8-1991

Counting Centralizers in Finite Groups

Sarah Marie Belcastro
Haverford College

Gary J. Sherman
Rose-Hulman Institute of Technology

MSTR 91-04

COUNTING CENTRALIZERS IN FINITE GROUPS

Sarah Marie Belcastro and Gary J. Sherman

MS TR 91-04

August 1991

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198

Phone: (812) 877-8391

Counting Centralizers in Finite Groups

SARAH MARIE BELCASTRO*
Haverford College
Haverford, PA 19041

GARY J. SHERMAN*
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

A finite (and all groups mentioned in this paper are finite) abelian group is the direct product of cyclic groups of prime power order. Thus, one expects group structure to become increasingly complex with decreasing 'abelianness'. Indeed, the basic classification scheme for groups reflects the importance of the notion of commutativity in understanding group structure because labeling a group as abelian, nilpotent, supersolvable, solvable or simple indicates, at least in a qualitative sense, the degree of commutativity the group enjoys.

Beginning abstract algebra students tend to ignore the subtleties of the commutativity issue – xy = yx as far as they are concerned. Thirteen or fourteen years of commutative arithmetic are hard to dismiss. An effective way to deal with this misconception is to deal with it directly by asking 'How many pairs of elements of a group commute?' or 'What is the probability that two group elements commute?'. The formal answers are $\mathrm{Com}(G) = |\{ (x,y) \mid xy = yx \}|$ and $\mathrm{Prob}(G) = \mathrm{Com}(G)/|G|^2$, respectively. These questions and their (formal) answers put the notion of commutativity on a numerical

---

*Work supported by National Science Foundation grant DMS - 8922674.

Mathematics Subject Classification 20D60.

basis, which students enjoy, and provide motivation for a delightful excursion through some nice elementary group theory. Indeed, the fact that $\mathrm{Com}(G) = k\,|G|$, where k is the number of conjugacy classes in G, is woven from elementary results on subgroups, centralizers, Lagrange's theorem and conjugacy classes [3]. The equivalent probabilistic statement, $\mathrm{Prob}(G) = k / |G|$, leads, unsurprisingly, to a reassuring result,

$$G \text{ is abelian if, and only if } \mathrm{Prob}(G) = 1, \tag{1}$$

and, pleasantly, to a surprising result,

$$G \text{ is nonabelian if, and only if, } \mathrm{Prob}(G) \leq 5/8. \tag{2}$$

Another, less precise, way to say this is that either all of the elements commute or at most 5/8 of the elements commute. For details of the development of the '5/8-bound' for commutativity see [5] or pages 329 and 330 of [4].

Here's another question relating numbers and commutativity.

How many centralizers can a group have?

Recall that the centralizer of x in G, denoted by C(x), is the subgroup of G consisting of all elements which commute with x; i.e., $C(x) = \{y \in G \mid xy = yx\}$. If we denote the number of distinct centralizers in G by Cent(G), then $\mathrm{Cent}(G) = |\{C(x) \mid x \in G\}|$ and our question becomes 'What can we say about Cent(G)?'. This paper is an itinerary for an excursion in elementary group theory motivated by this question. Our goal is to provide some answers and some more questions which we think are interesting, in their own right, and useful, if you teach abstract algebra.

Since G is abelian if, and only if, $C(x) = G$ for each element of G, we may begin by stating the analogue of (1).

FACT 1. G is abelian if, and only if, $\mathrm{Cent}(G) = 1$.

Is there a centralizer 'gap' for nonabelian groups like the probability 'gap' between 1 and 5/8?

FACT 2. If G is not abelian, then $\mathrm{Cent}(G) \geq 4$.

