1. For each of the following, prove whether or not the set G with the specified operation represents a group.

   (a) $G = \mathcal{C}$, the set of complex numbers, and the operation is standard addition of complex numbers.

   (b) $G = \mathcal{C}$, the set of complex numbers, and the operation is standard multiplication of complex numbers.

Solution: 1.(a) $G = \mathbf{C}$ with $+$:

Closure: for any $(a+bi), (c+di) \in \mathbf{C}, (a+bi)+(c+di) =$
$[(a+c)+(b+d)i] \in \mathbf{C}$.

Associativity: for any $(a+bi), (c+di), (e+fi) \in \mathbf{C}$,
$(a+bi)+[(c+di)+(e+fi)] = (a+bi)+[(c+e)+(d+f)i]$
$= (a+c+d)+(b+d+f)i = [(a+c)+(b+d)i]+(e+fi) = [(a+bi)+(c+di)]+(e+fi)$.

Identity element is $0 \in \mathbf{C}$: for any $(a+bi) \in \mathbf{C}$,
$(a+bi)+0 = 0+(a+bi) = (a+bi)$.

Inverse elements exist: for any $(a+bi), \exists(-a-bi) \in \mathbf{C}$,
such that $(a+bi)+(-a-bi) = 0$.

Therefore, $\mathbf{C}$ with $+$ is a group.

(b) $G = \mathbf{C}$ with $*$:

Closure: for any $(a+bi), (c+di) \in \mathbf{C}$,
$(a+bi)*(c+di) = [(ac-bd)+(ad+bc)i] \in \mathbf{C}$.

Associativity: for any $(a+bi), (c+di), (e+fi) \in \mathbf{C}$,
$(a+bi)*[(c+di)*(e+fi)] = (a+bi)*[ce+dei+cfi-df]$
$= ace+bcei+adei-bde+acfi-bcf-adf-bdfi = [ac+bci+adi-bd]*(e+fi)$
$= [(a+bi)*(c+di)]*(e+fi)$.

Identity element is $1 \in \mathbf{C}$: for any $(a+bi) \in \mathbf{C}$,
$(a+bi)*1 = 1*(a+bi) = (a+bi)$.

However, inverse element may not exist: since $0 \in C$,
but there is no element $a+bi \in C$ such that $0*(a+bi) = 1$.

Therefore, $\mathbf{C}$ with $*$ is not a group.

■

2. Follow the same instructions as for the previous problem.

   (a) G is the set of all binary strings of length 5, and the operation is bitwise exclusive or (XOR).

   Solution: G is a group with XOR. We verify the four group axioms:(use * to represent XOR)
   (Closure) Let $a \in G$, $b \in G$, a,b are binary strings of length 5, after the operation XOR, the result must be a binary string of length 5, that is $a*b \in G$.
   (Identify) Let $e = 00000$, so $e \in G$, and for every $a \in G$, we have $a*e \in G$.
   (Inverse) Let $a^{-1} = a$, so $a*a^{-1} = e$
   (Associativity) XOR applys on each bit individually, we can check associativity on each bit, there are eight possibility for associativity, that is $(0*0*0)$,$(0*0*1)$,$(0*1*0)$,$(0*1*1)$,$(1*0*0)$,$(1*0*1)$,$(1*1*0)$,$(1*1*1)$, it is easy to check that with XOR, $a*(b*c) = (a*b)*c$. ■

(b) G is the set of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a, b, c, d \in \mathbb{R}$ and $ad - bc \neq 0$, and the operation is matrix multiplication.

Solution: G is a group with matrix multiplication. We verify the four group axioms:(use * to represent matric multiplication)
(Closure) Let $x = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $y = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$,such that $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in \mathbb{R}$ and $a_1d_1 - b_1c_1 \neq 0, a_2d_2 - b_2c_2 \neq 0$
$x * y = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} * \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$, we can verify that

$$(a_1a_2 + b_1c_2)(c_1b_2 + d_1d_2) - (a_1b_2 + b_1d_2)(c_1a_2 + d_1c_2) = (a_1d_1 - b_1c_1)(a_2d_2 - b_2c_2) \neq 0$$

So $x * y \in G$.
(Identity) Let $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so for every $x \in G$, $x * e = x$
(Inverse)For every x, $x = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$,we have $x^{-1} = \begin{pmatrix} \frac{d}{(ad-bc)} & \frac{-b}{(ad-bc)} \\ \frac{c}{(ad-bc)} & \frac{a}{(ad-bc)} \end{pmatrix}$.
(Associativity) The associativity is hold because of the property of matrix multiplication. ∎

3. Prove that if every element of a group, G, is equal to its own inverse, then G is an Abelian (commutative) group.

Solution: 3. Prove: $\forall a \in G, a = a^{-1} \Rightarrow$ G is Abelian.

