divisibility properties of integers. I am grateful to him and to Kit Nair and Alastair King for provoking me to complete this proof as a means of avoiding the more complicated induction proofs. I must thank the referee for suggestions which allowed me to extend my original presentation with $b = \pm 1$ to the general case, and for the outline of the alternative proof of Theorem B.

REFERENCES

[D] L. E. Dickson, History of the Theory of Numbers, vol. 1, 1919, (Chelsea reprint, New York 1971).

[L1] E. Lucas, Sur les rapports qui éxistent entre la théorie des nombres et le calcul intégral. Comptes Rendus, Paris 82 (1876), 1303–5.

[L2] E. Lucas, Sur la théorie des nombres premiers, Atti R. Accad. Sc. Torino (Math), 11 (1875–6), 928–937.

[HW] G. H. Hardy and E. M. Wright, Introduction to the Theory of Numbers. OUP, 1938.

Department of Pure Mathematics
University of Liverpool
P.O. Box 147
Liverpool, L69 3BX
UNITED KINGDOM
h.r.morton@liv.ac.uk

Generating Symmetric Groups

I. M. Isaacs and Thilo Zieschang

It is well known that the symmetric group S_n on the symbols $\{1, 2, 3, \ldots, n\}$ can be generated by two carefully chosen permutations. It is easy to check, for example, that the cycles $x = (1, 2)$ and $y = (1, 2, 3, \ldots, n)$ will do the job. We prove in this note that except when $n = 4$, care is needed in the choice of only one of the two generators.

Theorem A. *Assume that $n \neq 4$ and let $x \in S_n$ be an arbitrary nonidentity element. Then there exists an element $y \in S_n$ such that $S_n = \langle x, y \rangle$.*

We mention that when $n = 4$, the conclusion of Theorem A really fails. If $x = (1, 2)(3, 4)$, then x lies in the normal Klein subgroup K of S_4 of order 4. Since the factor group S_4/K is noncyclic, there can be no element $y \in S_4$ such that $\langle x, y \rangle$ is the whole group.

To prove Theorem A, we need a way to recognize when a subgroup $G \subseteq S_n$ is actually the whole group. A well-known (and nearly trivial) result of this type is that if G contains all transpositions (that is 2-cycles) of S_n, then $G = S_n$. It is almost as easy to see also that if G contains all 3-cycles of S_n, then it contains the alternating group A_n, and so either $G = A_n$ or $G = S_n$. In this case, if we can find some odd permutation in G, it follows that G is the whole group S_n.

To use the results of the previous paragraph, it may seem necessary to undergo the tedium of checking that the subgroup G contains every transposition or every 3-cycle. There is a marvelous short-cut, however, discovered around 1870 by

C. Jordan, that enables one to get away with establishing the existence of just one transposition or one 3-cycle in G. Obviously, this could not possibly work for a completely arbitrary subgroup $G \subseteq S_n$, and there is another hypothesis needed for Jordan's theorem.

Write $\Omega = \{1, 2, 3, \ldots, n\}$. If $x \in S_n$ and $\Delta \subseteq \Omega$, we write Δx to denote the image of Δ under the map x. (The subset $\Delta x \subseteq \Omega$ is called the **translate** of Δ under the permutation x.) Now fix a subgroup $G \subseteq S_n$. A nonempty subset $\Delta \subseteq \Omega$ is said to be a **block** for G if for each element $x \in G$, the translate Δx is either disjoint from or equal to Δ. Clearly, each singleton subset of Ω is a block and so too is the whole set Ω, but these are certainly not very interesting and they are referred to as **trivial** blocks. The situation in which Jordan's theorem applies is where the group G is **primitive**, which means that the *only* blocks for G are the trivial ones.

