Homework 2

Due: May 18th (Monday), 11:59 pm

- Please submit your work on Blackboard.
- You are required to submit your work as a single pdf.
- Please make sure your handwriting is clear enough to read. Thanks.
- No late work will be accepted.
- There are five randomly picked questions (2 pts for each) that will be graded.
  (3), (5), (8), (11), (12)

From now on, we refer to four axioms of the definition of a group as follows.
(i)↔"**Closure**", (ii)↔"**Associativity**", (iii)↔"**Identity**", (iv)↔"**Inverses**".

(1) Using ordinary addition of integers as the operation, show that the set of even integers is a group, but that the set of odd integers is not.

Even integers is a group under ordinary addition:
(i) Even+Even=Even ✓; (ii) ✓; (iii) 0; (iv) its negative.

Odd integers is NOT a group under ordinary addition, even the binary operation is NOT well-defined since (i) fails.

(2) For each binary operation $*$ defined on a set below, determine whether or not $*$ gives a group structure on the set. If it is **not** a group, **say which axioms fail to hold**.
  (a) Define $*$ on $\mathbf{Z}$ by $a * b = \max\{a, b\}$. Not a group, (iii) fails[1]
  (b) Define $*$ on $\mathbf{Z}$ by $a * b = a - b$. Not a group, (ii), (iii) fail
  (c) Define $*$ on $\mathbf{Z}$ by $a * b = |ab|$. Not a group, (iii) fails
  (d) Define $*$ on $\mathbf{R}^+$ by $a * b = ab$. Yes

(3) Let $(G, \cdot)$ be a group. Define a new binary operation $*$ on G by the formula $a * b = b \cdot a$, for all $a, b \in G$.
  (a) Show that $(G, *)$ is a group.
    (i) $a * b = b \cdot a \in G$ since $(G, \cdot)$ is a group.
    (ii) $(a * b) * c = (b \cdot a) * c = c \cdot (b \cdot a) \overset{!}{=} (c \cdot b) \cdot a = (b * c) \cdot a = a * (b * c)$
    Note that $\overset{!}{=}$ is true since $(G, \cdot)$ is a group.
    (iii) The identity element e, which is the same identity element e for $\cdot$.
$$a * e = e \cdot a \overset{!}{=} a \quad \text{and} \quad e * a = a \cdot e \overset{!}{=} a.$$
    Again, $\overset{!}{=}$ is true since $(G, \cdot)$ is a group.
    (iv) For each a, the inverse is a^{-1}, which is the same one w.r.t. $(G, \cdot)$.
$$a * a^{-1} = a^{-1} \cdot a \overset{!}{=} e \quad \text{and} \quad a^{-1} * a = a \cdot a^{-1} \overset{!}{=} e.$$
  (b) Give examples to show that $(G, *)$ may or may not be the same as $(G, \cdot)$.
  If $(G, *)$ is the same as $(G, \cdot)$, this just means $a * b = a \cdot b \Leftrightarrow b \cdot a = a \cdot b$ for all $a, b \in G$. Since they have the same identity element and the same inverses from above discussion. Thus, $(G, *)$ is the same as $(G, \cdot)$ if and

[1] Just note that if (iii) fails, so does (iv).

only if $b \cdot a = a \cdot b$ for all $a, b \in G$, i.e., $(G, \cdot)$ is an abelian group.
Example of a nonabelian group: $\mathrm{GL}_n(\mathbf{R})$ under matrix multiplication.
Example of an abelian group: $\mathbf{Z}$ under ordinary addition.

(4) Write out the multiplication table for $\mathbf{Z}_7^\times$.

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(5) Let $G = \{x \in \mathbf{R} \mid x > 0 \text{ and } x \neq 1\}$. Define the operation $*$ on G by $a * b = a^{\ln b}$, for all $a, b \in G$. Prove that G is an abelian group under the operation $*$.

(i) $a * b = a^{\ln b} > 0$ and $a^{\ln b} \neq 1$ since $\ln b \neq 0$ for $b \in G$.
(ii) $(a * b) * c = a^{\ln b} * c = (a^{\ln b})^{\ln c} = a^{\ln b \ln c} = a^{\ln c \ln b}$
$a * (b * c) = a * (b^{\ln c}) = a^{\ln(b^{\ln c})} = a^{\ln c \ln b} = (a * b) * c \quad \checkmark$

Commutative: $a * b = a^{\ln b} = e^{\ln(a^{\ln b})} = e^{\ln b \ln a} = e^{\ln a \ln b} = e^{\ln(b^{\ln a})} = b^{\ln a} = b * a$

(iii) Identity element is the natural number e. In particular,
$$a * e = a^{\ln e} = a^1 = a \quad \text{and} \quad e * a = e^{\ln a} = a.$$
It suffices to just check $e * a = a$ since $e * a = a * e$ by communicativity.
(iv) For each $a \in G$, the inverse is $e^{1/\ln a}$. In particular,
$a * e^{1/\ln a} = a^{\ln(e^{1/\ln a})} = a^{(1/\ln a)\ln e} = a^{1/\ln a} = a^{\ln e/\ln a} = a^{\log_a^e} = e$
$e^{1/\ln a} * a = (e^{1/\ln a})^{\ln a} = e^{(1/\ln a)\ln a} = e^1 = e$
Again, by communicativity it suffices to just check $e^{1/\ln a} * a = e$.

