

# ON THE DERIVED SUBGROUP OF A FINITE $p$ -GROUP

CSABA SCHNEIDER

## 1. INTRODUCTION

Sylow in his famous 1872 paper [Syl72] proved that algebraic equations whose Galois groups have prime-power order can be solved by radicals. In modern terms this amounts to saying that groups of prime-power order are soluble. There are a number of open questions related to this fact and we shall address one of them here.

The commutator of two group elements  $a$  and  $b$  is defined as  $[a, b] = a^{-1}b^{-1}ab = a^{-1}a^b$ . If  $H_1$  and  $H_2$  are subgroups then their commutator  $[H_1, H_2]$  is the subgroup generated by all elements of the form  $[a, b]$  where  $a \in H_1$  and  $b \in H_2$ . In a group  $G$  we define the *derived series*  $\{G^{(k)}\}_{k \geq 0}$  whose terms are

$$G^{(0)} = G \quad \text{and} \quad G^{(k+1)} = [G^{(k)}, G^{(k)}] \quad \text{for} \quad k \geq 0.$$

The terms  $G^{(1)}$  and  $G^{(2)}$  are usually denoted by  $G'$  and  $G''$ , respectively. One can reformulate Sylow's theorem to say that for each finite  $p$ -group  $G$  there exists an  $l \geq 1$  such that  $G^{(l)} = 1$ . The smallest such  $l$  is called the *soluble length* of the group.

Burnside [Bur13] initiated research into finding the order of the smallest  $p$ -groups whose soluble length is a given  $l$ . When  $l = 2$  Burnside's question asks to find the order of the smallest non-abelian  $p$ -groups. It is well-known that groups of order  $p$  and  $p^2$  are all abelian, but there exist non-abelian groups with order  $p^3$  for each  $p$ ; this settles the problem for  $l = 2$ .

When  $l = 3$  we want to find the smallest  $p$ -groups  $G$  in which  $G'' \neq 1$ . It is not difficult to see that  $G'' \neq 1$  implies that  $|G'/G''| \geq p^3$  (see Hilfssatz III.7.10 in Huppert [Hup67]). As  $|G/G'| \geq p^2$  and  $|G''| \geq p$ , we obtain that  $|G| \geq p^6$ . For  $p \geq 5$  this bound is sharp, as some groups of maximal class exhibit the required properties (see Blackburn [Bla58] or Huppert [Hup67] III.14). For  $p = 2, 3$  the smallest order is  $p^7$ .

---

*Date:* 4 November 1999.

*1991 Mathematics Subject Classification.* 20D15, 20F40, 17B70, 17B60.

*Key words and phrases.* finite  $p$ -groups, derived subgroup, Lie algebras, Lie ring method.

For  $l = 4$  the sharp bound for most primes was found very recently. Blackburn in his PhD dissertation [Bla56] proved that  $G^{(3)} \neq 1$  implies  $|G| \geq p^{14}$  for  $p \geq 5$ . Using computational techniques and the Lie ring method, Evans-Riley et al. [ERNS99] constructed examples  $G$  for each  $p \geq 5$  such that  $|G| = p^{14}$  and  $G^{(3)} \neq 1$ . This proves that for these primes Blackburn's bound is sharp. For  $p = 2, 3$  the smallest order is expected to be  $p^{15}$ .

The order of the smallest  $p$ -groups with soluble length  $l \geq 5$  is still unknown. It is a well-known result of P. Hall that the order of such a group is at least  $p^{2^{l-1}+l-1}$  (see Huppert [Hup67] Satz III.7.11). This was recently improved by Mann [Man98], namely we have  $|G| \geq p^{2^{l-1}+2l-4}$ . Further asymptotic improvement by the author [Sch99] is that  $|G| \geq p^{2^{l-1}+3l-10}$ .

