Journal of Algebra 337 (2011) 335–344

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Recognizing the prime divisors of the index of a proper subgroup ☆

Andrea Lucchini [a,*], Marta Morigi [b]

[a] Dipartimento di Matematica Pura e Applicata, Università di Padova, Via Trieste 63, 35121 Padova, Italy
[b] Dipartimento di Matematica, Università di Bologna, Piazza di Porta San Donato 5, 40126 Bologna, Italy

ARTICLE INFO

Article history:
Received 21 December 2010
Available online 30 March 2011
Communicated by E.I. Khukhro

MSC:
20F05
20D60

Keywords:
Generators
Index

ABSTRACT

Let G be a finite group and let C be a subgroup of G. We prove that in order to get information on the set of primes dividing the index $|G:C|$ of C in G it is enough to look at the primes dividing $|H:C\cap H|$, where H is a suitable subgroup of G with few generators.

1. Introduction

In a recent paper, Camina, Shumyatsky and Sica proved the following theorem: let x be an element of a finite group G and let $\mathrm{Ind}_G(x)$ be the index in G of the centralizer $C_G(x)$ of x in G; if $\mathrm{Ind}_{\langle a,b,x\rangle}(x)$ is a prime-power for every $a,b\in G$, then $\mathrm{Ind}_G(x)$ is a prime-power [2]. The above theorem can be restated as follows: let x be an element of a finite group G and let $C=C_G(x)$; if there is more than one prime dividing $|G:C|$, then there exist $a,b\in G$ such that $|\langle a,b,x\rangle : C\cap\langle a,b,x\rangle|$ is divisible by more than one prime.

In this paper we aim at generalizing this result. If we want to consider any subgroup C of G, instead of limiting ourselves to centralizers of elements, it is more natural to look at $|H:C\cap H|$

☆ The authors were partially supported by MIUR (Project "Teoria dei Gruppi e applicazioni").
* Corresponding author.
E-mail addresses: lucchini@math.unipd.it (A. Lucchini), mmorigi@dm.unibo.it (M. Morigi).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2011.02.041

where H is a subgroup with "few" generators. If n is a positive integer we denote by $\pi(n)$ the set of primes dividing n. Our result is the following.

Theorem A. *Let G be a finite group and let X, C be two subgroups of G such that $X \leqslant C$. Then there exist $a, b, c \in G$ such that $\pi(|G : C|) \subseteq \pi(|\langle a, b, c, X\rangle : C \cap \langle a, b, c, X\rangle|)$.*

When X is the identity subgroup we obtain the type of result we were originally aiming at.

Corollary B. *Let G be a finite group and let C be a subgroup of G. Then there exist $a, b, c \in G$ such that $\pi(|G : C|) \subseteq \pi(|\langle a, b, c\rangle : C \cap \langle a, b, c\rangle|)$.*

When $X = C$ we have a new type of result.

Corollary C. *Let G be a finite group and let C be a subgroup of G. Then there exist $a, b, c \in G$ such that $\pi(|G : C|) = \pi(|\langle a, b, c, C\rangle : C|)$.*

In order to deal with the case of prime-power index we need a stronger conclusion than that of Theorem A.

Theorem D. *Let G be a finite group and let X, C be two subgroups of G such that $X \leqslant C$. If $|\pi(|G : C|)| \geqslant 2$, then there exist $a, b \in G$ such that $|\pi(|\langle a, b, X\rangle : C \cap \langle a, b, X\rangle|)| \geqslant 2$.*

This imply the result in [2] when $C = C_G(x)$ and $X = \{x\}$.

We conjecture that Theorem A can be improved, because just 2 suitable generators could be enough in order to reach the conclusion, instead of 3, but proving this would need good estimates on the probability of generating 2-generated almost simple groups with 2 elements, and these results are not available at the moment. On the other hand, just one suitable generator is not enough to reach the conclusion of Theorem A, as the example of $G = S_3$ shows, when taking $X = C = 1$.

The following two propositions support this conjecture and give partial answers, in the case of soluble groups and in the case when no "small" prime divides $|G : C|$.

Theorem E. *Let G be a finite soluble group and let X, C be two subgroups of G such that $X \leqslant C$. Then there exist $a, b \in G$ such that $\pi(|G : C|) \subseteq \pi(|\langle a, b, X\rangle : C \cap \langle a, b, X\rangle|)$.*

Theorem F. *Let G be a finite group and let X, C be two subgroups of G such that $X \leqslant C$. Then there exists an absolute constant $\bar{c}$ with the following property: if $\mathcal{Q}$ is the set of primes which are bigger than $\bar{c}$, then there exist $a, b \in G$ such that $\pi(|G : C|) \cap \mathcal{Q} \subseteq \pi(|\langle a, b, X\rangle : C \cap \langle a, b, X\rangle|)$.*

2. Background material

In what follows $\mathrm{d}(G)$ denotes the minimal number of generators of the group G and if X is a subset of G then $\mathrm{d}_X(G)$ denotes the minimum integer d such that there exist d elements $g_1, \dots, g_d \in G$ with the property that $G = \langle X, g_1, \dots, g_d\rangle$. If p is a prime, $|G|_p$ denotes the order of a Sylow p-subgroup of G and if x is an element of G then we will write $|x|_p$ instead of $|\langle x\rangle|_p$. Moreover, $\operatorname{Aut} G$ is the automorphism group of G and we recall that the socle $\mathrm{Soc}(G)$ of G is the subgroup generated by all minimal normal subgroups of G.

Throughout the paper, we will often have to consider a quotient group G/N of a group G. For the sake of brevity, if g (resp. U) is an element (resp. subgroup) of G, then $\bar{x}$ (resp. $\bar{U}$) will denote the image of x (resp. U) in G/N.

Let L be a primitive monolithic group, that is a group with a unique minimal normal subgroup A such that if A is abelian, then it has a complement in L. For each positive integer k we let L^k be the