqslant r.$

Corollary 1. (Dickson [4]) *An integer $m = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r} > 1$ satisfies $\nu_i \leqslant 2$ and $(p_i, p_j^{\nu_j} - 1) = 1$ for $1 \leqslant i \leqslant r$ and $1 \leqslant i, j \leqslant r$, respectively, if and only if every group of order m is abelian.*

This is the case $c = 1$ of Theorem 1, while setting $c = \infty$ gives the following.

Corollary 2. (Pazderski [11]) *A positive integer m satisfies $(m, \psi(m)) = 1$ if and only if every group of order m is nilpotent.*

Corollary 1 was first established in [4] in connection with certain axiomatic investigations; it was rediscovered by Rédei as an application of his classification of minimal non-abelian groups, cf. [12, Satz 10]. Note that, writing the numbers m occurring in Corollary 1 as

$$m = p_1 \cdots p_a q_1^2 \cdots q_b^2$$

with distinct primes $p_1, \ldots, p_a, q_1, \ldots, q_b$ coprime to

$$(p_1 - 1) \cdots (p_a - 1)\big(q_1^2 - 1\big) \cdots \big(q_b^2 - 1\big),$$

Dirichlet's theorem on primes in arithmetic progressions[1] ensures existence of infinitely many numbers m with the above property for each pair (a, b) of nonnegative integers.

Corollary 2, which is [11, Satz 1], in particular implies another result of Rédei [12, Satz 9] to the effect that a group whose Sylow subgroups are abelian and whose order n satisfies $(n, \psi(n)) = 1$ is itself abelian.

[1] Cf. [14, Chapter II.8] for an up to date discussion of the prime number theorem for arithmetic progressions, as well as [2, Chapter X] for a leisurely exposition of a version of Dirichlet's original approach, integrating ideas of Landau and Siegel.

The short proof of Theorem 1 given below makes use of Philip Hall's bound on the automorphism group of a finite p-group as well as Rédei's classification of minimal non-nilpotent groups in [13]. The paper concludes with an application of Corollary 1 to the theory of Schreier systems.

2. Proof of Theorem 1

(a) $\Rightarrow$ (b) We use induction on m, our claim being true for $m = 1$. Let

$$m = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r} > 1$$

be an integer of the form described in (a), suppose that our claim holds for all integers m', $1 < m' < m$, satisfying (i) and (ii), and assume, by way of contradiction, that there exists a group G of order m which is not nilpotent of class at most c; in particular, G is not cyclic. In what follows, we take a closer look at this counterexample G.

Clearly, the set of numbers in $\mathbb{N} \setminus \{1\}$ satisfying (i) and (ii) is closed under taking proper divisors; hence, every proper subgroup of G is nilpotent of class at most c by the inductive hypothesis.

Moreover, $r = 1$ would imply $|G| = m = p_1^{\nu_1}$ with $2 \leqslant \nu_1 \leqslant c + 1$, so G would be nilpotent of class[2]

$$c(G) \leqslant \max\{1, \nu_1 - 1\} = \nu_1 - 1 \leqslant c.$$

As this contradicts our assumption on G, we must have $r > 1$.

Therefore, each Sylow subgroup of G is proper, hence nilpotent of class $\leqslant c$, and G is not nilpotent; for, if it were, then, by a result of Burnside,[3] G would be the direct product of its Sylow subgroups $P_1, P_2, \ldots, P_r$, and the class of G would satisfy[4]

$$c(G) = \max_{1 \leqslant i \leqslant r} c(P_i) \leqslant c,$$

again contradicting our assumption on G.

We conclude from the previous discussion that G is *minimal non-nilpotent* (a non-nilpotent group all of whose proper subgroups are nilpotent). These groups have been investigated by Rédei in [13]; cf. also [7, Chapter III, Satz 5.2]. It follows in particular from Rédei's results that $r = 2$, $m = p^\lambda q^\mu$ with primes $p \neq q$, say, and that one of the Sylow subgroups (the Sylow p-subgroup P, say) is normal in G.

Fix a Sylow q-subgroup Q_0 of G. Then Q_0 is a complement to P in G; that is, G is a split extension of P by Q_0. Think of G as a semi-direct product

$$G \cong P \rtimes_\Theta Q_0,$$

[2] Cf. [8, Lemma 1.2.2] or [9, Proposition 2.1.4].

[3] Cf. [1, Chapter IX, §130] or [7, Chapter III.2, Hauptsatz 2.3].