For a given  $l \geq 5$  the order of the smallest known  $p$ -groups with soluble length  $l$  is higher than these lower bounds. For  $p \geq 3$  and  $l \geq 2$  Hall [Hal64] exhibited a series of  $p$ -groups which have soluble length  $l$  and order  $p^{2^{l-1}}$  (see also Huppert [Hup67] III.17). For  $p \geq 5$  the smallest known  $p$ -groups with soluble length  $l \geq 4$  were constructed by Evans-Riley et al. [ERNS99]; they have order  $p^{2^{l-2}}$ . It would be interesting to close the gap – at least in some asymptotic sense.

The lower bounds for the order of a  $p$ -group with a given soluble length are built from bounds for individual factors of the derived series. This leads to study  $p$ -groups in which  $G^{(k)}/G^{(k+1)}$  is as small as possible for some  $k \geq 1$ . As we already mentioned, if  $G$  is a  $p$ -group with  $G'' \neq 1$  then  $|G'/G''| \geq p^3$ . So we investigate groups of this kind with  $|G'/G''| = p^3$ . It is a result of Blackburn [Bla87] that  $G''$  must be abelian with at most two generators. For odd primes one can say much more, namely  $|G''| = p$ . This result is usually attributed to P. Hall, see Blackburn [Bla87]. In this note we give more information about  $G$  in the odd prime case. According to the theorem presented in Section 3, for odd primes  $G'/[G', G]$  is cyclic of order  $p$ . This has strong consequences on the structure of  $G$  and some of them are explored in the author's PhD thesis [Sch99]. Our result is obtained as an application of the Lie ring method, which is briefly described in Section 2.

## 2. THE LIE RING METHOD

We obtain our results using Lie rings associated with  $p$ -groups. A brief summary of this technique is presented in this section. For the proofs of our claims and more information

on the Lie ring method one can refer to Chapter VIII of Huppert & Blackburn [HB82]. The survey article by Shalev [Sha95] also contains a summary and a lot of applications.

A Lie ring is a non-associative ring  $L$  whose product – usually denoted by brackets – satisfies the identities

$$(1) \quad [a, a] = 0$$

$$(2) \quad [[a, b], c] + [[c, a], b] + [[b, c], a] = 0.$$

Rings in which (1) holds are called anti-commutative, as a standard calculation shows that (1) implies the identity  $[a, b] = -[b, a]$ . Identity (2) is referred to as the Jacobi identity. To simplify long products we use the left-normed convention, namely we write  $[a, b, c]$  for  $[[a, b], c]$ .

Group elements satisfy a number of well-known identities which involve commutators. For instance,

$$[a, a] = 1$$

$$[ab, c] = [a, c]^b [b, c] \quad \text{and} \quad [a, bc] = [a, c][a, b]^c$$

$$[[x, y], z^x][[z, x], y^z][[y, z], x^y] = 1$$

are some of the most important ones. A close inspection reveals that these identities are formally quite similar to the defining axioms for Lie rings. There are several methods which exploit this connection and assign a Lie ring to a given group. Via this assignment we reduce questions about group commutators to questions about products in Lie ring elements. As the properties of the Lie product are significantly simpler than those of the group commutator, proving the corresponding Lie ring result is often much easier.

The *lower central series*  $\{\gamma_k(G)\}_{k \geq 1}$  of a group  $G$  is defined recursively as

$$\gamma_1(G) = G \quad \text{and} \quad \gamma_{k+1}(G) = [\gamma_k(G), G] \quad \text{for} \quad k \geq 1.$$

An important property of the lower central series is that

$$(3) \quad [\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G) \quad \text{for all} \quad i, j \geq 1.$$

