THE CHARM OF ELEMENTARY GROUP THEORY

MARIAN DEACONESCU

Communicated by Lucian Beznea

This material surveys about twenty results in Group Theory. They are quite general, their proofs are not very technical and some are rather surprising. They are collected here to illustrate the beauty of elementary Group Theory.

AMS 2010 Subject Classification: 20-02, 20D45, 20D60, 20D25, 20E34, 20F12, 20F45.

Key words: group actions, affine actions, automorphisms, orbits, fixed points, commutators.

1. INTRODUCTION

This is a survey type material containing a presentation of a few of my own favorite elementary results in Group Theory. They were found during the past 20 years or so and they are the outcome of work I have done mostly as a member of a team or another of co-authors.

One may consider a group-theoretical result to be elementary if its proof is as close to first principles as reasonably feasible. Results with proofs using deep theorems like the CFSG (this stands for the Classification of the Finite Simple Groups) or the Odd Order Theorem can hardly be seen as elementary. The statement itself might sometimes be viewed as elementary if it involves simple, familiar concepts as commutativity, order of elements, commutators, automorphisms etc. All group theory texts contain a healthy dose of elementary results simply because some (as for example Lagrange's theorem, the isomorphism theorems etc.) are unavoidable, while others have short proofs that illustrate essential techniques.

Elementary Group Theory, whatever it might mean, is similar to elementary Number Theory in one respect: conceptual proofs, using few calculations, are quite common and this creates a powerful impression of beauty and elegance. Two good sources of elementary results are the classic group theory texts and the work of the old masters.

The term *elementary* corresponds to a subjective concept which depends on context and level of expertise. The larger context for the stated results is

presented here, for it has the rôle of the out of focus background on which the main crisp subject is projected.

Throughout this paper G stands for "group". When G appears in text or in a statement with no qualification, it means that G is an arbitrary group.

2. A DROP OF ORDER IN A CUP OF CHAOS

Let G be finite and let $S(G)$ denote the lattice of all subgroups of G. This is a complete lattice with a quite irregular structure. For example, an open question is if the number of maximal subgroups of G, i.e. of the dual atoms of $S(G)$ is less than or equal to $|G| - 1$. The lattice $S(G)$ is not modular in general and a classic result of Ø. Ore states that $S(G)$ is distributive if and only if G is cyclic.

The Frattini subgroup of G is the intersection $\Phi(G)$ of all maximal subgroups of G. For a subgroup H of G one considers the intersection $H_\circ$ of all maximal subgroups of G not containing H. It is plain that $\Phi(G) \leqslant H_\circ$ for every $H \in S(G)$. The subgroup generated by H and $H_\circ$ might or might not be equal to G and this leads to considering the subset $L(G)$ of $S(G)$ whose elements are the subgroups H of G with the property that $\Phi(G) \leqslant H$ and $G = \langle H, H_\circ \rangle$. When G is a nontrivial finite group the set $L(G)$ contains at least two elements, namely $\Phi(G)$ and G. For many finite groups G the set $L(G)$ consists only of $\Phi(G)$ and G - this happens whenever $G/\Phi(G)$ is simple. However, $L(G)$ could be large; in fact, $L(G)$ is largest possible when $L(G)$ equals the set of all subgroups of G containing $\Phi(G)$ and this happens precisely when G is cyclic.

The surprising fact is that $L(G)$ has very regular properties – see [4] for details.

THEOREM 1. *If G is finite, then $L(G)$ is a sub-lattice of $S(G)$, it consists of characteristic subgroups of G and it is a Boolean algebra.*

Theorem 1 says that the "wild" lattice $S(G)$ of a finite group G contains a generic sub-lattice (which is defined canonically) which can be seen as a sort of a core of crystalline order. The algebraic structure of G gets more regular as $L(G)$ gets larger. For example, when G is a finite nilpotent group the elements of $L(G)$ are the pre-images in G of the Hall subgroups of the factor group $G/\Phi(G)$.

3. A CURIOUS GENERIC SECTION

A homomorphic image of a subgroup of G is called a section of G. In particular, if $H \triangleleft K \triangleleft G$ then K/H is a section of G. In the preceding situation, if both H and K are *generic* subgroups of G, i.e. they are defined in terms of G for any abstract group G, one may say that the section K/H is a generic section of G. For example, if $Z(G)$ is the center of G and $Z_2(G)$ is the second center of G, the section $Z_2(G)/Z(G)$ is a generic section of G.

Let $R_2(G)$ be the set of all elements $g \in G$ satisfying $xx^g = x^g x$ for every $x \in G$. The fact that $R_2(G)$ is a subgroup of G came as a surprise, as it was published in 1961 by W. Kappe in [10]. The group $R_2(G)$ is called the group of right 2-Engel elements of G; it is a characteristic subgroup of G and it contains $Z_2(G)$. If G' denotes the commutator subgroup of G, i.e. the subgroup of G generated by the commutators $[x, y] := x^{-1}y^{-1}xy$ where $x, y \in G$, then $Z_2(G)$ is also contained in the centralizer $C_G(G')$ of G' in G. The factor group $E(G) := \frac{R_2(G) \cap C_G(G')}{Z_2(G)}$ is thus a generic section of the abstract group G and can be regarded as an invariant of G.