Proof: G is certainly the union of its centralizers. But, the center of G,

$$Z = \{ z \mid zx = xz \text{ for each } x \in G \} = \bigcap_{x \in G} C(x),$$

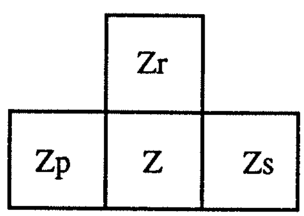
is a subset of each centralizer, so G is the union of its proper centralizers. If Cent(G) = 2, then G is one of its proper subgroups, which is impossible. If Cent(G) = 3, then G is the union of two proper subgroups, say H and K. This is also impossible because if we choose $x \in H - K$ and $y \in K - H$, we have no place to put xy. For example, $xy \in H$ implies $y \in H$ because $y = x^{-1}xy$.

Can Cent(G) =4? Yes, the dihedral group on four symbols, D_4, and the quaternion group of order eight, Q, are groups with exactly four centralizers. For example, the distinct centralizers of D_4, written as unions of right cosets of the center, are

$$D_4 = Z \cup Z\cdot(1,2,3,4) \cup Z\cdot(1,2)(3,4) \cup Z\cdot(1,3),$$
$$P = Z \cup Z\cdot(1,2,3,4),$$
$$R = Z \cup Z\cdot(1,2)(3,4),$$
$$S = Z \cup Z\cdot(1,3),$$

where $Z = \langle(1,3)(2,4)\rangle$.

The essence of this example can be captured graphically,



,

and mathematically:

FACT 3. Cent(G) = 4 if, and only if, $G/Z \cong Z_2 \oplus Z_2$; i.e., G modulo its center is isomorphic to the Klein four group.

Proof: If $G/Z \cong Z_2 \oplus Z_2$, then there are noncentral elements, p, r and s, of G such that $G = Z \cup Zp \cup Zr \cup Zs$. It follows that the the three proper subgroups of G containing Z are $P = Z \cup Zp$, $R = Z \cup Zr$ and $S = Z \cup Zs$. Let x be one of p, r or s and let X be the corresponding subgroup. Notice that for $zx \in Zx$, $G \supset C(zx) \supseteq X$. So,

$$[G : X] = [G : C(zx)][C(zx) : X] = 2 \text{ and } [G : C(zx)] \neq 1,$$

thus $C(zx) = X$. Therefore the proper centralizers of G are precisely P, R and S; i.e., $|\mathrm{Cent}(G)| = 4$.

For the converse, it is sufficient to show that $[G : Z] = 4$ because then

$$\text{either } G/Z \cong Z_2 \oplus Z_2 \text{ or } G/Z \cong Z_4.$$

As G is nonabelian, G/Z can not be cyclic which means the latter case is impossible. So, suppose $|\mathrm{Cent}(G)| = 4$ and let $P = C(p)$, $R = C(r)$ and $S = C(s)$ be the three proper centralizers of G. Since G can not be written as the union of two proper subgroups and since an element must belong to its centralizer, we may choose p, r and s in $G - (R \cup S)$, $G - (P \cup S)$ and $G - (P \cup R)$, respectively. Moreover, at least one of the proper centralizers, say P, has index two in G. For otherwise,

$$|G| \leq |P| + |R| + |S| - 2|Z| \leq |G|/3 + |G|/3 + |G|/3 - 2 < |G|.$$

Further,

$$P \cap R = P \cap R \cap S = Z$$

because if $x \in (P \cap R) - Z$, then

i) $C(x) \neq G$ because $x \notin Z$,

ii) $C(x) \neq P$ and $C(x) \neq R$ because $p, r \in C(x)$,

iii) $C(x) \neq S$ because $x \notin S$,

which means that $|\mathrm{Cent}(G)|$ must be at least 5.

Now we can compute $|Z|$ using the fact that for subgroups X and Y of G,

$$|X \cap Y| = \frac{|X|\,|Y|}{|XY|}$$

$$\geq \frac{|X|\,|Y|}{|G|}. \tag{3}$$

Indeed,

$$|Z| = |P \cap R|$$

$$\geq \frac{|P|\,|R|}{|G|}$$

$$= \frac{|R|}{2},$$

since $|P| = |G|/2$. But $Z \neq R$, so $|Z| = |R|/2$. Similarly, $|Z| = |S|/2$. Thus

$$|G| = |P| + |R| + |S| - 2|Z| = |G|/2 + 2|Z| + 2|Z| - 2|Z| = |G|/2 + 2|Z|$$

implies $|G|/2 = 2|Z|$; i.e., $[G : Z] = 4$, as desired.

