TEACHING NOTES

The proving of Cayley's theorem at Further Mathematics level

Oey Liang Hien

Undoubtedly one of the hardest theorem to prove in "A" level syllabus of Further Mathematics is Cayley's theorem in group theory : "Every finite group of order n is isomorphic to a permutation group on n symbols." This poses to teachers who must teach the theorem at pre-university level a challenge to make their students understand it and its proof on the spot without much difficulty.

In this article, I like to present a method of proof which I think is the most suitable one at this level. In choosing a suitable method of proof, I have been guided by the following points :

(1) Students are, in general, weak in abstract concepts.

(2) No use should be made of concepts which are not in the syllabus. (For example, the proof given by J. A. Green [1] is not suitable as it makes use of the homomorphism theorem.)

(3) It is preferable to have a long but intelligible proof rather than a short but difficult proof. Students are quite prepared to follow a long chain of carefully reasoned steps.

Thus, to overcome the abstractness of whatever proof we present, we could first make the proof more "concrete" by proving the theorem for one particular case before giving the general proof. I estimate that should I prove it generally at once, about 20 per cent of the students would understand it whereas if I prove a particular case and then generalize, 85 to 90 per cent would understand it.

This method of proof is given by Frank Ayres, Jr [2] . Moreover, in this proof there is only one step which is not easily understood by students : if $G = \{g_1, g_2, \ldots, g_n\}$ is a group with respect to the operation $*$ and p_j is the permutation

$$p_j = \begin{pmatrix} g_1 & g_2 & \cdot & \cdot & \cdot & g_n \\ g_1 * g_j & g_2 * g_j & \cdot & \cdot & \cdot & g_n * g_j \end{pmatrix},$$

where $g_j \in G$, then p_j can also be written as

$$p_j = \begin{pmatrix} g_1 * g_k & g_2 * g_k & \cdot & \cdot & \cdot & g_n * g_k \\ (g_1 * g_k) * g_j & (g_2 * g_k) * g_j & \cdot & \cdot & \cdot & (g_n * g_k) * g_j \end{pmatrix}$$

for any given g_k in G.

To convince students, we first give an example to show that in the expression of a permutation, the ordering of the columns is not important :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 5 & 4 & 1 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 2 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}, \text{ etc.}$$

Next, we point out that the columns and rows of a group multiplication table satisfy the Latin square property. That is, each row (or column) contains all the elements of the group without repetition :

$*$	g_1	g_2	$\cdot\ \cdot\ \cdot$	g_k	$\cdot\ \cdot\ \cdot$	g_n
g_1				$g_1 * g_k$		
g_2				$g_2 * g_k$		
$\cdot$				$\cdot$		
$\cdot$				$\cdot$		
$\cdot$				$\cdot$		
g_n				$g_n * g_k$		

These two observations will convince the students of the validity of the second expression for p_j .

Let us verify Cayley's theorem in the case of a particular group G with the following multiplication table

$*$	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_1	g_2	g_3	g_4	g_5	g_6
g_2	g_2	g_1	g_5	g_6	g_3	g_4
g_3	g_3	g_6	g_1	g_5	g_4	g_2
g_4	g_4	g_5	g_6	g_1	g_2	g_3
g_5	g_5	g_4	g_2	g_3	g_6	g_1
g_6	g_6	g_3	g_4	g_2	g_1	g_5

Using the previous notations, define

$$p_5 = \begin{pmatrix} g_1 & g_2 & \cdot & \cdot & \cdot & g_6 \\ g_1 * g_5 & g_2 * g_5 & \cdot & \cdot & \cdot & g_6 * g_5 \end{pmatrix}$$

$$= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_5 & g_3 & g_4 & g_2 & g_6 & g_1 \end{pmatrix}.$$

Or write it simply as

$$p_5 = (156)\ (234)\ .$$

Thus we have the permutations

$$p_1 = (1) \quad , \quad p_2 = (12)\ (36)\ (45)\ ,$$

$$p_3 = (13)\ (25)\ (46) \quad , \quad p_4 = (14)\ (26)\ (35)\ ,$$

$$p_5 = (156)\ (234) \quad , \quad p_6 = (165)\ (243)\ .$$

Form the multiplication table of the set $P = \{ p_1, p_2, p_3, p_4, p_5, p_6 \}$ under composition of permutations :

	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_6	p_1	p_5	p_4	p_2
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_2	p_3	p_6	p_1
p_6	p_6	p_3	p_4	p_2	p_1	p_5

Thus P forms a group under composition.

Define the mapping α from G to P by

$$\alpha(g_i) = p_i \ , \quad i = 1,2,\dots,6 \ .$$

It can be easily seen from the table that α is one-to-one and onto, and also preserves the binary operations. Hence G is isomorphic to P.

