Binary operations

CJ Quines

June 19, 2025

Warmup (fake)

1. Let $f\colon \mathbb{R}^2 \to \mathbb{R}$ be a function. Suppose there exists $\ell, r \in \mathbb{R}$ such that for all $x \in \mathbb{R}$, $f(\ell, x) = f(x, r) = x$. Prove that $\ell = r$.
2. Let $f\colon \mathbb{R}^2 \to \mathbb{R}$ be a function. Suppose that for all $x, y \in \mathbb{R}$ there exists a unique $z \in \mathbb{R}$ such that $f(x, z) = y$. Prove there exists $g\colon \mathbb{R}^2 \to \mathbb{R}$ such that for all $x, y \in \mathbb{R}$,
$$f(x, g(x, y)) = g(x, f(x, y)) = y.$$
3. Let $f, g\colon \mathbb{R}^2 \to \mathbb{R}$ be functions. Suppose there exists $i, j \in \mathbb{R}$ such that
$$\begin{gathered} f(i, x) = f(x, i) = g(j, x) = g(x, j) = x, \\ f(g(x, y), g(z, w)) = g(f(x, z), f(y, w)), \end{gathered}$$
for all $x, y, z, w \in \mathbb{R}$. Prove that f and g are the same function.

Words

As the title suggests, these warmups are about binary operations.[1] Here's a bunch of words about binary operations; italic ones are rare enough that I'd define them when I talk or do writeups.

- For a binary operation $\star$ over S, if for all $x, y, z \in S$:
  - ℓ is its **left identity** if $\ell \star x = x$.
  - It's *unital* if it has a left and right identity.
  - It's **commutative** if $x \star y = y \star x$.
  - It's **associative** if $(x \star y) \star z = x \star (y \star z)$.
  - It's *left cancellative* if $x \star y = x \star z$ implies $y = z$.
  - It has *left quotients* if there exists a unique d such that $x \star d = y$.
  - It **left distributes** over $\circ$ if $x \star (y \circ z) = (x \star y) \circ (x \star z)$.
  - It's *idempotent* if $x \star x = x$.
- We also have words for a set with a binary operation satisfying certain properties:
  - A *magma* is a set with a binary operation.[2]
  - A *semigroup* is an associative magma.
  - A **monoid** is a unital semigroup.
  - A **group** is a monoid with (left and right) quotients.

  This is in addition to phrases like "unital magma" or "commutative monoid" which hopefully have obvious definitions, and words that I'll define as-needed which appear much less often.

---

[1] I had to start with FEs to make it look like an olympiad handout.

[2] Old texts will call this a *groupoid*. These days that means something different.

Notes

- When we don't say what a variable x ranges over, we assume it's "for all $x \in S$", for a set S which should be clear from context.
- Note that "closure" ($x \star y \in S$) is part of the definition of $\star$ being a binary operation (that is, a function $\star\colon S \times S \to S$).
- Sometimes we omit the operation when we only have one binary operation. For example, we can write $(a \star b) \star (c \star (d \star e))$ as $(ab)(c(de))$. Parentheses are needed when it's not associative.
- I only chose problems that (I think) could appear in an olympiad. Each one has a solution that's self-contained, and mostly involves substituting variables and rewriting equations, rather than using theory.[3]

Warmup (real)

1. Prove that if a binary operation has a left identity ℓ and a right identity r, then $\ell = r$.
2. Suppose that $\star$ is a binary operation with left quotients. Prove there exists a binary operation $\setminus$ such that $x \star (x \setminus y) = x \setminus (x \star y) = y$.
3. (Eckmann–Hilton argument) A magma has two unital operations $\star$ and $\circ$, which satisfy $(x \star y) \circ (z \star w) = (x \circ z) \star (y \circ w)$. Prove that $\star = \circ$.

Quotients

Recall that $\star$ has **left quotients** if, for all $x, y \in S$, there's a unique $d \in S$ such that $x \star d = y$.

1. Recall that $\star$ is left cancellative if $x \star y = x \star z$ implies $y = z$. Find a "good" example of a left cancellative operation without a left quotient.
2. Which of these operations have left quotients? (a) Multiplication on $\mathbb{Q}$. (b) Subtraction on $\mathbb{Z}$. (c) Over $\mathbb{Z}$, the operation $a \star b = \left\lfloor \frac{a}{b} \right\rfloor$. (d) Over $\mathbb{R}^2$, reflecting a point over another point.
3. By warmup item 2, if $\star$ has left quotients, there's some $\setminus$ such that $x \star (x \setminus y) = x \setminus (x \star y) = y$. We call $\setminus$ itself the left quotient of $\star$; you can read it as "under".

