Math 212, Assignment 1

Due Friday, January 26, 2018

All questions are equally weighted. They will be marked for correctness and clarity of explanation.

1. For each of the following sets, determine if the given operation is a binary operation or not. Explain your answers.

   (a) The set of all 2×2 matrices with real entries whose second row is twice its first row:

   $$X = \left\{ \begin{bmatrix} a & b \\ 2a & 2b \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

   with matrix multiplication.

   Solution. Let $A = \begin{bmatrix} a & b \\ 2a & 2b \end{bmatrix}$ and $C = \begin{bmatrix} c & d \\ 2c & 2d \end{bmatrix}$, so A and C are both in X. We will show that AC is in X as well.

   $$\begin{aligned} AC &= \begin{bmatrix} a & b \\ 2a & 2b \end{bmatrix} \begin{bmatrix} c & d \\ 2c & 2d \end{bmatrix} \\ &= \begin{bmatrix} ac + 2bc & ad + 2bd \\ 2ac + 4bc & 2ad + 4bd \end{bmatrix} \\ &= \begin{bmatrix} ac + 2bc & ad + 2bd \\ 2(ac + 2bc) & 2(ad + 2bd) \end{bmatrix} \end{aligned}.$$

   Since the second row of AC is twice the first row, AC is in X. Therefore matrix multiplication is a binary operation on X.

   (b) Vectors in $\mathbb{R}^3$ with dot product: $(x, y, z) \cdot (x', y', z') = xx' + yy' + zz'$.

   Solution. The dot product of two vectors in $\mathbb{R}^3$ is a real number, and not another vector in $\mathbb{R}^3$, so this is *not* a binary operation.

2. Let S be any set. Consider the binary operation *intersection* on the power

set of S, $\mathcal{P}(S)$. Is this operation associative? Is it commutative? Does it have an identity? Find it, or explain why it doesn't have one.

Solution. We know from the rules of set theory that $\cap$ is both associative and commutative. I'll prove them here for completeness.
To see that $\cap$ is associative, let A, B and C be subsets of S; that is, let $A, B, C \in \mathcal{P}(S)$. Then

$$\begin{aligned} A \cap (B \cap C) &= \{x | x \in A \text{ or } x \in (B \cap C)\} \\ &= \{x | x \in A \text{ or } (x \in B \text{ or } x \in C)\} \\ &= \{x | x \in A \text{ or } x \in B \text{ or } x \in C\} \\ &= \{x | (x \in A \text{ or } x \in B) \text{ or } x \in C\} \\ &= \{x | x \in (A \cap B) \text{ or } x \in C\} \\ &= (A \cap B) \cap C. \end{aligned}$$

To see that it is commutative, again, let B and C be arbitrary subsets of A. Then

$$\begin{aligned} A \cap B &= \{x | x \in A \text{ or } x \in B\} \\ &= \{x | x \in B \text{ or } x \in A\} \\ &= B \cap A. \end{aligned}$$

Finally, the identity for the operation $\cap$ is the set S itself. To see this, note that

$$A \cap S = A = S \cap A$$

for all $A \subseteq S$, that is, for all $A \in \mathcal{P}(S)$.

3. Prove that matrix multiplication is a binary operation on the set

$$X = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in R, ad - bc \neq 0 \right\}.$$

(This set is $GL_2(\mathbb{R})$, but don't use that here.)

Solution. Let $L = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $M = \begin{bmatrix} e & f & g & h \end{bmatrix}$ and assume $ad - bc \neq 0$ and $eh - fg \neq 0$, so that L and M are in X. To see that LM is in X, note that

$$LM = \begin{bmatrix} w & x \\ y & z \end{bmatrix},$$

where $w = ae + bg$, , $x = af + bh$, $y = ce + dg$, and $z = cf + dh$, so

$$\begin{aligned} wz - xy &= (ae + bg)(cf + dh) - (af + bh)(ce + dg) \\ &= adeh + bcfg - adfg - bceh \quad \text{after cancelling inverse terms} \\ &= ad(eh - fg) - bc(eh - fg) \\ &= (ad - bc)(eh - fg). \end{aligned}$$

Since $ad - bc$ and $eh - fg$ are both nonzero, their product is also nonzero. Therefore $LM \in X$.

4. **Definition:** Let X be a set with a binary operation, and let a be an element of X. We say that an element $b \in X$ is a *left inverse* of a if $ba = e$. We say that b is a *right inverse* of a if $ab = e$. (Therefore b is an inverse of a if it both a left inverse and a right inverse of a.)

   Let A be a non-empty set and $f : A \to A$. Prove that f has a right inverse in F_A if and only if f is surjective (onto).

   Solution. First, we suppose that f has a right inverse, g. This means that $f \circ g = \varepsilon_A$. Now, we prove that f is surjective. Let a be in A. We compute

   $$f(g(a)) = f \circ g(a) = \varepsilon_A(a) = a,$$

   so we have found an element of A, namely $g(a)$, which maps to a under f. Hence f is surjective.

   Now, suppose that f is surjective. We show it has a right inverse, which we call g. Let a be in A and we define $g(a)$ in the following way: as f is surjective, there is some b in A (depending on a) such that $f(b) = a$. Choose such a b and let $g(a) = b$. Let us show that g is a right inverse for f: for any a in A, we compute $f \circ g(a) = f(g(a))$. The element $g(a)$ was chosen such that $f(g(a)) = a = \varepsilon_A(a)$.

5. For each of the following, determine (with proof) whether the given set is a group with respect to the given operation.

