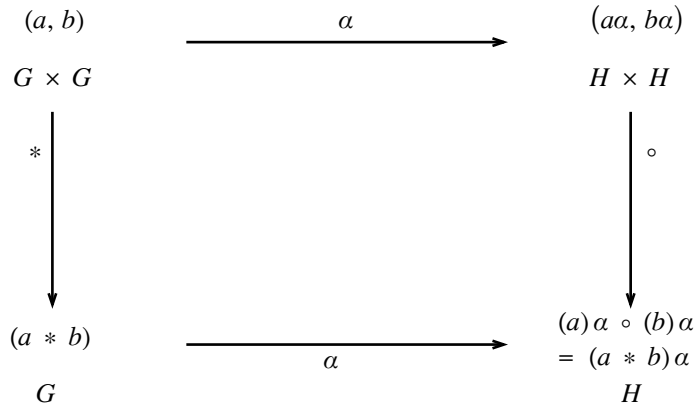
Verifying non-isomorphism of groups

DES MacHALE

The concept of isomorphism is central to group theory, indeed to all of abstract algebra. Two groups $\{G, *\}$ and $\{H, \circ\}$ are said to be *isomorphic* to each other if there exists a set bijection α from G onto H, such that $(a * b)\alpha = (a)\alpha \circ (b)\alpha$ for all $a, b \in G$. This can be illustrated by what is usually known as a *commutative diagram*:



Roughly speaking, this tells us that if we follow the fortunes of an ordered pair of elements (a, b) of G along the top and then down the right hand side of the diagram, we wind up with the same element as if we first went down the left hand side of the diagram and then along the bottom.

More importantly however, the existence of an isomorphism between groups $\{G, *\}$ and $\{H, \circ\}$ means that $\{G, *\}$ and $\{H, \circ\}$ have the 'same group theoretic structure' and that $\{H, \circ\}$ is the 'same' group as $\{G, *\}$, except possibly for a change of notation.

From now on we adopt the usual convention of dropping the binary operations $*$ and $\circ$ where no danger of confusion exists, so that groups G and H are isomorphic if there exists a bijection α from G onto H such that $(ab)\alpha = (a)\alpha\,(b)\alpha$, for all a and b in G.

A very useful application of the concept of isomorphism of groups is the following. Isomorphism is easily seen to be an equivalence relation on groups and the resulting equivalence classes are called abstract groups. Thus when we say there are just two abstract groups of order four, we mean that any group with exactly four elements is isomorphic either to the cyclic group of order four (called C_4) or the Klein four group (called $C_2 \times C_2$). Each of these two abstract group types has infinitely many concrete manifestations among which are:

https://doi.org/10.1017/mag.2021.114 Published online by Cambridge University Press

The cyclic group of order four C_4

(i) $\{1, i, -i, -1\}$ under multiplication of complex numbers.

(ii) $\{e, (1234), (13)(24), (1432)\}$ of permutations on four symbols under composition.

(iii) Rotations of a square with fixed centre under composition.

(iv) $C_4 = \{x \mid x^4 = 1\}$ (abstract version).

The Klein four-group $C_2 \times C_2$

(i) Symmetries of a non-square rectangle under composition.

(ii) Permutations $\{e, (12), (34), (12)(34)\}$ under composition.

(iii) Permutations $\{e, (12)(34), (13)(24), (14)(23)\}$ under composition.

(iv) $\{a, b \mid a^2 = b^2 = 1; ab = ba\}$ (Abstract version).

But in general verifying that groups G and H are isomorphic to each other is not an easy task. Of course if the sets G and H have different cardinalities, we are done at once and no isomorphism can exist. If both sets G and H are infinite, one could spend forever checking bijections and still not be able to decide, but even if G and H are finite and of the same cardinality, very many bijections need to be checked. In the long run, to show an isomorphism exists, one must produce a bijection with the required property or prove a result implying that it exists.

And how can one go about showing that two groups G and H are not isomorphic to each other? At first glance it might appear that one would have to examine all bijections from G onto H, and show that none of them has the desired property, but this is not the case. Another possibility is to find a group theoretic property that G has and that H does not have, or vice versa. By a group theoretic property we mean one that follows from the group axioms.

Examples of non-group theoretic properties are:

(i) G is a group of matrices under matrix multiplication.

(ii) G is a group containing odd permutations.

