the dancing problem, we conjecture that the probability converges to $\frac{1}{\sqrt{e}} \approx 0.606530659$. Finally, we leave the interested reader with a few problems to explore.

1. Determine the probability that *exactly* k pairs of players will be selected as first-round opponents in both draws, for $0 \le k \le 64$; then calculate the expected number of repeated pairs.
2. Find a non-recursive formula for the simple dancing problem probabilities, $d_{n,0}$.
3. Prove (or disprove) that $\lim_{n\to\infty} d_{n,0} = \frac{1}{\sqrt{e}}$.

Acknowledgment. I thank the referees for many valuable comments and suggestions.

REFERENCES

1. R. A. Brualdi, *Introductory Combinatorics*, North-Holland, New York, NY, 1992.
2. R. J. Clarke and M. Sved, Derangements and Bell numbers, this MAGAZINE 66 (1993), 299–303.
3. A. Hald, *A History of Probability and Statistics and Their Applications Before* 1750, John Wiley and Sons, New York, NY, 1990.
4. G. R. Sanchis, Swapping hats: a generalization of Montmort's problem, this MAGAZINE 71 (1998), 53–57.
5. H. J. Straight, *Combinatorics: An Invitation*, Brooks/Cole, Pacific Grove, CA, 1993.
6. L. Takács, On the "Problème des Ménages," *Discrete Math.* 36 (1981), 289–297.
7. H. S. Wilf, *generatingfunctionology*, Academic Press, San Diego, CA, 1990.

Variations on a Theme: A_4 Definitely Has No Subgroup of Order Six!

MICHAEL BRENNAN
Cork Institute of Technology
Cork, Ireland

DES MACHALE
University College
Cork, Ireland

Introduction To obtain *one* valid proof of a theorem is an achievement, but there may be many different proofs of the same theorem. For example, there are said to be over 370 of Pythagoras's theorem. Once a result has been proved, the story seldom ends. Instead the search begins for refined, reduced, or simplified proofs.

It is just as important to have a collection of different approaches to proving a given result as it is to have a collection of different results that can be derived using a given technique. An advantage of this attitude is that if one has already proved a result using a certain technique, then a different method of proving the same result may sometimes yield a generalization of the original result which may *not* be possible with the original technique of proof. We illustrate this phenomenon by examining various proofs of the fact that A_4, the alternating group on four symbols, has no subgroup of order six.

Preliminaries One of the cornerstones of theory of finite groups is the following theorem of the Italian mathematician J. L. Lagrange (1736–1813):

LAGRANGE'S THEOREM. *If G is a finite group with $|G| = n$ and H is a subgroup of G with $|H| = d$, then d is a divisor of n.*

Lagrange stated the theorem for the special case where G was a subgroup of the symmetric group S_n which arose out of his study of the permutations of the roots of a polynomial equation. The theorem as stated above was probably first proved by Galois **[9]** around 1830.

Is the converse true?

CONVERSE TO LAGRANGE'S THEOREM. *If G is a finite group with $|G| = n$, and d is a divisor of n, then G has a subgroup of order d.*

It is well known that this converse is false, and that a counterexample of smallest order is provided by A_4, the alternating group on 4 symbols. This group of order 12 has no subgroup of order 6. We write A_4 as the group of all even permutations on the four symbols $\{1, 2, 3, 4\}$.

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132),$$
$$(124), (142), (134), (143), (234), (243)\}$$

We now present eleven elementary proofs of the fact that A_4 has no subgroup of order 6. Several attempts **[2, 4, 6]** at presenting the "simplest" or "best" proof of showing that A_4 has no subgroup of index 2 have recently been made. Since notions like "best" or "simplest" proof are subjective, we present a range of possible candidates. All eleven proofs involve only elementary concepts from group theory: cosets, element orders, conjugacy classes, normality, isomorphism classes, commutator subgroup, cycle structure. The variety of topics that arise is a valuable review of basic group theory!

Proofs of the falsity of the converse Let H be an alleged subgroup of A_4 of order 6. Each proof following implies that such an H cannot exist. Of course, the most simple-minded approach is to look at all $\binom{12}{6} = 924$ subsets of A_4 and show that none of them forms a subgroup. However, as *Proof* 1 illustrates, this number can be halved immediately.

Proof 1. (Basic but crude)

H must contain the identity element e, so H has five nonidentity elements. There are $\binom{11}{5} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 462$ possible subsets to consider. We leave it for the reader to check that none of these 462 subsets is closed under composition of cycles. This is an arduous task to undertake by hand but quite feasible for a computer where the Cayley table for A_4 has been entered. Paradoxically, this crude approach forms the basis of a later proof which we nominate as the "simplest" but not "easiest" proof of the converse.

Proof 2. (Using cosets)

Since H has index 2 we have $A_4 = H \cup Ha$ for all $a \in A_4 \setminus H$. Consider Ha^2; now $Ha^2 = H$ or $Ha^2 = Ha$. If $Ha^2 = Ha$, then $Ha = H$ by cancellation and $a \in H$, a contradiction. Thus $Ha^2 = H$; but $Hh^2 = H$ for all $h \in H$ and so $Hg^2 = H$ for all $g \in A_4$. Thus $g^2 \in H$ for all $g \in A_4$. By direct calculation A_4 has nine distinct squares, so $|H| \geq 9$, contradicting $|H| = 6$.

