Solutions to Homework #1

1. (2 points) Saracino, Section 0, Problem 0.1: Let $S = \{2, 5, \sqrt{2}, 25, \pi, 5/2\}$ and $T = \{4, 25, \sqrt{2}, 6, 3/2\}$. Find $S \cap T$ and $S \cup T$.

Solution. By inspection, we have

$$\boxed{S \cap T = \{25, \sqrt{2}\}} \qquad \text{and} \qquad \boxed{S \cup T = \{2, 4, 5, 6, 25, 3/2, 5/2, \pi, \sqrt{2}\}}$$

---

2. Saracino, Section 0, Problem 0.5: A, B, C are sets. Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. ($\subseteq$): Given $x \in A \cap (B \cup C)$, we have $x \in A$ and $x \in B \cup C$.
Since $x \in B \cup C$, we have either $x \in B$ or $x \in C$, so we consider these two cases:
Case 1: Suppose $x \in B$. Then since $x \in A$, we have $x \in A \cap B \subseteq (A \cap B) \cup (A \cap C)$
Case 2: Suppose $x \in C$. Then since $x \in A$, we have $x \in A \cap C \subseteq (A \cap B) \cup (A \cap C)$.
Either way, we have $x \in (A \cap B) \cup (A \cap C)$, as desired. QED ($\subseteq$)

($\supseteq$): Given $x \in (A \cap B) \cup (A \cap C)$, we have either $x \in A \cap B$ or $x \in A \cap C$, so we consider these two cases:
Case 1: Suppose $x \in A \cap B$. Then $x \in A$, and also $x \in B \subseteq B \cup C$. Therefore, $x \in A \cap (B \cup C)$.
Case 2: Suppose $x \in A \cap C$. Then $x \in A$, and also $x \in C \subseteq B \cup C$. Therefore, $x \in A \cap (B \cup C)$.
Either way, we have $x \in A \cap (B \cup C)$, as desired. QED

---

3. Saracino, Section 0, Problem 0.8: Prove that $\displaystyle\sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2$ for all $n \geq 1$.

Proof. By induction on $n \geq 1$.

Base: For $n = 1$, we have LHS $= 1^3 = 1 = \left[\frac{1(2)}{2}\right]^2$.

Inductive: Suppose the statement is true for n. Then

$$\sum_{i=1}^{n+1} i^3 = \left(\sum_{i=1}^{n} i^3\right) + (n+1)^3 = \left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 = \left[\frac{n+1}{2}\right]^2 \Big(n^2 + 4(n+1)\Big)$$
$$= \left[\frac{n+1}{2}\right]^2 \big(n^2 + 4n + 4\big) = \left[\frac{n+1}{2}\right]^2 (n+2)^2 = \left[\frac{(n+1)(n+2)}{2}\right]^2.$$ QED

---

4. Saracino, Section 1, Problem 1.3(a,c,g). In each case, if $*$ **is** a binary operation, give a short explanation why but not a formal proof. If $*$ is **not** a binary operation, give one explicit example of $x * y$ that shows this failure.

Solutions. (a): $S = \mathbb{Z}$, $a * b = a + b^2$: $\boxed{\text{YES}}$ this is a binary operation, because for any $a, b \in \mathbb{Z}$, we have $a * b \in \mathbb{Z}$.

(c): $S = \mathbb{R}$, $a * b = \dfrac{a}{a^2 + b^2}$: $\boxed{\text{NO}}$ this is **not** a binary operation, because $a = 0, b = 0 \in \mathbb{R}$ gives $a * b = \dfrac{0}{0}$ is undefined.

(g): $S = \{1, -2, 3, 2, -4\}$, $a * b = |b|$: $\boxed{\text{NO}}$ this is **not** a binary operation, because $a = 1 \in S$ and $b = -4 \in S$ gives $a * b = |-4| = 4 \notin S$.

[**Note**: in (g), any choice of $a \in S$ paired with $b = -4 \in S$ gives $a * b \notin S$.]

---

5. Saracino, Section 2, Problem 2.1(b,c,f,g). For each part, if you say it **is** a group, give a short explanation, but not a formal proof, of why each of the four group axioms holds (binary operation, associative, identity, inverses), including saying what the identity element is and what the inverse of an arbitrary element g is. If you say it is **not** a group, give one explicit example of one axiom failing.