If  $G$  is a finite  $p$ -group then there is a  $c \geq 2$  such that  $\gamma_c(G) = 1$ . The quotients  $\gamma_k(G)/\gamma_{k+1}(G)$  are all abelian and we form their direct sum

$$L = \bigoplus_{k \geq 1} \gamma_k(G)/\gamma_{k+1}(G).$$

A product on this abelian group can be introduced as follows. If  $a \in \gamma_i(G)$  and  $b \in \gamma_j(G)$  then  $a\gamma_{i+1}(G), b\gamma_{j+1}(G) \in L$ . From (3) we have  $[a, b] \in \gamma_{i+j}(G)$ , thus  $[a, b]\gamma_{i+j+1}(G)$  also lies in  $L$ . Hence we can define the product of  $a\gamma_{i+1}(G)$  and  $b\gamma_{j+1}(G)$  as

$$[a\gamma_{i+1}(G), b\gamma_{j+1}(G)] = [a, b]\gamma_{i+j+1}(G).$$

After extending this product linearly to the whole of  $L$ , it is not difficult to prove that we obtain a Lie ring; it is called *the Lie ring associated with the lower central series of  $G$* . For  $k \geq 1$  set  $L_k = \gamma_k(G)/\gamma_{k+1}(G)$ . Using (3) one can prove that  $[L_i, L_j] \leq L_{i+j}$ , so one may regard  $L$  a *graded* Lie ring with  $L_k$  as the homogeneous component of degree  $k$ . It is easy to see that  $L$  is generated by  $L_1$ , hence  $L_{k+1} = [L_k, L_1]$  for  $k \geq 1$  holds.

The derived series, the lower central series, solubility and nilpotency can be defined in Lie rings just as they are defined in groups. Note that if  $L$  is the Lie ring associated with the lower central series of a  $p$ -group, then  $L$  is always nilpotent – and hence is soluble – moreover  $\gamma_k(L) = \bigoplus_{i \geq k} L_i$  for  $k \geq 1$ .

### 3. APPLICATION OF THE LIE RING METHOD TO THE DERIVED SERIES

As we said in the introduction, our aim has been to learn something about finite  $p$ -groups  $G$  in which  $|G'/G''| = p^3$  and  $G''$  is non-trivial. Let  $G$  be such a group. Recall that  $G' = \gamma_2(G)$  and it follows from (3) that  $G'' \leq \gamma_4(G)$ . So we have a chain of normal subgroups

$$(4) \quad G \supsetneq G' = \gamma_2(G) \supsetneq \gamma_3(G) \supsetneq \gamma_4(G) \supseteq G'' \supsetneq 1.$$

It is easy to see that our condition on  $G$  immediately implies that the order of  $G'/\gamma_3(G)$  is  $p$  or  $p^2$ .

Let us first suppose that this order is  $p^2$ . If  $G'/\gamma_3(G)$  is cyclic then

$$G'' = [G', G'] = [G', \gamma_3(G)] \leq \gamma_5(G),$$

hence  $G'/G''$  has order at least  $p^4$ . (Here we use that  $N \trianglelefteq G$  and  $G/N$  is cyclic imply  $G' = [G, N]$ ; see, for example, Lemma 2.1 of Blackburn [Bla58].) So  $G'/\gamma_3(G) \cong C_p \times C_p$ , where  $C_n$  denotes the cyclic group of order  $n$ . From (4) it is also clear that  $G'' = \gamma_4(G)$ . If this holds then we say that  $G$  is in the *diamond case*. The reason for the name is that a section isomorphic to  $C_p \times C_p$  is usually represented by a diamond in a subgroup lattice.

If, however,  $|G'/\gamma_3(G)| = p$  then, as above, we obtain that  $G'' \leq \gamma_5(G)$ . In fact, the condition on  $G'/G''$  implies that  $1 \neq G'' = \gamma_5(G)$ . It is easy to see that in this case  $G$  acts uniserially on  $G'$ , thus we say that  $G$  belongs to the *uniserial case*.

Our main result is the following theorem.