A group G is a torsion group (a periodic group) if every element of G has finite order. Some of the torsion groups have the property that the orders of their elements are bounded by a maximum value, say n. This means that $x^n = 1$ for every $x \in G$ and that n is the smallest positive integer with this property. In this case we call n the exponent of G and we write $n = exp(G)$.

The next result from [1] is surprising because it shows that all groups have a generic section of very restricted structure.

THEOREM 2.

$$exp(E(G)) \leq 2.$$

Very often $E(G) = 1$ and in this case $R_2(G) \cap C_G(G') = Z_2(G)$. This happens, for example, when G is a finite group of odd order. When $E(G) \neq 1$, then $E(G)$ is a (possibly infinite) elementary abelian 2-group. The proof of Theorem 2 relies on commutator calculations and it is thus elementary.

4. AFFINE ACTIONS

Things are getting more abstract here, so this is a good place to introduce some general notation. When S is a finite non-empty set and A is a group acting on the set S, the number $t_A(S)$ will denote the number of orbits of A in S. For $s \in S$ the notation $O_A(s)$ is used for the orbit $\{s^a \mid a \in A\}$ of s under the action of A. For a subset T of S one considers the subgroup $N_A(T)$ of A consisting of all elements of A that leave T invariant and the subgroup $C_A(T)$

of A consisting of those elements of A that fix T element-wise and note that $C_A(T)$ is a normal subgroup of $N_A(T)$.

If G, A are groups and if $f : A \to Aut(G)$ is a group morphism, the image $f(A)$ is a subgroup of $Aut(G)$ and acts naturally on G as a group of automorphisms. In this situation we say that A acts on G via automorphisms. And so, by a slight abuse of language, when we say that A acts on G via automorphisms we actually refer to the action of $f(A)$ on G. The typical situation is that of G acting via conjugation on a normal subgroup H of G.

In all results presented in the sequel about fixed points and orbits one can replace $A \leqslant Aut(G)$ with A acts on G via automorphisms and the conclusions are preserved. The statements are cast here in automorphism groups terms for the sake of simplicity.

If V is a K-vector space the semi-direct product $[V]GL(V)$ with respect to the natural action of $GL(V)$ on V is called the affine group of V. As it happens, this definition is a particular case of a more general one that works for arbitrary groups. What is interesting is that one obtains a whole class of such general affine actions and that the whole story is related to a class of measures in the particular case of finite groups.

One starts with an arbitrary group G and with an arbitrary subgroup $A \leqslant Aut(G)$. For $g \in G$ and for $a \in A$ write $[g, a] := g^{-1}g^a$ where g^a is the image of g under the automorphism a. In this situation it is customary to write $g^{ab} := (g^a)^b$ for $a, b \in A$. Suppose that H is an A-invariant subgroup of G, that is, $[h, a] \in H$ for all $h \in H$ and all $a \in A$. Such A-invariant subgroups of G are in great supply in general. For if H is a subgroup of G, then the intersection of all images H^a for a running over A, denoted by $core_A(H)$, is clearly A-invariant.

Since H is A-invariant, A acts on H via automorphisms and one considers the semi-direct product $X = [H]A = A[H] = \{(a, h) \in A \times H\}$ endowed with the group operation defined by $(a, h)(b, k) := (ab, h^b k)$ for $a, b \in A$ and $h, k \in H$. The next observation is that the group X acts on the whole group G in a natural way. Indeed, for $g \in G$ and for $(a, h) \in X$, we let $g^{(a,h)} := g^a h$. It is easy to check that this is indeed an action of X on G, albeit not an action via automorphisms. It is also clear that the orbit $O_X(g)$ of $g \in G$ under the action of X is just $O_A(g)H$.

When A consists only of the identity automorphism id_G of G this is denoted by $A = 1$. In this particular case of $A := 1$ and taking $H := G$ as the A-invariant subgroup in the above construction we get Cayley's right regular representation: $x^{(1,h)} := xh$ for all $g, h \in G$.

It is only natural to call this action of X on G an affine action – it depends, of course, on the choice of A and H. As we will see, this affine action

has interesting applications when the group G is finite.

Let $C(G,A)$ denote the set of all commutators $[g,a]$ for $g \in G$ and $a \in A$ and let $[G,A] := \langle C(G,A)\rangle$. A natural question related to the action of A on G is to determine, for $g \in G$ whether $g \in C(G,A)$. This is a difficult problem in general even when A is a nice group of automorphisms. There is no doubt that the most important subgroup of $Aut(G)$ is the group $Inn(G)$ of the inner automorphisms of G, consisting of the maps $T_g : G \to G$ defined by $x^{T_g} := g^{-1}xg$ for every $x \in G$. In this case, for $x \in G$ and for $T_g \in Inn(G)$ the element $[x,T_g] = [x,g] = x^{-1}g^{-1}xg$ is the usual commutator of x and g.