Groups for which $G/Z \cong Z_2 \oplus Z_2$ are as abelian as an nonabelian group can be in the probabilistic sense also. To see this, recall that the order of the conjugacy class of an element is the index of the centralizer of that element. Thus, each conjugacy class of G is of order one or two. Therefore the number of conjugacy classes in G is

$$k = |Z| + (|G| - |Z|)/2 = |G|/4 + 3|G|/8 = 5|G|/8$$

and Prob(G) = 5/8. This computation also suggests why Prob(G) $\leq$ 5/8 for nonabelian groups: Prob(G) is as large as possible when the center is as large as possible and all of the noncentral elements are in conjuugacy classes of size two. This occurs when $[G : Z] = 4$; i.e., when $G/Z \cong Z_2 \oplus Z_2$. The threshold of 'abelianness', as measured by Cent(G) or Prob(G), is occupied by the same class of groups:

FACT 4. Prob(G) = 5/8 and Cent(G) = 4 are equivalent to $G/Z \cong Z_2 \oplus Z_2$.

Some readers may recognize the last two statements in our proof of FACT 2 and D_4 or Q as a solution to an old Putnam problem [6].

> Show that a finite group can not be the union of two of its proper subgroups. Does the statement remain true if "two" is replaced by "three"?

Not long after this problem appeared, Bruckheimer, Bryan and Muir [1] provided an elementary proof that

A group can be written as the union of three proper subgroups, H, K and L, if, and only if, $N = H \cap K \cap L$ is a normal subgroup of G and $G/N \cong Z_2 \oplus Z_2$. (4)

FACT 3 is seen to a special case of (4). Indeed, it is an easy exercise to modify our proof of FACT 3 and thereby prove (4). However, we chose to give a direct proof of FACT 3 to serve as a warm-up for the more complicated proof of

FACT 5. $\mathrm{Cent}(G) = 5$ if, and only if, $G/Z \cong Z_3 \oplus Z_3$ or $G/Z \cong S_3$ where S_3 is the symmetric group on three symbols.

Proof: If $G/Z \cong Z_3 \oplus Z_3$ or $G/Z \cong S_3$, we may argue as we did in the proof of FACT 3. Specifically, if $G/Z \cong S_3$, then $G = Z \cup Zx \cup Zx^2 \cup Zy \cup Zyx \cup Zyx^2$ where x^3, y^2, $(xy)^2 \in Z$. There are exactly four proper subgroups of G properly containing Z,

$$Z \cup Zx \cup Zx^2,\ Z \cup Zy,\ Z \cup Zyx,\ Z \cup Zyx^2,$$

each of which is the centralizer of its non-central elements because it is abelian and of prime index in G.

For the converse, suppose $\mathrm{Cent}(G) = 5$ and let P, R, S and T be the four proper centralizers of G. It is convenient to weave the proof from a sequence of lemmas.

LEMMA 1. No one of P, R, S or T is contained in the union of the other three.

Proof: Suppose to the contrary, and without loss of generality, that T is a subset of $P \cup R \cup S$. Then, since $G = P \cup R \cup S \cup T$, we must have $G = P \cup R \cup S$. It follows from (4) that $G/(P \cap R \cap S) \cong Z_2 \oplus Z_2$. So, if we can show $P \cap R \cap S = Z$, FACT 3 will yield $\mathrm{Cent}(G) = 4$ – a contradiction.

