

ON SOME INVARIANTS OF FINITE GROUPS

J. KREMPA AND A. STOCKA*

Communicated by Patrizia Longobardi

ABSTRACT. In this note we are going to survey several invariants of finite groups related either to their orders or to generating sets or to lattices of subgroups. Some relations among these invariants will be exhibited. Special attention will be paid to monotonicity of them.

1. Around orders

All groups considered here are finite. Our notation will be standard, and similar to that in [5]. By an invariant of a group G we mean a nonnegative integer, say $\alpha(G)$, chosen in such a way that $G \simeq H$ implies $\alpha(G) = \alpha(H)$. We say, that our invariant α is *monotone (on G)* if α is defined for all subgroups of G and $\alpha(H) \leq \alpha(K)$, whenever $H \leq K \leq G$.

For any group G we have an obvious invariant $|G|$, the order of G . This invariant is monotone and is well connected with standard operations on groups, because for any subgroup H of G we have a Lagrange Formula:

$$(1.1) \quad |G| = |H| \cdot |G : H|.$$

The order is helpful, for example in inductive proofs and in computational group theory (see for example [5, 8] and [3]), but the usual ordering of natural numbers is not well connected with properties of groups having increasing orders. That's why some arithmetic functions (see [13]) of the order are often applied.

If G is a group then let $\omega|G|$ be the number of distinct prime divisors of $|G|$ and $\Omega|G|$ be the number of prime divisors of $|G|$ counted with multiplicities. From the Formula 1.1 we know that both these

MSC(2010): Primary: 20D10; Secondary: 20F05.

Keywords: Generating set, independent set, (p, q) -group, lattice of subgroups.

Received: 18 December 2012, Accepted: 20 February 2013.

*Corresponding author.

invariants are monotone and their small values give some interesting classes of groups. For example, $\Omega|G| = 1$ if and only if G is simple abelian. Groups with $\Omega|G| \leq 3$ are solvable and well described (see [8] I, 8.11, 8.13).

Groups G with $\omega|G| = 1$ are known as p -groups and are extensively studied, with some specific methods (see [2] and subsequent volumes of this monograph). They have many interesting properties. For example, they are nilpotent groups and every nilpotent group is a direct product of p -groups with coprime orders.

Groups G with $\omega|G| = 2$ are known as (p, q) -groups. They have no specific theory, but they appear in many considerations. In particular, due to W. Burnside we know that such groups are solvable, but need not be nilpotent. Note that for the alternating group A_5 we have $\omega|A_5| = 3$ and $\Omega|A_5| = 4$, but A_5 is not solvable.

Next well known invariant of a group G is $Exp(G)$, the exponent of G . This invariant is also monotone and is connected with the order by

$$(1.2) \quad Exp(G) \mid |G| \quad \text{and} \quad |G| \mid (Exp(G))^r$$

for some r depending on G . Hence, the function ω applied to Exp gives no new invariant of groups.

The following simple observations, consequences of Formula 1.2 about connections of order and exponent of a group G should be noticed here:

- Every Sylow p -subgroup of G is cyclic if and only if $Exp(G) = |G|$.
- If $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $n = p_1^{\beta_1} \cdots p_r^{\beta_r}$, where p_i are distinct primes and $1 \leq \alpha_i \leq \beta_i$ for $i = 1, \dots, r$ then there exists an abelian group G such that $Exp(G) = m$ and $|G| = n$.

Groups with $Exp(G) = |G|$ were considered with details and are completely described (see [14, Theorem 10.1.10]). As a special case one can consider groups with $\omega|G| = \Omega|G|$, that of course are precisely groups with square free orders.

2. Generators

For every group G let $\Phi(G)$ denotes the Frattini subgroup of G , the set of nongenerators of G . A subset X of G is said here to be:

- g -independent if $\langle Y, \Phi(G) \rangle \neq \langle X, \Phi(G) \rangle$ for all $Y \subset X$;
- a generating set of G if $\langle X \rangle = G$;
- a g -base of G , if X is a g -independent generating set of G .

