Variations on a Theme of Desmond MacHale

LUISE-CHARLOTTE KAPPE

Für Martin Newell mit den besten Wünschen
für einen angenehmen Ruhestand.

Abstract. This article is based on a talk that the author gave at Groups in Galway 2005. We discuss four conjectures, known to be false, and give a progress report on finding minimal counterexamples for them. These conjectures are variations on the 47 (false) conjectures Desmond MacHale gave in his 1981 paper "Minimum Counterexamples in Group Theory".

My variations are on an Irish tune, the theme is in Desmond MacHale's 1981 paper "Minimum Counterexamples in Group Theory" [7]. In this paper, 47 conjectures are stated, all known to be false, and MacHale asks for minimal counterexamples. Conjecture 7 in [7] reads as follows.

Conjecture 7. *In any group G, the set of commutators forms a subgroup.*

The commutator of elements g and h, $[g,h] = g^{-1}g^h$, in a group G can be viewed as the deviation from g of the image of g under the inner automorphism induced by h. For $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, the automorphism group of G, we define the autocommutator of g and α as $[g,\alpha] = g^{-1}g^\alpha$ that is the deviation from g of the image of g under the automorphism α. This brings us to the first variation to be discussed.

Conjecture 7*. *In any group G, the set of autocommutators forms a subgroup.*

Of course, Conjecture 7* is false, but until a few months ago nobody knew a counterexample, let alone a minimal one. The first time I heard about the conjecture was at Groups in Galway 2003,

where I had a discussion with Desmond MacHale during a coffee break. He wrote up the conjecture for me and added that there might be abelian counterexamples and that perhaps the two groups of order 96 given by Guralnick [5], which are the minimal counterexamples for Conjecture 7, are also counterexamples for Conjecture 7*. I took the sheet home with me and started work with my two collaborators David Garrison and Denise Yull [4].

But before reporting on the outcome, let me introduce some notation. For a group G, let $K(G) = \{[g,h] \mid g,h \in G\}$ be the set of commutators in G and set $G' = \langle K(G)\rangle$, the commutator subgroup of G, and let $K^*(G) = \{g^{-1}g^\alpha \mid g \in G, \alpha \in \mathrm{Aut}(G)\}$ be the set of autocommutators of G and set $G^* = \langle K^*(G)\rangle$, the autocommutator subgroup of G. With this notation, Conjectures 7 and 7* now read as follows.

Conjecture 7. *For any group G, $K(G) = G'$.*

Conjecture 7*. *For any group G, $K^*(G) = G^*$.*

Back home, my two collaborators and I wrote a GAP program [3] which determines $K^*(G)$ and G^* for a finite group G that outputs whether $K^*(G)$ is equal to G^* or not. In an attempt to get a counterexample for Conjecture 7*, we tested the program on the two groups of order 96, the groups of smallest order in which the set of commutators is unequal to the commutator subgroup. For both groups G we obtained that $K^*(G) = G^* = G$.

After that we let our program run through the GAP Small Groups Library [3]. If for a group G the output is that $G^* = K^*(G)$, the program proceeds to the next group and halts as soon as it finds a group with the set of autocommutators unequal to the autocommutator subgroup. As soon as the program reached groups of order 32, in particular the abelian groups, the size of the automorphism group became a problem. With the following results we can exclude abelian groups as counterexamples.

Proposition 1. *For an abelian torsion group without elements of even order we have $K^*(G) = G^*$.*

Proposition 2. *Let G be a finite abelian 2-group. Then $K^*(G) = G^*$.*

The two propositions above together with the following lemma yield our main result.

Lemma 1. *Let P and Q be finite groups of relatively prime order. Then $K^*(P \times Q) = K^*(P) \times K^*(G)$ and $(P \times Q)^* = P^* \times Q^*$.*

Theorem 1. *Let G be a finite abelian group. Then $K^*(G) = G^*$.*

After excluding the abelian groups, we still had problems with groups having a very large automorphism group. After some trial and error, we limited the order of the automorphism group to 400,000. Anytime the program would not test a group, there would be an output indicating which group was skipped and what the order of the automorphism group was. With these restrictions the program halted after all groups of order 64 had been checked. Denoting with $G(k, n)$ the n-th group of order k in the GAP Small Groups Library, the output consisted of the three groups $G(64, n)$, $n = 261$, 262, and 266. There were no groups of order less than 64 which had to be skipped because of the size of the automorphism group. However, the groups $G(64, 261)$ and $G(64, 262)$ with orders of the automorphism group being 688,128 and 2,064,384, respectively, were skipped. It can be easily seen that for these two groups the set of autocommutators is equal to the autocommutator subgroup by observing that $G(64, 261) \cong D_4 \times C_2 \times C_2 \times C_2$ and $G(64, 262) \cong Q_8 \times C_2 \times C_2 \times C_2$, where D_4 is the dihedral group of order 8 and Q_8 is the group of quaternions of order 8. The group $G(64, 266)$, in which the autocommutators do not form a subgroup, gives the desired minimal counterexample for Conjecture 7*. Our results are summarized in the following theorem.

