1.12 Answers

1.12.1 Solution to 1.10 Example

The question ask for an axiomatic proof that the inverse of each element of a group is unique.

An axiomatic proof is one that only uses the defining properties of a group. They are: closure, identity, inverses and associativity.

When asked to show that something is unique, that there is only one of them, a fruitful line of approach is to assume that there are two. The claim is that there is only one, to which you say "Oh no there isn't !" and the maths bites back with "Oh yes there is !"

In other words "a proof by contradiction".

Assume that y and z are two different inverses for the element x.
In consequence,

$$\begin{aligned} y &= ey && \text{where } e \text{ is the identity in the group (Identity)} \\ &= (zx)\,y && \text{since } z \text{ is an inverse for } x \text{ (Inverses)} \\ &= z\,(xy) && \text{(Associativity)} \\ &= ze && \text{since } y \text{ is an inverse for } x \text{ (Inverses)} \\ &= z && \text{as } e \text{ is the identity (Identity)} \end{aligned}$$

The assumption that y and z are different inverses to x results in a statement that y and z are the same.
$\therefore$ The inverse of each element of a group is unique. $\square$

[4 marks]

1.12.2 Solutions to 1.11 Exercise

Answer 1

Assume there exists a column in a Cayley table in which the same element occurs twice. Given two distinct elements, p and q, in column b the situation is;

$\circ$	…	$\boldsymbol{b}$	…
…	…	…	…
$\boldsymbol{p}$	…	$\boldsymbol{p \circ b}$	…
…	…	…	…
$\boldsymbol{q}$	…	$\boldsymbol{q \circ b}$	…
…	…	…	…

Under the assumption that the same element occurs twice,

$$p \circ b = q \circ b$$

$$(p \circ b) \circ b^{-1} = (q \circ b) \circ b^{-1} \qquad \text{Post-multiply both sides}$$

$$p \circ (b \circ b^{-1}) = q \circ (b \circ b^{-1}) \qquad \text{(Associativity)}$$

$$p \circ e = q \circ e \qquad \text{(Inverses)}$$

$$p = q \qquad \text{(Identity)}$$

But this contradicts the starting assumption that p and q are distinct elements.
$\therefore$ the same element cannot occur twice in any column in a group's Cayley table.

In conjunction, the two parts together prove that all group Cayley tables will be Latin squares.

$\square$

[4 marks]

Answer 2
Statement : The identity element of a group is unique.

Proof:
From the definition of a group;

- **Identity:** There exists an identity element $e \in G$.
  This is such that, for all $g \in G$, $g \circ e = g = e * g$

Assume that there exists a group which has two different identity elements.

Let those identity elements be, e_1 and e_2

Now, it must be true that $e_1\, e_2 = e_2$ because e_1 is an identity element.

And, it must be true that $e_1\, e_2 = e_1$ because e_2 is an identity element.

For both of the above two sentences to be true, $e_1 = e_2$

The assumption that e_1 and e_2 are different identity elements results in a statement that e_1 and e_2 are the same.

$\therefore$ The identity element of a group is unique. $\square$

[4 marks]

Answer 3

Statement: If x and y are elements of a group, $(xy)^{-1} = y^{-1}x^{-1}$

Proof:

From the definition of a group;

- **Inverses:** For each $g \in G$, there exists an inverse element $g^{-1} \in G$

  This is such that $g \circ g^{-1} = e = g^{-1} \circ g$

Thinking of xy as an element, g, of the group (closure) and $y^{-1}x^{-1}$ as another element, g^{-1}, of the group (closure) it has to be shown that,

$$(xy) \circ (y^{-1}x^{-1}) = e = (y^{-1}x^{-1}) \circ (xy)$$

Then, each of (xy) and $(y^{-1}x^{-1})$ is the other's inverse.