From now on G will denote in this section a *finite* group. In this particular case and for $g \in G$ one can define $m(g)$ to be the number of ordered pairs $(x,y) \in G \times G$ such that $g = [x,y]$. Of course, $m(g) > 0$ if and only if $g \in C(G) = C(G, Inn(G)) = \{[x,y] \mid x,y \in G\}$. The precise value of $m(g)$ was calculated by Frobenius as a sum in terms of characters and it is a nice exercise to show that $m(g)$ is a multiple of the order of the centralizer $C_G(g)$ of g in G. No general expression is known for $m(g)$ apart from that found by Frobenius; the only exception is the trivial element 1, for $m(1) = |G|k(G)$, where $k(G)$ is the number of conjugacy classes of G.

The preceding remarks suggest to define, for a finite group G, a subgroup A of $Aut(G)$ and for $g \in G$ the number $m_A(g) := |\{(a,x) \in A \times G \mid g = [x,a]\}|$. Then $g \to m_A(g)$ is a measure on G and if S is a subset of G one defines $m_A(S)$ to be simply the sum of the measures of all elements in S. It should be clear that $m_A(G) = m(C(G,A)) = |G||A|$ and that for a subset S of G we have $m_A(S) = |G||A|$ if and only if $C(G,A) \subseteq S$.

So, for an arbitrary finite group G, and for an arbitrary subgroup A of $Aut(G)$ we have a measure (depending on A) on G. If H is an A-invariant subgroup of G, then A is acting on the set $G/H = \{xH \mid x \in G\}$ via $(xH)^a := x^aH$ with a number $t_A(G/H)$ of orbits. All of the above are now coming together in a surprising way, linking affine actions with number of orbits and with measures. The next theorem is the only new result presented here; it gives the natural general framework for the consequences in this section.

THEOREM 3. *Let G be finite, let $A \leqslant Aut(G)$, let H be an A-invariant subgroup of G and let $X = [H]A$ act naturally on G. Then*

$$t_X(G) = t_A(G/H) \text{ and } |X|t_X(G) = m_A(H).$$

The second equality appears in [6], being proved by using the Cauchy-Frobenius lemma. The first equality is left as an exercise to the reader.

Theorem 3 has several direct consequences. The first gives the exact number of commutators contained in a normal subgroup of a finite group.

Recall that if G is finite the number $k(G)$ is the number of conjugacy classes of G.

COROLLARY 1. *If G is finite and if H is a normal subgroup of G, then the number of ordered pairs $(x, y) \in G \times G$ with $[x, y] \in H$ equals $|H||G|k(G/H)$.*

Another consequence gives a characterization of the finite abelian groups in terms of numerical invariants.

COROLLARY 2. *If G is finite, then $|G|k(\Phi(G)) \geq k(G)|\Phi(G)|$ and equality holds if and only if G is abelian.*

The characterization of the finite groups of nilpotency class at most two given in [7] uses similar numerical invariants.

COROLLARY 3. *If G is finite, then*

$$|Z_2(G)| \leq |\Phi(G)|k(G/\Phi(G))$$

and the equality holds if and only if $G = Z_2(G)$.

It is well known that if G is a finite group and if χ is an irreducible complex character of G then the kernel of χ, i.e. the set of all elements $g \in G$ with the property that $\chi(g) = \chi(1)$, is a normal subgroup of G. Moreover, every normal subgroup of G is the intersection of certain such kernels. The next consequence from [7] is not elementary because it uses characters. However, it has a strong combinatorial flavour and the proof uses only rudiments of character theory.

COROLLARY 4. *If G is finite and if H is the intersection of more than half of the kernels of complex irreducible characters of G, then every element of the normal subgroup H is a commutator in G.*

If H, K are subgroups of G it is a natural question to ask whether the set $C(G)$ of all commutators in G is contained in the union $H \cup K$. This is certainly a nontrivial question, for it is well-known that $C(G)$ is not always a subgroup of G. Also, assuming that $C(G)$ is contained in the said union, another question is to decide if $C(G)$ is contained either in H or in K. Of course, the answer to this second question is affirmative when $C(G) = G'$.

More generally, consider two subgroups H, K of G, a subgroup A of $Aut(G)$ and the set $C(G, A) = \{[g, a] \mid g \in G, a \in A\}$. When is $C(G, A)$ contained in $H \cup K$? And, if $C(G, A) \subseteq H \cup K$ is it true that $C(G, A)$ is contained in either H or K? When G is finite a definitive answer to the last question is given in [8].

COROLLARY 5. *If G is finite and $A \leqslant Aut(G)$, let H, K be subgroups of G with $X = core_A(H)$ and $Y = core_A(K)$. Then*

$$|G| \geq |X|t_A(G/X) + |Y|t_A(G/Y) - |X \cap Y|t_A(G/(X \cap Y))$$

and the equality holds if and only if either H or K contains $[G, A]$.

