Mathematics 1214: Introduction to Group Theory

Homework exercise sheet 2

Due 12:50pm, Friday 5th February 2010

1. Let $*$ be an operation on a set S. Suppose that S contains an identity element for $*$. Prove that if x is an element of S which is invertible with respect to $*$, then x^{-1} is also invertible with respect to $*$ and $(x^{-1})^{-1} = x$.

   Solution Let e be the identity element for $*$. Recall that an element $a \in S$ is invertible, with inverse b, if and only if $a * b = e = b * a$. We know that $x * x^{-1} = e = x^{-1} * x$. Taking $a = x^{-1}$ and $b = x$ shows that x^{-1} is invertible, with inverse x.

2. For each of the following sets G and operations $*$, determine whether or not $(G, *)$ is a group. As always, you should prove that your answers are correct.

   (a) $G = \mathbb{Z}$, $* =$ addition

   (b) $G = 7\mathbb{Z} = \{7n \colon n \in \mathbb{Z}\}$, $* =$ addition

   (c) $G = 7\mathbb{Z} + 4 = \{7n + 4 \colon n \in \mathbb{Z}\}$, $* =$ addition

   (d) $G = 7\mathbb{Z}$, $* =$ multiplication

   (e) $G = \{e, f\}$, $x * y = e$ for all $x, y \in G$

   (f) $G = \mathbb{C}^\times = \{z \in \mathbb{C} \colon z \neq 0\}$, $* =$ multiplication

   (g) $G = \mathbb{R}^2$, $* =$ vector addition

   (h) $G = \mathbb{R}$, $* =$ multiplication

   Solution (a) This is a group. Indeed,

   - $\mathbb{Z}$ is closed under addition, since $n, m \in \mathbb{Z} \implies n + m \in \mathbb{Z}$. Hence addition is an operation on $\mathbb{Z}$.
   - For $n, m, k \in \mathbb{Z}$ we have $(n+m)+k = n+(m+k)$. So addition is associative.
   - $n + 0 = 0 + n = n$ for all $n \in \mathbb{Z}$. Hence 0 is the identity element for $(\mathbb{Z}, +)$.
   - If $n \in \mathbb{Z}$ then $-n \in \mathbb{Z}$, and $n + (-n) = (-n) + n = 0$. So every $n \in \mathbb{Z}$ is invertible with respect to addition.

   (b) This is a group. Indeed,

   - $7\mathbb{Z}$ is closed under addition, since $n, m \in \mathbb{Z} \implies 7n + 7m = 7(n + m) \in 7\mathbb{Z}$. Hence addition is an operation on $\mathbb{Z}$.
   - For $n, m, k \in \mathbb{Z}$ we have $(7n + 7m) + 7k = 7n + (7m + 7k)$. So addition is associative.
   - $7n + 0 = 0 + 7n = 7n$ for all $n \in \mathbb{Z}$, and $0 = 7 \times 0 \in 7\mathbb{Z}$. Hence 0 is the identity element for $(7\mathbb{Z}, +)$.
   - If $n \in \mathbb{Z}$ then $-7n \in \mathbb{Z}$, and $7n + (-7n) = (-7n) + 7n = 0$. So every element of $7\mathbb{Z}$ is invertible with respect to addition.

(c) This is not a group, since it does not contain an identity element. Indeed, if there was some $n \in \mathbb{Z}$ such that $e = 7n + 4$ were the identity element for $(G, +)$, then taking the element $4 \in G$ in the defining property of e, we would have $e+4 = 4$, so $e = 0$, so $7n + 4 = 0$, so $7n = -4$, so $n = -\frac{4}{7}$, so $n \notin \mathbb{Z}$ which contradicts our earlier assumption.

(d) This is not a group, since it does not contain an identity element. Indeed, if there was some $n \in \mathbb{Z}$ such that $e = 7n$ were the identity element for $(G, *)$, then taking the element $7 \in G$ in the defining property of e, we would have $7n * 7 = 7$, i.e. $49n = 7$, so $n = \frac{1}{7}$, so $n \notin \mathbb{Z}$ which contradicts our earlier assumption.