Proof: Let e be the identity element of G, with juxtaposition denoting the operation on G.
For any $a, b \in G, ab = (ae)b = (a((ab)(ab)))b$ ...property of elements in G.
$= ((aa)(bab))b = ((e)(bab))b = (ba)(bb) = (ba)e = ba \in \mathbf{G}$.
We have shown that $\forall a, b \in G, ab = ba \Rightarrow$ G is Abelian.

∎

4. Let $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, in which $\mathbb{Q}$ is the set of all rational numbers. Prove that G is a subgroup of $\mathbb{R}$ under the operation of addition.

Solution: We need to prove that: For every $x, y \in G$, $x + y^{-1} \in G$
(Introduction To Theory of Computation, P51).

Let $x = a_1 + b_1\sqrt{2} \mid a_1, b_2 \in \mathbb{Q}\}$,$y = a_2 + b_2\sqrt{2} \mid a_2, b_2 \in \mathbb{Q}\}$
In group $\mathbb{R}$ under the operation of addition, it is trivial that $e = 0$, so $y^{-1} = -a_2 - b_2\sqrt{2}$
So $x + y^{-1} = (a_1 - a_2) + (b_1 - b_2)\sqrt{2}$, as $(a_1 - a_2)$ $(b_1 - b_2)$ are both rational, so $x + y^{-1} \in G$. ∎

5. Consider the group $\mathbb{Z}_{12}$ (mod 12 addition on the integers).
   (a) Give the inverse of every element.
   (b) Find all of the generators.
   (c) Determine the order of each element of the group.

Solution: 5.(a) For $\mathbf{Z}_{12}$ with $\oplus$:

Identity element is 0. Thus, for any $a, b \in \mathbf{Z}_{12}, a \oplus b = 0 \Rightarrow a$ is inverse of b.

Inverse elements: 0 inverse of itself: $0 \oplus 0 = 0$.

1, 11 inverses of each other: $1 \oplus 11 = 11 \oplus 1 = 0$.

2, 10 inverses of each other: $2 \oplus 10 = 10 \oplus 2 = 0$.

3, 9 inverses of each other: $3 \oplus 9 = 9 \oplus 3 = 0$.

4, 8 inverses of each other: $4 \oplus 8 = 8 \oplus 4 = 0$.

5, 7 inverses of each other: $5 \oplus 7 = 7 \oplus 5 = 0$.

6 inverse of itself: $6 \oplus 6 = 0$.

(b) By thm 1.3.16, if s is a generator for $\mathbf{Z}_{12}, |s| = 12/gcd(12, s)$.

$\Rightarrow gcd(12, s) = 1$.

Therefore s has no common factors with 12, except 1.

This is true for $1, 5, 7, 11 \in \mathbf{Z}_{12}$.

All these are generators of $\mathbf{Z}_{12}$.

(c) For the generators—1,5,7,11—order is 12.

$2 : 2.1 = 2, 2.2 = 4, 2.3 = 6, 2.4 = 8, 2.5 = 10, 2.6 = 0, ... \Rightarrow |2| = 6$.

$3 : 3.1 = 3, 3.2 = 6, 3.3 = 9, 3.4 = 0, ... \Rightarrow |3| = 4$.

$4 : 4.1 = 4, 4.2 = 8, 4.3 = 0, ... \Rightarrow |4| = 3$.

$6 : 6.1 = 6, 6.2 = 0, ... \Rightarrow |6| = 2$.

$8 : 8.1 = 8, 8.2 = 4, 8.3 = 0, ... \Rightarrow |8| = 3$.

$9 : 9.1 = 9, 9.2 = 6, 9.3 = 3, 9.4 = 0, ... \Rightarrow |9| = 4$.

$10 : 10.1 = 10, 10.2 = 8, 10.3 = 6, 10.4 = 4, 10.5 = 2, 10.6 = 0, ...$

$\Rightarrow |10| = 6$.

(Note: multiplication is mod 12.) ■

6. Consider the following permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 3 & 2 & 1 & 4 & 5 \end{pmatrix}.$$

   (a) Find all of its orbits.
   (b) Express the permutation as a product of 2-cycles.

Solution: Orbits: $(1, 7, 5)$, $(2, 6, 4)$
Permutation: $(1, 5)(1, 7)(2, 4)(2, 6)$
Please see Professor Lavalle's newsgroup post on permutation and 2-cycles for detailed explanation. ■