Theorem 2. *There exists exactly one group G of order 64 for which $K^*(G) \neq G^*$ and $|K^*(G)| = 62$, $|G^*| = 64$, and for all groups of order less than 64 the autocommutators form a subgroup. The group G can be given by generators and defining relations as follows:*

$$\begin{aligned} G = \langle a, b, c, d, e \mid\ & a^2 = b^2 = c^2 = d^2 = e^4 = 1, \\ & [a, b] = [a, c] = [a, d] = [b, c] = [b, d] = [c, d] = e^2, \\ & [a, e] = [b, e] = [c, e] = [d, e] = 1 \rangle. \end{aligned}$$

The proof that G is a counterexample for Conjecture 7* does not require the use of GAP. But for proving the minimality of G, the use of GAP is indispensable.

Now let us turn to the next variation. The first conjecture in [7] reads as follows.

Conjecture 1. *In a group G, the set of all squares of elements of G is a subgroup of G.*

MacHale gives $T = \langle a, b \mid a^3 = b^4 = 1, a^b = a^{-1} \rangle$ and A_4, the alternating group on 4 letters, as the minimal counterexamples for Conjecture 1. We consider now the following variation of the above conjecture.

Conjecture 1*. *For a given integer n, $n > 1$, and any group G, the set of n-th powers of elements in G is a subgroup of G.*

Of course, the above conjecture is false. The topic of Gabriela Mendoza's master's thesis [8] was to determine the minimal counterexamples for $n > 2$. Before reporting on her results, let me introduce some notation and definitions. For a group G and an integer n we let $G^{(n)} = \{x^n \mid x \in G\}$, the set of n-th powers in G, and $G^n = \langle G^{(n)} \rangle$. The following definition facilitates formulating our results.

Definition 1. *Let n be an integer, $n > 1$. We say the minimal number of n is $\mu(n)$, if there exists a group G of order $\mu(n)$ with $G^{(n)} \neq G^n$, and $G^{(n)} = G^n$ for all groups G of order less than $\mu(n)$.*

For odd n, we have a complete and easy answer.

Theorem 3. *Let n be an odd integer, $n \geq 3$, and let p be the smallest prime dividing n. Then $\mu(n) = 2p$.*

If n is even, the answer is much more complex and it depends on the exact 2-divisor of n. Our first result is the following.

Theorem 4. *Let $n = 2k$ be an integer with k odd. Then $\mu(n) = 16$, unless $n \not\equiv 0 \bmod 3$ and then $\mu(n) = 12$.*

We still have a complete answer if the exact 2-divisor is 4.

Theorem 5. *Let $n = 4k$ be an integer with k odd. Then $\mu(n) = 64$, unless $n \not\equiv 0 \bmod 3$, or $n \equiv 0 \bmod 3$ and $n \not\equiv 0 \bmod 5$, or $n \equiv 0 \bmod 15$ and $n \not\equiv 0 \bmod 7$, in which case $\mu(n) = 12$, 40, or 56, respectively.*

To get some guidance how results like those in the preceding two theorems may look like for higher powers of 2, we turned to GAP. The following table summarizes our GAP calculations for groups of order 2^m, $m = 4$, 5, 6, 7, 8, indicating the number of groups G with

$G^{(n)} \neq G^n$ for specified n. The first column gives the order of the group, the second the total number of groups, the remaining four columns give the number of groups with $G^{(n)} \neq G^n$ for $n = 2$, 4, 8, 16.

Table 1

Order	Number of Groups	$n = 2$	$n = 4$	$n = 8$	$n = 16$
16	14	2	0	0	0
32	51	16	9	0	0
64	267	127	9	0	0
128	2328	1391	176	0	0
256	56092	27290	3052	18	0

From the above table we can read off that $\mu(n) \leq 256$ for $n = 8k$, where k is odd. We conjecture $\mu(n) \leq 2^{2\alpha+2}$ for $n = 2^\alpha k$ with k odd. There are many exceptions for the case $n = 8k$ that still need to be determined. There emerges no pattern how the exceptions for general α can be given in closed form.

Finally, I want to look at two more conjectures, both definitely false. They have no counterpart in [7], though the first one can be viewed sort of a dual to Conjectures 1 and 1*. So we just call them Conjectures A and B.

Conjecture A. *For a given prime p, the elements of order dividing p in a group G always form a subgroup of G.*

Conjecture B. *For a given prime p, a Sylow p-subgroup of a group is always normal in the group.*

In ongoing research by Gabriela Mendoza, Michael Ward and myself [6], we have been looking into finding minimal counterexamples to Conjectures A and B. We started out with minimal counterexamples for Conjecture A, but soon were led to Conjecture B and its minimal counterexamples and found that they were intimately connected. Minimal counterexamples for Conjecture A potentially can have p-power order. But it turned out not to be the case. To make our notions more precise, we make the following definition.

Definition 2. *Let p be a prime. We denote with $f(p)$ the order of a group whose elements of order dividing p do not form a subgroup, and for every group of order less than $f(p)$ these elements do form a subgroup.*

In the case of Mersenne primes we can determine $f(p)$ precisely.