It is instructive to play a little with the definitions of blocks and primitive groups. Fix a subgroup $G \subseteq S_n$ and observe that if the set Ω can be decomposed into pairwise disjoint parts that are permuted by the translations via elements of G, then each part is a block. (We call such a decomposition of Ω a **G-invariant partition**.) Conversely, every block for G must be one of the parts of some **G-invariant partition**. To see this, let Δ be an arbitrary block and observe that the translates of Δ via elements of G must also be blocks. The distinct translates of Δ are pairwise disjoint, therefore, and if their union is the whole set Ω, we have a G-invariant partition. Otherwise, we can get a G-invariant partition by creating one additional part consisting of all the left-over points.

We can always decompose Ω into its orbits under the action of G and we observe that this is trivially a G-invariant partition. Orbits are thus blocks and it follows that if G is primitive, then either all orbits are singleton sets and G is the trivial group, or else the whole set Ω is an orbit and G is transitive. It is easy to see for $n > 2$ that the trivial group is not primitive and it follows (for $n \neq 2$) that primitive groups are always transitive.

To see a natural example of a transitive group that is not primitive, imaging marking the faces of a cube with the numbers 1 through 6 and let $G \subseteq S_6$ be the group of permutations induced by rotations of the cube. (Note that G is transitive and $|G| = 24$.) For definiteness, suppose that the cube is numbered as is standard for dice, so that on each pair of opposite faces, the numbers total 7. Since every rotation of the cube carries a pair of opposite faces to a pair of opposite faces, we see that the three sets $\{1, 6\}$, $\{2, 5\}$ and $\{3, 4\}$ form a G-invariant partition of $\Omega = \{1, 2, 3, 4, 5, 6\}$, and hence each of them is a nontrivial block for G, which is therefore imprimitive.

In general, if Δ is a block of a transitive subgroup $G \subseteq S_n$, then the G-translates of Δ cover Ω, and hence they form a G-invariant partition in which all parts have equal size. It follows in this case that $|\Delta|$ must divide n. Also, if Δ is nontrivial, then so are its translates, and hence if G is transitive but imprimitive, it follows that every element of Ω lies in a nontrivial block. We state this observation formally for future reference.

Lemma. *Suppose $G \subseteq S_n$ is transitive and let $a \in \Omega$. Then G is primitive if the only blocks containing a are $\{a\}$ and Ω.* ∎

One of the goals of this paper is to provide a direct and elementary proof of Jordan's theorem, which we can now state.

Theorem (Jordan). *Suppose that G is a primitive subgroup of S_n.*

(a) *If G contains a transposition, then $G = S_n$.*
(b) *If G contains a 3-cycle, then either $G = S_n$ or $G = A_n$.*

Proof: We prove part (a) first. Build an undirected graph $\mathcal{G}$ with vertex set $\Omega = \{1, 2, 3, \ldots, n\}$ by joining distinct vertices a and b if the transposition (a, b) happens to lie in the group G. The connected components of $\mathcal{G}$ partition the vertex set Ω and we claim that these components are blocks for G. It suffices to show that the components form a G-invariant partition, and so we must prove that they are permuted by the elements of G. Since it is clear that the components are permuted by graph automorphisms, we want to show that each element of G actually is an automorphism of $\mathcal{G}$.

If vertices a and b are joined in $\mathcal{G}$, we must show for each element $g \in G$ that vertices $(a)g$ and $(b)g$ are also joined. If a and b are joined, however, then the transposition $t = (a, b)$ lies in G and hence $t^g = g^{-1}tg$ is also an element of g. Since t^g is the transposition $((a)g, (b)g)$, however, we deduce that $(a)g$ and $(b)g$ actually are joined in $\mathcal{G}$, as required.

We now know that the connected components of $\mathcal{G}$ are blocks for G. By assumption G is primitive, however, and this tells us that either each component is a singleton and the graph is totally disconnected, or else the whole set Ω is one component and the graph is connected. Since we are given that G contains a transposition, we know that $\mathcal{G}$ contains an edge and it is not totally disconnected. It follows that $\mathcal{G}$ is a connected graph.