The following result is an immediate consequence of the definition of the Frattini subgroup.

Proposition 2.1. *Let G be any group, $X \subset G$ a subset and \bar{X} the natural image of X in $G/\Phi(G)$. If $|X| = |\bar{X}|$, then:*

- X is g -independent in G if and only if \bar{X} is g -independent in $G/\Phi(G)$;
- X is a generating set of G if and only if \bar{X} is a generating set of $G/\Phi(G)$;
- X is a g -base of G if and only if \bar{X} is a g -base of $G/\Phi(G)$.

In connection with generating sets we can consider, for any group G , the following natural invariants:

$$(2.1) \quad sg(G) = \sup_X |X| \quad \text{and} \quad ig(G) = \inf_X |X|,$$

where X runs over all g-bases of G .

Example 2.2. Let G be a p -group, $X \subset G$ a subset and let $|G/\Phi(G)| = p^r$. Then, by Burnside Basis Theorem, X is a generating set of G if and only if $|X| = |\overline{X}|$ and \overline{X} is a base of $G/\Phi(G)$ considered as a vector space over the prime field \mathbb{F}_p . Hence, in this case, $ig(G) = sg(G) = r$.

Example 2.3. Let G be abelian. Then $sg(G)$ is the usual abelian rank, $r(G)$. If, in particular, $n = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$ where p_i are distinct primes and $k_i > 0$, then $sg(C_n) = r = \omega|C_n|$, while $ig(C_n) = 1$.

In the literature on nonabelian groups special attention is paid to the invariant $ig(G)$, sometimes denoted by $d(G)$ or $m(G)$ (see for example [10]). However, some interesting results for sg can also be found.

Theorem 2.4 ([17]). *For any $n > 2$ we have: $sg(S_n) = n - 1$, while $ig(S_n) = 2$.*

For constructing further examples of groups with $ig \neq sg$ the following observation is helpful.

Proposition 2.5. *Let G and H be groups with coprime orders. Then*

- (i) $ig(G \times H) = \max(ig(G), ig(H))$;
- (ii) $sg(G \times H) = sg(G) + sg(H)$.

Proof. Let $ig(G) = k$ and $ig(H) = l$. Assume that x_1, \dots, x_k is a g-base of G and y_1, \dots, y_l is a g-base of H . We can assume that $k \geq l$. Put $z_i = (x_i, y_i)$ for $i = 1, \dots, k$, where $y_i = y_l$ for $i \geq l$. It is easy to calculate that the set $\{z_1, \dots, z_k\}$ is a g-base of $G \times H$. This means that

$$\max(ig(G), ig(H)) = k \geq ig(G \times H).$$

The converse inequality follows by projections of $G \times H$ on G and on H .

Now let x_1, \dots, x_k be a g-base of G of maximal cardinality and y_1, \dots, y_l a g-base of H also of maximal cardinality. Clearly the set $\{(x_1, 1), \dots, (x_k, 1), (1, y_1), \dots, (1, y_l)\}$ is a g-base of $G \times H$.

On the other hand, if z_1, \dots, z_m is a g-base of $G \times H$ of maximal cardinality, then let $z_i = (u_i, v_i)$ for $i = 1, \dots, m$. If in our base we replace z_i by a pair $\{(u_i, 1), (1, v_i)\}$ then from this pair exactly one element should remain for obtaining a new base. After finite number of such replacements we obtain a base with m elements, but with all of the form either $(x, 1)$ or $(1, y)$. From this we have $k + l \geq m$, and the result follows. □

Now, as a consequence of earlier results one can easily obtain:

Corollary 2.6. *Let $1 \leq m \leq n < \infty$. Then there exists even an abelian group G such that $ig(G) = m$ and $sg(G) = n$.*

In [12, 9, 15] groups with *property* \mathcal{B} , that is groups G with $ig(G) = sg(G)$, were investigated. In this case we will call this invariant a g -dimension of G . In the same papers also groups with *the basis property*, that is groups such that all its subgroups have property \mathcal{B} , hence have g -dimension, were studied. For considering monotonicity we are going to concentrate on groups with the basis property. Among other things the following result is proved in [12]:

Theorem 2.7. *Let G be a group. If G has the basis property, then either G is a p -group, or G is a semidirect product $P \rtimes Q$, where P is a p -group, Q is a cyclic q -group, for some prime $q \neq p$, and every non-identity element of Q acts fixed-point-freely on P . Hence $\omega|G| \leq 2$.*

From Example 2.2 we know that p -groups have the basis property. For further consideration let us take a modified version of an example from [12, §3].

