Modern Algebra (MATH 6302), Fall 2024
Homework Assignment I

Joel Sleeba

August 30, 2024

1. **Solution:**

   (a) False. Let $A = (0,1), B = (-1,1), C = (0,1)$ and let $f : A \to B := x \to x$, $g : B \to C := x \to x^2$. Clearly $g \circ f : (0,1) \to (0,1) := x \to x^2$ is injective. But g is not injective.

   (b) False. The same functions above give the counterexample.

2. **Solution:**

   (a) Yes. Let $B, C \in \mathcal{P}(X)$ be elements with $f(B) = f(C)$. That is $B^c = C^c$. Then taking complements on both sides preserve the equality and hence, we get

   $$(B^c)^c = (C^c)^c$$
   $$B = C$$

   This shows that f is one-to-one

   (b) Yes. Let $C \in \mathcal{P}(X)$. Now since $(C^c)^c = C$, we get that $f(C^c) = C$. Since C was chosen arbitrarily, this holds true for any subset of X and hence f is onto.

3. **Solution:**

   (a) We claim that the function f_A is injective if and for if $A = X$. If $A = X$, and $f_A(B) = f_A(C)$ for subsets B, C of X, then $B = A \cap B = f_A(B) = f_A(C) = A \cap C = C$ shows that f_A is injective.

Conversely If $A \neq X$ and $X \neq \emptyset$, then there exists a $b \in X$ with $b \notin A$. Now consider the subsets $\emptyset$ and $\{b\}$ of X. Both $f_A(\emptyset) = \emptyset$ and $f_A(\{b\}) = \emptyset$. But clearly $\{b\} \neq \emptyset$. Therefore, f_A cannot be injective.

Hence f_A is injective if and only if $A = X$.

(b) Again we claim that f_A is surjective if and only if $A = X$. If $A = X$ and C is an arbitrary subset of X, then $f_A(C) = A \cap C = X \cap C = C$. Since C was arbitrary, this proves that f is surjective.

Conversely if $A \neq X$ and $X \neq \emptyset$, then like in the last question we get an element $b \in X$ with $b \notin A$. Since $f_A(B) = A \cap B \subset A$, and $b \notin A$, there is not any set $C \subset X$ for which $f_A(C) = \{b\}$. Therefore, f_A cannot be surjective.

Hence f_A is surjective if and only if $A = X$

4. **Solution:**

(a) f_A is injective for every set $A \subset X$. To see this, let A, B be nonempty subsets of X with $A\Delta B = A\Delta C$. We need to show $B = C$. Instead we will show that $B = (A\Delta B)\Delta A$ for all $B \subset X$. Then $B = (A\Delta B)\Delta A = (A\Delta C)\Delta A = C$, and this would prove the injectivity of f_A

Let $x \in (A\Delta B)\Delta A$, then there are two cases.

i. $x \in A\Delta B = (A \setminus B) \cup (B \setminus A)$ and $x \notin B$. This implies $x \in A \setminus B$

ii. $x \in A \setminus (A\Delta B)$, which implies $x \in A \cap B$

Combining both of them we get $x \in (A \setminus B) \cup (A \cap B) = A$, which gives $x \in A$. Therefore $A \subset (A\Delta B)\Delta A$ and retracing the argument back, we get the reverse inclusion. Hence $A = (A\Delta B)\Delta A$.

(b) f_A is surjective for all $A \subset X$. Let C be an arbitrary subset of X. Since we know $C = (A\Delta C)\Delta A = A\Delta(A\Delta C)$, we immediately see $f_A(A\Delta C) = C$, which completes our proof.

5. **Solution:**

(a) Using the euclidean algorithm, we get that the gcd of the given numbers is 1.

$$106823 = 3 \times 35603 + 14$$
$$35603 = 2543 \times 14 + 1$$
$$1 = 1 \times 1 + 0$$

(b) We isolate 1 from the above calculation and work our way back to a and b

$$\begin{aligned}
1 &= 35603 - 2543 \times 14 \\
&= 35603 - 2543 \times (106823 - 3 \times 35603) \\
&= (1 + 2543 \times 3) \times 35603 - 2543 \times 106823 \\
&= 7630 \times 35603 - 2543 \times 106823
\end{aligned}$$

6. **Solution:**

(a) Given that $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime factorization of n. Now if $m = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$ is the prime factorization of a divisor of n, then each q_i must be equal to some p_j with $\beta_i \leq \alpha_j$. Therefore for each i, we have $(\alpha_i + 1)$ choices (including zero) for the power of p_i while constructing a divisor of n. Now using the multiplication principle of counting, we get the number of divisors to be equal to $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$

(b) Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factor of number below 1000 with exactly 15 divisors. Then $15 = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$. Also $15 = 3 \times 5 = 15 \times 1$. So the possible set of values of α_i is from the set $\{0, 2, 4, 14\}$. But for any prime p_i, we have $p_i^{14} > 2^{14} > 1000$. Hence α_i cannot take the value 14 for any i.

