MATH 113 HOMEWORK 1 SOLUTIONS

1. Special Assignment

Problem 1.1. Come to my office hours this week – either Wednesday 2-3:30 or Thursday 2-3:30 (note the special time) – and introduce yourself. This problem will definitely be graded.

2. Basic Problems

Sets and Functions.

Problem 2.1. Let A, B, and C be sets. Prove that:

(1) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.
(2) $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$.
(3) Draw Venn diagrams that explain why these statements are true.

Solution to (1): We first show that $C \setminus (A \cup B) \subseteq (C \setminus A) \cap (C \setminus B)$. Let $x \in C \setminus (A \cup B)$ be arbitrary. Then by definition, $x \in C$ and $x \notin A \cup B$. Hence $x \notin A$ and $x \notin B$. Since $x \in C$ and $x \notin A$, we have $x \in C \setminus A$. Likewise, since $x \in C$ and $x \notin B$, we have $x \in C \setminus B$. Thus $x \in (C \setminus A) \cap (C \setminus B)$. Thus $C \setminus (A \cup B) \subseteq (C \setminus A) \cap (C \setminus B)$.

Now we must show that $C \setminus (A \cup B) \supseteq (C \setminus A) \cap (C \setminus B)$. Let $x \in (C \setminus A) \cap (C \setminus B)$ be arbitrary. Then $x \in (C \setminus A)$ and $x \in (C \setminus B)$. Hence $x \in C$, $x \notin A$, and $x \notin B$. Thus $x \notin (A \cup B)$. Hence $x \in C \setminus (A \cup B)$, so $C \setminus (A \cup B) \supseteq (C \setminus A) \cap (C \setminus B)$.

Since $C \setminus (A \cup B) \subseteq (C \setminus A) \cap (C \setminus B)$ and $C \setminus (A \cup B) \supseteq (C \setminus A) \cap (C \setminus B)$, it follows that $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.

Note: The solution to (2) is essentially identical. For part (3) I'm just asking for pictures that suggest why these statements are true. Come ask at office hours this week if you're confused by the question.

Problem 2.2. Let A, B, and C be sets and let $f : A \to C$ and $g : B \to C$ be functions. Define

$$D := \{(a, b) \in A \times B \mid f(a) = g(b)\}.$$

Let $h : D \to A$ be defined by $h(a, b) = a$ and let $k : D \to B$ be defined by $k(a, b) = b$.

(1) Show that $f \circ h = g \circ k$.
(2) Compute D explicitly in the case that $A = B = C = \mathbb{Z}$, $f(n) = 2n$, and $g(n) = n^2$.

Solution to (1): To show that the functions $f \circ h$ and $g \circ k$ are equal, we take an arbitrary element in their domain and show that the two functions give the same output on this input. Both functions have domain D. So, let $x \in D$ be arbitrary. By the definition of D, we have that $x = (a, b)$ where $a \in A$, $b \in B$, and $f(a) = g(b)$. We calculate:

$$\begin{aligned}(f \circ h)(x) &= f(h(x)) \\ &= f(h(a,b)) \\ &= f(a) \\ &= g(b) \\ &= g(k(a,b)) \\ &= g(k(x)) \\ &= (g \circ k)(x).\end{aligned}$$

Since x was arbitrary, it follows that $f \circ h = g \circ k$.

Solution to (2): By definition, we have $D = \{(a, b) \in \mathbb{Z}^2 \mid 2a = b^2\}$. Let's try to give a nicer description; suppose $(a, b) \in \mathbb{Z}^2$ with $2a = b^2$. Then in particular, b^2 is even, so b must be even, i.e. $b = 2c$ for some $c \in \mathbb{Z}$. Then $2a = b^2 = 4c^2$, so $a = 2c^2$. Hence we can rewrite D as

$$D = \{(2c^2, 2c) \mid c \in \mathbb{Z}\}.$$

Problem 2.3. Do Judson, Ch. 0, Exercises 17 and 24.

Solution to Exercise 17: (a) The mapping $f : \mathbb{Q} \to \mathbb{Q}$ defined by

$$f(p/q) = \frac{p+1}{p-2}$$

is not well-defined: we have $f(1/2) = 2/(-1) = -2$, whereas $f(4/8) = 5/2 \neq f(1/2)$. Note that the definition has other problems, too: to find the value $f(2/4)$ we would have to divide by 0!

(b) The mapping $f : \mathbb{Q} \to \mathbb{Q}$ defined by

$$f(p/q) = \frac{3p}{3q}$$

is well-defined. In fact, this is just the identity function on $\mathbb{Q}$. To prove well-definition rigorously, suppose $p/q = p'/q'$. Then $pq' = p'q$. Hence $(3p)(3q') = 9pq' = 9p'q = (3p')(3q)$, so $f(p/q) = \frac{3p}{3q} = \frac{3p'}{3q'} = f(p'/q')$.

(c) The mapping $f : \mathbb{Q} \to \mathbb{Q}$ defined by

$$f(p/q) = \frac{p+q}{q^2}$$

is not well-defined: we have $f(1/2) = 3/4$, whereas $f(2/4) = 6/16 = 3/8 \neq f(1/2)$.

(d) The mapping $f : \mathbb{Q} \to \mathbb{Q}$ defined by

$$f(p/q) = \frac{3p^2}{7q^2} - \frac{p}{q}$$

is well-defined. Suppose $p/q = p'/q'$, so $pq' = p'q$. Squaring both sides and multiplying by 21, we get $(3p^2)(7q'^2) = 21p^2q'^2 = 21p'^2q^2 = (3p'^2)(7q^2)$, so $\frac{3p^2}{7q^2} = \frac{3p'^2}{7q'^2}$. Subtracting $p/q = p'/q'$ from this equation, we get that

$$f(p/q) = \frac{3p^2}{7q^2} - \frac{p}{q} = \frac{3p'^2}{7q'^2} - \frac{p'}{q'} = f(p'/q'),$$

as desired.