Choose $p \in P - (R \cup S)$, $r \in R - (P \cup S)$ and $s \in S - (P \cup R)$ such that $C(p) = P$, $C(r) = R$ and $C(s) = S$. This is possible because if, for example, no such p existed, we would have $C(p) = T$ for each $p \in P - (R \cup S)$; i.e., $P - (R \cup S) \subseteq T - (R \cup S)$ and we could interchange the roles of P and T. Now, let $x \in (P \cap R \cap S) - Z$ and consider $C(x)$:

$$C(x) \neq G \text{ because } x \notin Z,$$

$C(x) \neq T$ because $x \notin T$,

$C(x) \neq P$ because $r,s \in C(x) - P$,

$C(x) \neq R$ because $p,s \in C(x) - R$,

$C(x) \neq S$ because $p,r \in C(x) - S$.

Thus , $(P \cap R \cap S) - Z$ is empty and the contradiction, Cent(G) =4, follows.

In view of LEMMA 1, a proper centralizer, X, contains an element, x, not belonging to the union of the other three proper centralizers. Thus, $C(x) = X$.

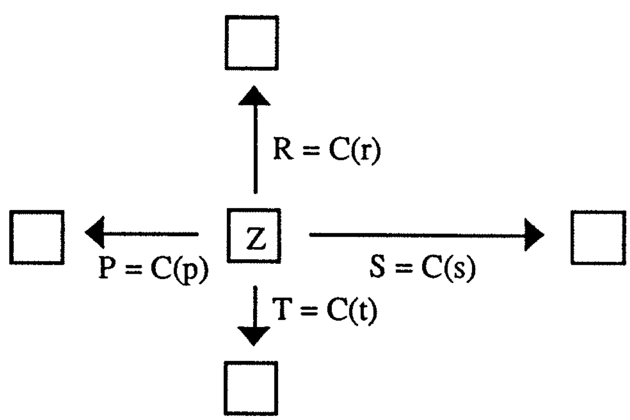
LEMMA 2. No element of G is in exactly two proper centralizers.

Proof: Suppose, for example, that $g \in (P \cap R) - (S \cup T)$. The only candidates for $C(g)$ are $P = C(p)$ and $R = C(r)$. However, the fact that both p and r are elements of $C(g)$ means that $C(g)$ can be neither $C(p)$ nor $C(r)$; i.e., $(P \cap R) - (S \cup T)$ is empty.

A similar proof establishes

LEMMA 3. No element of G is in exactly three proper centralizers.

The upshot of these lemmas is that G is 'almost' a disjoint union of its four proper centralizers.



The arithmetical summary is

LEMMA 4. $|G| = |P| + |R| + |S| + |T| - 3|Z|$.

And so, just as in the proof of FACT 3, it is essential to constrain $|Z|$.

LEMMA 5. If X and Y are distinct proper centralizers of G, then

$$|X||Y|/|G| \le |Z| \le |G|/6.$$

Proof: The lower bound for $|Z|$ follows from (3) because LEMMA 2 and LEMMA 3 imply $Z = X \cap Y$. The upper bound follows because $[G : Z] > 4$ and $[G : Z] = 5$ imply G is abelian.

To sharpen the lower bound let's concentrate on the orders of the centralizers. We may assume, without loss of generality, that $|P| \ge |R| \ge |S| \ge |T|$. Thus, LEMMA 4 and the fact that P is a subgroup of G imply $|P| = |G|/2$ or $|P| = |G|/3$. Now we can proceed by cases.

CASE: $|P| = |G|/2$. In this case LEMMA 4 guarantees that $|R| > |G|/6$. On the other hand, LEMMA 5 applied to P and R implies $|G|/6 \ge |G||R|/2|G|$; i.e., $|R| \le |G|/3$. Thus $|R|$ is one of $|G|/3$, $|G|/4$ or $|G|/5$. Reapplying LEMMA 5 to P and R yields $|G|/10 \le |Z| \le |G|/6$. Thus, $|Z|$ is one of $|G|/6$, $|G|/8$, or $|G|/10$, because Z is a subgroup of P.

i) Let $|Z| = |G|/6$. The only choices for G/Z are S_3 and Z_6 so G/Z is S_3. Recall that if G/Z is cyclic, then G is abelian.

ii) Let $|Z| = |G|/8$. Since Z is a subgroup of R, $|R| = |G|/4$. It follows from LEMMA 4 that $|S| + |T| = 5|G|/8$, which is impossible because $|S|, |T| \le |G|/4$.

iii) Let $|Z| = |G|/10$. Since Z is a subgroup of R, $|R| = |G|/5$. It follows from LEMMA 4 that $|S| + |T| = 7|G|/10$, which is impossible because $|S|, |T| \le |G|/5$.