**Theorem** *Let  $p \geq 3$  and  $G$  be a finite  $p$ -group such that  $|G'/G''| = p^3$  and  $G'' \neq 1$ . Then  $|G'/\gamma_3(G)| = p$  and  $G'' = \gamma_5(G)$ . In other words such a group is in the uniserial case.*

To prove our theorem we argue by contradiction and suppose that  $|G'/G''| = p^3$ ,  $G'' \neq 1$  and  $G'/\gamma_3(G) \cong C_p \times C_p$  for some  $p \geq 3$ . Let  $\bar{L}$  be the Lie ring associated with the lower central series of  $G$ . As  $G'/\gamma_3(G) \cong C_p \times C_p$  we obtain that  $\bar{L}_2$  has order  $p^2$  and  $p\bar{L}_2 = 0$ . By induction it is easy to prove that  $p\bar{L}_i = 0$  for all  $i \geq 2$ . The quotient  $L = \bar{L}/p\bar{L}$  can be viewed as a Lie algebra over  $\mathbb{F}_p$ . It is easy to see that  $L$  is also graded; indeed,  $L = \bigoplus_{k \geq 1} L_k$ , where  $L_1 \cong \bar{L}_1/p\bar{L}_1$  and  $L_k \cong \bar{L}_k = \gamma_k(G)/\gamma_{k+1}(G)$  for  $k \geq 2$ . Furthermore,  $L$  is generated by  $L_1$ . Some further relevant properties of the Lie algebra  $L$  are that  $\dim L_2 = 2$  and  $\dim L_3 = 1$ . Moreover, it is easy to see that there must be  $a, b, c, d \in L_1$  such that  $0 \neq [[a, b], [c, d]] \in L_4 \cap L''$ . The following lemma excludes the existence of such an  $L$ .

**Lemma** *Let  $p \geq 3$  and  $L$  be a graded Lie algebra over  $\mathbb{F}_p$ , generated by  $L_1$  such that  $\dim L_2 = 2$  and  $\dim L_3 = 1$ . Then  $L_4 \cap L'' = 0$ .*

A detailed proof of this result can be found in the author's PhD thesis [Sch99] and, hopefully, will be published soon. We only outline the most important steps. The calculations are elementary and only the defining axioms for Lie algebras and the properties of the grading are used. The interested reader may want to fill in the details.

We start arguing by contradiction and suppose that  $L$  is as in the lemma, yet  $L_4 \cap L'' \neq 0$ . In the first step we show that one can assume without loss of generality that  $L$  is 3-generated, that is  $\dim L_1 = 3$ ; let  $\{a, b, c\}$  be a basis. It is not difficult to prove that we may further suppose that  $\{[a, b], [a, c]\}$  is a basis for  $L_2$  and  $[b, c] = 0$ . Then our condition implies that  $[[a, b], [a, c]] = [a, b, a, c] - [a, b, c, a] \neq 0$ . From this it follows that at least one of  $[a, b, a, c]$  and  $[a, b, c, a]$  is non-zero. In particular at least one of  $[a, b, a]$  and  $[a, b, c]$  is also non-zero. Hence  $\{[a, b, a]\}$  or  $\{[a, b, c]\}$  is a basis for  $L_3$ . Now we only have to evaluate enough instances of the Jacobi identity to show that in both cases  $[[a, b], [a, c]] = 0$  holds, thus we obtain a contradiction.

According to our lemma, the Lie algebra that we constructed in the discussion following the statement of the theorem cannot exist. For odd primes this rules out the existence of the diamond case, thus the theorem is proved.

Having excluded the diamond case, we can obtain further information on the structure of  $G$ . For instance, we can characterise  $G'$  as follows. By Hall's theorem mentioned in the introduction, we have that  $|G'| = p^4$ . It is a consequence of our theorem that  $G'$  must be isomorphic to a direct product of a non-abelian group of order  $p^3$  and  $C_p$ . This reduces the possibilities for  $G'$  to two isomorphism types. This and some further results are proved in the author's PhD thesis [Sch99].

If  $p = 2$  then the situation is rather different. There are 2-groups in which  $|G'/G''| = 8$  and  $G''$  is arbitrarily large. Moreover, in 2-groups the diamond case is also possible. Examples to justify these assertions can be obtained from Newman & O'Brien [NO99]. One can take finite quotients of the groups whose number is 7, 18, 24, 56, 62 or 72 in the list given in Appendix A of [NO99].