This gives that if $1000 > n$ has exactly 15 divisors, then the prime factorization of $n = p_1^2 p_2^4$. Now since p_1 is atleast 2, we get $4 \times p_2^4 \leq n \leq 1000$, which gives $p_2^4 \leq 250$. Also, $4^4 = 256 > 250$, hence the only options for p_2 are 2 and 3.

Now we proceed in cases. If $p_2 = 3$, then the only choice for $p_1 = 2$, since $2^2 \times 3^4 = 324 \leq 1000$, but for the very next prime different from 3, we have $5^2 \times 3^4 = 2025 > 1000$.

If $p_2 = 2$, then we have a couple of more options. Specifically

- $3^2 \times 2^4 = 144$
- $5^2 \times 2^4 = 400$
- $7^2 \times 2^4 = 789$

Hence in total there are 4 distinct positive integers under 1000 with exactly 15 positive integer divisors.

7. **Solution:**

   (a) A binary operation on S is a function from $f : S \times S \to S$. Since we know that $|S| = n$, $S \times S$ has n^2 elements. Moreover for every $x \in S \times S$, $f(x)$ has n possible values. Then by the multiplication principle of counting, there are n^{n^2} possibilities for f. Hence there are that many binary operations on S

   (b) Now imagine the Cayley table of a commutative binary operation $f : S \times S \to S$. Since $|S| = n$, the Cayley table has n^2 cells. Moreover, since the binary operation is commutative, the Cayley table must be symmetric about its main diagonal. Equivalently, the image of the upper triangular entries under f completely determine f. Hence by the counting formula $1 + 2 + \ldots n = \frac{n(n+1)}{2}$, we get that there are $n^{\frac{n(n+1)}{2}}$ commutative binary operations.

8. **Solution:** Now we'll try to approch this question using Cayley tables. For this we'll draw the Cayley tables of all possible commutative binary operations on the set. From the above exercise, we get that there are 8 of them.

I	1	2
1	1	1
2	1	1

II	1	2
1	1	2
2	2	1

III	1	2
1	1	1
2	1	2

IV	1	2
1	2	2
2	2	1

V	1	2
1	2	2
2	2	2

VI	1	2
1	2	1
2	1	2

VII	1	2
1	1	2
2	2	2

VIII	1	2
1	2	1
2	1	1

   Now to verify if the binary operations are associative, we just need to verify associativity for the forms $(a \cdot a) \cdot a$, $(a \cdot b) \cdot a$, and $(a \cdot a) \cdot b$. Now by commutativity of the operation $\cdot$, we get

   - $(a \cdot a) \cdot a = a \cdot (a \cdot a)$
   - $(a \cdot b) \cdot a = a \cdot (a \cdot b) = a \cdot (b \cdot a)$

   Hence on the above Cayley tables, we just need to verify if $(a \cdot a) \cdot b = a \cdot (a \cdot b)$. Moreover we see that tables *V*-*VIII* are just a relabelling of *I*-*IV*, in that order. So verifying $(a \cdot a) \cdot b = a \cdot (a \cdot b)$ when $a \neq b$ for just the operations *I*-*IV*.

I Trivially associative since its constant 1

II
- $(1 \cdot 1) \cdot 2 = 1 \cdot 2 = 2 = 1 \cdot 2 = 1 \cdot (1 \cdot 2)$
- $(2 \cdot 2) \cdot 1 = 1 \cdot 2 = 2 = 2 \cdot 1 = 2 \cdot (2 \cdot 1)$

III
- $(1 \cdot 1) \cdot 2 = 1 \cdot 2 = 1 = 1 \cdot 1 = 1 \cdot (1 \cdot 2)$
- $(2 \cdot 2) \cdot 1 = 2 \cdot 1 = 1 = 2 \cdot 1 = 2 \cdot (2 \cdot 1)$

IV
- $(1 \cdot 1) \cdot 2 = 2 \cdot 2 = 1 \neq 2 = 1 \cdot 2 = 1 \cdot (1 \cdot 2)$
- $(2 \cdot 2) \cdot 1 = 1 \cdot 1 = 2 \neq 1 = 2 \cdot 2 = 2 \cdot (2 \cdot 1)$

Hence the binary operations corresponding to *I-III* are associative and by relabelling we get *V-VII* are also associative. Hence they give the exhaustive list of binary operations in $\{1, 2\}$ which are associative and commutative.