First, to show that $(xy) \circ (y^{-1}x^{-1}) = e$

$$\begin{aligned}
\text{LHS} &= (xy)(y^{-1}x^{-1}) && \\
&= x(yy^{-1})x^{-1} && \text{(Associativity)}\\
&= x\,e\,x^{-1} && \text{(Inverses)}\\
&= x\,x^{-1} && \text{(Identity)}\\
&= e && \text{(Inverses)}\\
&= \text{RHS} \quad \square &&
\end{aligned}$$

Second, to show that $(y^{-1}x^{-1}) \circ (xy) = e$

$$\begin{aligned}
\text{LHS} &= (y^{-1}x^{-1})(xy) && \\
&= y^{-1}(x^{-1}x)y && \text{(Associativity)}\\
&= y^{-1}\,e\,y && \text{(Inverses)}\\
&= y^{-1}y && \text{(Identity)}\\
&= e && \text{(Inverses)}\\
&= \text{RHS} \quad \square &&
\end{aligned}$$

Thus, $(xy)^{-1} = y^{-1}x^{-1}$ as required. $\square$

[5 marks]

Answer 4

Statement : When an Abelian group $(G, \circ)$ contains elements *a* and *b* such that *a* is self-inverse and *b* is self-inverse then $a \circ b$ is also self-inverse.

Proof:

When an element, *x*, is self-inverse it means that

$$
\begin{aligned}
x &= x^{-1} \\
x\,x &= x\,x^{-1} && \text{pre-multiply both sides by } x \\
x^2 &= e && \text{(Identity)}
\end{aligned}
$$

When two elements, *x* and *y* are in an Abelian group it means that the elements in the group are commutative. That is, $xy = yx$

To show that $a \circ b$ is self-inverse, show that $ab = (ab)^{-1}$

$$
\begin{aligned}
\text{LHS} &= ab \\
&= e(ab)e && \text{(Identity)} \\
&= \left(a^{-1}a\right)(ab)\left(b\,b^{-1}\right) && \text{(Inverses)} \\
&= a^{-1}\,(a\,a)(b\,b)\,b^{-1} && \text{(Associativity)} \\
&= a^{-1}\left(a^2\right)\left(b^2\right)b^{-1} \\
&= a^{-1}\,(e)\,(e)\,b^{-1} && \text{(Identity)} \\
&= a^{-1}b^{-1} \\
&= b^{-1}a^{-1} && \text{As the group is Abelian} \\
&= (a\,b)^{-1} && \text{Using the Question 3 result} \\
&= \text{RHS} \qquad \square
\end{aligned}
$$

[5 marks]

Answer 5

Statement: If x, y are elements of a group G, and if all three of x, y, xy have order 2, then that the group is Abelian.

Proof: Since xy has order 2,

$$
\begin{aligned}
(xy)^2 &= e \\
(xy)(xy) &= e \\
x(xy)(xy) &= xe && \text{Pre-multiply both sides by } x \\
(x\,x)\,y\,(xy) &= xe && \text{(Associativity)} \\
x^2\,y\,(xy) &= xe \\
ey(xy) &= xe && \text{As } x \text{ has order 2} \\
y(xy) &= x && \text{(Identity)} \\
y(xy)\,y &= xy && \text{Post-multiply both sides by } y \\
yx(y\,y) &= xy && \text{(Associativity)} \\
yx\,y^2 &= xy \\
(yx)\,e &= xy && \text{As } y \text{ has order 2} \\
yx &= xy && \text{(Identity)}
\end{aligned}
$$

It has been shown that any two elements, x and y, are commutative.

$\therefore$ The group is Abelian □

[5 marks]

Answer 6

Statement : Given a group of order 10, every proper subgroup must be cyclic.

Proof: By Lagrange's theorem, a group of order 10 can only have possible proper subgroups of order 2 or 5

A group (or subgroup) of prime order is cyclic.

Thus, every prober subgroup of a group of order 10 is cyclic.

