Homework 1

1. Verify the axioms of a group for the general linear group $\mathrm{GL}_2(\mathbb{R})$.

First check that matrix multiplication gives a well-defined binary operation on $GL_2(\mathbb{R})$:

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in GL_2(\mathbb{R})$ so that $a, b, c, d, a', b', c', d'$ are real and
$\det(A) = ad - bc \neq 0$
$\det(A') = a'd' - b'c' \neq 0$

Then $AA' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$ has real entries and
$\det(AA') = \det(A)\det(A') \neq 0$

Therefore $AA' \in GL_2(\mathbb{R})$.

<u>Axioms:</u>

1) Associativity This is just associativity of matrix multiplication which you have seen before.

2) Identity $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the 2×2 identity matrix and satisfies $eA = Ae = A$ for all 2×2 real matrices.
Note that its entries are real and $\det(e) = 1 \neq 0$ so that $e \in GL_2(\mathbb{R})$.

2) Inverses
$$A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
has real entries and $\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{ad-bc} \neq 0$

thus $A^{-1} \in GL_2(\mathbb{R})$. Check:

$$A(A^{-1}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} ad-bc & -ab+ba \\ cd-dc & -cb+da \end{pmatrix}$$

$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$, and similarly $(A^{-1})A = e$.

2. For each of the following examples, either show that it is a group, or explain why it fails to be a group. If the example is a group, also determine whether it is abelian.

   (a) The set of natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ with the operation of addition.

   (b) The integers $\mathbb{Z}$ with the operation $a \circ b = a - b$.

   (c) The integers $\mathbb{Z}$ with the operation $a \circ b = a + b + 1$.

   (d) The set of positive integers with the operation of multiplication.

   (e) The following set of 2×2 matrices with matrix multiplication:

$$\left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{Z}, \quad ad - bc = 1, \quad a, d \text{ odd}, \quad b, c \text{ even} \right\}$$

(a) Not a group. Does not satisfy axiom of inverses. For example 1 does not have an inverse ($-1 \notin \mathbb{N}$).

(b) Not a group. Axioms 1 and 2 fail.
For example $(1 \circ 1) \circ 1 = (1-1) \circ 1 = 0 \circ 1 = 0 - 1 = -1$
$\neq 1 \circ (1 \circ 1) = 1 \circ (1-1) = 1 \circ 0 = 1 - 0 = 1$

(c) It's a group.

Associativity: $(a \circ b) \circ c = (a+b+1) \circ c = (a+b+1) + c + 1$
$= a + b + c + 2$

$a \circ (b \circ c) = a \circ (b + c + 1) = a + (b+c+1) + 1$
$= a + b + c + 2$ ✓

Identity: $e = -1$.

$a \circ e = a + (-1) + 1 = a$, $e \circ a = (-1) + a + 1 = a$ ✓

Inverses: for $a \in \mathbb{Z}$ define $a^{-1} := -a-2$. Then

$a \circ a^{-1} = a + (-a-2) + 1 = -1 = e$, $a^{-1} \circ a = (-a-2) + a + 1 = -1 = e$. ✓

The group is abelian: $a \circ b = a + b + 1 = b + a + 1 = b \circ a$ for all a, b.

(d) Not a group. Axiom of inverses fails.
For example 2 has no inverse.

See next page for (e)

3. For which subsets of integers $S \subset \mathbb{Z}$ does the set S with the operation of multiplication define a group? Explain your reasoning.

$S = \{1\}$ $\qquad S = \{1, -1\}$ $\qquad S = \{0\}$

These are groups:

These sets are closed under multiplication (i.e. $a, b \in S$ implies $ab \in S$)

Each has an identity (the first two have $e = 1$ and the last one has $e = 0$).

Inverses: in each case, every element is its own inverse.

why these are the only possibilities:

If $S \subseteq \mathbb{Z}$ is a group with $\times$, it has some identity $e \in \mathbb{Z}$. Then $e \cdot e = e$ implies $e = 0$ or 1.

Suppose $S \neq \{e\}$. Then let $a \in S$ with $a \neq e$.

$a \cdot e = a$ implies $e = 1$ (if $e = 0$, $a \cdot e = 0 = e \neq a$).

Also $a^{-1} \cdot a = e$ implies $\frac{1}{a} \in S \Rightarrow a = -1$.

Thus $S = \{1, -1\}$ if $S \neq \{e\}$.

2(e): $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in S \Rightarrow AA' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$

$\left.\begin{matrix} a, d, a', d' \text{ odd} \\ b, c, b', c' \text{ even} \end{matrix}\right\} \Rightarrow \begin{matrix} aa' + bc' \\ cb' + dd' \end{matrix}$ odd, $\begin{matrix} ab' + bd' \\ ca' + dc' \end{matrix}$ even.

(We show S is a subgroup of $GL_2(\mathbb{R})$ and thus a group)

Also $\det(AA') = \det(A)\det(A') = 1 \cdot 1 = 1$. Thus $AA' \in S$.

$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ and $\det(A^{-1}) = \frac{1}{\det(A)} = 1$

odd even

So $A^{-1} \in S$. Finally, $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$.

odd even det = 1

Non-abelian

4. Consider the set $G = \{e, r, b, g, y, o\}$ with operation defined in Lecture 1. In this exercise you will verify that the operation defined by the Cayley table makes G a group.