9. **Solution:** To show injectivity, let $f_g(i) = f_g(j)$. Then we get $gi = gj$. Left multiplying by g^{-1}, we get $i = j$. To show surjectivity, let $h \in G$, then $f_g(g^{-1}h) = gg^{-1}h = h$. This shows f_g is bijective.

10. **Solution:**

    (a) To show injectivity, let $f_g(i) = f_g(j)$. This gives us $gig^{-1} = gig^{-1}$. Left multiplying by g^{-1} and right multiplying by g, we get $g^{-1}gig^{-1}g = g^{-1}gjg^{-1}g$. Associativity of the group operation gives us $i = j$. Hence f_g is injective. Similarly, let $h \in G$, then $f_g(g^{-1}hg) = gg^{-1}hgg^{-1} = h$, shows that$f_g$ is surjective. Hence f_g is bijective.

    (b) Since the group operation is associative, we get

$$\begin{aligned} f_g(h_1h_2) &= gh_1h_2g^{-1} \\ &= gh_1g^{-1}gh_2g^{-1} \\ &= f(h_1)f(h_2) \end{aligned}$$

11. **Solution:**

    (a) The function composition is associative. Let $f, g, h : \mathbb{R} \to \mathbb{R}$. Then

consider $(f \circ g) \circ h$ and $f \circ (g \circ h)$. For any $x \in \mathbb{R}$

$$\begin{aligned}((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) \\ &= f(g(h(x)) \\ &= f((g \circ h)(x)) \\ &= (f \circ (g \circ h))(x))\end{aligned}$$

Which gives $f \circ (g \circ h) = (f \circ g) \circ h$.

But the function composition is not commutative. Let $f(x) = x + 1$ and $g(x) = x^2$. Then $(f \circ g)(x) = x^2 + 1$, but $(g \circ f)(x) = (x + 1)^2$, which are not equal.

(b) No. $(S, \circ)$ is not a group since there are elements in S without inverses. For example $f : \mathbb{R} \to \mathbb{R} := x \to x^2$ is not invertible.

12. **Solution:** From above problem we see that the function composition is an associative binary operation. To show S is a group, we need to show that S has an identity element and that every element in S has an inverse.

Let $I : \mathbb{R} \to \mathbb{R} := x \to x$. Clearly $I \in S$ since it is bijective. Moreover for any $f \in S$ and $x \in \mathbb{R}$, $(f \circ I)(x) = f(I(x)) = f(x) = (I \circ f)(x)$. Therefore I acts as the identity element in S

Since every element in S is a bijective map, is has an inverse. Hence $(S, \circ)$ is a group.

But the group is non-Abelian. Let $f : \mathbb{R} \to \mathbb{R} := x \to 2x + 1$ and $f : \mathbb{R} \to \mathbb{R} := x \to x + 1$. Then $f, g \in S$ and $f \circ g : x \to 2(x + 1) + 1 = 2x + 3$ and $g \circ f : x \to 2x + 2$. Hence $f \circ g \neq g \circ f$

13. **Solution:**

(a) By the properties of the dihedral group, we know that $sr^i s = r^{-i}$. Then $(sr^i)^2 = sr^i sr^i = r^{-i} r^i = e$

(b) Since $r^{2m} = e$, $r^m = r^{-m}$. Now we need to show $xr^m = r^m x$ for all $x \in D_{2n}$. If $x = r^j$ for some $j \in \{0, 1, \ldots n-1\}$, then $r^j r^m = r^{(j+m)=r^m r^j}$.

If $x = sr^i$ for some $i \in \{0, 1, \ldots n-1\}$, then $xr^m = sr^i r^m = sr^{i+m} = sr^m r^i = r^m sr^i = r^m x$. Note that $sr^i = r^i s$ since $sr^i s = r^{-i}$.

14. **Solution:** $C_{20}, D_{20}, Z_{10} \otimes Z_2$.

C_{20} is not isomorphic to $Z_{10} \otimes Z_2$ since C_{20} is cyclic while the latter is not. Also see that $Z_{10} \otimes Z_2$ has three elements of order 2, $(0,1), (5,0)$ and $(5,1)$, while the only element of order 2 in C_{20} is a^{10}, where a is any generator of C_{20}.

Both are not isomorphic to D_{20} since D_{20} is non-Abelian while the rest of them are Abelian.