Results similar to the second part of Corollary 5 are obtained in [8] for the more general case of periodic groups.

5. **ON FIXED THINGS**

Let $A \leqslant Aut(G)$. Two A-invariant subgroups of G are important in what follows. The first is the subgroup $C_G(A)$ of all elements of G fixed by all elements of A and the second is the subgroup $[G, A]$ generated by all the commutators $[g, a]$ for $g \in G$ and all $a \in A$. The subgroup $[G, A]$ is also a normal subgroup of G. When $A := Inn(G)$ we have $C_G(Inn(G)) = Z(G)$ is the center of G and $[G, Inn(G)] = [G, G] = G'$ is the commutator subgroup of G.

One good source of general elementary results is to look at the pair (G, A) where G is an arbitrary group and A is an arbitrary subgroup of $Aut(G)$. There is a fascinating interplay between the structure of G and that of its group of automorphisms $Aut(G)$; the study of the pair $(G, Aut(G))$ was in full swing at the beggining of the twentiest century and theorems by O. Hölder, W. Burnside, P. Hall are elegant classic gems included in most of the serious group theoretical texts.

There is an extensive literature studying the situation where $a \in Aut(G)$ and a is fixed-point-free, i.e. $C_G(a) = 1$. The most well-known result is a theorem of J.G. Thompson (formerly a conjecture of Frobenius) asserting that if G is finite and a is fixed-point-free automorphism of prime order, then G is nilpotent. If the prime order condition is dropped, the finite group G is not necessarily nilpotent and when the order of a is 2 a theorem of W. Burnside states that G is abelian and of odd order.

If X is a finite group, let $F(X)$ denote the Fitting subgroup of X, i.e. the largest normal nilpotent subgroup of X. The next result shows that all non-abelian finite groups have a common property.

THEOREM 4. *If G is finite and nonabelian and if $a \in Inn(G)F(Aut(G))$, then $C_G(a) \neq 1$.*

In fact, as shown in [3], the only finite groups G admitting a fixed-point-free automorphism in the Fitting subgroup of $Aut(G)$ are either abelian of odd order or direct products of an abelian group of odd order and the Klein group with four elements. This can be viewed as a far reaching generalization of the mentioned theorem of Burnside.

Here is an interesting question: can we say something nontrivial about all groups with at least three elements? Three is important here because if $|G| \geq 3$ then $Aut(G)$ is non-trivial. The answer if affirmative and it involves such a group G and a subgroup A of $Aut(G)$ such that $Inn(G) \leqslant A$.

One constructs the semi-direct product $AG = GA$. The elements of AG are pairs $(a, x) \in A \times G$ and the multiplication is given by $(a, x)(b, y) := (ab, x^b y)$. The essential observation appears in the particular case of $A = Aut(G)$ in [11] and it is mentioned there in passing as if being well-known; I wish to thank E. Wilcox for mentioning that bibliographical source to me.

It is easy to check that the map $t : AG \to AG$ defined by $(a, x)^t := (aT_x, x^{-1})$ is in fact an automorphism of AG. It is also easy to see that t fixes both A and $\Omega_1(Z(G))$ and this means that whenever G is not an elementary abelian 2-group then t is an automorphism of AG of order 2. In the case when G is an elementary abelian 2-group, AG still has an automorphism of order 2, namely the inner automorphism of AG induced by an involution of G.

There are infinitely many examples of finite p-groups G (where p is an odd prime) such that $Aut(G)$ is also a p-group. Therefore it is not true that every group of order at least 3 has an automorphism of order 2. The next result gives a very large class of groups having a canonical automorphism of order 2. Here canonical means that the image of every element is given by a formula depending only on the element itself. A famous and very important example of a canonical automorphism of order 2 is $x \to x^{-1}$ where $x \in G$ and G is a free abelian group. And of course, when G is non-abelian, the inner automorphisms of G are canonical, too.

THEOREM 5. *If G is a group with at least 3 elements and if $Inn(G) \leqslant A \leqslant Aut(G)$, then the group AG has a canonical automorphism of order 2.*

There exists a large collection of results of the following type: if G is a group, if $A \leqslant Aut(G)$ and if one knows something about A and $C_G(A)$, then something is said about the structure of G. Conditions like $(|G|, |A|) = 1$ and/or $C_G(A) = 1$ are frequently present and sometimes extra conditions on A are also imposed. And so, one may ask if anything general and nontrivial can be said about the action of $A \leqslant Aut(G)$ on G.

The first remark has to do with the affine action in section 3. If G is a group , and if $A \leqslant Aut(G)$, let $F := C_G(A)$ denote the subgroup of the fixed points of A in G. Then clearly F is A-invariant and so $X = AF = FA$ acts on G as indicated in Theorem 3. Moreover, if $O(G, A)$ is the set of all orbits of A in G, then F acts on the set $O(G, A)$ in the following manner: if $O_A(g) \in O(G, A)$ and if $f \in F$, we let $(O_A(g))^f := O_A(g)f = O_A(gf)$. This means that F permutes the orbits of A in G. The stabilizer $S_F(O_A(g))$ of the

orbit $O_A(g)$ is seen to be $F \cap g^{-1}O_A(g)$ and therefore it is a subgroup of F. On the other hand, it is isomorphic to the factor group $N_A(gF)/C_A(gF)$, which is a section of A.