Proof 3. [4] (A variation of Proof 2)

As in Proof 2 we have $g^2 \in H$ for all $g \in A_4$. If $a^3 = e$ then $a^2 = a^{-1}$, so $a^2 \in H \Rightarrow a^{-1} \in H \Rightarrow a \in H$. But this would mean that H contains all eight elements of order 3 in A_4, which is a contradiction.

Proof 4. (Using normality)

A subgroup of index 2 is also a normal subgroup. Hence $H \lhd A_4$ and the factor group A_4/H is a cyclic group of order 2. Thus $H = (Hg)^2 = Hg^2$ for all $g \in A_4$, so $g^2 \in H$. We finish the proof using the same argument as in Proof 2.

Proofs 2, 3, and 4 display the characteristic that was mentioned in the introduction; they generalize easily to yield the following result.

THEOREM. *Let G be a finite group of even order and suppose that more than half the elements of G have odd order. Then G has no subgroup H of index 2.*

This result implies that the direct product $A_4 \times C_n$, where C_n is the cyclic group of odd order, has no subgroup of index 2. Thus there exists a counterexample to the converse of Lagrange's theorem of order $12n$ for each odd integer n.

Proof 5. (Using conjugacy classes)

The conjugacy classes of A_4 are

$$\{e\}, \{(12)(34), (13)(24), (14)(23)\}, \{(123), (124), (134), (234)\},$$
$$\{(132), (142), (143), (243)\}$$

with cardinalities 1, 3, 4, and 4 respectively. Since H has index 2, H is a normal subgroup of A_4 and so H must consist of *complete* conjugacy classes, one of which must be $\{e\}$. But it is clearly not possible to make up the 5 remaining elements with sets of size 3 and 4. Hence H does not exist.

Proof 6. (Using isomorphism classes)

Since $|H| = 6$, H must be isomorphic to one of the following groups; S_3, the group of all permutations on 3 symbols $\{a, b, c\}$ or C_6 the cyclic group of order 6. Since A_4 clearly has no element of order 6 the latter possibility is ruled out. Hence $H \approx S_3$. Now S_3 has exactly three elements of order 2, namely $X = \{(ab), (bc), (ac)\}$ and A_4 (and hence H) has exactly three elements of order 2, given by $Y = \{(12)(34), (13)(24), (14)(23)\}$. The isomorphism, which preserves the order of an element, must map Y onto X. But the elements of Y commute pairwise whereas no two distinct elements of X commute. This contradicts a property of isomorphisms and hence these groups cannot be isomorphic. We conclude that H does not exist.

Proof 7. (Variation on Proof 6)

$H \approx S_3$ implies that H contains the three elements of A_4 of order 2, and therefore H contains $V = \{e, (12)(34), (13)(24), (14)(23)\}$. But V is a group of order 4 and 4 does not divide 6, contradicting Lagrange's theorem.

Proof 8. (Using the commutator subgroup)

Since H is a subgroup of index 2, $H \lhd A_4$ and the factor group A_4/H is an abelian group of order 2. Thus $H \supseteq A_4'$ where A_4' denotes the commutator subgroup. A little computation shows that $A_4' = \{e, (12)(34), (13)(24), (14)(23)\}$. As in Proof 7, 4 does not divide 6, again contradicting Lagrange's theorem.

Proof 8 offers an easy alternative proof of the result of Mackiw [9] that the group $SL(2, 3)$ (the group of all 2×2 invertible matrices of determinant 1 with entries in Z_3)

of order 24 has no subgroup of order 12. If K is such a subgroup, then $K \triangleleft SL(2,3)$ and since the factor group $SL(2,3)/K$ is abelian, $K \supseteq SL(2,3)'$, the commutator subgroup. But it is easy to see that $|SL(2,3)'| = 8$ and we get a contradiction since 8 does not divide 12.

Proof 9. (Using normal subgroups)

The group $V = \{e, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of A_4 as is the subgroup H. Since HV contains V properly and V is a maximal subgroup we must have $HV = A_4$. By a well known result **[9]**,

$$12 = |A_4| = |HV| = \frac{|H||V|}{|H \cap V|} = 12 = \frac{6 \times 4}{|H \cap V|}.$$

Hence $|H \cap V| = 2$. But this is a contradiction since A_4 has no *normal* subgroup of order 2, as is easily checked.

In the final two proofs all that is used is the closure property, i.e., if $a, b \in H$ then $ab \in H$.

Proof 10. **[1]** (Using order of an element)

Since $e \in H$ there is space only for five remaining elements in H. The elements of A_4 are either of order 2 or of order 3. Elements of order 3 occur in pairs and hence we must have an *even* number of elements of order 3 in H. Since A_4 has eight elements of order 3 and only three elements of order 2, H must contain at least one element of order 3, and, because elements of order 3 come in pairs (ρ and ρ^2), there are two possible cases to consider.