CASE: $|P| = |G|/3$. Applying LEMMAS 4 and 5, as in the previous case, yields

$$|G|/4 \le |R| \le |G|/3 \text{ and } |G|/12 \le |Z| \le |G|/6.$$

And again, the fact that Z is a subgroup of P enables us to restrict $|Z|$ to one of $|G|/6$, $|G|/9$ or $|G|/12$.

i) Let $|Z| = |G|/6$. The only choices for G/Z are S_3 and Z_6 so G/Z is S_3.

ii) Let $|Z| = |G|/9$. The only choices for G/Z are Z_9 and $Z_3 \oplus Z_3$ so G/Z is $Z_3 \oplus Z_3$.

iii) Let $|Z| = |G|/12$. If $|R| = |G|/3$, then LEMMA 5 applied to P and R yields the contradiction $|Z| \geq |G|/9$. If $|R| = |G|/4$, LEMMA 4 implies that $|S| + |T| = 2|G|/3$, which is impossible because $|S|, |T| \leq 1/4$.

A connection with Prob(G), while looser, still exists when Cent(G) = 5. For example, if $G/Z \cong S_3$ there are $|Z|$ conjugacy classes in Z, $|Z|$ conjugacy classes in $Zx \cup Zx^2$ and $|Z|$ conjugacy classes in $Zy \cup Zyx \cup Zyx^2$ so Prob(G) = 1/2. Similarly, if $G/Z \cong Z_3 \oplus Z_3$, Prob(G) = 11/27. Conversely, an elementary, but subtle, proof that Prob(G) = 1/2 implies $G/Z \cong S_3$ exists [8]. And, if Prob(G) = 11/27 and the smallest prime divisor of $|G|$ is three, then $G/Z \cong Z_3 \oplus Z_3$.

The proof of the previous statement is lurking in the paragraph preceding FACT 4. Well, what's really lurking there is a proof of a more general result: If the smallest prime divisor of $|G|$ is p, then Prob(G) = $(p^2 + p - 1)/p^3$ if, and only if, $G/Z \cong Z_p \oplus Z_p$. How many centralizers does such a group have? For p = 2 and for p = 3 we have shown that the answer is Cent(G) = 4 and Cent(G) = 5, respectively. These results are special cases of

FACT 6. Let p be a prime. If $G/Z \cong Z_p \oplus Z_p$, then Cent(G) = p + 2. If p is odd and $G/Z \cong D_p$, then Cent(G) = p + 2.

Proof: A quick check of our proofs of FACTS 3 and 5 will convince you that the crucial observations are

i) each proper subgroup of G properly containing Z is abelian and of prime index in G; i.e., it is a centralizer, and

ii) both $Z_p \oplus Z_p$ and D_p (p odd) have exactly p + 1 proper subgroups.

So, if for each prime there are groups satisfying the hypothesis of FACT 6, we can make Cent(G) as large as we like. For p= 2, D_4 and Q will do. If p is an odd prime, we can use D_p, since it has a trivial center, or either of the two groups of order p^3,

$$< a,b \mid a^{p^2} = e, b^p = e \text{ and } b^{-1}ab = a^{1+p} >,$$

$$< a,b,c \mid a^p = b^p = c^p = e, ab = bac, ca = ac \text{ and } cb = bc >,$$

since their centers must be of order p.

QUESTION. Can we make Cent(G) anything we like; i.e., if n is a positive integer other than two or three, does there exist a group with n = Cent(G) centralizers? Which values of Cent(G), other than 4 and 5, characterize G.

