Homework 1

Elliott Yoon

September 25, 2023

1 9/20

1. If S and I are sets, let S^I be the set of functions $f : I \to S$. Let $I = \{0, 1\}$. Prove that for any set S there is a bijection $p : S^I \to S \times S$.

   - Let $x, y \in S$. Define $f_{xy} : I \to S$ such that $f(0) = x$ and $f(1) = y$. Then define $g : S^I \to S \times S$ by
   $$g(f_{xy}) = (x, y)$$
   and $g' : S \times S \to S^I$ by
   $$g'((x, y)) = f_{xy}.$$
   So $g(g'(x, y)) = (x, y)$ and $g'(g(f_{xy})) = f_{xy}$. g is invertible, and thus a bijection. $\square$

2. Let $S = \{1, \ldots, n\}$ for some $n \in \mathbb{Z}^+$. Compute the number of binary operations on S.

   - Each binary operation $m : \{1, \ldots, n\} \times \{1, \ldots, n\} \to \{1, \ldots, n\}$ assigns n possible values to $n \times n = n^2$ inputs to give a total number of n^{n^2} binary operations. $\square$

3. Show that if m is a unital, associative binary operation on a set S, then inverses are unique when they exist: if $a \in S$ and $x, y \in S$ are inverses of a, then $x = y$.

   - Let $a \in S$, $x, y \in S$ be inverses of a, and e be the identity element of m. Notating $m(a, b) := a \cdot b$ where $a, b \in S$, we have that
   $$x = x \cdot e = x \cdot (a \cdot y) = (x \cdot a) \cdot y = e \cdot y = y$$
   by associativity and x, y being inverses of a. $\square$

4. (The Eckmann-Hilton argument). Let S be a set with two binary operations $\bullet$ and $\circ$ satisfying the following two axioms:

   (a) $\bullet$ and $\circ$ each have a two-sided identity element $1_\bullet$ and $1_\circ$, respectively;

   (b) for each $a, b, c, d \in S$, there is the identity $(a \circ b) \bullet (c \circ d) = (a \bullet c) \circ (b \bullet d)$.

   Prove that (a): $1_\bullet = 1_\circ$, (b): $\bullet = \circ$, (c): $\bullet$ is associative, and (d): $\bullet$ is commutative.

   - Let $x, y, z \in S$.

     (a) Notice that by the identity properties and axiom (b) listed above,
     $$1_\bullet = 1_\bullet \bullet 1_\bullet = (1_\circ \circ 1_\bullet) \bullet (1_\bullet \circ 1_\circ) \overset{(b)}{=} (1_\circ \bullet 1_\bullet) \circ (1_\bullet \bullet 1_\circ) = 1_\circ \circ 1_\circ = 1_\circ.$$
     For sake of notation, we will now confuse $1_\circ$ with $1_\bullet$ by writing $1 := 1_\circ = 1_\bullet$.

(b) Similarly, we have

$$x \bullet y = (x \circ 1) \bullet (1 \circ y) = (x \bullet 1) \circ (1 \bullet y) = x \circ y,$$

and we will thus also confuse $\circ$ with $\bullet$ by writing $\cdot := \bullet = \circ$ for the rest of the problem. Thus, we can rewrite axiom (b) as

$$(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d).$$

(c) Thus, we get

$$x \cdot (y \cdot z) = (x \cdot 1) \cdot (y \cdot z) = (x \cdot y) \cdot (1 \cdot z) = (x \cdot y) \cdot z.$$

(d) Finally, we have that

$$x \cdot y = (1 \cdot x) \cdot (y \cdot 1) = (1 \cdot y) \cdot (x \cdot 1) = y \cdot x,$$

as desired.

□

5. Find a binary operation which is not commutative and not associative.

   - Consider the cross product for vectors in $\mathbb{R}^3$. Notice $\vec{e_1} \times \vec{e_2} = \vec{e_3}$ but $\vec{e_2} \times \vec{e_1} = -\vec{e_3} \neq \vec{e_3}$. Also,

   $$(\vec{e_3} \times \vec{e_1}) \times (\vec{e_1} + \vec{e_2}) = \vec{e_2} \times (\vec{e_1} + \vec{e_2}) = -\vec{e_3}$$

   but

   $$\vec{e_3} \times (\vec{e_1} \times (\vec{e_1} + \vec{e_2})) = \vec{e_3} \times \vec{e_3} = \vec{0} \neq -\vec{e_3}.$$