The following result holding for arbitrary G was obtained in [2].

THEOREM 6. *Let $A \leqslant Aut(G)$ and $F = C_G(A)$. For every $g \in G$*

$$F \cap g^{-1}O_A(g) \cong N_A(gF)/C_A(gF).$$

Theorem 6 is quite powerful when G is *finite,* because the action of F on the orbits of A in G sends an orbit to an orbit *of the same length.* M. Isaacs found in [9] the following very general consequence.

COROLLARY 6. *If G is finite and if $A \leqslant Aut(G)$, then the number of orbits of A in G is a multiple of the order of the factor group $C_G(A)[G, A]/[G, A]$.*

Corollary 6 says nothing when $C_G(A)$ is contained in $[G, A]$, but the next consequence, also from [9], is surprising indeed.

COROLLARY 7. *Let G be finite with a prime number p of conjugacy classes and suppose that the center of G is not contained in the commutator subgroup of G. Then $|G| = p$.*

Another application of Theorem 6 concerns the finite p-groups. When p is a prime and G is a finite p-group it is not uncommon to have $(p, k(G)) = 1$. For example, both non-abelian groups of order 8 have 5 conjugacy classes. In this situation one can say something non-trivial.

COROLLARY 8. *If G is a finite p-group and if $(p, k(G)) = 1$, then every element of $Z(G)$ is a commutator in G.*

A few more consequences may be found in [2] and if one applies Theorem 6 in the holomorph of a finite group as was done in [5] one obtains a surprising property of automorphisms of finite groups. Let G be finite and let $a \in Aut(G)$. If H is an a-invariant normal subgroup of G, then a induces naturally an automorphism of the factor group G/H, which is denoted, by abuse of language, also by a. The fact is that the fixed point subgroups $C_G(a)$ and $C_{G/H}(a)$ are known to be feebly related, in the sense that $|C_G(a)| \geq |C_{G/H}(a)|$. When $H := Z = Z(G)$, however, one can say much more: in fact, $|C_{G/Z}(a)|$ divides $|C_G(a)|$. I am stating here the most important particular case of a result in [5].

THEOREM 7. *Let G be finite, let $Z := Z(G)$, let $a \in Aut(G)$ and let $Z_a := Z \cap \{[g, a] \mid g \in G\}$. Then*

$$|C_G(a)| = |C_{G/Z}(a)||Z : Z_a|.$$

Easy examples show that Theorem 7 is no longer true if one takes some other characteristic subgroup of G in place of the center $Z(G)$ and this shows the special rôle the center plays among the generic subgroups of G.

Since the holomorph $H := [G]Aut(G)$ was mentioned above, I mention here a surprisingly simple application of the holomorph to a 100 years old open problem. It is well-known that finite cyclic groups have abelian automorphism groups and that finite abelian noncyclic groups have non-abelian automorphism groups. More than 100 years ago, G. A. Miller produced an example of a finite nonabelian p-group G with $Aut(G)$ abelian. Infinitely many examples were constructed over the years (they must all be nilpotent of class two) but no classification is in sight. Consider the holomorph $H = AG$ where $A = Aut(G)$ and observe that both subgroups G and A of H act on H via conjugation. If one denotes by $t_G(H)$ the number of G-orbits on H and by $t_A(H)$ the number of A-orbits on H, then (by applying the Cauchy-Frobenius lemma three times) one obtains the characterization in [5].

THEOREM 8. *Let G be finite, let $A := Aut(G)$ and let H be the holomorph of G. Then $t_G(H) \geq t_A(H)$ and the equality holds if and only if $Aut(G)$ is abelian.*

Theorem 8 is just another good example of a general inequality involving invariants. The extreme (equality) case is again characterizing an interesting class of finite groups. This seems to be the case in group theory and it was one of the main reasons for looking for general inequalities. Recall that what I call the Cauchy-Frobenius lemma is what used to be called "Burnside's lemma" - it involves the number of orbits and fixed points for the action of a group on a finite set.

Returning to the main theme of this section, which is fixed points, consider again a finite group G, a subgroup A of $Aut(G)$ and the subgroup $F = C_G(A)$ of the fixed points of A in G. We have seen that F acts naturally on the set of orbits of A in G. Another consequence of that action is a surprising property of the order of F which was established in [6]. The proof given there by G. Walls is surprisingly short.