Theorem 6. *Let p be a prime. Then $f(p) = p(p+1)$ if and only if p is Mersenne or $p = 2$.*

To determine $f(p)$ in case p is not a Mersenne prime, we consider p-closed and minimal non-p-closed groups. The following definition is due to Reinhold Baer [1].

Definition 3. *If Σ is a set of primes and if the set of elements in the group G whose orders are divisible by primes in Σ only is actually a subgroup of G, then G is called Σ-closed.*

A Σ-closed group for which the set Σ consists of a single prime p is called *p-closed*. For finite groups the class of p-closed groups coincides with the class of groups having a normal Sylow p-subgroup. Following standard practice, we define minimal non-p-closed groups as follows.

Definition 4. *A group is called a minimal non-p-closed group, if it is not p-closed but every subgroup and homomorphic image is.*

In the literature, non-p-closed groups are called *inner p-closed*, if they are not p-closed but every proper subgroup is (see for example [2]). Our next theorem characterizes the minimal non-p-closed groups.

Theorem 7. *For a prime p, a minimal non-p-closed group is either simple or $G = QP$ with $|G| = pq^n$ for some prime q and if $Q \in \mathrm{Syl}_q(G)$, then Q is a minimal normal subgroup of G and Q is elementary abelian of rank n. Furthermore, if $P \in \mathrm{Syl}_p(G)$, then $N_G(P) = P$ and $q^n \equiv 1 \bmod p$.*

For given p, there is more than one minimal non-p-closed group. We are interested in those of minimal order. This leads to the following definition.

Definition 5. *Let $n(p)$ denote the order of the smallest group which is minimal non-p-closed and denote with $s(p)$ the order of the smallest simple group which is minimal non-p-closed.*

As a corollary to Theorem 7 we obtain the following result.

Corollary 1. *Let p be a prime. Then $n(p) = \min(s(p), p(kp+1))$, where k is the smallest integer such that $kp+1$ is a prime power.*

To determine $f(p)$ for an odd prime p which is not Mersenne, we have to distinguish between two cases, namely that the Sylow p-subgroup is normal in G or this is not the case. In the first case we arrive at $f(p) = p^{p+1}$, the order of the smallest non-regular p-group, and in the second case we arrive at $f(p) = n(p)$. However, $|\mathrm{PSL}(2,p)| = \frac{1}{2}p(p^2-1) < p^{p+1}$ for all $p \geq 5$ and it can be shown that $\mathrm{PSL}(2,p)$ is a minimal non-p-closed group. Hence we arrive at the following result.

Theorem 8. *Let p be an odd prime which is not Mersenne. Then*

$$f(p) = \min(p(kp+1), s(p)),$$

where k is the smallest integer such that $kp+1$ is a prime power.

The above theorem together with Theorem 6 leads to the following corollary.

Corollary 2. *For any prime p we have $f(p) = n(p)$.*

By Dirichlet's Theorem, infinitely many integers k exist such that $kp+1$ is prime, and not much can be said about the minimal k. To obtain a prime power, smaller values of k may suffice. For example, if $p = 13$, then $4 \cdot 13 + 1 = 53$ but already $2 \cdot 13 + 1 = 3^3$. We observe that in Corollary 1 and Theorem 8 both cases can occur. For example, if $p = 5$, then $k = 2$ and $p(kp+1) = 55 < 60 = s(5)$. However, if $p = 19$, then $k = 10$ and $p(kp+1) = 3629 > 3420 = s(19) = |\mathrm{PSL}(2,19)|$. Though there appears no way for determining exact values for the minimal k, we conjecture that for $p > 3$ we have $s(p) = \frac{1}{2}p(p^2-1) = |\mathrm{PSL}(2,p)|$. Currently, we are in the process of checking our conjecture by using the classification of Finite Simple Groups and examining the simple groups of order divisible by p.

REFERENCES

[1] Reinhold Baer, Classes of finite groups and their properties, *Illinois J. of Math.* **1** (1957), no. 2, 115–187.

[2] Zhong Mu Chen, Inner p-closed groups, *Adv. in Math (Beijing)* **15** (1986), no. 4, 371–372.

[3] The GAP Group. *GAP – Groups, Algorithms, and Programming*, Version 4.4, 2004. (http://www.gap-system.org).

[4] David Garrison, Luise-Charlotte Kappe, and Denise Yull, Autocommutators and the autocommutator subgroup, submitted.

[5] R. M. Guralnick, Expressing group elements as products of commutators, *Rocky Mountain J. Math.* **10** (1981), 651–654.

[6] Luise-Charlotte Kappe, Gabriela Mendoza, and Michael Ward, Groups of smallest order in which the elements of order dividing p do not form a subgroup, in preparation.
[7] Desmond MacHale, Minimum counterexamples in group theory, *Math. Mag.* **54** (1981), no. 1, 23–28.
[8] Gabriela Mendoza. *On the power structure of finite groups*. Master's thesis, Binghamton University, State University of New York, May 2004.

Luise-Charlotte Kappe,
Department of Mathematical Sciences,
SUNY at Binghamton,
Binghamton, NY 13902-6000,
USA
menger@math.binghamton.edu