Assignment 13, Introduction To Mathematics

Oleg Sivokon

<2014-11-22 Sat>

Contents

1 Problems

1.1 Problem 1

1. Given G is a group under $\circ$ and $(\forall x, y \in G) : x \circ y \circ x = y$. Show that every member of G is its own inverse and that G is commutative.
2. Given G is a group under $\circ$, $x, y \in G$ and x being the inverse of $x \circ y$, show that G is commutative.

1.1.1 Answer 1

First, we will show that every element of G is its own inverse. By definition of invertibility, $y \circ y^{-1} = 1$, 1 being the identity element. Thus:

$$\begin{array}{lcl} x \circ y \circ x = y & \iff & \text{given} \\ x \circ (y \circ y^{-1}) \circ x = y \circ y^{-1} & \iff & \text{using group cancellation property} \\ x \circ x = 1 & & \text{by definition of identity element} \end{array}$$

Since we selected x arbitrary, it follows that $(\forall x \in G) : x \circ x = 1$, in other words, each element is its own inverse.

Having shown that $(\forall x \in G) : x = x^{-1}$, we can use this fact to show that G is commutative. Since $(x \circ y)$ is in G, it must be that $(x \circ y) \circ (x \circ y)^{-1} = 1$ (1 being the identity element). By associativity, we can remove the parenthesis, and use the fact that each element is its own inverse: $x \circ y \circ x \circ y = 1$, (*).

$$\begin{array}{rcll} x \circ y & = & x \circ (1 \circ y) & 1 = 1 \circ y \\ & = & x \circ (x \circ y \circ x \circ y) \circ y & \text{invoke (*)} \\ & = & (x \circ x) \circ y \circ x \circ (y \circ y) & \text{by associativity} \\ & = & y \circ x & \text{completes the proof} \end{array}$$

1.1.2 Answer 2

In order to prove commutativity we need to show that $y \circ x = x \circ y$. We will start by restating the problem *(1 is the identity element)*:

$$
\begin{array}{lcl}
(x \circ y) \circ x = 1 & \iff & \text{given} \\
(x \circ y) \circ x = x \circ x^{-1} & \iff & \text{by definition of identity} \\
(x \circ y) \circ x = x \circ (x \circ y) & \iff & \text{from } x^{-1} = (x \circ y) \\
x \circ (y \circ x) = x \circ (x \circ y) & \iff & \text{by associativity} \\
y \circ x = x \circ y & & \text{by group cancellation property}
\end{array}
$$

Having showed that $y \circ x = x \circ y$ we completed the proof.

1.2 Problem 2

Let $H = \{a, b, c, e\}$, all four elements of H being distinct, and * being the binary operation on H. e is the identity element under *, and $a * a = e$, $b * b = e$.

1. Prove that if H has cancellation property, than it must be that $c*a \neq e$.
2. Prove that if * is associative, then $c * b \neq e$.
3. Prove that if H is a group under *, then $c * c = e$.
4. Complete the operation table of $(H, *)$, assuming H is a group.

1.2.1 Answer 3

It is possible to have at most one identity element in a monoid. If there was a c such that both $c * a = e$ and $a * a = e$, the cancellation property would require that $c = a$, but this is not possible, because we are given that $c \neq a$. Hence $c * a \neq e$.

1.2.2 Answer 4

We will again use the fact that all elements of H must be distinct, and show that $c * b \neq e$ if H is associative.

$$
\begin{array}{lcl}
c * b = e & \iff & \text{Assume the opposite} \\
c * b = b * b & \iff & \text{Because } b * b = e \\
(c * b) * b = (b * b) * b & \iff & \text{Apply *once again} \\
c * (b * b) = b * (b * b) & \iff & \text{By associativity} \\
c = b & & \text{Contradiction, } c \neq b
\end{array}
$$

We assumed $c * b = e$, but derived $c = b$, which is a contradiction, thus it must be the case that $c * b \neq e$. This completes the proof.

1.2.3 Answer 5

In 1.2.1 and 1.2.2 we have shown that both $c * a \neq e$ and $c * b \neq e$. Since by definition of the group every element must have an inverse, we are only left with c as a candidate. e is not a candidate because it is the identity element, which means $c * e = c$. So it must be the case that $c * c = e$.

1.2.4 Answer 6

This table was constructed so that any pair of elements under * will produce the third element (excluding the identity element). In this way it is ensured that $x * y * z = e$ for any elements of H, in any order.

	a	b	c	e
a	e	c	b	a
b	c	e	a	b
c	b	a	e	c
e	a	b	c	e

1.3 Problem 3

1. Prove that if in the group G every element is its own inverse, then this group is commutative.
2. Prove that the group $G = (\{0, 1, 2, 3, 4\}, \circ)$ where $x \circ y = mod(x + y, 5)$ is commutative, but no member of this group is its own inverse, except for the identity element.
3. Give an example of a non-commutative group, such that it has an element which is its own inverse, and isn't its identity element.