[4] Cf. [3, Chapter A, Theorem 8.2(b)].

where $\Theta : Q_0 \to \mathrm{Aut}(P)$ is the homomorphism describing the conjugation action of Q_0 on P. Our assumptions on m imply that

$$q \nmid \big(p^{\lambda} - 1\big)\big(p^{\lambda-1} - 1\big) \cdots (p-1). \tag{1}$$

Let $|P/\Phi(P)| = p^d$. Then, by a famous result of P. Hall, the order of $\mathrm{Aut}(P)$ divides

$$p^{d(\lambda-d)}\big(p^d - 1\big)\big(p^d - p\big) \cdots \big(p^d - p^{d-1}\big); \tag{2}$$

cf. [5, Section 1.3] or [7, Chapter III, Satz 3.19]. Rewriting (2) as

$$p^{\binom{d}{2}+d(\lambda-d)}\big(p^d - 1\big)\big(p^{d-1} - 1\big) \cdots (p-1),$$

and noting that $d \leqslant \lambda$, we see that (1) ensures in fact that

$$q \nmid \big|\mathrm{Aut}(P)\big|.$$

This in turn forces Θ to be the trivial homomorphism, implying that $G \cong P \times Q_0$ is nilpotent; the desired contradiction.

(b) $\Rightarrow$ (a) In order to establish the converse, we need a supply of p-groups of *maximal class*, that is p-groups of order p^{λ} and class $\lambda - 1$ with $\lambda \geqslant 2$. This is provided, for example, by the following explicit construction.

Let p be a prime, $n \geqslant 2$ an integer, and let $\mathcal{O}_p$ be the ring of integers in the pth cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a pth root of unity. Let $\mathfrak{p}_p = (\zeta - 1)$, the maximal ideal of $\mathcal{O}_p$, and define $E(p,n)$ to be the split extension of $\mathcal{O}_p/\mathfrak{p}_p^{n-1}$ by a cyclic group $C = \langle x \rangle$ of order p, with x acting on $\mathcal{O}_p/\mathfrak{p}_p^{n-1}$ as multiplication by ζ. Then $E(p,n)$ is a group of order p^n and class precisely $n-1$. In particular, $E(2,n) \cong D_{2^n}$ is the dihedral group of order 2^n; cf. [8, Section 3.1] or [9, Section 2.2].

Suppose first that $m = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r} > 1$ does not satisfy condition (i); that is, one of the exponents (to fix ideas, say ν_1) is strictly larger than $c + 1$. Then

$$G = E(p_1, \nu_1) \times C_{p_2^{\nu_2}} \times \cdots \times C_{p_r^{\nu_r}}$$

is a group of order m, which is nilpotent of class

$$c(G) = \max\{1, \nu_1 - 1\} = \nu_1 - 1 > c.$$

In order to treat the case where m violates condition (ii), consider the group $\mathfrak{R}(p,q;\mu)$ generated by elements $A, B_0, B_1, \ldots, B_{\nu-1}$ subject to the relations

$$\begin{aligned}
A^{p^{\mu}} &= B_0^q = B_1^q = \cdots = B_{\nu-1}^q = 1,\\
B_i B_j &= B_j B_i \quad (0 \leqslant i, j \leqslant \nu - 1),\\
A^{-1} B_i A &= B_{i+1} \quad (0 \leqslant i \leqslant \nu - 2),\\
A^{-1} B_{\nu-1} A &= B_0^{c_0} B_1^{c_1} \cdots B_{\nu-1}^{c_{\nu-1}},
\end{aligned}$$

where p and q are primes, μ is a positive integer, ν is the exponent of q mod p, and

$$x^{\nu} - c_{\nu-1}x^{\nu-1} - \cdots - c_1 x - c_0$$

is an irreducible factor of $\frac{x^p-1}{x-1}$ mod q. The groups $\mathfrak{R}(p,q;\mu)$ are precisely those minimal non-abelian groups which are not of prime power order, as was shown in [12]. For our present purposes we only note that $\mathfrak{R}(p,q;\mu)$ has order $p^{\mu}q^{\nu}$, and is not nilpotent (its Sylow p-subgroups are self-normalizing); cf. [12, Satz 8].

Now suppose that m as above does not satisfy condition (ii); that is, there exist distinct prime divisors p_i, p_j of m such that

$$p_i \mid \psi\bigl(p_j^{\nu_j}\bigr) = \bigl(p_j^{\nu_j} - 1\bigr)\bigl(p_j^{\nu_j-1} - 1\bigr)\cdots(p_j - 1).$$

Then the exponent ν of p_j mod p_i satisfies $\nu \leqslant \nu_j$, and we can form the group

$$G = \mathfrak{R}(p_i, p_j; 1) \times C_{p_i^{\nu_i - 1}} \times C_{p_j^{\nu_j - \nu}} \times \prod_{\substack{1 \leqslant \rho \leqslant r \\ \rho \neq i, j}} C_{p_\rho^{\nu_\rho}},$$

which is of order m, but not nilpotent.

