Homework 2

Jaden Wang

Problem (3.2)**.** Yes.

i) injective: Given $x, y \in \mathbb{Z}$, we have $\phi(x) = -x, \phi(y) = -y$, if $\phi(x) = \phi(y)$, then $-x = -y \Rightarrow x = y$.

ii) surjective: Given $b \in \mathbb{Z}$, choose $a = -b \in \mathbb{Z}$. We see that $\phi(a) = -(-b) = b$.

iii) $\phi(x * y) = -(x + y) = -x + (-y) = \phi(x) *' \phi(y)$.

Hence ϕ satisfies the definition of an isomorphism.

Problem (3.3)**.** No. Because ϕ is not surjective: $\phi(a) = 2a \neq 1 \quad \forall a \in \mathbb{Z}$.

Problem (3.11)**.** No. Consider $f, g \in F$ where $f(x) = 1$ and $g(x) = 2$. Clearly $\phi(f(x)) = 0 = \phi(g(x))$. However, $f(x) \neq g(x)$. ϕ is then not injective and thus cannot be an isomorphism.

Problem (3.12)**.** No. Consider the same f, g as above. $\phi(f(x)) = f'(0) = 0 = g'(0) = \phi(g(x))$, yet $f(x) \neq g(x)$. Thus injectivity failed.

Problem (4.1)**.** Not a group. $\mathcal{G}_3$ doesn't hold because 0 doesn't have an inverse such that $0 * 0^{-1} = 1$.

Problem (4.2)**.** It is a group.

(i) scalar addition is associative.

(ii) The identity $e = 0 \in 2\mathbb{Z}$, since $0 + a = a + 0 = a \quad \forall a \in 2\mathbb{Z}$.

(iii) Given $a \in 2\mathbb{Z}$, let $a^{-1} = -a \in 2\mathbb{Z}$ so that

$$a * a^{-1} = a + (-a) = 0 = -a + a = a^{-1} * a.$$

Problem (4.8)**.** Consider the set $\{1, 3, 5, 7\}$ and the operation $* = \cdot_8$:

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Problem (4.11)**.** Yes. Let's denote this set as D_n. Given $A \in D_n$,

(i) matrix addition is associative.

(ii) Let O_n be the $n \times n$ matrix with all 0 entries. Given $A \in D_n$, $A + O_n = O_n + A = A$. Hence O_n is the identity.

(iii) Since $A + (-A) = -A + A = O_n$, the inverse $A^{-1} = -A$ exists for all $A \in D_n$.

Problem (4.12)**.** No. Notice that O_n doesn't have an inverse such that $O_n \times O_n^{-1} = I_n$.

Problem (4.13)**.** Yes.

(i) matrix multiplication is associative.

(ii) Let I_n be the $n \times n$ identity matrix. Then given $A \in D_n$ $I_n \times A = A \times I_n = A$, so I_n is the identity.

(iii) Let $B_{ii} = \frac{1}{A_{ii}}$ for $i \in [1, n] and i \in \mathbb{N}$. Then $A_{ii} \cdot B_{ii} = B_{ii} \cdot A_{ii} = 1$, and $A \cdot B = B \cdot A = I_n$. So $A^{-1} = B$.

Problem (4.14)**.** Yes. It's trivially true because this is a special case of Problem 4.13.

Problem (4.19)**.**

a) Given $a, b \in S$, we want to show that $a * b \in S$. Instead we will prove the contrapositive. That is, if $a * b \notin S$, then $a \notin S$ or $b \notin S$. Since -1 is the only real number not in S, and that $+$ is only defined on real numbers, we only need to check this one case by setting $a * b = -1$:

$$\begin{aligned} a + b + ab &= -1 \\ a + b + ab + 1 &= 0 \\ a(b+1) + b + 1 &= 0 \\ (a+1)(b+1) &= 0 \end{aligned}$$

The solution is that either $a = -1 \notin S$ or $b = -1 \notin S$ as required. Hence by the contrapositive, we prove that $a*b \in S$, which makes $*$ a binary operation.

b)

(i) Since scalar multiplication and addition are associative and commutative, we can do the following:

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= a + b + ab + c + ac + bc + abc \\ a * (b * c) &= a * (b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \\ &= a + b + ab + c + ac + bc + abc \\ &= (a * b) * c \end{aligned}$$

(ii) Let $e = 0$, we see that $a * e = a + 0 + a \cdot 0 = a = 0 + a + 0 \cdot a = e * a$. Hence 0 is the identity.

(iii) Let $b = -\frac{a}{1+a}$. Note that since $a \neq -1$, $\frac{a}{1+a} \neq 1$ so $b \neq -1$. Thus $b \in S$.

$$\begin{aligned} a * b &= a - \frac{a}{1+a} - \frac{a^2}{1+a} \\ &= \frac{a + a^2 - a - a^2}{1+a} \\ &= 0 \end{aligned}$$

$$\begin{aligned} b * a &= -\frac{a}{1+a} + a - \frac{a^2}{1+a} \\ &= \frac{-a + a + a^2 - a^2}{1+a} \\ &= 0 \end{aligned}$$

Hence $a * b = b * a = 0$, so a has an inverse $a^{-1} = b = -\frac{a}{1+a}$.

Hence $(S, *)$ is a group.

c)

$$\begin{aligned} 2 * x * 3 &= 7 \\ (2 + x + 2x) * 3 &= 7 \\ 2 + x + 2x + 3 + 6 + 3x + 6x &= 7 \\ 12x &= -4 \\ x &= -\frac{1}{3} \in S \end{aligned}$$

Problem (4.25)**.**

a) False. Given a group $(G, *)$, suppose there exist two identities e_1, e_2 such that given $a \in G$, $a * e_1 = e_1 * a = a$, $a * e_2 = e_2 * a = a$. Then $e_1 * e_2 = e_1 = e_2$, so the identity is unique.

b) True. In class we see that there is only one way to arrange the table so that it is a valid group.

c) True. Because linear equations can be represented by $Mx = b$, where M is a matrix. Since matrices in a group have to be invertible, there always exists a solution $x = M^{-1}b$.

d) False. The proper attitude should be to understand instead of memorize definitions through struggling with challenging problems, so after engaging with them so deeply you would know them by heart without spending effort memorizing them.

e) False. This only shows one direction. It is possible that there exists $a \in G_{text}$ such that $a \notin G_{person}$. Then G_{person} would not be the correction definition.

f) True. If both definitions describe the exact objects, then they can be used interchangeably. If and only if is equivalent to an definition.

g) True. We know from class that for a group with at most three elements, there is only one way to arrange them in a table per distinct number of elements. And these arrangements happen to be commutative. Hence these groups are abelian.

h) True. Since this equation is in the context of a group, the identity e and a^{-1},

b^{-1} exist.

$$\begin{aligned} a^{-1} * a * x * b &= a^{-1} * c \\ e * x * b * b^{-1} &= a^{-1} * c * b^{-1} \\ x * e &= a^{-1} * c * b^{-1} \\ x &= a^{-1} * c * b^{-1} \end{aligned}$$

Which yields a unique element as the solution as $*$ is a function.

i) False. We also need a binary operation to construct a group.

j) True. A group is a set with a binary operation $*$, which satisfies the definition of a binary algebraic structure.