To prove that G is the full symmetric group, it suffices to show that it contains an arbitrary transposition (a, b). Seeking a contradiction, we assume that vertices a and b are not directly joined in $\mathcal{G}$. We know that there is some path leading from a to b in the graph and we suppose that a, m and n are three consecutive vertices in some shortest path from a to b. (Note the possibility that $n = b$.) Since transpositions (a, m) and (m, n) are in G, it follows that $(a, n) = (m, n)(a, m)(m, n)$ is also an element of G, and thus a is joined directly to n in $\mathcal{G}$. This is a contradiction since it follows that we can delete m from a shortest path from a to b to obtain a still shorter path.

The proof of (b) is similar, but a little more complicated. Again we construct an undirected graph $\mathcal{G}$ with vertex set Ω, but this time, we join vertices a and b if G contains some 3-cycle moving both a and b. (In other words, a and b are joined iff G contains both the 3-cycle (a, b, u) and its inverse (b, a, u) for some point $u \in \Omega$.) Here too, the permutations $g \in G$ are graph automorphisms since if $t = (a, b, u)$ lies in G, then $t^g = ((a)g, (b)g, (u)g)$ also lies in G. As in the proof of part (a), the hypotheses on G enable us to deduce that the graph $\mathcal{G}$ is connected.

Continuing to parallel the proof of part (a), we show next that $\mathcal{G}$ is a complete graph. Exactly as before, it suffices to show that if a, m and n are three distinct vertices such that a is joined to m and m is joined to n, then a and n are directly joined. We know that G contains a 3-cycle g that moves a and m and a 3-cycle h that moves m and n, and our task is to produce a 3-cycle in G that moves a and n. We are done unless $(n)g = n$ and we can assume that $g = (m, a, u)$ so that $(m)g = a$. Now h is a 3-cycle moving m and n and it follows that its conjugate h^g is a 3-cycle moving $(m)g = a$ and $(n)g = n$, as desired.

To show that G is either A_n or S_n, it suffices to show that G contains an arbitrary 3-cycle (a, b, c). Since the graph $\mathcal{G}$ is known to be complete, vertices a

and b are joined and thus G contains the 3-cycle $t = (a, b, u)$ for some element $u \in \Omega$. Similarly, G contains $s = (b, c, v)$ and we can certainly assume that $u \neq c$ and that $v \neq a$. If $u = v$, then $st = (b, c, u)(a, b, u) = (a, b, c)$ and this lies in G, as required. If $u \neq v$, on the other hand, we compute that

$$t^{-1}s^{-1}tst = (u, b, a)(v, c, b)(a, b, u)(b, c, v)(a, b, u) = (a, b, c)$$

and again, $(a, b, c) \in G$. ∎

The following result has appeared in various places as a problem, apparently with the intention that it should be done by 'brute force'. In fact, it provides a good demonstration of the power of Jordan's theorem, and that is why we present it here.

Theorem B. *In the symmetric group S_n, write $x = (1, 2, 3, \ldots, n)$ and let $y = (1, 2, 3, \ldots, m)$ for some integer m such that $1 < m < n$. Then $\langle x, y \rangle$ is the whole symmetric group unless both n and m are odd, in which case $\langle x, y \rangle$ is the alternating group A_n.*

Proof: We show first that $G = \langle x, y \rangle$ is primitive. Certainly, G is transitive, and so by the lemma, it suffices to show that a block Δ containing 1 and at least one other number $a \in \Omega$ must be the whole set Ω. If $a > m$, then $(a)y = a$, and so $a \in \Delta \cap \Delta y$. But Δ is block, and hence $\Delta y = \Delta$. Since $1 \in \Delta$, we see that $2 \in \Delta$, and thus $2 \in \Delta \cap \Delta x$. We conclude that $\Delta x = \Delta$ and thus Δ must be the whole set Ω, as desired.

If, on the other hand, $a \leq m$, then since $a > 1$, we see that $a = (a)x^{-1}y$. Thus $a \in \Delta \cap \Delta x^{-1}y$ and we conclude that $\Delta x^{-1}y = \Delta$. Thus $n = (1)x^{-1}y$ lies in Δ and we are in the case of the previous paragraph.