THEOREM 9. *Let G be finite, let A be a subgroup of $Aut(G)$ and let $F := C_G(A)$. Let T be a set of representatives for the orbits of A in G. Then, for every positive integer k,*

$$|F| \mid \sum_{x \in T} |O_A(x)|^k.$$

Of course, Theorem 9 says nothing when $F = C_G(A) = 1$. Note, however, that very often $F \neq 1$ and in this case there exists at least one prime p which

divides $|F|$. As an application, let in Theorem 9 $A := Inn(G)$, $F := Z(G)$ and $k = p - 1$ to get the following consequence.

COROLLARY 9. *Let G be finite and let p be a prime dividing $|Z(G)|$. Then the number of conjugacy classes of G whose length is co-prime to p is a multiple of p.*

So, as we see, F has a significant influence on the number $t_A(G)$ of the orbits of A in G. And then one may ask if the converse is also true, that is, if having information on $t_A(G)$ can be translated somehow into information on $C_G(A)$. As a case in point, suppose that G is finite, that $A \leqslant Aut(G)$ and that $t_A(G)$ is odd. This is not a strong condition. For it is trivial to show that if $|G|$ is odd, then $k(G)$ is odd too and there exist many other finite groups of even order with an odd number of conjugacy classes. And after all, $t_A(G)$ is either odd or even. The following was established in [8].

THEOREM 10. *Let G be finite, let $A \leqslant Aut(G)$ and suppose that $t_A(G)$ is odd. Suppose that H is a normal subgroup of G and that A acts trivially on H, i.e. $H \leqslant C_G(A)$. Then either $|H/Z(H)|$ is odd, or $Z(H) \neq 1$.*

The condition that H is a normal subgroup of G is a strong one. However, the situation when a subgroup of $Aut(G)$ acts trivially on some normal subgroup is very common indeed - one just have to take a look at group cohomology.

The deep Odd Order Theorem of W. Feit and J.G. Thompson states that groups of odd order are solvable. Combining it with Theorem 10 it follows that if the finite group G has a nontrivial minimal normal subgroup H acted upon trivially by some subgroup of $Aut(G)$ that has an odd number of orbits in G, then H must be an elementary abelian p-group for some prime p. This very particular application is yet another illustration of the connection between orbits and fixed points of group automorphisms.

6. KRUTIK SETS AND A LEMMA OF BURNSIDE

Few things are more rewarding than extending a result of an old master and the reason is that the result must be itself old. One such old result is a well-known lemma of W. Burnside, stating that if G is finite, if P is a Sylow p-subgroup of G and if x, y are elements of $C_G(P)$ that are conjugate in G, then they are conjugate in $N_G(P)$.

This situation is described shortly by saying that $N_G(P)$ controls G-fusion in $C_G(P)$ and it refers to the action of G on G via conjugation. This gives the

impression that Burnside's result is a property of the *base group* G while, in fact, it is a property of the *acting group* G.

To substantiate the last claim, consider a finite non-empty set S, a finite group A acting on S and a non-empty subset X of S. If X is not A-invariant, there exists some $x \in X$ and some $a \in A$ such that $x^a \notin X$ and this suggests considering the subset $K_A(x, X) := \{a \in A \mid x^a \in X\}$. Let's call $K_A(x, X)$ a *Krutik set.* Thus, a Krutik set is a subset of A and it depends, of course, on the choice of x in S and of the subset X containing x.

Another notion related to the above situation is that of fusion control. Let's say that a subgroup B of A controls A-fusion in X if whenever $x^a \in X$ for $a \in A$ and $x \in X$ there exists $b \in B$ such that $x^a = x^b$. Given a subset X of S it is important in many situations to determine a *minimal* subgroup of A that controls A-fusion in X. Stated in these very general terms, this is clearly an impossible task. However, this can be done for at least one special choice of X, which was suggested by Burnside's lemma – see [6] for a short proof.

THEOREM 11. *Let S be a finite non-empty set and let A be a finite group acting on S. Let P be a Sylow p-subgroup of A and suppose that the set $C_S(P)$ of elements of S fixed by all elements of P is not empty. Then, $N_A(P)$ controls A-fusion in $C_S(P)$, $N_A(C_S(P)) = C_A(C_S(P))N_A(P)$ and for every $x \in C_S(P)$ we have $K_A(x, C_S(P)) = C_A(x)N_A(P)$.*

In the above statement, $N_A(P)$ is the normalizer of P in A and $C_A(x)$ is the subgroup of those elements of A fixing x. If one looks at the statement, the only condition that is there is that P fixes at least one element of S. This is not a very strong condition: because the order of P is a p-power, $C_S(P)$ is non-empty whenever $(|S|, p) = 1$. And, of course, if S itself is a group and if $A \leqslant Aut(G)$ acting naturally on S, then again $|C_S(P)| \geq 1$. Theorem 11 shows clearly that this control of fusion is about the group A that is acting on the set S.

Similarly, if G is finite if P is a Sylow p-subgroup of G and if A is a finite group acting via automorphisms on G, then $N_A(P) = N_A(N_A(P))$. The well-known equality $N_G(P) = N_G(N_G(P))$ obscures the fact that this happens in the group $A := G$ that acts on G via conjugation.