Example 2.8. Let $p \neq q$ be primes and let H be a cyclic group of order q^m for some $m \geq 1$. It is known from the field theory that there exists the smallest n such that $q^m \mid p^n - 1$. Then H is contained in the multiplicative group of the field $K = F_{p^n}$ of the cardinality p^n . If V is a vector space over K , then there is a natural action $\phi : H \rightarrow \text{Aut}V$ via multiplication, $h\phi : v \rightarrow vh$. Every element of K is a sum of elements of H with coefficients in the prime field \mathbb{F}_p . Then H -invariant subgroups of V are exactly K -subspaces of V . We are interested in the semidirect product $G = V \rtimes H$ with the above mentioned action of H on V . In what follows we shall refer to such a semidirect product as being *constructed via the field multiplication on V* . We shall exploit the structure of V as a vector space over K . If x_1, x_2, \dots, x_r is a base of V over K then $V = \bigoplus_{i=1}^r Kx_i$ and every summand Kx_i has no proper H -invariant subgroups.

Now one can simply obtain the proof of the following result.

Lemma 2.9 ([12], Lemma 3.1). (i) *Every element in G has order either p or a power of q .*
(ii) *If v and w are non-zero vectors in V , then $Kv \simeq_K Kw$ and Kv is irreducible as a H -module.*

Theorem 2.10 ([12], Theorem 3.2). *Let $G = V \rtimes H$ be the semidirect product of an elementary abelian p -group by a cyclic q -group constructed via the field multiplication on V . Then, under notation from Example 2.8, we have*

- (i) G has property \mathcal{B} ;
- (ii) $ig(G) = r + 1$, where V is an r dimensional space over K ;
- (iii) $\Phi(G) = 1$.

Proposition 2.11 ([12], Proposition 4.4). *Let G be a group with the basis property. Then $G/\Phi(G)$ is a semidirect product constructed via the multiplication on some vector space over a finite field.*

Proposition 2.12. *Let G be a group with the basis property. If the g -dimension is monotone on G , then $G/\Phi(G)$ is a semidirect product of an elementary abelian p -group V and a cyclic q -group H and*

- (a) H acts by power automorphisms on V or
- (b) H acts irreducibly on V and $|V| = p^2$.

Proof. Let G be a group with the basis property. Then, by Proposition 2.11, $G/\Phi(G)$ is a semidirect product of an elementary abelian p -groups V and a cyclic q -group H with the help of field multiplication. Moreover $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$ is a direct sum of irreducible H -submodules and $V_i \simeq V_j$ for $i, j = 1, \dots, k$.

First we assume that $k \geq 2$. If $v_1 \in V_1, \dots, v_k \in V_k$ are non-zero elements, then these elements generate V as an H -module. So G is generated by the set

$$\{(v_1, 1), (v_2, 1), \dots, (v_k, 1), (1, x)\},$$

where x is a generator of H . On the other hand, if V_1 is a p -group of order p^l , then V is of order p^{kl} and the g -dimension of V is equal to kl . Since the g -dimension of G is monotone, the g -dimension of V , equal to kl , is less or equal to $k + 1$. It follows that $l = 1$ and every V_i is a cyclic group of order p . This means that H induces a power automorphism on V .