It is interesting to note that one of our choices for making Cent(G) arbitrarily large is the class of 'most abelian' nonabelian groups ($G/Z \cong Z_p \oplus Z_p$) and the other is a class of 'fairly' abelian groups: $\mathrm{Prob}(D_p) = k/2p = 1/4 + 3/4p$ which is bounded below by 1/4. Here's an attempt at saving face: normalize Cent(G) by defining

$$\rho(G) = \mathrm{Cent}(G)/|G|.$$

Then, for the 'most abelian' nonabelian groups

$$\rho(G) = (p + 2)/p^2|Z| = 1/p|Z| + 2/p^2|Z|,$$

which decreases monotonically and reassuringly to 0 (the limiting value of $\rho(G)$ for abelian G) as p approaches infinity. Could it be that $\rho(G)$ approaches zero as $|G|$ approaches infinity for arbitrary G? No, not even for our class of 'fairly' abelian groups: $\rho(D_p) = 1/2 + 1/p$ is bounded below by 1/2. But, we can get a '5/8-like' bound for $\rho(G)$.

FACT 7. Let p be the largest prime divisor of $|G|$.

$$\rho(G) \le \begin{cases} 1/2, & \text{if } p = 2 \\ 3/4 + 1/4p, & \text{if } p \text{ is odd} \end{cases}.$$

Proof: Our strategy is to find a tractable partition of G which is compatible with the partition of G that is created when elements are assigned to their centralizers. If p = 2, then G is a 2-group and has a nontrivial center. Since elements in the same coset of the center have the same centralizer, the cosets of Z will do: $\rho(G) \le [G : Z]/|G| = 1/|Z| \le 1/2$.

If p is odd we aren't guaranteed the existence of a nontrivial center. However, Lagrange's theorem guarantees the existence of elements of order p. Such an element is distinct from its inverse, but, as is the case for all group elements, has the same centralizer as its inverse. The partition we are looking for has sets of the form $\{x, x^{-1}\}$ as its components. Unfortunately, some of these components may consist of only one element. This occurs if, and only if, $x^2 = e$; i.e., x is an involution. Let's denote the number of involutions in G by Inv(G) and summarize:

$$\mathrm{Inv}(G) < |G|,$$

$$\mathrm{Cent}(G) \leq \mathrm{Inv}(G) + (\,|G| - \mathrm{Inv}(G))/2.$$

$$= (\mathrm{Inv}(G) + |G|)/2,$$

$$\rho(G) \leq 1/2 + \mathrm{Inv}(G)/2|G|. \tag{5}$$

And, it is known that if not all elements of G are involutions, then

$$\mathrm{Inv}(G)/|G| \leq (p + 1)/2p. \tag{6}$$

Our result follows immediately from (5) in conjunction with (6).

The result quoted in (6) first appeared in an article published by G. A. Miller in 1905 [7]. We choose not to repeat any of the details here because Miller's paper is perfect reading for a beginning abstract algebra student – elementary and (old enough to be) refreshingly wordy.

While the bounds established in FACT 7 are sharp for $p = 2$ ($\rho(D_4) = \rho(Q) = 1/2$) and $p = 3$ ($\rho(S_3) = 5/6$) that is not the case for $p > 3$. Indeed, if $\rho(G) = 3/4 + 1/4p$, then $\mathrm{Inv}(G)/|G|$ must also be a maximum; i.e., $\mathrm{Inv}(G)/|G| = (p + 1)/2p$. This is precisely the value of $\mathrm{Inv}(D_p)/|D_p|$. A coincidence? No, Miller's paper also establishes that if $\mathrm{Inv}(G)/|G| = (p + 1)/2p$, then

$$G \cong D_p \oplus Z_2 \oplus Z_2 \oplus \cdots \oplus Z_2.$$

Fortunately, Cent(G) is a multiplicative function; i.e., the number of distinct centralizers in a direct sum is the product of the numbers of centrralizers in each factor. Thus, for G as in (7), $\mathrm{Cent}(G) = \mathrm{Cent}(D_p) = p + 2$ and so $\rho(G) = (p + 2)/2pp^j$ where j is the number of times Z_2 occurs as a direct factor in G. It is easy to check that $(p + 2)/2pp^j$ is as large as $3/4 + 1/4p$ if, and only if, $p = 3$. FACT 8 and the succeeding question are natural corollaries to FACT 7 and this discusssion.