   Prove that these definitions are equivalent. In other words, if two binary operations $\star$ and $\setminus$ satisfy $x \star (x \setminus y) = x \setminus (x \star y) = y$, then there's a unique d such that $x \star d = y$.
4. Thus, left quotients are a way to define right inverses for a binary operation, even if it doesn't have a (left and right) identity. Which of the operations from item 2 have identities?
5. Given *any* binary operation $\star$ over S, and some $x \in S$, we define **left multiplication by** x as the function $L_x(y) := x \star y$. This is also called *left translation*, and sometimes written $x \star -$.

   Prove that if $\star$ has left quotients, then L_x is injective and surjective, and thus, a bijection.
6. There's another way to prove L_x is a bijection: by finding an inverse function. Prove there exists a function L_x^{-1} such that $L_x L_x^{-1}$ and $L_x^{-1} L_x$ are both the identity.

[3] If I had to pin down the field of study here, I'd say it's universal algebra. It's not quite abstract algebra. These days that refers to studying groups, rings, or fields, but we're looking at weaker structures.

Quasigroups

A **quasigroup** is a magma Q whose operation $\star$ has a left quotient $\backslash$ and a right quotient $/$:

$$x \star (x \backslash y) = x \backslash (x \star y) = y,$$
$$(x \,/\, y) \star y = (x \star y) \,/\, y = x.$$

1. Prove that $x \,/\, (y \backslash x) = (x \,/\, y) \backslash x$.
2. (↗) A **loop** is a quasigroup whose operation $\star$ has a left and right identity. Recall that $\star$ is idempotent if $x \star x = x$. Suppose that Q is an idempotent loop. Prove that $|Q| = 1$.
3. Suppose that $\star$ is associative. Prove that if $x \star b = a \star y$, then $x \backslash a = b \,/\, y$.
4. (↗) Suppose that $\star$ is associative and Q is non-empty. Prove that Q is a group under $\star$.

Semigroups

Recall that a **semigroup** S is an associative magma.

1. (↗) How many different semigroups are there with two elements? (Formally, I have to say *non-isomorphic* semigroups. Informally, *isomorphic* means "same up to relabelling.")
2. (↗) Suppose $0 < |S| < \infty$. Prove there exists some x such that $xx = x$.
3. (↗) Find all pairs $(I, Q) \in \{\text{left}, \text{right}\}^2$ that make this statement true: A semigroup with I identities and Q quotients is a group.
4. (↗) Recall that $\star$ is left cancellative if $x \star y = x \star z$ implies $y = z$. Suppose that S is (left and right) cancellative, and that $|S|$ is finite. Prove that S is a group. What if $|S|$ is infinite?
5. (↗, ↗) We say y is a **pseudoinverse** of x if $xyx = x$. We say S is **regular** if all elements have a pseudoinverse. Suppose S is regular.

   Prove the following are equivalent: (a) there's a unique x such that $xx = x$; (b) S is (left and right) cancellative; (c) all elements have a *unique* pseudoinverse; (d) S is a group.

Bands

Recall that $\star$ is idempotent if $x \star x = x$. A **band** is an idempotent semigroup.

1. (↗) Suppose $xy = y$ and $yx = x$. Prove that $zxzy = zy$ and $zyzx = zx$.
2. (↗) A **semilattice** is a commutative band. Given a semilattice, define a relation $\leq$ by saying $x \leq y$ iff $x = x \star y$. Prove that $\leq$ is a partial order.

   That is: show that $\leq$ is reflexive ($x \leq x$), antisymmetric ($x \leq y$ and $y \leq x$ imply $x = y$), and transitive ($x \leq y$ and $y \leq z$ imply $x \leq z$). Why does $\star$ need to be commutative?
3. (↗) A **rectangular band** is a semigroup satisfying $xyx = x$. Prove that $xyz = xz$. Prove that rectangular bands are bands.
4. (↗) Let S be a semigroup. Prove the following are equivalent: (a) $xy = yx$ implies $x = y$; (b) S is a rectangular band.

Shelves

A **left shelf** is a magma whose operation $\triangleright$ left distributes over itself: $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z)$. (Some texts will use $\triangleleft$ for this, so be careful.)

1. (1.6) Prove that a unital left shelf is associative. In other words: if there exists 1 such that $1 \triangleright x = x \triangleright 1 = x$, then $\triangleright$ is associative.

2. A **rack** is a set R with two operations $\triangleright$ and $\triangleleft$, such that R is a left shelf over $\triangleright$ and a right shelf over $\triangleleft$ satisfying $x \triangleright (y \triangleleft x) = (x \triangleright y) \triangleleft x = y$. Prove that $x \triangleright (y \triangleleft z) = (x \triangleright y) \triangleleft (x \triangleright z)$.