1.3.1 Answer 7

The proof is essentially the same as 1.1.2. Let's first express the identity element. Let x and y be two arbitrary chosen members of G, then it follows that $x * x = y * y$, $*$ being the group operation. Consequently, $x * y * y * x = 1$ (1 being the identity element) because $x * x = 1$, $y * y = 1$ and $x * 1 * x = 1$.

Now we will use this presentation of identity element to show that $x * y = y * x$:

$$x * y = x * 1 * y = x * x * y * y * x * y = 1 * 1 * x * y = x * y$$

This completes the proof.

1.3.2 Answer 8

Commutativity of G trivially follows from commutativity of addition. It doesn't matter whether we add $x + y$ or $y + x$ and then take the modulo of the sum, the sum is guaranteed to be the same in both cases and modulo is left-concealable.

Let's establish the identity element of this group. It must be 0 since mod 5 slices the set of integers into five slices, each member of this group stands for a distinct slice. The remainder of the $x + 0$, x bein any element of the group is thus x itself. Since we know that G is commutative, $x \circ 0 = 0 \circ x = x$.

Now we can use direct calculation to verify that no element of G under $\circ$ is its own inverse (except for the identity element).

$$\begin{aligned} 0 \circ 0 &= 0 \\ 1 \circ 1 &= 2 \\ 2 \circ 2 &= 4 \\ 3 \circ 3 &= 1 \\ 4 \circ 4 &= 3 \end{aligned}$$

1.3.3 Answer 9

The example of a group which is non-commutative, but has elements which are their own inverses could be a dyhedral group of rank 6. I found a mention of this group on the internet, so I didn't come up with it myself. I've verified by direct calculation that it indeed meets the requirements.

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	1	c	b	e	d
b	b	d	1	e	a	c
c	c	e	a	d	c	b
d	d	b	e	1	c	a
e	e	c	d	a	b	1

The calculation follows.

First define some utility functions:

```
(defun op (table elements)
  "Creates an operation from the TABLE describing the results
of this operation on the group of ELEMENTS."
  (lambda (a b)
    (loop :with result := (aref table (car a) (car b))
       :for (head . tail) :in elements :do
       (when (eql tail result)
         (return (cons head tail))))))

(defun elements (table)
  "Collects all the elements of the group whose operation is
defined in TABLE."
  (loop :for i :below (array-dimension table 0)
     :collect (cons i (aref table i 0))))
```

Next define the predictates validating different aspects of the group.

```
(defun verify-associativity (operations-table)
  (loop
     :with elements := (elements operations-table)
     :with op := (op operations-table elements)
     :for x :in elements :do
     (loop :for y :in elements :do
        (loop :for z :in elements :do
           (unless (equal (funcall op (funcall op x y) z)
                          (funcall op x (funcall op y z)))
             (return-from verify-associativity
               (list x y z)))))))

(defun find-identity (operations-table)
  "Searches for identity element of the group defined by
OPERATIONS-TABLE."
  (loop
     :with elements := (elements operations-table)
     :with op := (op operations-table elements)
     :for x :in elements :do
     (loop :for y :in elements :do
        (unless (equal (funcall op x y) (funcall op y x))
          (return))
        :finally (return-from find-identity (cdr x)))))

(defun find-inverses (operations-table identity-element)
  "Searches for inverses of each element of the group given
by the OPERATIONS-TABLE.  This relies on the identity element
being previously calculated."
  (loop
     :with elements := (elements operations-table)
     :with op := (op operations-table elements)
     :for x :in elements :nconc
     (loop :for y :in elements
        :when (eql (cdr (funcall op x y)) identity-element)
        :collect (list (cdr x) (cdr y)))))
```

Similarly, define a predicate for commutativity:

```
(defun verify-commutativity (operations-table)
  "Verifies whether the group given by OPERATIONS-TABLE
 is commutative."
  (loop
     :with elements := (elements operations-table)
     :with op := (op operations-table elements)
     :for x :in elements :do
     (loop :for y :in elements :do
        (unless (equal (funcall op x y) (funcall op y x))
          (return-from verify-commutativity
            (list (cdr x) (cdr y)
                  (cdr (funcall op x y))
                  (cdr (funcall op y x))))))))
```

