# Some proofs in group theory

Peter Rowlett

## 1 Unique identity

It is not necessary for an identity element to exist, but if a set $A$ does contain an identity element $e$ for the operation $\circ$, then $e$ is unique, as we will see in the following theorem.

**Theorem 1.1.** *If $e, f \in A$ are both identity elements for an operation $\circ$, then $e = f$.*

*Proof.* By definition, since $e$ is an identity element, we have

$$e \circ x = x$$

for any $x \in A$. Putting $x = f$, we have

$$e \circ f = f.$$

Similarly, since $f$ is an identity element, we have

$$x \circ f = x$$

for any $x \in A$. Putting $x = e$, we have

$$e \circ f = e.$$

Since

$$e = e \circ f = f$$

we have $e = f$, as required. □

## 2 Unique annihilator

It is not necessary for an annihilator to exist, but if a set $A$ does have one for an operation $\circ$, then it is unique.

**Theorem 2.1.** *If $n, p \in A$ are both annihilators for $\circ$, then $n = p$.*

*Proof.* By definition, since $n$ is an annihilator, we have

$$n \circ x = n$$

for any $x \in A$. Putting $x = p$, we have

$$n \circ p = n.$$

Similarly, since $p$ is an annihilator, we have

$$x \circ p = p$$

for any $x \in A$. Putting $x = n$, we have

$$n \circ p = p.$$

Since

$$n = n \circ p = p$$

we have $n = p$, as required. $\square$

# 3 Inverses

**Theorem 3.1.** *For $(G, \circ)$, if $x, y \in G$ then there is one and only one $a \in G$ such that $a \circ x = y$, namely $a = y \circ x^{-1}$. Similarly, there is one and only one $b \in G$ such that $x \circ b = y$, namely $b = x^{-1} \circ y$.*

*Proof.* If $a \circ x = y$, operate on the right by $x^{-1}$, giving $(a \circ x) \circ x^{-1} = y \circ x^{-1}$. But

$$\begin{aligned}(a \circ x) \circ x^{-1} &= a \circ (x \circ x^{-1}) && \text{(associativity)}\\ &= a \circ e && \text{(inverse)}\\ &= a && \text{(identity)}\end{aligned}$$

therefore $a \circ x = y$ implies $a = y \circ x^{-1}$. Conversely, if $a = y \circ x^{-1}$, then $a \circ x = (y \circ x^{-1}) \circ x = y \circ (x^{-1} \circ x) = y \circ e = y$. So we have $a \circ x = y \iff a = y \circ x^{-1}$.

If $x \circ b = y$, then $x^{-1} \circ (x \circ b) = x^{-1} \circ y$, but $x^{-1} \circ (x \circ b) = (x^{-1} \circ x) \circ b = e \circ b = b$, therefore $x \circ b = y$ implies $b = x^{-1} \circ y$. Conversely, if $b = x^{-1} \circ y$ then $x \circ b = x \circ (x^{-1} \circ y) = (x \circ x^{-1}) \circ y = e \circ y = y$. So we have $x \circ b = y \iff b = x^{-1} \circ y$. $\square$

**Corollary 3.1.1.** *If $x \in G$ and $a$ is any element of $G$ such that $a \circ x = e$, then $a = x^{-1}$. Similarly if $b$ is any element such that $x \circ b = e$, then $b = x^{-1}$.*

*Proof.* In theorem 3.1, let $y = e$. Then we have that $a \circ x = e \iff a = e \circ x^{-1} = x^{-1}$ and $x \circ b = e \iff b = x^{-1} \circ e = x^{-1}$, as required. $\square$

**Corollary 3.1.2.** *If $x \in G$, then $(x^{-1})^{-1} = x$.*

*Proof.* In corollary 3.1.1, replace $x$ with $x^{-1}$ and $a$ with $x$. Now we have $x \circ x^{-1} = e \iff x = (x^{-1})^{-1}$. $\square$

**Corollary 3.1.3.** *If $x, y \in G$, then $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.*

*Proof.* In corollary 3.1.1, replace $a$ with $(y^{-1} \circ x^{-1})$ and $x$ by $(x \circ y)$. Now,

$$\begin{aligned} (y^{-1} \circ x^{-1})(x \circ y) &= (y^{-1} \circ (x^{-1} \circ x) \circ y) && \text{(associativity)} \\ &= (y^{-1} \circ e \circ y) && \text{(inverse)} \\ &= (y^{-1} \circ y) && \text{(identity)} \\ &= e && \text{(inverse)} \end{aligned}$$

Hence corollary 3.1.1 gives $y^{-1} \circ x^{-1} = (x \circ y)^{-1}$. □

**Corollary 3.1.4.** *The inverse of $e$ is $e$.*

*Proof.* Let $a = x = e$ in 3.1.1. Then $e \circ e = e$ by identity. □

# 4 Latin square property

**Theorem 4.1.** *Every element in a group occurs exactly once in every row.*

*Proof.* Suppose there is an element appearing twice within a row in a group with operation $\circ$.

$$\begin{array}{c|ccccccc} & 1 & 2 & \dots & b & \dots & c & \dots \\ \hline 1 & \ddots & & & \vdots & & \vdots & \\ 2 & & \ddots & & \vdots & & \vdots & \\ \vdots & & & \ddots & \vdots & & \vdots & \\ \text{a} & \dots & \dots & \dots & \text{d} & \dots & \text{d} & \dots \\ \vdots & & & & \vdots & & \vdots & \ddots \end{array}$$

Now $a \circ b = d$ and $a \circ c = d$. Hence $a \circ b = a \circ c$.
We know $a^{-1}$ exists in the set because we have a group, so

$$\begin{aligned} & a^{-1} \circ (a \circ b) && = a^{-1} \circ (a \circ c) && \\ \implies & (a^{-1} \circ a) \circ b && = (a^{-1} \circ a) \circ c && \text{(associativity)} \\ \implies & e \circ b && = e \circ c && \text{(inverse)} \\ \implies & b && = c && \text{(identity)} \end{aligned}$$

Therefore the columns for $b$ and $c$ are in fact the same column, and every element must appear exactly once in each row. □

A similar argument works the same for columns.

That each element appears exactly once in each row and column is called the Latin square property.