3. (2.1.3) We say $\star$ is **medial** if $(x \star y) \star (z \star w) = (x \star z) \star (y \star w)$. Let R be a rack, and suppose $\triangleright$ is medial. Show that $y \triangleright ((z \triangleright w) \triangleleft x) = z \triangleright ((y \triangleright w) \triangleleft x$.

4. Recall that $\star$ is idempotent if $x \star x = x$. Let R be a rack, and suppose $\triangleright$ is idempotent. Prove that $\triangleleft$ is idempotent. A **quandle** is an idempotent rack, and they represent the algebraic structure of the Reidemeister moves from knot theory!

5. We say $\star$ is **left involutive** if $x \star (x \star y) = y$. Prove that an idempotent, left involutive, left shelf is a quandle. An involutive quandle is sometimes called a **kei**. Point reflection over $\mathbb{R}^2$ is a kei, where you set $x \triangleright y$ as the reflection of y over x.

6. (Laver tables) This is tricky and long, but completely elementary.

   a) Prove there exists a unique magma S_N over $\{1, 2, \ldots, N\}$, whose binary operation $\triangleright$ satisfies $x \triangleright 1 = (x + 1) \bmod N$ and $x \triangleright (y \triangleright 1) = (x \triangleright y) \triangleright (x \triangleright 1)$.

   b) Prove that S_N is a left shelf if and only if $x \triangleright N = N$ for all x.

   c) Suppose S_{2^n} is a left shelf. Let the operations of S_{2^n} and $S_{2^{n+1}}$ be $\triangleright$ and $\triangleright'$. Prove that $(x \triangleright' y) \bmod 2^n = (x \bmod 2^n) \triangleright (y \bmod 2^n)$.

   d) More specifically, prove that

   $$x \triangleright' y = \begin{cases} (x \bmod 2^n) \triangleright (y \bmod 2^n) + 2^n & \text{if } x \in (2^n, 2^{n+1}] \\ (y \bmod 2^n) + 2^n & \text{if } x = 2^n \\ (x \bmod 2^n) \triangleright (y \bmod 2^n) - (2^n \text{ or } 2^{n+1}) & \text{otherwise.} \end{cases}$$

   Conclude by induction that S_{2^n} is a left shelf.

Single-law magmas

1. (Putnam 2001/A1) An operation satisfies $(xy)x = y$. Prove that $x(yx) = y$. (It's self-dual!)

2. (Putnam 1978/A4–) An operation satisfies $(wx)(yz) = wz$. Prove that $(xz)y = xy$.

3. () An operation satisfies $(xy)y = y(yx) = x$. Prove that it's commutative.

4. () An operation is **central** if $(xy)(yz) = y$. Let S be a central magma.

   a) Define $L_x(y) := xy$ and $R_x(y) := yx$. Prove that $L_x R_y L_x = L_x$ and $R_x L_y R_x = R_x$.

   b) Suppose $|S|$ is finite. Prove that $|L_x(S)| = |R_y(S)|$. Let this value be n.

   c) Let $R_x^{-1}(z) := \{y \in S \mid xy = z\}$. Prove that $|R_x^{-1}(z)| = n$. Conclude that $|S| = n^2$.

5. (↗) An operation satisfies $(ab)(b(ca)) = b$. Prove that $((ac)b)(ba) = b$. (Another self-dual!)
6. (↗) An operation over S satisfies $(a(bc))a = bc$. Prove that if $|S|$ is finite, then $a((bc)a) = bc$. Find a counterexample when $|S|$ is infinite.

See also the Equational Theories Project. ↗

Actual olympiad problems

1. (Russia 1998/10/6 ↗) Find all operations $\star$ over $\mathbb{R}$ such that $(x \star y) \star z = x + y + z$.
2. (Estonia TST 2011/3 ↗) Is there an associative operation over $\mathbb{Z}$ with $xxy = yxx = y$?
3. (Belarus 2023/11/1 ↗) Let A, B, C be non-empty pairwise disjoint sets. Does there exist an associative operation over $A \cup B \cup C$ such that if $a \in A$, $b \in B$, and $c \in C$, then $ab \in C$, $bc \in A$, and $ca \in B$?
4. (USA TSTST 2019/1 ↗) Find all operations $\star$ over $\mathbb{R}_{>0}$ such that $x \star (y \star z) = (x \star y) \cdot c$ (where $\cdot$ is multiplication), and if $x \geq 1$, then $x \star x \geq 1$.
5. (Utah 2023/6 ↗) Find all associative operations $\star$ over $\mathbb{Z}$ such that $+$ left distributes over $\star$. (This is ridiculously hard.)