Now let $k = 1$. Then the g -dimension of G is equal to 2 and the set $\{(v_1, 1), (1, x)\}$ is a g -base of V . Hence the order of V is not greater than p^2 . □

Proposition 2.13. *Let $G = V \rtimes H$ be the semidirect product of an elementary abelian p -group by a group of order q , constructed via the field multiplication on a vector space over a finite field. Then G has the basis property.*

Proof. In view of Theorem 2.10, G has property \mathcal{B} . Let M be a proper subgroup of G . If M is either a p -group or a q -group then, by Example 2.2, M has property \mathcal{B} . So we assume that M is neither a p -group nor a q -group. In this case M is a semidirect product $V_M \rtimes H_M$, where $V_M \subseteq V$ is a H -invariant subgroup, and H_M is a Sylow q -subgroup of M of order q . Now one can check that M is constructed via the field multiplication. Hence, again by Theorem 2.10, we have that M has property \mathcal{B} . It follows that G has the basis property. □

In [4, 11] all p -groups with monotone g -dimension were described. In particular, for every prime p there exists a p -group with nonmonotone g -dimension. Among other groups with the basis property such examples also could be produced. We provide such examples using the field multiplication.

Lemma 2.14. *Let $G = V \rtimes H$ be a semidirect product of elementary abelian p -group of order p^n with $n > 2$, by a cyclic group of order q , constructed via the field multiplication, where p, q are distinct primes, $q \mid p^n - 1$ but $q \nmid p^m - 1$ for $1 \leq m < n$. Then, G has the basis property. Moreover in this case V has no H -invariant proper subgroups. In such a group G we have $sg(G) = ig(G) = 2$, but $sg(V) = ig(V) = n > 2$. So neither ig nor sg can be monotone.*

Example 2.15. Assume that $|V| = 2^3$ and $|H| = 7$. Then, by Proposition 2.13, G has the basis property. In this group, according to the above lemma, $sg(G) = ig(G) = 2$, but $sg(V) = ig(V) = 3$.

Example 2.16. Assume that $|V| = 2^5$ and $|H| = 31$. Then, by Proposition 2.13, G has the basis property. In this group, according to the above lemma, $sg(G) = ig(G) = 2$, but $sg(V) = ig(V) = 5$.

Example 2.17. Assume that $|V| = 2^6$ and $|H| = 7$. Then, by Proposition 2.13, G has the basis property. Now C_7 is a subgroup of units of the field $K = \mathbb{F}_8$, hence V is a 2-dimensional space over K . In this group, according to the above lemma and earlier results, $sg(G) = ig(G) = 3$, but $sg(V) = ig(V) = 6$. However, if $|H| = 3$ then V is a 4-dimensional vector space over the field \mathbb{F}_4 . Hence, $ig(G) = 5$ and $ig(V) = 6$.

Question. Let $2 \leq m < n < \infty$. Does there exist a group G with the basis property, such that: $ig(G) = m$, $ig(N) = n$ for a subgroup $N \leq G$ and $ig(L) \leq n$ for every subgroup $L \leq G$?

3. Lattices of subgroups

In this section we express properties discussed in previous section in terms of finite lattices, usually L . For details on such lattices one can see [6, 16]. If $a \in L$ then the ideal \hat{a} generated by $a \in L$ is equal to

$$\hat{a} = \{x \in L : x \leq a\} = [0, a].$$

Considered lattices are finite. Hence we have the following simple observation.

Proposition 3.1. *The embedding $a \rightarrow \hat{a}$ is an isomorphism of our lattice L onto the lattice of all ideals of L .*

This observation helps to interpret some notions natural for ideals in terms of elements of the lattice and we will do this here. As in [7] denote by $rad(L)$ the radical of L , the meet of all maximal elements of L . If $rad(L) = r$ then the ideal \hat{r} is the set of all nongenerators of L as an ideal.

An element $a \in L$ will be named a *d-element* if the ideal \hat{a} is a distributive lattice. Let a_1, a_2, \dots, a_n be a set of d-elements. We call this set *d-independent* if for every $1 \leq k \leq n$ we have:

$$(3.1) \quad a_1 \vee \dots \vee a_{k-1} \vee a_{k+1} \vee a_{k+2} \vee \dots \vee a_n \vee rad(L) \neq \bigvee_{j=1}^n a_j \vee rad(L).$$

Every subset X of d-elements of L will be called a *d-covering* of L if $\bigvee X = 1$; If X is a d-covering which is also d-independent, then X will be called a *d-base* of L . There are, even very small lattices having no d-covering and hence no d-base.