Since we now know that G is primitive, we will be able to apply Jordan's theorem if we can find a 3-cycle in G. Observe that

$$(a)xy = a + 2 = (a)yx \qquad \text{if } 1 \leq a \leq m - 2 \quad \text{and}$$

$$(a)xy = a + 1 = (a)yx \qquad \text{if } m + 1 \leq a \leq n - 1,$$

and so xy and yx agree on all numbers in Ω except possibly $m - 1$, m and n. It follows that $xyx^{-1}y^{-1}$ fixes all but these three numbers and we compute that

$$(m - 1)xyx^{-1}y^{-1} = n,$$

$$(m)xyx^{-1}y^{-1} = m - 1 \quad \text{and}$$

$$(n)xyx^{-1}y^{-1} = m.$$

It follows that $xyx^{-1}y^{-1} = (m - 1, n, m)$ and G does contain a 3-cycle.

By Jordan's theorem, G is either A_n or S_n and our remaining task is to determine which group we actually have. If n is even, then x is an odd permutation and if m is even, then y is an odd permutation, and so in these cases $G \neq A_n$ and we conclude $G = S_n$. If m and n are both odd, however, then x and y are even permutations, which lie in A_n. It follows that $G \subseteq A_n$ and hence $G = A_n$ in this case. ∎

Proof of Theorem A. The result is clear when $n < 4$, and so we can assume that $n > 4$ and we consider first the case where n is odd. By renaming the symbols being permuted, we can suppose that x moves 1 but that $(1)x \neq 2$. Let $y =$

$(1,2)(3,4,\ldots,n)$, the product of a transposition and a cycle having odd length $n-2$ and write $G = \langle x, y\rangle$. Since $n-2$ is odd, the element y^{n-2} is a transposition in G and it suffices by Jordan's theorem to show that G is primitive.

Since x carries 1 to something other than 2, we see that G is transitive. Let $\Delta < \Omega$ be a block containing 1, so that by the lemma, it suffices to show that $\Delta = \{1\}$. Note that $|\Delta|$ is a proper divisor of n and in particular, it is odd and at most $n/2$. Since y^2 fixes 1, we see that $1 \in \Delta \cap \Delta y^2$, and thus $\Delta = \Delta y^2$. But $\{3,4,\ldots,n\}$ is an orbit for $\langle y^2\rangle$ (since $n-2$ is odd), and thus if any one of the numbers a with $3 \le a \le n$ lies in Δ, they all do, and $|\Delta| \ge n-1 > n/2$, a contradiction. Also $2 \notin \Delta$ since otherwise $|\Delta| = 2$, and this is a contradiction too. Thus $\Delta = \{1\}$ and we are now done in the case where n is odd.

Now, assume that n is even. If x is a transposition, we can suppose that $x = (1,2)$ and we take $y = (1,2,3,\ldots,n)$ so that $\langle x, y\rangle$ is the whole symmetric group. If x is a 3-cycle, we can suppose that $x = (1,2,3)$ and again we take $y = (1,2,3,\ldots,n)$. In this case too, $\langle x, y\rangle$ is the whole symmetric group by Theorem B, since n is even.

We can now assume that x moves at least four points. By renaming symbols if necessary, we can suppose that $(3)x = 4$. There are at least two numbers other than 3 and 4 moved by x and at least one of these, say 1, is not carried to 3 and we can assume $(1)x = 2$. Now let $y = (2,3)(4,5,\ldots,n)$, the product of a transposition and a cycle of odd length $n-3$, and let $G = \langle x, y\rangle$. Since $n-3$ is odd, y^{n-3} is a transposition in G and by Jordan's theorem, it suffices to show that G is primitive.

Since x carries 1 to 2 and 3 to 4, we see that G is transitive on Ω. The lemma thus applies, and so as before, if we suppose that $\Delta < \Omega$ is a block for G containing 1, it suffices to show that $\Delta = \{1\}$. Now y fixes 1, and so $1 \in \Delta \cap \Delta y$ and we conclude that $\Delta y = \Delta$. It follows that if any one of the numbers a with $4 \le a \le n$ lies in Δ, they all do. In this situation, $|\Delta| \ge n-2 > n/2$, where the strict inequality holds because $n > 4$. This is a contradiction since $|\Delta|$ is a proper divisor of n, and we conclude that $\Delta \subseteq \{1,2,3\}$.