(e) This is not a group, since f is not invertible. Indeed, the identity element for $(G, *)$ is clearly e, but $f * y = e$ for every $y \in G$, so $f * y \neq f$ for every $y \in G$.

(f) This is a group. Indeed,

- $\mathbb{C}^\times$ is closed under multiplication, since $z, w \in \mathbb{C}^\times \implies z * w \in \mathbb{C}^\times$ (the product of two non-zero complex numbers is always non-zero). Hence multiplication is an operation on $\mathbb{C}^\times$.
- For $z, v, w \in \mathbb{C}^\times$ we have $(z * v) * w = z * (v * w)$. So multiplication is associative.
- $z * 1 = 1 * z = z$ for all $z \in \mathbb{C}^\times$, and $1 \in \mathbb{C}^\times$. Hence 1 is the identity element for $(\mathbb{C}^\times, *)$.
- If $z \in \mathbb{C}^\times$ then $z \neq 0$, so $\frac{1}{z} \in \mathbb{C}^\times$, and $z * \frac{1}{z} = 1 = \frac{1}{z} * z$. So every $z \in \mathbb{C}^\times$ is invertible with respect to multiplication.

(g) This is a group. Indeed,

- $\mathbb{R}^2$ is closed under vector addition, since $v, w \in \mathbb{R}^2 \implies v + w \in \mathbb{R}^2$. Hence addition is an operation on $\mathbb{R}^2$.
- For $v, w, x \in \mathbb{R}^2$ we have $(v+w)+x = v+(w+x)$. So addition is associative.
- Writing $0 = (0, 0)$ for the zero vector in $\mathbb{R}^2$, we have $v + 0 = 0 + v = v$ for all $v \in \mathbb{R}^2$. Hence 0 is the identity element for $(\mathbb{R}^2, +)$.
- If $v \in \mathbb{R}^2$ then $-v \in \mathbb{R}^2$, and $v + (-v) = (-v) + v = 0$. So every $v \in \mathbb{R}^2$ is invertible with respect to addition.

(h) This is not a group. While $1 \in \mathbb{R}$ is the identity element for $(\mathbb{R}, *)$, the equation $0 * y = 1$ has no solutions $y \in \mathbb{R}$. So the element $0 \in \mathbb{R}$ is not invertible.

3. Let $(G, *)$ be a group. Prove the following assertions:

   (a) For each $x \in G$, the mapping $L_x \colon G \to G$, $y \mapsto x * y$ is a bijection.

(b) Every element of G appears exactly once in each row of the Cayley table for $*$.

(c) For each $x \in G$, the mapping $R_x \colon G \to G$, $y \mapsto y * x$ is a bijection.

(d) Every element of G appears exactly once in each column of the Cayley table for $*$.

Solution (a) If $L_x(y_1) = L_x(y_2)$ then $x * y_1 = x * y_2$, so $y_1 = x^{-1} * (x * y_1) = x^{-1} * (x * y_2) = y_2$. Hence L_x is injective. If $y \in G$ then $y = L_x(x^{-1} * y)$, so L_x is surjective.

(b) The row labelled x in the Cayley table for $*$ consists of the elements of the form $x * y = L_x(y)$ for $y \in G$. Since L_x is a bijection, this shows that every element of G appears exactly once in this row.

(c) If $R_x(y_1) = R_x(y_2)$ then $y_1 * x = y_2 * x$, so $y_1 = (y_1 * x) * x^{-1} = (y_2 * x) * x^{-1} = y_2$. Hence R_x is injective. If $y \in G$ then $y = R_x(y * x^{-1})$, so R_x is surjective.

(b) The column labelled x in the Cayley table for $*$ consists of the elements of the form $y * x = R_x(y)$ for $y \in G$. Since R_x is a bijection, this shows that every element of G appears exactly once in this row.

4. Let $S = \{a, b, c\}$.

   (a) How many elements does the set $S \times S$ contain?

   (b) How many operations are there on S?

   (c) Find the Cayley table for an operation $\star$ on S such that $(S, \star)$ is a group with identity element a.
   [You should check that $(S, \star)$ really is a group with identity element a].

   (d) Prove that the operation you have found is the only operation on S such that $(S, \star)$ is a group with identity element a.