Solutions. (b): $3\mathbb{Z}$ with $+$: $\boxed{\text{YES}}$ this is a group. If x, y are divisible by 3, so is $x + y$, so it's a binary operation. And we already know addition is associative, and 0 is the identity (and 0 **is** in $3\mathbb{Z}$, since $0 = 3 \cdot 0$). And the inverse of $x \in 3\mathbb{Z}$ is $-x$, which is also a multiple of 3 and so also in $3\mathbb{Z}$.

(c): $\mathbb{R} \setminus \{0\}$ under $a * b = |ab|$: NO this is not a group. There cannot be an identity element, as follows. Suppose c were an identity, and let $a = -1 \in \mathbb{R} \setminus \{0\}$. Then $a * c = |ac| = |-c| \geq 0$ cannot possibly equal $a = -1$.

(f): $\mathbb{R}^2$ with $(x, y) * (z * w) = (x + z, y - w)$: NO this is not a group. Associativity fails [because of the second coordinate]. For example,

$$\Big((0,1) * (0,2)\Big) * (0,3) = (0,-1) * (0,3) = (0,-4) \neq (0,2) = (0,1) * (0,-1) = (0,1) * \Big((0,2) * (0,3)\Big).$$

[But FYI, it also fails the identity axiom, again because of the second coordinate.]

(g): $\{(x, y) \in \mathbb{R}^2 : y \neq 0\}$, with $(x, y) * (z, w) = (x + z, yw)$: YES this is a group. It's a binary operation (note especially $yw \neq 0$ since $y, w \neq 0$), and it's associative because both addition and multiplication of real numbers is associative.
The identity is $(0, 1)$, which *is* in the set, and $(0, 1) * (x, y) = (x, y) = (x, y) * (0, 1)$.
The inverse of (x, y) is $(-x, 1/y)$, because $(x, y) * (-x, 1/y) = (0, 1) = (-x, 1/y) * (x, y)$.

---

6. Saracino, Section 2, Problem 2.1(i). Perhaps surprisingly, this one **is** a group. Give a formal proof of this fact.

Proof. We have $G = \mathbb{Z}$ with $a * b = a + b - 1$. This is a binary operation because for any $a, b \in \mathbb{Z}$, we have $a + b - 1 \in \mathbb{Z}$.

Associative: Given any $a, b, c \in G$, we have

$$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + (b + c - 1) - 1 = a * (b + c - 1) = a * (b * c).$$

Identity: We claim $e = 1 \in G$ is the identity element. To prove this, given any $a \in G$, we have

$$a * e = a * 1 = a + 1 - 1 = a$$

and

$$e * a = 1 * a = 1 + a - 1 = a.$$

Inverses: Given any $a \in G$, let $b = 2 - a \in G$. We claim b is an inverse of a. To verify this, we check:

$$a * b = a * (2 - a) = a + 2 - a - 1 = 1 = e$$

and

$$b * a = (2 - a) * a = 2 - a + a - 1 = 1 = e.$$

We have verified all the axioms, so G is a group. QED

Note 1: About inverses, remember to show that $a * b = e$, whatever the identity e was; don't just try to get $a * b = 0$, because e might be something other than 0.
Also, how did I think of choosing $b = 2 - a$? By scratchwork that I didn't show you, but that I will show you now. I knew I was trying to solve $a * b = e$ for the unknown b. Since $e = 1$ (from the identity step), that means we need to solve $a + b - 1 = 1$. *That* equation uses only familiar operations (and not this wacky operation $*$), and so I can use high school algebra to solve for b, yielding $b = 2 - a$.

Note 2: In proving the identity axiom, I said not just $e = 1$ but $e = 1 \in G$, and similarly in the inverse axiom, I said not just $b = 2 - a$ but $b = 2 - a \in G$. The appearance of $\in G$ here is not just a minor point; it is an important part of the axiom that the identity and inverse are **also in the group**. In this case it is obvious from the formula — 1 is an integer, and if a is an integer, then so is $2 - a$ — but in other problems it might not be so obvious that the expression you write down for the identity or inverse is in the set G; so in some cases it might take a bit more work to justify that statement. But whether obvious or not, that statement (about $\in G$) **needs** to be said explicitly.