For example, we have already mentioned these two groups of order 4:

$$G_1 = \{e, (12), (34), (12)(34)\}$$

$$\text{and } G_2 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

These two groups are in fact isomorphic to each other despite the fact that G_1 contains odd permutations on $\{1, 2, 3, 4\}$ whereas G_2 does not.

In this paper we pick two abstract finite groups of the same cardinality and show in very many ways that they are not isomorphic to each other. The first group we pick is $S_3 = \{e, (12), (13), (23), (123), (132)\}$ of all permutations on three objects, under composition of permutations. S_3 is

https://doi.org/10.1017/mag.2021.114 Published online by Cambridge University Press

isomorphic to the group of all symmetries of an equilateral triangle with vertices labelled 1, 2, 3, under composition of symmetries. The second group we pick is $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$ of all rotations of a regular hexagon fixed at its centre under composition of rotations, where x represents a counter-clockwise rotation through 60°. Both groups have order 6.

In each case we show S_3 and C_6 are not isomorphic to each other by demonstrating a group-theoretic property which they do not share. For brevity, we do not define all of the terms we use, but these are standard and may be found in textbooks such as MacDonald [1] and Herstein [2].

1. S_3 is not a cyclic group whereas C_6 is a cyclic group, i.e. S_3 does not consist of the powers of a single element whereas C_6 does.
2. Elements (12) and (123) do not commute with each other, whereas $ab = ba$ for all $a, b \in C_6$. That is, S_3 is a non-abelian group whereas C_6 is abelian.
3. The orders of the elements of S_3 are {1, 2, 2, 2, 3, 3} whereas the orders of the elements in C_6 are {1, 2, 3, 3, 6, 6}. It can be shown that an isomorphism sends an element of a given order to an element of the same order.
4. S_3 has precisely six subgroups whereas C_6 has precisely four subgroups.
5. S_3 has precisely three normal subgroups whereas C_6 has precisely four normal subgroups.
6. S_3 has precisely five cyclic subgroups whereas C_6 has precisely four cyclic subgroups.
7. S_3 has precisely five abelian subgroups whereas C_6 has precisely four abelian subgroups.
8. S_3 has precisely three conjugacy classes of subgroups whereas C_6 has precisely four conjugacy classes of subgroups.
9. S_3 has trivial centre $Z(S_3)$ with $|Z(S_3)| = 1$, whereas C_6 has non-trivial centre $Z(C_6)$, with $|Z(C_6)| = 6$.
10. S_3 has central factor group $S_3/Z(S_3)$ of order 6, whereas C_6 has trivial central factor group $C_6/Z(C_6)$ of order 1.
11. S_3 has exactly three conjugacy classes of elements, whereas C_6 has exactly six conjugacy classes of elements.
12. S_3 has commutator subgroup S_3 cyclic of order 3, whereas C_6 has commutator subgroup C_6 of order 1.
13. S_3/S_3' is cyclic of order 2, whereas C_6/C_6' is cyclic of order 6.
14. S_3 has automorphism group of order 6 whereas C_6 has automorphism group of order 2.
15. S_3 has conjugacy class equation $6 = 1 + 2 + 3$, whereas C_6 has conjugacy class equation $6 = 1 + 1 + 1 + 1 + 1 + 1$.
16. S_3 has exactly three Sylow subgroups of order 2 whereas C_6 has just one Sylow subgroup of order 2.

https://doi.org/10.1017/mag.2021.114 Published online by Cambridge University Press

If we are prepared to use more advanced concepts in group theory, we also have:

17. S_3 has matrix representation degree equation $6 = 1^2 + 1^2 + 2^2$ whereas C_6 has the equation $6 = 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2$.
18. S_3 has derived length 2, whereas C_6 has derived length 1.
19. S_3 is not nilpotent, whereas C_6 is nilpotent.
20. The only element in S_3 which is invariant under all automorphisms of S_3 is the identity element, whereas C_6 has two such elements – the identity and the unique element of order 2.

Doubtless many other reasons could be given and we invite the reader to add to the list.

We now set the reader two exercises:

1. The dihedral groups of order 8, D_4, and the Quaternion group of order 8, Q_2, are not isomorphic to each other. How many of the twenty reasons given previously will demonstrate this? Of course one reason is enough, but the more reasons we can give, the better we will understand the structure and properties of these groups.
2. In which of the twenty cases we have given is it possible to have non-isomorphic groups (of the same order if possible) which share a given property? For example, there are two non-isomorphic groups of order 27 each of which has exactly 11 conjugacy classes. In addition, there are two non-isomorphic groups of order 27 each of which has 1 element of order 1 and 26 elements of order 3.

