Homework 1

Kevin Guillen

MATH 200 — Algebra I — Fall 2021

I'd like my problem 2.3 to be my graded problem please.

Problem 1.1 Determine the invertible elements of the monoids among the examples in 1.2.

Solution.

- A) For the monoid $(\mathbb{N}_0, +)$ the only invertible element is 0, we can see $0 + 0 = 0$
  For $(\mathbb{N}_0, \cdot)$ we see the only invertible element is 1, we can see $1 \cdot 1 = 1$. Then for $(\mathbb{N}, \cdot)$ the only invertible element is also 1, we can see $1 \cdot 1 = 1$.
- B) For the monoid $(\mathcal{P}(X), \cup)$ the only invertible element is the empty set, $\varnothing \cup \varnothing = \varnothing$. The only invertible element in $(\mathcal{P}(X), \cap)$ is X itself, we can see $X \cap X = X$.
- C) For $(F(X, X), \circ)$ the only invertible element is id_X

□

Problem 1.2 Let

$$M := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}.$$

M is a non-commutative monoid under matrix multiplication. The element $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ is invertible if and only if $a, c \in \{\pm 1\}$. In this case one has,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} a & -abc \\ 0 & c \end{pmatrix}.$$

Solution. First to verify we have a non-commutative monoid we will show associativity. We see for any 3 matrices in M we have the following,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \left[\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} u & v \\ 0 & w \end{pmatrix} \right] = \left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right] \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \left[\begin{pmatrix} xu & xv + yw \\ 0 & zw \end{pmatrix} \right] = \left[\begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix} \right] \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}$$

$$\begin{pmatrix} axu & axv + ayw + bzw \\ 0 & czw \end{pmatrix} = \begin{pmatrix} axu & axv + ayw + bzw \\ 0 & czw \end{pmatrix}.$$

As we can see associativity holds. We also know under matrix multiplication this set is closed based on the above, and the fact that the integers are closed under multiplication and addition. Now we need to show there exists an identity in M, this will simply be $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We verify through the following,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a1 & b1 \\ 0 & c1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1a & 1b \\ 0 & 1c \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

Finally, we know this set is non-commutative by the following counterexample,

$$\begin{pmatrix} 1 & 3 \\ 0 & -5 \end{pmatrix}\begin{pmatrix} -2 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} -2+0 & 3+-6 \\ 0 & -10 \end{pmatrix} = \begin{pmatrix} -2 & 9 \\ 0 & -10 \end{pmatrix}$$
$$\begin{pmatrix} -2 & 3 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 0 & -5 \end{pmatrix} = \begin{pmatrix} -2 & -6+-15 \\ 0 & -10 \end{pmatrix} = \begin{pmatrix} -2 & -21 \\ 0 & -10 \end{pmatrix}$$

We can see $\begin{pmatrix} -2 & -21 \\ 0 & -10 \end{pmatrix} \neq \begin{pmatrix} -2 & 9 \\ 0 & -10 \end{pmatrix}$. Thus M is a non-commutative monoid.

$\Rightarrow$ Given that there exists some matrix $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ that serves as the inverse for $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$. This means,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We know though the elements a, b, c are integers. We know in the ring of integers the only units are ± 1. So for $ax = 1$ and $cz = 1$ to be true, a and c have to be -1 or 1.

$\Leftarrow$ Given that $a, c \in \{\pm 1\}$, we will show $\begin{pmatrix} a & -abc \\ 0 & c \end{pmatrix}$ serves as its inverse.

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a & -abc \\ 0 & c \end{pmatrix} = \begin{pmatrix} aa & -aabc+bc \\ 0 & cc \end{pmatrix} \qquad a, c \in \{\pm 1\} \text{ so, } aa = cc = 1$$
$$= \begin{pmatrix} 1 & -ab+ab \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

□

Problem 1.3 Let S be the set of all matrices

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$$

with entries $a, b \in \mathbb{Z}$. Show that S is a semigroup under matrix multiplication and show that S has a right identity but no left identity. Determine all the right identities. Give an example of a semigroup which has a left identity but no right identity.

Solution. First we will show that S is **closed** under matrix multiplication through the following,

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} = \begin{pmatrix} 0 & ay \\ 0 & by \end{pmatrix}.$$

We know this is in the set S since the integers are closed under multiplication meaning bx and by are also integers.

Now we will show **associativity**, consider the elements $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, $\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix}$, and $\begin{pmatrix} 0 & u \\ 0 & v \end{pmatrix}$ in S. We see through the following,

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \left[\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \begin{pmatrix} 0 & u \\ 0 & v \end{pmatrix} \right] = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \left[\begin{pmatrix} 0 & xv \\ 0 & yv \end{pmatrix} \right] = \begin{pmatrix} 0 & ayv \\ 0 & byv \end{pmatrix}$$
$$\left[\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \right] \begin{pmatrix} 0 & u \\ 0 & v \end{pmatrix} = \left[\begin{pmatrix} 0 & ay \\ 0 & by \end{pmatrix} \right] \begin{pmatrix} 0 & u \\ 0 & v \end{pmatrix} = \begin{pmatrix} 0 & ayv \\ 0 & byv \end{pmatrix}$$

we associativity holds. Satisfying these two things we have shown that S is indeed a semigroup.