   (a) The set P of all polynomial functions from $\mathbb{R}$ to $\mathbb{R}$ with the operation composition. That is, the set

   $$P = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = a_0 + a_1 x + \cdots a_n x^n, \text{ where } a_0, \ldots, a_n \in \mathbb{R}\},$$

with composition.

Solution. We claim that the set P does not contain an inverse for every element, and therefore it is not a group under composition. To see this, note that the function $\epsilon_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ defined by $\epsilon_{\mathbb{R}}(x) = x$ for all $x \in \mathbb{R}$ is an identity for composition in P. Now consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ for all $x \in \mathbb{R}$, and suppse for a contradiction that there is a function g such that $f \circ g = \epsilon_{\mathbb{R}}$.
That is, suppose $f(g(x)) = x$ for all $x \in \mathbb{R}$. By our definition of f, this implies that $(g(x))^2 = x$, for all $x \in \mathbb{R}$, including $x = -1$. That is, we have $(g(-1))^2 = -1$, but this is a contradiction since $g(-1) \in \mathbb{R}$.

(b) The set $\mathbb{R} \setminus \{-1\}$ with the operation $*$ defined by

$$a * b = a + b - ab.$$

Solution. This is not a group because it is not closed under the operation. For example, let $a = 2$ and $b = 3$. Then

$$a * b = a + b - ab = 2 + 3 - 6 = -1.$$

(c) The power set $\mathcal{P}(S)$ of a set S, with the operation intersection.

Solution. We proved in (3) that intersection is associative and commutative and that S is an identity for intersection in $\mathcal{P}(S)$. However, we will show that $\emptyset \in \mathcal{P}(S)$ does not have an inverse for intersection. For any $A \in \mathcal{P}(S)$, $\emptyset \cap A = \emptyset$.
Therefore (unless S is the emptyset) $\mathcal{P}(S)$ is not a group under intersection.

6. Find, with proof, the order of $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ in $GL_2(\mathbb{R})$?

Solution. We prove by induction that for all $k \in \mathbb{Z}^+$, $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}$.

For the base case ($k = 1$), there is nothing to prove.

For the induction hypothesis, assume that for some $k \geq 1$ we have

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}.$$

In that case,

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{k+1} &= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad , \\ &= \begin{bmatrix} 1 & 0 \\ k+1 & 1 \end{bmatrix} \end{aligned}$$

as required.

From the above, it follows that for all $k \geq 1$,

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^k \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

So $o\left(\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\right) = \infty$.

7. Let k be a positive integer and let a be a negative integer. Prove using the axioms for the integers that $a^k = (-a)^k$ if and only if k is even, using the axioms for the integers. (You may also use the results from Chapter 1 and the results from Chapter 2 that follow from the axioms.)

Solution. ($\Leftarrow$) Let $k = 2n$, for some positive integer n. First we prove that $a^2 = (-a)^2$.

By Proposition 1.2.17, $(-a) = ((-a)1) = a(-1)$, so

$$\begin{aligned} (-a)^2 &= (a(-1))^2 \\ &= a^2(-1)^2 && \text{by Axioms 2b (associativity) and 2c (commutativity)} \\ &= a^2 && \text{by Proposition 1.2.17.} \end{aligned}$$

Therefore

$$\begin{aligned}(-a)^k &= (-a)^{2n} \\ &= ((-a)^2)^n && \text{by Axiom 2b (associativity)} \\ &= (a^2)^n \\ &= a^{2n} && \text{by Axiom 2b, again} \\ &= a^k.\end{aligned}$$

We have shown that

$$\text{for any even positive integer } k,\ (-a)^k = a^k. \tag{1}$$

($\Rightarrow$) We prove the contrapositive of the implication, " if $a^k = (-a)^k$ then k is even". That is, we prove the implication, " if k is odd then $a^k \neq (-a)^k$."

Let $k = 2n + 1$, for some nonnegative integer n (so that $k \in \mathbb{Z}^+$). Then

$$\begin{aligned}(-a)^2 &= (-a)^{2n+1} \\ &= (-a)^{2n}(-a) \\ &= a^{2n}(-a) && \text{by (1)} \\ &= -(a^{2n}a) && \text{by Proposition 1.2.17} \\ &= -a^{2n+1} \\ &= -a^k.\end{aligned}$$

By Axiom 4c, $-a^k \neq a^k$, since exactly one of these is in $\mathbb{Z}^+$.

8. Let G be a finite group of even order. Prove that there is an element $a \neq e$ of G such that $a^2 = e$.

Solution. Suppose for a contradiction that there is no element $a \neq e$ in G such that $a^2 = e$. This is equivalent to the saying that there is no element of G, besides e, which is its own inverse. Therefore, under our assumption, $G \setminus \{e\}$ can be partitioned into pairs $\{a, b\}$ such that a and b are inverses of each other, and $a \neq b$ (by "partition", we mean every element of $G \setminus \{e\}$ is in exactly one such pair). However, this implies that $G \setminus \{e\}$ has even cardinality, which contradicts our assumption that G has even cardinality (order).

Rules for group assignments. Make sure you follow the universal rules for group assignments (below) and any additional rules/procedures laid out in your Group Contract.

1. Each group member is expected to contribute to the best of their ability, and assignment submissions should only include the names of group members who meet this expectation.

2. Each group member should be able to explain the group's solution to me and answer any questions I may have about it. It is the whole group's responsibility to ensure that this standard is met.

3. The task of composing final solutions and writing them up in good copy must be shared equally among all group members (after a collaborative problem-solving process).

4. After good copy solutions are complete, they should be shared among all group members to be double-checked and proofread. This should be done in advance of the due date, to allow time for any necessary corrections. Corrections should be completed by the person who wrote the original solution.