7. SOME OPEN QUESTIONS

Group Theory thrives through the plethora of elegant open problems. Their statements look deceptively simple and that adds to their appeal.

I start with an open question about commutators in finite groups posed by Des MacHale.

QUESTION 1. *If G is finite and if exactly one element of G is not a commutator, is it true that $|G| = 2$?*

This is one of my favorite open questions; the surprise element is in the fact that, if true, a group-theoretical property singles out just *one group*.

An older open question was proposed by L. Kazarin.

QUESTION 2. *Let G be finite such that $G = AB$ where A and B are subgroups of G of co-prime order. Is it true that $k(G) \leq k(A)k(B)$?*

Very similar to the above is a question of L. Pyber. If G is a finite group, let G^+ be the direct product of copies of the Sylow p-subgroups of G, one for each prime dividing $|G|$. Pyber was asking the following.

QUESTION 3. *If G is finite, is it true that $k(G) \leq k(G^+)$?*

Another elegant question was posed by A. Mann.

QUESTION 4. *Is it true that the dihedral group of order 8 is the only finite non-trivial p-group isomorphic to its own automorphism group?*

I have, of course, several open problems and questions of my own. The first is a nice pendant for MacHale's question and I like to call it "poor man's Odd Order Theorem". The important Odd Order Theorem asserts that if G is non-trivial and of odd order, then $G' \neq G$ and thus a lot of elements in G are not commutators.

PROBLEM 1. *If G is non-trivial and of odd order, find an elementary proof to show that there exists an element in G that is not a commutator in G.*

The mentioned result of Frobenius saying that the number of pairs $(a, b) \in G \times G$ with $[a, b] = 1$ is equal to $|G|k(G)$ is suggesting a more complicated problem. Recall that $[x, y, z] := [[x, y], z]$ and solve the following.

PROBLEM 2. *If G is finite, find the number of triples $(a, b, c) \in G \times G \times G$ such that $[a, b, c] = 1$.*

The next open question is suggested by the finite dihedral groups.

QUESTION 5. *If G is finite and at least half of the elements in G have the same order, is it true that G solvable?*

When G is finite and s is an integer such that $(s, |G|) = 1$, the map sending $g \in G$ to g^s is clearly a permutation of the set G and it is clear that this map commutes with all automorphisms of G. Since $Aut(G)$ is clearly a subgroup of the group S_G of all permutations of the set G, the next question makes sense:

QUESTION 6. *What can be said about $C_{S_G}(Aut(G))$ when G is finite?*

The terms of Question 6 are rather vague. In fact: can we say *anything* in general? For if we denote the group of those power maps by V, it is clear that both $Z(Aut(G))$ and V are contained in $C_{S_G}(Aut(G))$. It is of course possible for *some* finite groups G to have $C_{S_G}(Aut(G)) = VZ(Aut(G)$. These would be groups G with small such centralizers. But it is also conceivable that for some other groups G the preceding equality doesn't hold. This is, I guess, a typical problem that can be explored by using computational group theory packages. Another question involves the Frattini subgroup of $Aut(G)$.

QUESTION 7. *Let G be finite and let $a \in Aut(G)$. Determine conditions on the action of a on G to force $a \in \Phi(Aut(G))$.*

Back in 1990 M. Newman and J. Neubüser proposed to me to construct an automorphism with special properties. Let G be a 2-group with two generators, so $G/\Phi(G)$ is the Klein four group. This factor group has an automorphism a which permutes cyclically its three maximal subgroups. Sometimes, this automorphism a extends to an automorphism of the full group G (as in the case when G is the quaternion group of order 8) and sometimes it does not (as when G is the dihedral group of order 8). The natural problem suggested by these remarks was initially to classify the finite 2-groups with two generators having such a "crown automorphism" a which permutes all maximal subgroups of G in a cyclical manner. This was completely solved in the particular case of the finite 2-group G with two generators being also of nilpotency class maximum 2. Since the finite p-groups of class 2 with 2 generators are known, my impression is that the following problem poses only technical difficulties.

PROBLEM 3. *Classify all finite p-groups of nilpotency class maximum 2 and with two generators which have a crown automorphism (i.e. an automorphism permuting the maximal subgroups of G cyclically).*

Consider next the set of all automorphisms a of G satisfying the equality $xx^a = x^a x$ for all $x \in G$ and denote this set by $\mathcal{A}(G)$. Gh. Silberberg gave an example of a finite 2-group G for which $\mathcal{A}(G)$ is not a subgroup of $Aut(G)$. Theorem 1.3 of [1] shows that when $Z(G) = 1$ and $\mathcal{A}(G)$ is not reduced to the identity automorphism of G then $\mathcal{A}(G)$ is an elementary abelian 2-group.

An important subgroup of $Aut(G)$ is the centralizer $Aut_c(G)$ of $Inn(G)$ in $Aut(G)$. Since $a \in Aut_c(G)$ if and only if $[x, a] \in Z(G)$ for all $x \in G$, it follows that $Aut_c(G) = 1$ whenever $Z(G) = 1$. Corollary 1.4 of [1] states that

if $Aut_c(G) = 1$ then $\mathcal{A}(G)$ is a group of exponent at most 2. If true, this would be a generalization of the stated Theorem 1.3 of [1].