Now we will show that S has a **right identity**, specifically $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, through the following,

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a1 \\ 0 & b1 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$$

If a left identity did exist in S, say $\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix}$, that means it serves as a left identity for all elements in S. Let us consider the element $\begin{pmatrix} 0 & 3 \\ 0 & 5 \end{pmatrix}$ We can see through the following that no such element can exist,

$$\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \begin{pmatrix} 0 & 3 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 0 & x5 \\ 0 & y3 \end{pmatrix}$$

since recall x and y must satisfy $\begin{pmatrix} 0 & x5 \\ 0 & y3 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 0 & 5 \end{pmatrix}$. The issue is there exists no integer x or y such that $x5 = 3$ or $y3 = 5$. Meaning there can exist no left identity since by definition it must be a left identity for all elements of S.

We can see through the following,

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0+a0 & 0y+a1 \\ 0+b0 & 0y+b1 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$$

that we actually have an infinite amount of right identities. The set of right identities, denoted by I_r is simply,

$$I_r := \left\{ \begin{pmatrix} 0 & y \\ 0 & 1 \end{pmatrix} \mid y \in \mathbb{Z} \right\}$$

It's obvious that a semigroup with a left identity and no right identity is simply $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ □

Problem 2.3 Let G be a group and let H be a subset of G. Prove the following are equivalent:
a) H is a subgroup G.
b) H is non-empty and if $x, y \in H$ then also $xy^{-1} \in H$.

Proof. $\Rightarrow$ Given that H is a subgroup, then by definition there has to exist an identity element in H, thus, H is non-empty. Since H is a subgroup it also means it is closed under group operation and every element has an inverse in H. So, if $x, y, \in H$ then by definition, y^{-1} exists in H and $xy^{-1} \in H$.

$\Leftarrow$ Given that H is nonempty and if $x, y \in H$ then also $xy^{-1} \in H$, we want to show H is a subgroup.

First we will begin by showing there exists an identity, given that if $x, y \in H$, xy^{-1} is also in H. We can simply let $y = x$ to get xx which implies that $xx^{-1} \in H$, and $xx^{-1} = e$. Therefore H contains an identity.

Now to show that every element has an inverse in H. Consider the element $x \in H$. We know by the given that for $ex \in H$ that ex^{-1} is also in H and thus x^{-1} is in H.

Given the elements x and y in H, we just showed that both their inverses are contained in H, in other words $y^{-1} \in H$. So consider xy^{-1}, by the given that means $x(y^{-1})^{-1}$ is also in H, but $(y^{-1})^{-1} = y$. Therefore xy is in H, meaning H is closed under a group operation. Making H a subgroup as desired. □

Problem 2.4 Let H and K be subgroups of the group G. Show that $HK \leqslant G$ if and only if $HK = KH$

Proof. $\Rightarrow$ Given that $HK \leqslant G$ we want to show $HK = KH$. We begin this by letting x be an element of HK. That means there exists and element h, and element k, in H and K respectively, such that, $x = hk$. Since HK is a subgroup that means it contains and identity e, and inverses for its elements, meaning there exists x^{-1} or in other words there exists $h' \in H$ and $k' \in K$ such that $x^{-1} = h'k'$. Giving us the following,

$$\begin{aligned} xx^{-1} &= e \\ hkh'k' &= e. && \text{multiply by } k'^{-1} \text{ on the right} \\ hkh' &= (k')^{-1} && \text{multiply by } h'^{-1} \text{ on the right} \end{aligned}$$

$$hk = (k')^{-1}(h')^{-1}.$$

Let $y = (k')^{-1}(h')^{-1}$. Recall though H and K themselves are subgroups which is why we knew $(k')^{-1}$ and $(h')^{-1}$ are in K and H respectively. This proves then that for every element $x \in HK$ there exists some element y in KH such that $x = y$ meaning $HK \subseteq KH$.

Now consider any element x in KH, we know it is of the form kh where $k \in K$ and $h \in H$. Given that KH is a subgroup then like the same reasoning above it has inverses for each of its elements meaning there exists $x^{-1} = k'h'$. Following the same reasoning as above,

$$\begin{aligned}
xx^{-1} &= e \\
khk'h' &= e. && \text{multiply by } h'^{-1} \text{ on the right} \\
khk' &= (h')^{-1} && \text{multiply by } k'^{-1} \text{ on the right} \\
kh &= (h')^{-1}(k')^{-1}.
\end{aligned}$$

Let $y = (h')^{-1}(k')^{-1}$. Obvious that $y \in HK$. Thus for every element $x \in KH$ there exists and element $y \in HK$ such that $x = y$, meaning $KH \subseteq HK$.

This gives us that $HK = KH$ as desired.

$\Leftarrow$ Given that $HK = KH$, we'd like to show $HK \subseteq G$ Firstly we know by definition $e \in H$ and $e \in K$, therefore $ee \in HK$ which obviously serves as the identity.

Secondly we must show that is closed under its group operation. Take elements $x, y \in HK$, so $x = hk$ and $y = h'k'$ we see through the following,

$$\begin{aligned} xy &= hkh'k' && KH = HK, \text{ thus } \exists h''k'' \in HK, \text{ s.t. } kh' = h''k'' \\ &= hh''k''k' \end{aligned}$$

Given that H and K were subgroups that means $hh'' \in H$ and $k''k' \in K$ and therefore $xy \in HK$.

Finally for any $x \in HK$ the inverse of x is simply,

$$\begin{aligned} x^{-1} &= (hk)^{-1} \\ &= k^{-1}h^{-1} \end{aligned}$$

This is obviously in KH, but recall $KH = HK$ so there exists some $h'k' = k^{-1}h^{-1}$. Giving us,

$$\begin{aligned} xx^{-1} &= hkh'k' \\ &= hkk^{-1}h^{-1} \\ &= heh^{-1} \\ &= hh^{-1} \\ &= e \end{aligned}$$

Therefore HK is indeed a subgroup of G. $\square$