We now proceed to give the general proof of Cayley's theorem.

Let $G = \{g_1, g_2, \dots, g_n\}$ be a group under the operation $*$. For each $i = 1,2,\dots,n$, define the permutation

$$p_j = \begin{pmatrix} g_1 & g_2 & \cdot & \cdot & \cdot & g_n \\ g_1 * g_j & g_2 * g_j & \cdot & \cdot & \cdot & g_n * g_j \end{pmatrix},$$

which we simply write as

$$p_j = \begin{pmatrix} g_i \\ g_i * g_j \end{pmatrix} .$$

Note that p_j is a permutation on the n elements of G since the elements in the second row occur in one column of a multiplication table of G and hence run through all the elements of G. We now show that the set

$$P = \{p_1, p_2, \ldots, p_n\}$$

is a permutation group on n symbols.

Let $p_j, p_k \in G$. Then

$$p_j \circ p_k = \begin{pmatrix} g_i \\ g_i * g_j \end{pmatrix} \circ \begin{pmatrix} g_i \\ g_i * g_k \end{pmatrix}$$

$$= \begin{pmatrix} g_i \\ g_i * g_j \end{pmatrix} \circ \begin{pmatrix} g_i * g_j \\ (g_i * g_j) * g_k \end{pmatrix},$$

by the remark mentioned earlier,

$$= \begin{pmatrix} g_i \\ (g_i * g_j) * g_k \end{pmatrix}$$

$$= \begin{pmatrix} g_i \\ g_i * (g_j * g_k) \end{pmatrix},$$

by the associativity of $*$,

$$= \begin{pmatrix} g_i \\ g_i * g_l \end{pmatrix} = p_l,$$

where $g_j * g_k = g_l$ for some $g_l \in G$. Hence P is closed under composition.

Composition is associative and the identity element is $\begin{pmatrix} g_i \\ g_i \end{pmatrix}$. The inverse of $\begin{pmatrix} g_i \\ g_i * g_j \end{pmatrix}$ is $\begin{pmatrix} g_i \\ g_i * g_j^{-1} \end{pmatrix}$.

$$\begin{pmatrix} g_i \\ g_i * g_j \end{pmatrix} \circ \begin{pmatrix} g_i \\ g_i * g_j^{-1} \end{pmatrix} = \begin{pmatrix} g_i \\ g_i * g_j^{-1} \end{pmatrix} \circ \begin{pmatrix} g_i * g_j \\ (g_i * g_j) * g_j^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} g_i \\ (g_i * g_j) * g_j^{-1} \end{pmatrix} = \begin{pmatrix} g_i \\ g_i * (g_j * g_j^{-1}) \end{pmatrix} = \begin{pmatrix} g_i \\ g_i \end{pmatrix} .$$

Similarly,

$$\begin{pmatrix} g_i \\ g_i * g_j^{-1} \end{pmatrix} \circ \begin{pmatrix} g_i \\ g_i * g_j \end{pmatrix} = \begin{pmatrix} g_i \\ g_i \end{pmatrix} .$$

Thus P is a group under the operation of composition.

Define the mapping α from G to P such that

$$\alpha(g_i) = p_i, \quad i = 1, 2, \ldots, n .$$

Moreover, α is clearly one-to-one. To show that α preserves the group operations, we have

$$\alpha(g_r) \circ \alpha(g_s) = \begin{pmatrix} g_i \\ g_i * g_r \end{pmatrix} \circ \begin{pmatrix} g_i \\ g_i * g_s \end{pmatrix}$$

$$= \begin{pmatrix} g_i \\ g_i * g_r \end{pmatrix} \circ \begin{pmatrix} g_i * g_r \\ (g_i * g_r) * g_s \end{pmatrix} = \begin{pmatrix} g_i \\ (g_i * g_r) * g_s \end{pmatrix}$$

$$= \begin{pmatrix} g_i \\ g_i * (g_r * g_s) \end{pmatrix} = \alpha(g_r * g_s) .$$

Hence α is an isomorphism from G onto P.

I would like to mention that I tried this method on my students at the National Junior College with satisfying results.

References

[1] J. A. Green, *Sets and groups*, Routledge and Kegan Paul, London, 1965, reprinted 1974, p. 76.

[2] Frank Ayres, Jr., *Modern algebra*, Schaum, New York, 1965, pp. 86, 94.

* * * * * * * * * * * * *

Research Fellowships in Germany

Notice has been received through the Singapore National Academy of Science (SNAS) regarding the availability of Research Fellowships sponsored by the Alexander von Humboldt Foundation in the Federal Republic of Germany. Information and application forms may be obtained from the Embassy of the Federal Republic of Germany in Singapore or from the Secretary General, Alexander von Humboldt Foundation, D-5300 Bonn-Bad Godesberg, Federal Republic of Germany.