Note that our lemma is interesting in the context of Lie algebras itself. Dixmier [Dix55] proves that in a nilpotent Lie algebra  $L$  the condition  $L'' \neq 0$  implies  $\dim L'/L'' \geq 3$ . One can study nilpotent Lie algebras  $L$  in which  $L'' \neq 0$  and  $\dim L'/L'' = 3$  and it is easy to see that one can introduce the diamond and the uniserial cases just as we did for  $p$ -groups. According to the lemma, for odd primes the diamond case does not occur in graded and degree-1 generated  $\mathbb{F}_p$ -Lie algebras. It is easy to see that the existence of the grading is not essential and the result can be stated generally for nilpotent Lie algebras over all fields whose characteristic is not 2.

#### 4. ACKNOWLEDGEMENT

I would like to thank the organisers of the conference for the opportunity to give a talk. I am also grateful to Alice Niemeyer and Alberto Basile for helping me refine my presentation; and to Laci Kovács, Cai Heng Li and Cheryl Praeger for their helpful comments on a draft of this paper. I am indebted to The Australian National University for financially supporting my research and to the The University of Western Australia for its hospitality while this paper was being written.

I would like to express my gratitude to my PhD supervisor, Mike Newman, for his masterly guidance. I owe my prize largely to him.

## REFERENCES

- [Bla56] Norman Blackburn. *Problems on the theory of finite groups of prime-power order*. PhD thesis, University of Cambridge, 1956.
- [Bla58] N. Blackburn. On a special class of  $p$ -groups. *Acta Math.*, 100:45–92, 1958.
- [Bla87] Norman Blackburn. The derived group of a 2-group. *Math. Proc. Cambridge Philos. Soc.*, 101(2):193–196, 1987.
- [Bur13] W. Burnside. On some properties of groups whose orders are powers of primes. *Proc. London Math. Soc.* (2), 11:225–243, 1913.
- [Dix55] J. Dixmier. Sur les algèbres dérivées d’une algèbre de Lie. *Proc. Cambridge Philos. Soc.*, 51:541–544, 1955.
- [ERNS99] Susan Evans-Riley, M. F. Newman, and Csaba Schneider. On the soluble length of groups with prime-power order. *Bull. Austral. Math. Soc.*, 59(2):343–346, 1999.
- [Hal64] P. Hall. A note on  $\overline{ST}$ -groups. *J. London Math. Soc.*, 39:338–344, 1964.
- [Hup67] B. Huppert. *Endliche Gruppen I*. Springer-Verlag, Berlin, 1967.
- [HB82] Bertram Huppert and Norman Blackburn. *Finite groups II*. Springer-Verlag, Berlin, 1982.
- [Man98] Avinoam Mann. The derived length of  $p$ -groups (preliminary version). Submitted, 1998.
- [NO99] M. F. Newman and E. A. O’Brien. Classifying 2-groups by coclass. *Trans. Amer. Math. Soc.*, 351(1):131–169, 1999.
- [Sch99] Csaba Schneider. *Some results on the derived series of finite  $p$ -groups*. PhD thesis, The Australian National University, Canberra, 1999.
- [Sha95] A. Shalev. Finite  $p$ -groups. In B. Hartley, G. M. Seitz, A. V. Borovik, and R. M. Bryant (eds) *Finite and locally finite groups (Istanbul, 1994)*, pages 401–450. Kluwer Acad. Publ., Dordrecht, 1995.
- [Syl72] L. Sylow. Théorèmes sur les groupes de substitutions. *Math. Ann.*, 5:584–594, 1872.

SCHOOL OF MATHEMATICAL SCIENCES, THE AUSTRALIAN NATIONAL UNIVERSITY, 0200 ACT CANBERRA, AUSTRALIA

*Current address:* Department of Mathematics and Statistics, The University of Western Australia, 6907 WA Nedlands, Australia

*E-mail address:* csaba@maths.uwa.edu.au