Our favorite lattice will be $L(G)$, the set of all subgroups of a group G , ordered by inclusion. It is visible, that $rad(L(G)) = \Phi(G)$. Since $L(G)$ is finite then, by Proposition 3.1, every ideal in $L(G)$ is of the form $\hat{H} = L(H)$, where $H \leq G$ is a subgroup. $L(C)$ is distributive for every cyclic group C . Hence we have:

Proposition 3.2. *If G is a group then the lattice $L(G)$ has a d-covering.*

Our crucial argument will be the following result of O. Ore:

Theorem 3.3 ([16]). *The subgroup lattice of a group G is distributive if and only if G is cyclic.*

As a consequence we obtain:

Theorem 3.4. *Let G be a group. If $X = \{x_1, \dots, x_n\}$ is a g -base of G , then $\widehat{X} = \{\hat{x}_1, \dots, \hat{x}_n\}$ is a d -covering of $L(G)$. Conversely, if $\{L(H_1), \dots, L(H_n)\}$ is a d -covering of $L(G)$, then for every $i \in \{1, \dots, n\}$ there exists $a_i \in H_i$ such that $\{a_1, \dots, a_n\}$ is a g -base of G .*

Using the above theorem one can adapt the results of the previous section concerning g -independence and g -bases of groups to the d -independence and d -coverings of lattices of subgroups, and conversely.

REFERENCES

- [1] A. Aljouiee and F. Alrusaini, Matroid groups and basis property, *Int. J. Algebra*, **4** (2010) 535-540.
- [2] Y. Berkovich, Groups of Prime Power Order, Vol. 1, *Walter de Gruyter*, Berlin, 2008.
- [3] H. U. Besche, B. Eick and E. A. O'Brien, A millenium project: constructing small groups, *Internat. J. Algebra Comput.*, **12** (2002) 623-644.
- [4] E. Crestani and F. Menegazzo, On monotone 2-groups, *J. Group Theory*, **15** (2012) 359-383.
- [5] D. Gorenstein, Finite Groups, *Chelsea Publishing Company*, New York, 1980.
- [6] G. Grätzer, *General Lattice Theory*, Birkhäuser Verlag, Basel, 1998.
- [7] P. Grzeszczuk and E. R. Puczyłowski, A radical of lattices and its applications to rings and modules, *Contributions to General Algebra*, **9** (1995) 203-212.
- [8] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1983.
- [9] P. R. Jones, Basis properties for inverse semigroups, *J. Algebra*, **50** (1978) 135-152.
- [10] G. Malle, J. Saxl and T. Weigel, Generation of classical groups, *Geom. Dedicata*, **49** (1994) 85-116.
- [11] A. Mann, The number of generators of finite p -groups, *J. Group Theory*, **8** (2005) 317-337.
- [12] J. McDougall-Bagnall and M. Quick, Groups with the basis property, *J. Algebra*, **346** (2011) 332-339.
- [13] W. Narkiewicz, *Number Theory*, World Scientific Publishing Co., Singapore, 1983.
- [14] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1995.
- [15] R. Scapellato and L. Verardi, Bases of certain finite groups, *Ann. Math. Blaise Pascal*, **1** (1994) 85-93.
- [16] R. Schmidt, *Subgroup Lattices of Groups*, Walter de Gruyter, Berlin, 1994.
- [17] J. Whiston, On the maximal size of independent generating sets of the symmetric group, *J. Algebra*, **232** (2000) 255-268.

Jan Krempa

Institute of Mathematics, University of Warsaw, Banacha 2, 02-097 Warszawa, Poland

Email: jkrepma@mimuw.edu.pl

Agnieszka Stocka

Institute of Mathematics, University of Białystok, Akademicka 2, 15-267 Białystok, Poland

Email: stocka@math.uwb.edu.pl