But there is a severe drawback to the procedure we have given which is rarely mentioned in textbooks. As n grows large, especially if n is a prime power, the number of isomorphism classes, or the number of pairwise non-isomorphic groups of order n, can increase dramatically. For example there are 49,487,365,422 group types of order $1024 = 2^{10}$. Within this set there are billions of groups which share every conceivable group theoretic property, but yet are known to be pairwise non-isomorphic for other theoretical reasons. The problem is that the number of possible group invariants is relatively small, whereas the number of groups is huge, so it is not surprising that some non-isomorphic groups appear indistinguishable from each other.

There is however another approach to isomorphism and non-isomorphism of (finite) groups. It is not elementary, but we now attempt to describe it in simple terms.

The existence of a bijection α between isomorphic groups G and H satisfying $(ab) = (a\alpha)(b\alpha)$, for all a, b in G, can be interpreted as meaning that G and H have the 'same' Cayley or multiplication table. What one needs is a way of expressing this fact in concrete terms. The first step towards this goal was achieved by the great German mathematician Frobenius [3] in 1896, when he introduced the concept of the group

https://doi.org/10.1017/mag.2021.114 Published online by Cambridge University Press

determinant, which can be calculated directly, given the group, or more precisely, its Cayley table. In 1991, Formanek and Sibley [4] established definitively that the group determinant determines the (isomorphism type of) the group.

Let H be a finite group with $|H| = h$ and let the elements of H, E (the identity), $A, B, C, \ldots$ correspond to h independent commuting variables $x_E, x_A, x_B, x_C, \ldots$ so that $x_L = x_M x_N$ if $L = MN$ in the group, which means that $x_{LN^{-1}} = x_M$. The group matrix is then defined to be

$$\begin{pmatrix} x_{EE^{-1}} & x_{EA^{-1}} & x_{EB^{-1}} & \ldots & x_{EQ^{-1}} & \ldots \\ x_{AE^{-1}} & x_{AA^{-1}} & x_{AB^{-1}} & \ldots & x_{AQ^{-1}} & \ldots \\ \vdots & \vdots & \vdots & \cdots & \vdots & \cdots \\ x_{PE^{-1}} & x_{PA^{-1}} & x_{PB^{-1}} & \ldots & x_{PQ^{-1}} & \ldots \\ \vdots & \vdots & \vdots & \cdots & \vdots & \cdots \end{pmatrix} = \left(x_{PQ^{-1}}\right).$$

This matrix determines the Cayley table for H. The determinant $\left|\left(x_{PQ^{-1}}\right)\right|$ of the matrix $\left(x_{PQ^{-1}}\right)$ is called the *group determinant* of H.

Example: Consider the cyclic group of order 3, composed of elements $\{E, A, B\}$ satisfying $A^3 = E, B^2 = A$ and $A^2 = B$, with $E^{-1} = E, A^{-1} = B$ and $B^{-1} = A$. The Cayley table is given by Table 1 and the group matrix

$$\begin{pmatrix} x_E & x_B & x_A \\ x_A & x_E & x_B \\ x_B & x_A & x_E \end{pmatrix}$$

follows from Table 2.

	E	A	B
E	E	A	B
A	A	B	E
B	B	E	A

TABLE 1

	$E^{-1} = E$	$A^{-1} = B$	$B^{-1} = A$
E	$EE^{-1} = E$	$EA^{-1} = B$	$EB^{-1} = A$
A	$AE^{-1} = A$	$AA^{-1} = E$	$AB^{-1} = B$
B	$BE^{-1} = B$	$BA^{-1} = A$	$BB^{-1} = E$

TABLE 2

The group determinant

$$\begin{vmatrix} x_E & x_B & x_A \\ x_A & x_E & x_B \\ x_B & x_A & x_E \end{vmatrix} = x_E\left(x_E^2 - x_A x_B\right) - x_B\left(x_A x_E - x_B^2\right) + x_A\left(x_A^2 - x_B x_E\right)$$

$$= x_E^3 + x_A^3 + x_B^3 - 3x_A x_B x_E,$$

a polynomial of degree 3 in the commuting indeterminates x_E, x_A and x_B.

https://doi.org/10.1017/mag.2021.114 Published online by Cambridge University Press

The reader at this stage may wish to construct the group determinants for the non-isomorphic groups C_4 and $C_2 \times C_2$, perhaps the smallest interesting and relevant case, and see how they compare.