3. An application to Schreier systems

Let F be a free group with basis X. Recall that a set $S \subseteq F$ has the *Schreier property with respect to* X, if S contains the identity element 1 and is closed under forming initial segments; that is,

$$1 \neq \sigma = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \cdots x_{i_r}^{\varepsilon_r} \in S \quad \Rightarrow \quad \sigma_\rho = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \cdots x_{i_\rho}^{\varepsilon_\rho} \in S \quad \text{for all } 1 \leqslant \rho \leqslant r,$$

where $\varepsilon_1, \ldots, \varepsilon_r \in \{1, -1\}$, $x_{i_1}, \ldots, x_{i_r} \in X$, and σ, σ_ρ are written as reduced words. A set $S \subseteq F$ is a *Schreier system* of F, if S has the Schreier property with respect to some basis of F. A subgroup $U \leqslant F$ is *associated* with a Schreier system S, if S is a right transversal for U in F.

Given a concrete Schreier system S in a free group F together with a basis X for which S has the Schreier property, it is possible to parametrize (and, if countable, to explicitly enumerate) the collection of subgroups of F which are associated with S; cf. [6] or [10]. On the other hand, it is quite hard to decide in general whether or not S has associated normal or maximal subgroups. In this direction, Corollary 1 is easily seen to imply for instance the following.

Proposition 1. *Let F be a free group, and let $S \subseteq F$ be a finite Schreier system of F. Suppose that*

(i) *S contains elements σ_1, σ_2 with $\sigma_1 \neq \sigma_2$ having representations as (not necessarily reduced words) $w_X(\sigma_1)$, $w_X(\sigma_2)$ with respect to some basis X of F, which can be transformed into each other by permuting the elements of $X \cup X^{-1}$, and that*
(ii) *the length $|S|$ of S is cube-free and satisfies $(|S|, \psi(|S|)) = 1$.*

Then S does not have an associated normal subgroup.

As an illustration, let $F = F_2$ be the free group freely generated by x and y, and let S be the Schreier system with respect to $\{x, y\}$ generated by the words $\sigma_1 = x^2yx^{-1}yx$, $\sigma_2 = xy^2x$, and $\sigma_3 = y^2xyx^{-1}$; that is,

$$S = \{1, x, y, x^2, y^2, xy, x^2y, xy^2, y^2x, x^2yx^{-1}, xy^2x, y^2xy, x^2yx^{-1}y, y^2xyx^{-1}, x^2yx^{-1}yx\},$$

a set of 15 elements. Then one can show that S is associated with exactly

$$7! \cdot 8! = 203212800$$

subgroups in F; but, according to Proposition 1, none of these subgroups is normal.

References

[1] W. Burnside, Theory of Groups of Finite Order, second ed, Cambridge Univ. Press, Cambridge, 1911, reprinted by Dover, New York, 1955.
[2] K. Chandrasekharan, Introduction to Analytic Number Theory, Springer, Berlin, 1968.
[3] K. Doerk, T. Hawkes, Finite Soluble Groups, de Gruyter, Berlin, 1992.
[4] L.E. Dickson, Definitions of a group and a field by independent postulates, Trans. Amer. Math. Soc. 6 (1905) 198–204.
[5] P. Hall, A contribution to the theory of groups of prime power order, Proc. London Math. Soc. 36 (1933) 29–95.
[6] M. Hall, T. Radó, On Schreier systems in free groups, Trans. Amer. Math. Soc. 64 (1948) 386–408.
[7] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967.
[8] C.R. Leedham-Green, S. McKay, The Structure of Groups of Prime Power Order, Oxford Univ. Press, London, 2002.
[9] S. McKay, Finite p-Groups, Queen Mary Math. Notes, vol. 18, Queen Mary & Westfield College, University of London, London, 2000.
[10] T.W. Müller, Combinatorial group theory via Schreier systems in arbitrary groups (working title), monograph, in preparation.
[11] G. Pazderski, Die Ordnungen, zu denen nur Gruppen mit gegebenen Eigenschaften gehören, Arch. Math. 10 (1959) 331–343.
[12] L. Rédei, Das schiefe Produkt in der Gruppentheorie, Comm. Math. Helv. 20 (1947) 225–264.
[13] L. Rédei, Die endlichen einstufig nichtnilpotenten Gruppen, Publ. Math. Debrecen 4 (1956) 303–324.
[14] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, Cambridge Univ. Press, Cambridge, 1995.