PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 116, Number 4, December 1992

A GROUP DETERMINANT DETERMINES ITS GROUP

RICHARD MANSFIELD

(Communicated by Ronald M. Solomon)

ABSTRACT. The determinant of a group's multiplication table determines the group.

Let G be a finite group with base set $\{1, 2, \ldots, n\}$ and identity 1. Let $x_1, x_2, \ldots, x_n$ be (commuting) formal variables. Consider the determinant of the matrix whose i, j entry is x_k where $k = ij^{-1}$. Call this determinant $D_G(x_1, x_2, \ldots, x_n)$. D_G is a polynomial with integer coefficients. This somewhat arcane construction was presented by Frobenius [3]. The purpose of this note is to show that given D_G, we can actually calculate G. Formanek and Sibley [2] prove a similar theorem, but their proof does not provide a practical method of calculating G. (The best they can do is to enumerate all n-element groups, until one is found with the right determinant.) The present proof is also much shorter and much more elementary than theirs.

In the course of proving this theorem, we will prove a lemma similar to a proposition in Bourbaki [1, p. 139]. We will show that if G is a group and we are given the function that associates to each pair x, y from G the unordered pair $\{xy, yx\}$, then we can calculate the group operation. Bourbaki's result says that G is determined by this function, but it does not give a method of calculation. The present proof is also shorter than Bourbaki's.

Lemma 1. *If the monomial* $x_{a(1)}x_{a(2)}\cdots x_{a(n)}$ *occurs in* D_G *then the* $a(i)$ *can be ordered so that their product is* 1.

Proof. Since the monomials in a determinant represent selectors of one element from each row and column, we might as well assume that the $a(i)$ have been numbered so that $a(i) = ip(i)^{-1}$ for some permutation p. Now consider the representation of p as a product of disjoint cycles.

Lemma 2. *If* $ab = 1$ *then the monomial* $x_1^{n-2}x_ax_b$ *occurs in* D_G.

Proof. Let $a = ij^{-1}$. Then $b = ji^{-1}$ and the permutation $p = (i, j)$ gives the desired monomial. Furthermore, any permutation giving this monomial must be the identity except for exactly two points and, therefore, must be a transposition with sign -1. Thus none of these monomials cancel each other

Received by the editors April 18, 1991.
1991 *Mathematics Subject Classification.* Primary 15A15; Secondary 16S99, 20B05, 20B40, 20C15.

in D_G. (Actually, the coefficient is $-n/2$ or $-n$ depending on whether or not $a = b$.)

Lemma 3. *If $abc = 1$ then the monomial $x_1^{n-3}x_a x_b x_c$ occurs in D_G.*

Proof. If either of a, b, or c equals 1, this lemma reduces to the previous one, so we might as well assume that none of them are 1. Let $a = ij^{-1}$. Pick k such that $b = jk^{-1}$. Then $c = ki^{-1}$. So the permutation $p = (i, j, k)$ gives the desired monomial. Furthermore, any permutation giving this monomial must be a 3-cycle and hence have sign $+1$. So again, no cancellation occurs. (The coefficient is n if $ab \neq ba$ or $a = b$. Otherwise it is $2n$.)

Lemma 4. *If G is a group and we are given the function that associates to each pair x, y from G the unordered pair $\{xy, yx\}$, then we can calculate the two functions $x, y \to xy$ and $x, y \to yx$. However, we may not know which is which.*

This is the lemma discussed in the introduction. Let us defer its proof for a moment and go on to the main theorem.

Theorem. *If G is a finite group with base set $\{1, 2, \ldots, n\}$ and identity 1 and we are given D_G, then we can calculate the two functions of Lemma 4, again with the proviso that we may not know which is which.*

Proof. From Lemmas 1 and 2, we can calculate $x \to x^{-1}$ by looking at the monomials $x_1^{n-2}x_a x_b$ occurring in D_G. Then $\{ab, ba\} = \{c^{-1} : x_1^{n-3}x_a x_b x_c$ occurs in $D_G\}$. Lemma 4 completes the proof.

Note that this proof is actually somewhat more general than we had claimed. Since the coefficients produced in Lemmas 2 and 3 are all divisors of $2n$, the theorem remains true when D_G is reduced mod K where K is any field whose characteristic does not divide $2n$.