   (e) Write down the Cayley table of each operation $*$ on S such that $(S, *)$ is a group, and determine which of these operations is commutative.

Solution (a) We have

$$S \times S = \{(x, y) \colon x, y \in S\} = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}.$$

So $S \times S$ contains nine elements.

(b) An operation on S is a mapping $S \times S \to S$. Since $S \times S$ contains 9 elements and S contains 3 elements and there are 3^9 mappings from a set with 9 elements to a set with 3 elements, there are $3^9 = 19683$ operations on S.

(c)

$\star$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

To check that $(S, \star)$ is a group:

- The element a acts as an identity element for $\star$, since, from the table, we have $a \star x = x$ for all $x \in S$ (since the element in the (a, x) position of the Cayley table is $a \star x = x$) and similarly, by examining the first column of the Cayley table we see that $x \star a = x$ for all $x \in S$.
- To check associativity, we must show that $(x \star y) \star z = x \star (y \star z)$ for all $x, y, z \in S$. So there are $3^3 = 27$ triples $x, y, z \in \{a, b, c\}$ to check. If $x = a$ then since a is an identity element, we have $(x \star y) \star z = y \star z$ and $x \star (y \star z) = y \star z$. Similarly, if $y = a$ or $z = a$ then it is easy to check that $(x \star y) \star z = x \star (y \star z)$. So it remains to check the cases when $x, y, z \in \{b, c\}$. There are $2^3 = 8$ of these:

x	y	z	$(x \star y) \star z$	$x \star (y \star z)$
b	b	b	$(b \star b) \star b = c \star b = a$	$b \star (b \star b) = b \star c = a$
b	b	c	$(b \star b) \star c = c \star c = b$	$b \star (b \star c) = b \star a = b$
b	c	b	$(b \star c) \star b = a \star b = b$	$b \star (c \star b) = b \star a = b$
b	c	c	$(b \star c) \star c = a \star c = c$	$b \star (c \star c) = b \star b = c$
c	b	b	$(c \star b) \star b = a \star b = b$	$c \star (b \star b) = c \star c = b$
c	b	c	$(c \star b) \star c = a \star c = c$	$c \star (b \star c) = c \star a = c$
c	c	b	$(c \star c) \star b = b \star b = c$	$c \star (c \star b) = c \star a = c$
c	c	c	$(c \star c) \star c = b \star c = a$	$c \star (c \star c) = c \star b = a$

  So $(x \star y) \star z = x \star (y \star z)$ for every $x, y, z \in S$, so $\star$ is associative.
- We have $a \star a = a$ so $a^{-1} = a$, and $b \star c = c \star b = a$, so $b = c^{-1}$ and $c = b^{-1}$. So every element of S has an inverse with respect to $\star$ in S. Hence $(S, \star)$ is a group.

(d) Suppose that $*$ is any operation on S such at $(S, *)$ is a group with identity element a. Then $a * x = x = x * a$ for all $x \in S$, so we are forced to have the following entries of the Cayley table:

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

We know that each entry of S appears exactly once in the second row. So either $b * b = c$ or $b * b = a$. If $b * b = a$ then we must have $b * c = c$ so that the second row contains every element of S exactly once; but then the third column would contain c twice, which is not allowed. So $b * b = c$ and $b * c = a$:

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

Now filling in the missing entries from the second and third columns gives $c * b = a$ and $c * c = b$. So $*$ has the same Cayley table as $\star$, so $* = \star$. This shows that $\star$ is the only group operation with these properties.

(e) The only group operations are:

$*_a$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*_b$	b	c	a
b	b	c	a
c	c	a	b
a	a	b	c

$*_c$	c	a	b
c	c	a	b
a	a	b	c
b	b	c	a

Indeed, we've shown that if a is the identity operation, then there's only one group operation, $*_a = \star$. So there are only two other group operations, the operation $*_b$ obtained when b is the identity and the operation $*_c$ obtained when c is the identity. These are found by interchanging the roles of a, b, c as appropriate in the operation $*$.

All of these operations are abelian, as their Cayley tables are all symmetric in the main diagonal, so $x * y = y * x$.