□

2 9/22

1. An associative loop is a group. Show that there exist non-associative loops.

   - Consider the magma $(S, +)$ defined on the set $S = \{0, 1, 2, 3, 4\}$ with binary operation $+$ given by the Cayley table in Figure 1 below. From the table, we can see that S is Latin-square, and

b →

a+b	0	1	2	3	4
a ↓ 0	0	1	2	3	4
1	1	2	4	0	3
2	2	3	1	4	0
3	3	4	0	1	2
4	4	0	3	2	1

Figure 1: My silly Cayley table

thus a quasi-group. Furthermore, it has identity element 0, and is thus a loop. However, we can compute that

$$(1 + 1) + 1 = 2 + 1 = 3$$

but

$$1 + (1 + 1) = 1 + 2 = 4,$$

so S is non-associative. □

2. Let G be a group and fix $a \in G$. Prove that $(a^{-1})^{-1} = a$.

   - Fix $a \in G$, where G is a group. Then

$$\begin{aligned}(a^{-1})^{-1} \cdot a^{-1} &= 1\\ (a^{-1})^{-1} \cdot (a^{-1} \cdot a) &= a\\ (a^{-1})^{-1} &= a\end{aligned}$$

   since G is unital, associative, and has inverses. □

3. Let G be a group and fix $a, b \in G$. Prove that $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

   - Fix $a, b \in G$, where G is a group. Then

$$\begin{aligned}(a \cdot b)^{-1} \cdot (a \cdot b) &= 1\\ (a \cdot b)^{-1} \cdot a \cdot b \cdot b^{-1} &= b^{-1}\\ (a \cdot b)^{-1} \cdot a \cdot a^{-1} &= b^{-1} \cdot a^{-1}\\ (a \cdot b)^{-1} &= b^{-1} \cdot a^{-1}\end{aligned}$$

   since G is unital, associative, and has inverses. □

4. Let G be a group with identity element e and fix $a \in G$ and $n \in \mathbb{Z}$. Set $a^0 = e$. For $n > 0$, define a^n inductively by $a^n = a \cdot a^{n-1}$. For $n < 0$, define $a^n = (a^{-n})^{-1}$. One has $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ for $m, n \in \mathbb{Z}$. Prove that if G is abelian, then $(a \cdot b)^n = a^n \cdot b^n$ for all $a, b \in G$.

   - Let $a, b \in G$, a group with identity element e. We'll first show by induction that $(a \cdot b)^n = a^n \cdot b^n$ for $n \in \mathbb{Z}^+$: Notice that by group axioms and our definition of exponentiation,

$$(a \cdot b)^0 = e = e \cdot e = a^0 \cdot b^0$$

   and
$$(a \cdot b)^1 = (a \cdot b) \cdot (a \cdot b)^0 = a \cdot b = (a \cdot e) \cdot (b \cdot e) = a^1 \cdot b^1.$$

   Now, suppose $(a \cdot b)^n = a^n \cdot b^n$ for some $n \in \mathbb{N}$. The inductive hypothesis and group axioms give that

$$(a \cdot b)^{n+1} = (a \cdot b) \cdot (a \cdot b)^n = (a \cdot b) \cdot (a^n \cdot b^n) = (a \cdot a^n) \cdot (b \cdot b^n) = a^{n+1} \cdot b^{n+1}.$$

   Hence, by induction, $(a \cdot b)^n = a^n \cdot b^n$ for $n \in \mathbb{N}$. Finally, suppose $n \in \mathbb{N}$. Previous results and commutativity give

$$(a \cdot b)^{-n} = ((a \cdot b)^n)^{-1} = (a^n \cdot b^n)^{-1} = (b^n)^{-1} \cdot (a^n)^{-1} = (a^n)^{-1} \cdot (b^n)^{-1} = a^{-n} \cdot b^{-n}.$$

   □

5. Let G be a finite group with identity element e. Show that there exists an integer $n > 0$ such that $a^n = e$ for all $a \in G$.

   - Let G be a finite group with identity e. Let $a \in G$. Since G is finite, the set

     $$\{a^n \mid n \in \mathbb{N}\}$$

     is finite. Further, G has a unique identity, so there must exist $p, q \in \mathbb{N}$ where $p < q$ and

     $$a^p = a^q$$

     to give repetition. Setting $n = q - p$, we have $n = q - p > 0$ and

     $$a^n = a^{q-p} = e,$$

     as desired. $\square$