Proof of Lemma 4. If G is abelian, there is nothing to prove. So assume that a and b are given with $ab \neq ba$ and that we know the value of ab. We show that the functions $x, y \to xy$ can then be calculated.

Claim 1. For any c, abc can be calculated.

Proof. Since ab is known, we can find $\{abc, cab\}$ as the two possible values of $(ab)c$. Likewise, using the two possible values of bc, we can calculate $\{abc, acb, bca, cba\}$ as the range of possible values for $a(bc)$. If these two sets have a one-element intersection, we are done. Otherwise $abc \neq cab$ and one of the three possibilities $cab = cba$ or $cab = acb$ or $cab = bca$ must hold.

In the first case, $ab = ba$, which is a contradiction. In the second, $ac = ca$. We can, of course, determine whether or not this is true by examining $\{ac, ca\}$. Then cab can be determined and, consequently, abc. To do this look at the two sets $\{cab, abc\}$ and $\{cab, bca\}$ as the range of possible values of $c(ab)$ and $(ca)b$, respectively. Their intersection is cab unless $abc = bca$. But then $bca = bac$, hence $abc = bac$ and $ab = ba$, which is a contradiction.

For the third case, let $x = cab = bca$. Then $xb^{-1} = b^{-1}x = ca$. Therefore, we can determine abc unless it also has this property; i.e., $b^{-1}(abc) = (abc)b^{-1} \in \{ac, ca\}$. If $b^{-1}abc = ac$ then $ab = ba$, which is a contradiction. If $abcb^{-1} = ca$ then $abc = cab$, which case has already been eliminated.

Claim 2. For any c, bc can also be calculated.

Proof. Apply the previous claim to $a^{-1}(ab)c$.

Claim 3. For any c and d, if $bc \neq cb$ then cd can be calculated.

Proof. bc can be calculated using the previous claim. Therefore, cd can also be calculated using the same claim with b, c in place of a, b.

From Claim 3 it easily follows that we can calculate cd whenever $ac \neq ca$ or $ad \neq da$ or $bc \neq cb$ or $bd \neq db$. Therefore, the proof of Lemma 4 is completed with the following claim.

Claim 4. If $ac = ca$ and $da = ad$ and $bc = cb$ and $bd = db$, then cd can be calculated.

Proof. Since $ac = ca$ and $bd = db$, we know these two values. Thus we can calculate $\{abcd, badc\}$ as the range of possible values for $(ac)(bd)$. Also since ab commutes with both cd and dc, we can calculate $(ab)\{cd, dc\} = \{abcd, abdc\}$. But $badc = abdc$ implies $ba = ab$. Therefore, these two sets have but one element in common and we can calculate $abcd$. Now apply Claim 1 to $b^{-1}a^{-1}(abcd)$.

References

1. N. Bourbaki, *Elements of mathematics–Algebra* I, Chapters 1–3, Springer-Verlag, Berlin, 1970.
2. E. Formanek and D. Sibley, *The group determinant determines the group*, Proc. Amer. Math. Soc. **112** (1991), 649–656.
3. F. G. Frobenius, *Über die Darstellung der endlichen Gruppen durch lineare substitionen*, Sitz. Kon. Preuss. Akad. Wiss. Berlin (1897), 944–1015; *F. G. Frobenius—Gessamelte Abhandlung*, vol. III, Springer-Verlag, Berlin, 1968.
4. H.-J. Hoenke and K. W. Johnson, *The 3-characters are sufficient for the group determinant*, preprint.
5. H.-J. Hoenke, *Über komponierbare Formen und konkordante hyperkomplexe Grössen*, Math. Z. **70** (1958), 1–12.
6. ——, *Über Bezeihungen zwischen Problemen von H. Brandt aus der Theorie der Algebren und den Automorphismen der Normenform*, Math. Nachr. **34** (1967), 229–256.
7. K. W. Johnson, *Latin square determinants*, Algebraic, Extermal and Metric Combinatorics 1986, London Math. Soc. Lecture Note Ser., vol. 131, Cambridge Univ. Press, Cambridge, 1988, pp. 146–154.
8. ——, *Latin square determinants*. II, Discrete Math. (to appear).
9. Moshe Roitman, *A complete set of invariants for finite groups and other results*, Adv. Math. **41** (1981), 301–311.

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802

E-mail address: melvin@math.psu.edu