[3 marks]

Answer 7

(i) **Statement:** Given that a, b are elements of a group and that

$$a^5 = e, \ b^4 = e, \ ab = b\,a^3 \text{ then } a^2 b = ba$$

Proof:

$$\begin{aligned}
\text{LHS} &= a^2\,b \\
&= a\left(ab\right) \\
&= a\left(b\,a^3\right) \\
&= \left(ab\right)a^3 \\
&= \left(b\,a^3\right)a^3 \\
&= ba\left(a^5\right) \\
&= ba\left(e\right) \\
&= ba \\
&= \text{RHS} \qquad \square
\end{aligned}$$

[5 marks]

(ii) **Statement:** Given that a, b are elements of a group and that

$$a^5 = e,\ b^4 = e,\ ab = b\,a^3 \text{ then } a\,b^3 = b^3\,a^2$$

Lemma :

$$\begin{aligned} ab &= b\,a^3 \\ ab\,a^2 &= b\,a^3\,a^2 \\ ab\,a^2 &= b\,a^5 \\ ab\,a^2 &= b \end{aligned}$$

Proof:

$$\begin{aligned} \text{LHS} &= a\,b^3 \\ &= (ab)\,b^2 \\ &= \left(b\,a^3\right)b^2 \\ &= b\,a^2\,(ab)\,b \\ &= b\,a^2\left(b\,a^3\right)b \\ &= ba\left(ab\,a^2\right)(ab) \\ &= ba\,(b)\left(b\,a^3\right) \\ &= b\,(ab)\,b\,a^3 \\ &= b\left(b\,a^3\right)b\,a^3 \\ &= b^2\,a^2\left(ab\,a^2\right)a \\ &= b^2\,a^2\,(b)\,a \\ &= b^2\,a\,(ab)\,a \\ &= b^2\,a\left(ba^3\right)a \\ &= b^2\left(ab\,a^2\right)a^2 \\ &= b^2\,(b)\,a^2 \\ &= b^3\,a^2 \\ &= \text{RHS} \qquad \square \end{aligned}$$

[5 marks]

Answer 8

Although not asked for, a Cayley Table will be useful !

$\times_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

(i) Using each element in turn as a generator;

$\langle 1 \rangle = \{1\}$ $\quad |1| = 1$

$\langle 2 \rangle = \{1, 2, 4, 8\}$ $\quad |2| = 4$

$\langle 4 \rangle = \{1, 4\}$ $\quad |4| = 2$

$\langle 7 \rangle = \{1, 4, 7, 13\}$ $\quad |7| = 4$

$\langle 8 \rangle = \{1, 2, 4, 8\}$ $\quad |8| = 4$

$\langle 11 \rangle = \{1, 11\}$ $\quad |11| = 2$

$\langle 13 \rangle = \{1, 4, 7, 13\}$ $\quad |13| = 4$

$\langle 14 \rangle = \{1, 14\}$ $\quad |14| = 2$

[4 marks]

(ii) The order of G is 8

Lagrange's theorem gives possible values of n as 1, 2, 4 or 8

[2 marks]

(iii) From part (i) the proper cyclic subgroups are,

{1, 4}, {1, 11}, {1,14}, {1, 2, 4, 8}, and {1, 4, 7, 13}

[4 marks]

(iv) **(a)** The set $\{0, 1, 2, 3, 4, 5, 6, 7\}$ under addition modulo 8 forms a group because it is closed, and has 0 as identity. The inverse pairs are (1, 7), (2, 6), (3, 5) and 4 is self inverse.
It is a cyclic group because, for example, the element 1 generates the whole group.
No element of *G* generated the whole group in part (i) and so *G* is not cyclic.
$\therefore$ This group is not isomorphic with *G*

[6 marks]

(b) The set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ under multiplication modulo 9 is not a group because it is not closed; $3 \times 3 = 0 \pmod 9$

[2 marks]

(c) The set of matrices does form a group, initially suspected because they are all two dimensional transformation matrices.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity matrix

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is a rotation of 90° about the origin

$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is a rotation of 180° about the origin

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is a rotation of 270° about the origin

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is a reflection in $y = x$

$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ is a reflection in $y = -x$

$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is reflection in the x-axis

$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ is a reflection in the y-axis

So, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is the inverse of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ with the other non-identity elements being self inverse.
With six self-inverse elements, this is not isomorphic to *G* which has only three.

[6 marks]

This document is a part of a **Mathematics Community Outreach Project** initiated by Shrewsbury School
It may be freely duplicated and distributed, unaltered, for non-profit educational use
In October 2020, Shrewsbury School was voted "**Independent School of the Year 2020**"
© 2021 Number Wonder
Teachers may obtain detailed worked solutions to the exercises by email from mhh@shrewsbury.org.uk