(6) Show that the set of all 2×2 matrices over $\mathbf{R}$ of the form $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ with $m \neq 0$ forms a group under matrix multiplication. Furthermore, find all elements that commute with $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ in this group.

(i) For nonzero $m_1, m_2 \in \mathbf{R}$ and $b_1, b_2 \in \mathbf{R}$,
$$\begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1 m_2 & m_1 b_2 + b_1 \\ 0 & 1 \end{bmatrix}, \text{ where } m_1 m_2 \neq 0.$$
(ii) Matrix multiplication is associative.
(iii) The identity matrix.
(iv) For $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ with $m \neq 0$, the inverse is $\begin{bmatrix} 1/m & -b/m \\ 0 & 1 \end{bmatrix}$.

For the second part,
$$\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{cases} m2 = 2m \\ b = 2b \end{cases} \Rightarrow b = 0$$
Thus, all elements $\left\{ \begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix} \middle| m \neq 0 \right\}$ are the required ones.

(7) Define $*$ on $\mathbf{R}$ by $a * b = a + b - 1$, for all $a, b \in \mathbf{R}$. Show that $(\mathbf{R}, *)$ is an abelian group.

(i) Trivial.

(ii) $(a * b) * c = (a + b - 1) * c = a + b - 1 + c - 1$
$a * (b * c) = a * (b + c - 1) = a + b + c - 1 - 1$

Commutative: $a * b = a + b - 1 = b + a - 1 = b * a$.

(iii) Identity is 1. By commutativity, we only need to check one equation.

$$a * 1 = a + 1 - 1 = a \text{ for all } a \in \mathbf{R}.$$

(iv) For each $a \in \mathbf{R}$, its inverse is $2 - a$.

$$a * (2 - a) = a + 2 - a - 1 = 1$$

The other equation follows from the commutativity.

(8) Let $S = \mathbf{R} - \{-1\}$. Define $*$ on S by $a * b = a + b + ab$, for all $a, b \in S$. Show that $(S, *)$ is an abelian group.

(i) We need to show $a * b \neq -1$ for all $a, b \in S$. Proof by contradiction: Suppose there exist $a, b \in S$ such that $a * b = -1$, by definition we have

$$a * b = a + b + ab = -1 \Rightarrow a + ab + b + 1 = 0 \Rightarrow (a + 1)(b + 1) = 0.$$

Then we get a contradiction since $a \neq -1$ and $b \neq -1$.

(ii) $(a * b) * c = (a + b + ab) * c = a + b + ab + c + (a + b + ab)c$
$a * (b * c) = a * (b + c + bc) = a + b + c + bc + a(b + c + bc)$

Commutative: $a * b = a + b + ab = b + a + ba = b * a$.

(iii) Identity is 0. By commutativity, we only need to check one equation.

$$0 * a = 0 + a + 0a = a \text{ for all } a \in S.$$

(iv) For each $a \in S$, its inverse is $\dfrac{-a}{a+1}$. It is well-defined since $a \neq -1$.

$$a * \frac{-a}{a+1} = a + \frac{-a}{a+1} + a\frac{-a}{a+1} = \frac{a(a+1) - a - a^2}{a+1} = 0$$

The other equation follows from the commutativity.

(9) Show that a nonabelian group must have at least five distinct elements.

Let e be an identity element in G. We omit $*$, i.e., just write ab for $a * b$.

A nonabelian group G at least have three distinct elements e, a, b since the groups of only one or two elements are abelian. We also have $ab \neq ba$ since G is nonabelian and they are both in G by closure axiom. Now we claim that

$$e, a, b, ab, ba \text{ are distinct elements.}$$

Thus, we just need to show e, a, b, ab are distinct elements and similar procedure can be applied to ba.

- If $ab = a$, then $b = e$ by cancellation law. Contradiction.
- If $ab = b$, then $a = e$ by cancellation law. Contradiction.
- If $ab = e$, then $a = ae = a(ab)$ and $a = ea = (ab)a$. Thus,

$$a(ab) = (ab)a = a(ba) \Rightarrow ab = ba. \text{ Contradiction.}$$

In fact, the simplest nonabelian group has order 6.

(10) Let G be a group. Prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

($\Rightarrow$) Since G is abelian, then $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

($\Leftarrow$) $(ab)^{-1} = a^{-1}b^{-1} \Rightarrow ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1} \Rightarrow ab = (b^{-1})^{-1}(a^{-1})^{-1} = ba$

(11) Let G be a group. Prove that if $x^2 = e$ for all $x \in G$, then G is abelian.
Since $x^2 = e$ for all $x \in G$, then $x = x^{-1}$. In particular, we also have $(xy)^2 = e$ for all $x, y \in G$. Thus $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

(12) Show that if G is a finite group with an even number of elements, then there must exist an element $a \in G$ with $a \neq e$ such that $a^2 = e$.
Suppose $a^2 \neq e$, then $a \neq a^{-1}$. Since G is a group, any such pair of elements

$$\{a, a^{-1} \mid a^2 \neq e\}$$

are also in the G. However $e^2 = e$, then there must exist at least one element $b \in G$ with $b \neq e$ such that $b^2 = e$. Otherwise, if no such element b exists, then this finite group G has an odd number of elements. Contradiction.