   (a) Explain why Axiom 2 holds.

   (b) Write down the inverse of each element in G. Conclude Axiom 3 holds.

   (c) Verify Axiom 1, associativity. For example, check $r \circ (b \circ g) = (r \circ b) \circ g$ using the Cayley table. Write down at least 3 other examples verifying this axiom. (On your own you can verify that all other possibilities satisfy the axiom.)

(a) Read directly from the table that $e \circ r = r$, $e \circ b = b$, etc. and also $r \circ e = r$, $b \circ e = b$, etc.

(b) $r^{-1} = r$ $b^{-1} = b$ $g^{-1} = g$ $y^{-1} = o$ $o^{-1} = y$ $e^{-1} = e$

(c)
$(r \circ b) \circ g = o \circ g = b$
$r \circ (b \circ g) = r \circ o = b$ ✓
$(r \circ y) \circ b = g \circ b = y$
$r \circ (y \circ b) = r \circ g = y$ ✓
$(b \circ g) \circ o = o \circ o = y$
$b \circ (g \circ o) = b \circ r = y$ ✓
$(y \circ r) \circ b = b \circ b = e$
$y \circ (r \circ b) = y \circ o = e$ ✓

5. Let G be an arbitrary group. Given the equations $ax^2 = b$ and $x^3 = e$, solve for x.

$$ax^2 = b \qquad x^3 = e$$

mult. on right sides by x

$$ax^3 = bx$$

substitute $x^3 = e$

$$ae = bx$$

$$a = bx$$

mult. on left sides by b^{-1}

$$b^{-1}a = b^{-1}bx$$

$$b^{-1}a = ex = x$$

thus $x = b^{-1}a$

6. For each of the following examples, show that the subset is a subgroup.
   (a) The subset $\{5k : k \in \mathbb{Z}\}$ of the group $(\mathbb{Z}, +)$.
   (b) The subset $\{3^k : k \in \mathbb{Z}\}$ of the group $(\mathbb{Q}^\times, \times)$.
   (c) The subset $\{a + b\sqrt{2} : a, b \in \mathbb{Q},\ a, b \text{ not both } 0\}$ of the group $(\mathbb{R}^\times, \times)$.

In each case check
1. $e \in S$
2. $a, b \in S$ implies $ab \in S$
3. $a \in S$ implies $a^{-1} \in S$.

(a) 1. $e = 0 = 5 \cdot 0 \in S$
2. $5k, 5\ell \in S$. then $5k + 5\ell = 5(k+\ell) \in S$.
3. $5k \in S$. then the additive inverse is $-5k = 5(-k) \in S$.

(b) 1. $e = 1 = 3^0 \in S$.
2. $3^k, 3^\ell \in S$. then $3^k \cdot 3^\ell = 3^{k+\ell} \in S$.
3. $3^k \in S$, the mult. inverse is 3^{-k} which is in S.

(c) 1. $e = 1 = 1 + 0 \cdot \sqrt{2} \in S$.
2. $a + b\sqrt{2}$, $c + d\sqrt{2} \in S$. Here $a, b, c, d \in \mathbb{Q}$ and $(a,b) \neq (0,0)$, $(c,d) \neq (0,0)$.

Then $(a+b\sqrt{2})(c+d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + bd \cdot 2$
$= (ac + 2bd) + (ad + bc)\sqrt{2}$

Suppose $ad + bc = 0$ & $ac + 2bd = 0$. Then one of $a + b\sqrt{2}$, $c + d\sqrt{2}$ is 0. Say $a + b\sqrt{2} = 0$. Then $a/b = -\sqrt{2}$. But a/b is rational, $-\sqrt{2}$ irrational, contrad.

Thus $(a+b\sqrt{2})(c+d\sqrt{2}) \in S$.

3. The inverse of $a + b\sqrt{2} \in S$ is $\dfrac{1}{a+b\sqrt{2}} = \dfrac{1}{a+b\sqrt{2}} \cdot \dfrac{a-b\sqrt{2}}{a-b\sqrt{2}} =$

$$= \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in S.$$

7. Suppose a group G has the property that $a^2 = e$ for all $a \in G$. Show that G is abelian.

For any $a \in G$ we have $a^2 = e$ and after mult. both sides on the left by a^{-1} we get $a = a^{-1}$.

In particular for $a, b \in G$ we obtain

$$ab = (ab)^{-1} = b^{-1}a^{-1}$$

Using $a = a^{-1}$ and $b = b^{-1}$ this gives

$$ab = b^{-1}a^{-1} = ba.$$

So $ab = ba$ for all $a, b \in G$ so G is abelian.

8. Show that the intersection of two subgroups of a group is again a subgroup.

Let $H, K \subseteq G$ be two subgroups.

1. $e \in H \cap K$ because H, K subgroups implies $e \in H$ and $e \in K$.

2. Suppose $a, b \in H \cap K$. Since H, K are subgroups, $ab \in H$ and $ab \in K$. Thus $ab \in H \cap K$.

3. Suppose $a \in H \cap K$. As H, K are subgroups, $a^{-1} \in H$ and $a^{-1} \in K$. Thus $a^{-1} \in H \cap K$.

Thus $H \cap K \subseteq G$ is a subgroup.