Finally, print out the results:

```
(defun print-report ()
  "Prints the report fo dyhedral group of rank 6."
  (let* ((dyhedral-group-6
          (make-array
           (list 6 6)
           :initial-contents
           '((1 a b c d e)
             (a 1 c b e d)
             (b d 1 e a c)
             (c e a d 1 b)
             (d b e 1 c a)
             (e c d a b 1))))
         (associativity (verify-associativity dyhedral-group-6))
         (identity (find-identity dyhedral-group-6))
         (inverses (find-inverses dyhedral-group-6 identity))
         (commutativity (verify-commutativity dyhedral-group-6)))
    (list
     (list "associativity" (null associativity))
     (list "identity" identity)
     (list "inverses" (format nil "~($~{~{~s*~s^{-1}~}=~}1$~)"
                              inverses))
     (list "commutativity"
      (apply 'format nil "~($~s*~s=~s, ~3:*~s*~s=~*~s$~)"
             commutativity)))))

(print-report)
```

associativity	T
identity	1
inverses	$1 * 1^{-1} = a * a^{-1} = b * b^{-1} = c * d^{-1} = d * c^{-1} = e * e^{-1} = 1$
commutativity	$a * b = c, a * b = d$

1.4 Problem 4

Let $A = \{e, a, b, c, ...\}$, e, a, b, c being distinct. $*$ is a binary operation defined on A, under which A is closed, has cancellation property, is associative. e is the identity element in A under $*$ and a is its own inverse.

1. Prove that $B = \{e, a, b, a * b\}$ has four distinct members.
2. Prove that if $c \notin B$, then $a * c \notin B$.
3. Prove that in a group of five elements no element but the identity element is its own inverse.

1.4.1 Answer 10

We are given that e, a, b are distinct by construction, what is left to show is that $a*b$ is equal to neither one of them. Recall that we are given that $*$ has cancellation property, this in other words means that $a*b \neq e$, otherwise the cancellation property wouldn't hold (since it would be both $a * a = e$ and $a * b = e$).

Suppose then, by contradiction that $a * b = a$, remembering that $*$ is associtative we would have that $(a * a) * b = a * (a * b)$, but this is not the case because $(a*a)*b = b$ and $a*(a*b) = e$, while we are given that $b \neq e$. So, $a * b \neq a$.

Suppose, again, by contradiction that $a * b = b$, this would also imply that $(a*a)*b = b$ and $(a*e)*b = b$, but we are given that $*$ has cancellation property, which must mean that $a*a = a*e$, but we also know that $a*a = e$ and $a * e = a$, thust it would have to be that $a = e$, but we are given that $a \neq d$. This means that $a * b \neq b$.

Sine we tried a, e and b and convinced that neither of them is a candidate for $a * b$, we conclude that $a * b$ must be distinct fourth member of B. This completes the proof.

1.4.2 Answer 11

This question becomes trivial, if you consider its negation:

$$\exists c \in B : a * c \notin B$$

Disproving this would prove the original claim. Observe now that $a * e$ is in B because e is the identity element and $a \in B$, $a * b$ is in B by construction and $a * a$ is again in B because we are given that a is its own inverse, meaning $a * a = e$ and $e \in B$. Lastly, $a * (a * b)$ is in B because by associativity, $a * (a * b) = (a * a) * b$, then a being its own inverse gives $(a * a) * b = b$, and b is in B by construction.

We exhausted all possibilities for c and none satisfies the existence condition, hence $\neg(\exists c \in B : a * c \notin B)$, hence $\forall c \notin B : a * c \notin B$.

1.4.3 Answer 12

Not exactly relevant to the question, I found that the number of groups of different orders are extensively studied and are well-known for various kinds of groups. For instance, just by looking at http://oeis.org/A000001 I would know that there is only one group of order 5, and so by constructing it, I'd have proved that there aren't elements in this group, which are their own inverses. But I would imagine this answer to not be satisfactory.

So, in order to prove this claim more generally, we can reuse the previous answers. So far we have worked with the group of size four and we were given that it has one element which is its own inverse. It is easy to see that $a * b$ must be in the group G (I will base it on the earlier definition of B). And c being either one of $b * a$, $a * b * b$, $b * b$ by pigeonhole principle.

I will now to construct a Cayley table and show its inconsistency:

	1	a	b	$a*b$	c
1	1	a	b	$a*b$	c
a	a	1	$a*b$	b	$a*c$
b	b	$b*a$	$b*b$	$b*a*b$	$b*c$
$a*b$	$a*b$	$a*b*a$	$a*b*b$	$a*b*a*b$	$a*b*c$
c	c	$c*a$	$c*b$	$c*a*b$	$c*c$

Look at the second row of this table, its last element $a*c$. Observe that while it has to be one of $\{1, a, b, a*b, c\}$ it is neither 1, nor a nor b nor $a*b$ (cancellation implies that all columns of the same row of the Cayley table must have distinct values). Then, it must be the case that $a*c = c$, but the same cancellation property prevents us from having same values in a single colum, but $a*c = c$ implies that c would appear in its column twice, which is a contradiction.

We selected a arbitrarily to be its own inverse, since we arrived at contradiction, we are free to assume that if there exists a group of rank five, it should not have a member which is its own inverse. Unfortunately we did not construct such a group, so we aren't free to claim (yet) this doesn't hold vacuously, but this should be enough to answer the question.