This is a good opportunity to make two corrections. E. Jabara discovered a long time ago that the first concluding remark of [1] is false. Also, M. Jafari discovered a gap in the proof of the Corollary 1.4 of [1] – thanks are due to both Enrico and Mohammed for the attention given to [1].

As M. Jafari observed, the proof given in [1] is not complete. It is shown there correctly that in the given conditions and for $a, b \in \mathcal{A}(G)$ one must have $a^2 = b^2 = [a, b] = 1$ – here 1 is the notation for the identity automorphism id_G. This shows that, if non-empty, the set of the nontrivial elements of $\mathcal{A}(G)$ is a set of commuting involutions in $Aut(G)$. And, unfortunately, this is not implying directly that $\mathcal{A}(G)$ is a subgroup of $Aut(G)$ as claimed in Corollary 1.4 of [1].

G. Walls informed me recently that if one imposes the additional condition that G' contains no involutions, then $\mathcal{A}(G)$ is indeed a subgroup of $Aut(G)$. This is because it is easy to check that for every $x \in G$ and every $a, b \in \mathcal{A}(G)$ we have $[x, x^{ab}]^2 = 1$. Consequently, if G' has no involutions, one obtains that if $a, b \in \mathcal{A}(G)$ then $ab \in \mathcal{A}(G)$. The general case is still open, so I mention it as an open question.

QUESTION 8. *Is it true that if $Aut_c(G) = 1$ then $\mathcal{A}(G)$ is a subgroup of $Aut(G)$?*

An interesting open problem has its origin in elementary Number Theory. It is easy to see that if n is an odd positive integer then every subgroup of the cyclic group C_n of order n is the fixed point subgroup of some $a \in Aut(C_n)$.

PROBLEM 4. *Classify all finite groups G with the property that for every subgroup H of G there exists some automorphism a of G such that $H = C_G(a)$.*

The last question in this section is probably the hardest. Consider a finite group G and a subgroup A of $Aut(G)$ such that A acts regularly on G. This means that $C_G(a) = 1$ whenever a is a non-trivial automorphism in A. In this situation it is easy to check that $|A|$ divides $|G| - 1$. The interesting question is if the converse is true when $A = Aut(G)$: if $|Aut(G)|$ divides $|G| - 1$, is it true that $Aut(G)$ acts regularly on G? As it turns out, this is just a translation into group-theoretical terms of a famous open 1932 problem of D.H. Lehmer: is it true that if $n > 1$ is an integer and if $\varphi(n)$ divides $n - 1$ then n is a prime?

QUESTION 9. *If G is finite and non-trivial and if $|Aut(G)|$ divides $|G| - 1$ is it true that $|G|$ is a prime?*

Acknowledgments. I was blessed to have M. I. Isaacs, and G.L. Walls as my co-authors and I thank them for their advice given to me over the years. Thanks are due to

Sorin Dăscălescu for the invitation to write this material and to Cezar Joiţa for his help in improving the quality of the manuscript. I am grateful to Kuwait University for a generous travel grant.

REFERENCES

[1] M. Deaconescu and G. L. Walls, *Right 2-Engel elements and commuting automorphisms of groups*. J. Algebra **238** (2001), 479–484.

[2] M. Deaconescu and G. L. Walls, *On the orbits of automorphism groups*. Siberian Math. J. **46** (2005), 413–416.

[3] M. Deaconescu and G. L. Walls, *On a theorem of Burnside on fixed-point-free automorphisms*. Arch. Math. (Basel) **90** (2008), 97–100.

[4] M. Deaconescu, I.M. Isaacs, and G.L. Walls, *A Boolean algebra of characteristic subgroups of a finite group*. Arch. Math. (Basel) **97** (2011) 17–24.

[5] M. Deaconescu and G. L. Walls, *Groups acting on groups*. Algebra and Logic **52** (2013), 387–391.

[6] M. Deaconescu and G. L. Walls, *Remarks on finite group actions*. Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **59 (107)** (2016), 225–231.

[7] M. Deaconescu and G. L. Walls, *Remarks on commutators in finite groups*. J. reine angew. Math. **732** (2017), 247–253.

[8] M. Deaconescu, *Three lemmas on commutators*. Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **61 (109)** (2018), 167–171.

[9] I.M. Isaacs, *Group actions and orbits*. Arch. Math. (Basel) **98** (2012), 399–401.

[10] W. Kappe, *Die A-Norm einer Gruppe*. Illinois J. Math. **5** (1961), 187–197.

[11] W.H. Mills, *On the non-isomorphism of certain holomorphs*. Trans. Amer. Math. Soc. **74** (1953), *3*, 428–443.

Kuwait University
Department of Mathematics
P.O. Box 5969, Safat 13060, Kuwait