FACT 8. $\rho(G) \le 5/6$. $\rho(G) = 5/6$ if, and only if, $G \cong S_3$.

QUESTION. Is it true that $\rho(G) < 1/2$ unless G is Q or D_p?

We close by proposing two class discussion topics which are suggested by viewing the centralizer of an element as the stabilizer of that element under the action of G on itself by conjugation:

$$C(x) = \{y \in G \mid xy = yx\} = \{y \in G \mid y^{-1}xy = x\}.$$

i) Let G act on its set of cyclic subgroups by conjugation. The stabilizer of $\langle x \rangle$ is referred to as the normalizer of x:

$$N(x) = \{y \in G \mid y^{-1}\langle x \rangle y = \langle x \rangle\} = \{y \in G \mid y^{-1}xy = x^j \text{ for some } j\}.$$

How many normalizers, say Norm(G), can a group have? It's a classic result (see pages 138-140 of [10]) that Norm(G) = 1 if, and only if, G is abelian or Dedekind – the direct sum of Q, an abelian group in which each element is of order two and an abelian group in which each element is of odd order. Can Norm(G) be two? Yes, here's an example,

$$Z_3 \oplus < a,b \mid a^9 = e, b^3 = e \text{ and } b^{-1}ab = a^4 > \oplus\ Q,$$

constructed from groups we have mentioned in this paper. It was shown just recently [9] that all groups with Norm(G) = 2 'resemble' this example; i.e., for some prime p, G is (loosely speaking) isomorphic to a direct sum of an abelian group of order p^k, a so called metacyclic group of order p^j and a Dedekind group whose order is not divisible by p. The proof is long and hard, particularly when contrasted with our characterization of those groups with Cent(G) = 4, so moving to Norm(G) = 3 could be tough. On the other hand, C(x) is a subgroup of N(x) and $N(x) = N(x^{-1})$, so all isn't lost.

ii) Let G be a finite abelian group and let A be its automorphism group [11]. The stabilizer of – well, just have your students take it from here.

ACKNOWLEDGEMENT. Group-theoretic experimentation and computation were facilitated with the computer algebra system CAYLEY [2].

REFERENCES

1. M. Bruckheimer, A. C. Bryan and A. Muir, Groups which are the union of three subgroups, *Amer. Math. Monthly,* 77(1970), 52-57.
2. D. F. Holt, The CAYLEY group theory system, *Notices Amer. Math. Soc.,* 35(1988) No. 8, 1135-1140.
3. P. Erdős and P. Turán, On some problems of a statistical group - theory, IV, *Acta Math. Acad, Sci. Hung.,* 19(1968), 413-415.
4. J. A. Gallian, *Contemporary Abstract Algebra,* 2nd edition, D. C. Heath 1990.
5. W. H. Gustafson, What is the probability that two group elements commute?, *Amer. Math. Monthly,* 80(1973), 1031-1034.
6. The Mathematical Association of America, *The Thirtieth William Lowell Putnam Mathematical Competition,* December 6, 1969, Problem B-2.
7. G. A. Miller, Groups containing the largest possible number of operators of order two, *Amer. Math. Monthly,* 12(1905), 149-151.
8. J. Leavitt, G. J. Sherman and M. J. Walker, Rewriteability in finite groups, Amer. Math. Monthly (to appear).
9. M. D. Pérez-Ramos, Groups with two normalizers, *Arch. Math.,* 50(1988), 199-203.
10. D. J. S. Robinson, *A Group in the Theory of Groups,* Springer-Verlag, 1980.
11. G. J. Sherman, What is the probability an automorphism fixes a group element?, *Amer. Math. Monthly,* 82(1975), 261-264.