Teaching Note

An odd fact about Cayley tables

All of the current Further Mathematics specifications for students in England have an optional paper that contains a brief introduction to group theory. Typically, these get as far as a statement (if not a proof) of Lagrange's theorem. Apart from the usual elementary results (such as uniqueness of identity and inverses, solutions of equations and the Latin square property of Cayley tables), it is relatively hard to give significant results at this introductory level. I thus offer the following little theorem stressing that, although the result is in the group theory literature, it does not seem to be widely known at school level. In what follows, groups are written multiplicatively with identity element e. By the diagonal of the Cayley table of a group, we will always mean the *leading* diagonal, consisting of the squares of the elements of the group.

Theorem: The diagonal of the Cayley table of a finite group G contains all the elements of G if, and only if, G has odd order.

Proof: Note that, because G is finite, the statement that the diagonal of the Cayley table contains all the elements of G is equivalent to saying that there are no repeated elements on the diagonal.

First, suppose that $|G| = 2k - 1$ is odd. Then, by a standard corollary to Lagrange's theorem, $x^{2k-1} = e$ or $x^{2k} = x$ (*) for all elements x in G. If two diagonal elements in the Cayley table of G are the same, we would have $x^2 = y^2$ with $x \neq y$. But then (*) gives the contradiction $x = (x^2)^k = (y^2)^k = y$.

Conversely, suppose that $|G|$ is even. We will show that G has an element of order 2, so that e appears on the diagonal of the Cayley table at least twice. To see this, we list the elements of G as follows. First list A, the set of elements satisfying $x^2 = e$. Stop if this exhausts G; otherwise there is an element x outside A with $x \neq x^{-1}$. Then either $G = A \cup \{x, x^{-1}\}$, or there is another element y satisfying $y \neq y^{-1}$ with $\{y, y^{-1}\}$ easily checked to be disjoint from $A \cup \{x, x^{-1}\}$. Continuing in this way, we end up listing the elements of G as A together with disjoint 2-element sets of the form $\{x, x^{-1}\}$. Since $|G|$ is even, $|A|$ is then even, which suffices to establish our claim.

An equivalent way of stating the result is that a finite group G has odd order if, and only if, every element of G is a square. For a finite group of even order, the diagonal of the Cayley table comprises all elements of odd order, e repeated for each of the even number of elements of order 2, and the squares of elements with orders which are multiples of 4.

The second half of the proof is a pretty result in its own right and generalises as Cauchy's theorem that, if the prime p divides $|G|$, then G has an element of order p. This has been given a delightful, short, elementary proof by James McKay in [1].

Finally, we should resist any urge to call this little theorem the odd-order theorem: this appellation is reserved for the famous Feit-Thompson theorem with its notoriously long and intricate proof.

https://doi.org/10.1017/mag.2023.119 Published online by Cambridge University Press

Acknowledgement
I am grateful to the referee for the encouraging report on this Note and helpful comments.

Reference

1. J. H. McKay, Another proof of Cauchy's group theorem, *Amer. Math. Monthly* **66** (February 1959) p. 119.

10.1017/mag.2023.119 © The Authors, 2023
Published by Cambridge University Press
on behalf of The Mathematical Association

NICK LORD
Tonbridge School,
Kent TN9 1JP
e-mail: *njl@tonbridge-school.org*

In the Pipeline for March 2024

$xy = \cos(x + y)$ and other implicit equations that are surprisingly easy to plot	*Michael Jewess*
Singular matrices and pairwise-tangent circles	*A. F. Beardon*
Infinitely many composites	*Nick Lord, Des MacHale*
Relating constructions and properties through duality	*David L. Farnsworth, Steven J. Kilner*
Some generalisations and extensions of a remarkable geometry puzzle	*Quang Hung Tran*
A characterisation of regular *n*-gons via (in)commensurability	*Silvano Rossetto Giovanni Vincenzi*
Extensions of Vittas' Theorem	*Nikolaos Dergiades, Quang Hung Tran*
The role of convexity in defining regular polyhedra	*Chris Ottewill*
Euler's prime-producing polynomial revisited	*Robert Heffernan, Nick Lord, Des MacHale*
ABC-Triangles	*Jonny Griffiths*
Patterns among square roots of the 2×2 identity matrix	*Howard Sporn*
The Eureka Theorem of Gauss	*Stan Dolan*
A slowly evolving conical pendulum	*Subhranil De*
Walk on a Grid	*Manija Shahali, H. A. Shahali*

10.1017/mag.2023.120 © The Authors, 2023
Published by Cambridge University Press on behalf of The Mathematical Association