Case I. H contains four distinct elements of order 3, say ρ, ω, ρ^2, ω^2.

In addition to the above four elements and the identity we would also get the distinct elements $\rho\omega$ and $\rho\omega^2$. Note that $\rho\omega \neq \rho$, ω, ρ^2 or ω^2 since otherwise, by cancellation we get that $\omega = e$, or $\rho = e$ or $\rho = \omega$, all of which are false. Similarly the element $\rho\omega^2$ is distinct from the six elements e, ρ, ω, ρ^2, ω^2, $\rho\omega$. Hence $|H| \geq 7$, a contradiction.

Case II. H contains exactly two elements of order 3, say ρ, ρ^2

This would mean that H contains e and the 3 elements of order 2, which form a subgroup of order 4, contradicting Lagrange's theorem.

We contend that the final proof is possibly the most elementary of all the proofs in that it utilizes only the closure property. It does involve a bit of computation but the number of cases to check is far more manageable than in Proof 1.

Proof 11. Partition G into "packets" as follows $\{(e)\}$, $\{(12)(34)\}$, $\{(13)(24)\}$ $\{(14)(23)\}$, $\{(123), (132)\}$,$\{(124), (142)\}$, $\{(134), (143)\}$, $\{(234), (243)\}$. Note that by closure, H must contain all the elements of a packet or no element of a packet.

Now $e \in H$ so H is made up of either

(i) three 1-packets and one 2-packet and e; or
(ii) one 1-packets and two 2-packets and e.

This gives $\binom{3}{3} \cdot \binom{4}{1} + \binom{3}{1} \cdot \binom{4}{2} = 1 \cdot 4 + 3 \cdot 6 = 22$ sets to be checked for closure. In each of the 22 sets, elements a and b can be found such that $ab \notin H$. Hence no such H exists.

We remark that in several textbooks **[3, 5, 7]**, the problem of disproving the converse to Lagrange's theorem is often relegated to an exercise. Sadly sometimes the proof is dismissed with the words "It can be shown," "As one can easily see," "It will be found." Other texts offer proofs that involve complicated arguments **[10]**. We invite readers to add to the above list of elementary proofs or variations of proofs.

Acknowledgment. We wish to thank the referee, whose suggestions led to a considerable improvement in the presentation of this paper.

REFERENCES

1. M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag, New York, NY, 1988.
2. M. Brennan, A note on the converse to Lagrange's theorem, *The Math. Gazette*, 82 (494), July 1998, 286–288.
3. J. D. Dixon, *Problems in Group Theory*, Dover, New York, NY, 1973.
4. J. Gallian, On the converse to Lagrange's theorem, this MAGAZINE, 66 (1993), 23.
5. I. N. Herstein, *Abstract Algebra*, 2nd ed., Macmillan, New York, NY, 1990.
6. G. T. Hogan, More on the converse to Lagrange's theorem, this MAGAZINE 69 (1996), 375–376.
7. T. W. Hungerford, *Algebra*, Springer-Verlag, New York, NY, 1974.
8. G. Mackiw, The linear group $SL(2,3)$ as a source of examples, *The Math. Gazette*, March 1997, 64–67.
9. J. J. Rotman, *An Introduction to the Theory of Groups*, 3rd ed., Wm. C. Brown, Dubuque, IA, 1988.
10. K. Spindler, *Abstract Algebra with Applications*, Dekker, New York, NY, 1994.

A Principle of Countability

ROBERT KANTROWITZ
Hamilton College
Clinton, NY 13323

Introductory courses in undergraduate analysis usually include a proof of the fact that the rational numbers are countable. In a note appearing in 1986 [**1**], Campbell presents an alternative to the usual diagonalization argument. Touhey's proof in the 1996 article [**4**] proceeds along similar lines. In both of these papers, two sets are declared to have the same cardinality if each can be mapped in a one-to-one manner into the other. Most sources refer to this condition as the Cantor–Bernstein Theorem [**5**, p. 103] or the Schröder–Bernstein Theorem [**2**, p. 99; **3**, p. 74], a deeper result that may not appear in an introductory analysis course.

In this note, I state a principle of countability and illustrate how it may be applied both to argue the countability of some familiar sets and to prove two well-known general results about countable sets. The main difference between the present approach and that in [**1**] and [**4**] is that, here, countability is established without any mention of Cantor/Schröder–Bernstein, but rather by appealing to the definition of, and an elementary result about, countable sets. The function defined in establishing the principle here is also slightly more general. The principle is likely part of the lore of the subject of infinite sets, but it certainly deserves to be better known. It appears in no textbook from which I have studied or taught. The underlying idea was shown to me in graduate school by Professor John L. Troutman at Syracuse University.

A set S is called *finite* if, for some natural number n, there is a one-to-one, onto function between S and the initial segment $\{1, 2, \ldots, n\}$ of the set of natural numbers $\mathbb{N}$. If there is a one-to-one, onto function between S and the set $\mathbb{N}$, then S is called *countably infinite*. A set that is either finite or countably infinite is said to be *countable*.

The main ingredients of the result that follows are a fixed, finite base set, called the *alphabet*, the elements of which are called *letters*, and the *words* that may be formed