We conclude by outlining how this procedure works in the case of the two groups S_3 and C_6 which we have discussed in the earlier part of this paper.

For S_3, E is the identity and $E^{-1} = E$; $A = (132)$ and $A^{-1} = B$; $B = (123)$ and $B^{-1} = A$; $C = (12)$ and $C^{-1} = C$; $D = (13)$ and $D^{-1} = D$; $F = (23)$ and $F^{-1} = F$.

The Cayley table for S_3 is given by Table 3 and the group determinant of S_3 then becomes

$$\begin{vmatrix} x_E & x_B & x_A & x_C & x_D & x_F \\ x_A & x_E & x_B & x_D & x_F & x_C \\ x_B & x_A & x_E & x_F & x_C & x_D \\ x_C & x_D & x_F & x_E & x_B & x_A \\ x_D & x_F & x_C & x_A & x_E & x_B \\ x_F & x_C & x_D & x_B & x_A & x_E \end{vmatrix}.$$

	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	B	E	D	F	C
B	B	E	A	F	C	D
C	C	F	D	E	B	A
D	D	C	F	A	E	B
F	F	D	C	B	A	E

TABLE 3

	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	B	C	D	F	E
B	B	C	D	F	E	A
C	C	D	F	E	A	B
D	D	F	E	A	B	C
F	F	E	A	B	C	D

TABLE 4

In the case of C_6, the Cayley table is given by Table 4 with $E^{-1} = E$; $A^{-1} = F$; $B^{-1} = D$; $C^{-1} = C$; $D^{-1}B$ and $F^{-1} = A$. The group determinant of C_6 is then given by

$$\begin{vmatrix} x_E & x_F & x_D & x_C & x_B & x_A \\ x_A & x_E & x_F & x_D & x_C & x_B \\ x_B & x_A & x_E & x_F & x_D & x_C \\ x_C & x_B & x_A & x_E & x_F & x_D \\ x_D & x_C & x_B & x_A & x_E & x_F \\ x_F & x_D & x_C & x_B & x_A & x_E \end{vmatrix}.$$

https://doi.org/10.1017/mag.2021.114 Published online by Cambridge University Press

The energetic reader is now invited to evaluate these two group determinants, either by brute force or using theorems on determinants, and show they are not equal. This establishes that the groups S_3 and C_6 are not isomorphic to each other. While theoretically correct, this method is not computationally feasible, since the expansion of an $n \times n$ determinant involves $n!$ terms, a number which grows very rapidly with n.

References

1. I. D. MacDonald, *Theory of Groups*, Oxford (1968).
2. I. N. Herstein, *Topics in Algebra*, Wiley (2013).
3. F. G. Frobenius, *Uber die Darstellung der endlichen Gruppen dursch lineare substitutionen*, Sitz. Kon. Preuss. Acad. Wiss. Berlin (1897) pp. 944-1015.
4. E. Formanek and D. Sibley, The Group Determinant determines the group, *Proc. Amer. Math. Soc.* **112** (3) (1991) pp. 649-656.

DES MacHALE
School of Mathematics, Applied Mathematics and Statistics,
University College Cork, Cork, Ireland
e-mail: *d.machale@ucc.ie*

10.1017/mag.2021.114
© The Mathematical Association 2021

In the Pipeline for March 2022

Fibonacci fraction circles	*Howard Sporn*
Golden right triangles and the golden quadrilateral	*Aldo Scimone*
Two short proofs of the formula $\sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} = \frac{\pi^2}{8}$	*Lubomir Markov*
An index for betting with examples from games and sports	*Talaat Abdin, Hosam Mahmoud, Arian Modarres, Kai Wang*
Power of a point: from Jakob Steiner to modern applications	*Alexandru Gîrban, Bogdan D. Suceavă*
Equal sums, sums of squares and sums of cubes	*G. J. O. Jameson*
Characterisation of equalisation problems via random walks	*Toshio Nakata*
An illustrative derivation of the sum of fifth powers	*Michael H. Baumann*
The arbitrariness of the angle semi-bisectors of a triangle	*Mowaffaq Hajja*
A look back at a long-forgotten trigonometric function: the versine function and its inverse	*Seán M. Stewart*
The majorisation principle for convex functions	*G. J. O. Jameson*
A probabilistic way to discover the rainbow	*Joscha Prochno, Michael Schmitz*

https://doi.org/10.1017/mag.2021.114 Published online by Cambridge University Press