Recall that $(1)x = 2$ and $(3)x = 4$ and hence $\{1,2,3\}x$ is neither equal to nor disjoint from $\{1,2,3\}$. Thus $\{1,2,3\}$ is *not* a block for G, and so Δ must be a proper subset of this set. Because $\Delta y = \Delta$, however, we see that if either 2 or 3 lies in Δ, they both do, and this is a contradiction. We conclude that $\Delta = \{1\}$, as required. ■

A result similar to Theorem A is known to be valid for the alternating group A_n for all values of n. Although it seems likely that a proof of this result along the lines of our proof of Theorem A might exist, there are technical difficulties in some cases, and we have not actually found such a proof.

Finally, we remark that Jordan proved much more than the result we credited him with here. He showed that if G is a primitive subgroup of S_n and H is a nontrivial subgroup of G that fixes m points and is primitive in its action on the remaining $n-m$ points, then G is $(m+1)$-fold transitive. (This means that given two arbitrary ordered $(m+1)$-tuples of distinct points of Ω, there exists an element of G that carries one to the other.) The result of Jordan that we stated follows easily from this by taking H to be the subgroup generated by the given transposition or 3-cycle. Much more can be obtained, however. For example, suppose that instead of a transposition or a 3-cycle, we know that G contains a p-cycle for some arbitrary prime number p. It is not too hard to show from Jordan's result that if $p \le n-3$, then G must be either A_n or S_n. We refer the reader to Wielandt's book [**1**] for more information on all of this.

REFERENCES

1. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

Department of Mathematics
University of Wisconsin
Madison, WI 53706-1313
isaacs@math.wisc.edu

Department of Computer Science
University of Saarland
Geb. 36, Postfach 1150
66041 Saarbruecken
zie@cs.uni-sb.de

On the Arithmetic–Geometric Mean Inequality

Lutz G. Lucht

Beckenbach and Bellman [**1**] contains many beautiful proofs of the well-known inequality between the weighted arithmetic and geometric means of n positive real numbers. In this note another short proof is given which is based on the common log properties: (i) the log curve is concave, (ii) the log function is a homomorphism of $\mathbb{R}_+$ onto $\mathbb{R}$.

Let t be a positive real number. Then

$$t - 1 > \log t \tag{1}$$

except for $t = 1$ when equality in (1) obviously holds. This comes, for example, from the mean-value theorem in analysis by considering the logarithmic function on the interval with endpoints $1, t$.

Suppose that the real numbers $\xi, x_1, \ldots, x_n$ and the weights $\lambda_1, \ldots, \lambda_n$ are positive, with $\lambda_1 + \cdots + \lambda_n = 1$. From (1), applied to $t = x_\nu/\xi$, we obtain after multiplication with $\lambda_\nu \xi$

$$\lambda_\nu x_\nu \geq \lambda_\nu \xi + \xi \log \frac{x_\nu^{\lambda_\nu}}{\xi^{\lambda_\nu}} \quad (\nu = 1, \ldots, n).$$

Addition gives

$$\lambda_1 x_1 + \cdots + \lambda_n x_n \geq \xi + \xi \log \frac{x_1^{\lambda_1} \ldots x_n^{\lambda_n}}{\xi}.$$

Now choose

$$\xi = x_1^{\lambda_1} \ldots x_n^{\lambda_n},$$

and the arithmetic-geometric mean inequality

$$\lambda_1 x_1 + \cdots + \lambda_n x_n \geq x_1^{\lambda_1} \ldots x_n^{\lambda_n} \tag{2}$$

follows. The above remark concerning equality in (1) shows that the inequality (2) is strict unless $x_1 = \cdots = x_n$.