Solution to Exercise 24 (b), (e): (b) As in the setup, $f : X \to Y$ is a function and $A_1, A_2 \subseteq X$ are subsets. We want to show $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. Let $y \in f(A_1 \cap A_2)$ be arbitrary. By definition, there exists an $x \in A_1 \cap A_2$ such that $y = f(x)$. Then in particular, $x \in A_1$, hence $y = f(x)$ is an element of $f(A_1)$. Likewise $x \in A_2$, so $y = f(x)$ is in $f(A_2)$. Hence $y \in f(A_1) \cap f(A_2)$, which shows the desired inclusion.

Now, let $X = \{1, 2\}$, let $Y = \{1\}$, and let $f : X \to Y$ be the function defined by $f(1) = f(2) = 1$. Let $A_1 = \{1\}$ and let $A_2 = \{2\}$. Then $A_1 \cap A_2 = \emptyset$, so $f(A_1 \cap A_2) = f(\emptyset) = \emptyset$. On the other hand $f(A_1) = \{f(1)\} = \{1\} = Y$ and likewise $f(A_2) = Y$, so $f(A_1) \cap f(A_2) = Y \neq \emptyset = f(A_1 \cap A_2)$. So this shows that equality can fail.

(e) Let $B \subseteq Y$. We want to show that $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$. First we show $f^{-1}(Y \setminus B) \subseteq X \setminus f^{-1}(B)$. Let $x \in f^{-1}(Y \setminus B)$ be arbitrary. Then by definition, $f(x) \in Y \setminus B$, hence $f(x) \notin B$. Thus $x \notin f^{-1}(B)$, and hence $x \in X \setminus f^{-1}(B)$.

Now we show $f^{-1}(Y \setminus B) \supseteq X \setminus f^{-1}(B)$. Let $x \in X \setminus f^{-1}(B)$ be arbitrary. Then $x \in X$ and $x \notin f^{-1}(B)$. Hence $f(x) \notin B$, so $f(x) \in Y \setminus B$. Thus $x \in f^{-1}(Y \setminus B)$, so we have proven the other inclusion.

Note: If you're stuck on (a),(c), or (d), they are similar to (b) and (e). Come ask at office hours if you can't see how to do them!

Remark: What you should take away from this problem: the preimage $f^{-1}(B)$ is considerably nicer than the image $f(A)$.

Relations.

Problem 2.4. Show that each of the following relations is an equivalence relation. In each case, identify the equivalence classes.

(1) The relation R on $\mathbb{Z}$ given by xRy if $|x| = |y|$.
(2) The relation R on $\mathbb{Z}$ given by xRy if $2x + y$ is divisible by 3.
(3) The relation R on $\mathbb{Q} \times \mathbb{Q} \setminus \{(0,0)\}$ given by $(a,b)R(c,d)$ if $ad = bc$. Why did we need to remove $(0,0)$ for this to work?

Solution to (1): I omit the proof that R is an equivalence relation (I will prove this for (2) and (3)). Let $a \in \mathbb{Z} \setminus \{0\}$. Then aRb if and only if $|a| = |b|$ if and only if $b = \pm a$. Thus $[a] = \{a, -a\}$. If $a = 0$ this is still true, but in this case $[0] = \{0\}$ is just a one-element set, since $0 = -0$. Note that in this case we can identify $\mathbb{Z}/R$ with $\mathbb{Z}_{\geq 0}$: we have a bijection $\mathbb{Z}_{\geq 0} \to \mathbb{Z}/R$ given by $a \mapsto [a]$. (If you're not comfortable with quotients yet, this is a good statement to verify for yourself!)

Solution to (2): **Reflexivity:** Let $x \in \mathbb{Z}$ be arbitrary. Then $2x + x = 3x$ is divisible by 3, so xRx.

Symmetry: Let $x, y \in \mathbb{Z}$ be arbitrary. Suppose that xRy, i.e. $3|2x + y$. Note that certainly $3|3x + 3y$. Hence $3|((3x + 3y) - (2x + y)) = 2y + x$. Thus yRx.

Transitivity: Let $x, y, z \in \mathbb{Z}$ be arbitrary. Suppose that xRy and yRz, i.e. $3|2x + y$ and $3|2y + z$. Certainly $3|3y$. Thus also $3|((2x + y) + (2y + z) - 3y) = 2x + y$. Hence xRz.

Now, let $x \in \mathbb{Z}$ be arbitrary. By definition, $[x] = \{y \in \mathbb{Z} \mid 3|2x + y\}$. We can give a better description, though.

Suppose $3|x$. Then $3|2x$, so $3|2x+y$ if and only if $3|((2x+y)-2x) = y$. Hence in this case $[x] = 3\mathbb{Z}$.

Suppose $x \equiv 1 (\text{mod } 3)$, i.e. suppose $x = 3n + 1$ for some $n \in \mathbb{Z}$. Then $2x = 6n + 2$, so $3|2x + y$ if and only if $3|6n + y + 2$ if and only if $3|y + 2$. Thus $y \in [x]$ if and only if $y \equiv -2 \equiv 1 (\text{mod } 3)$. Hence $[x] = \{y \in \mathbb{Z} \mid y \equiv 1 (\text{mod } 3)\} = 1 + 3\mathbb{Z}$ (we haven't introduced this latter terminology, so don't worry if you don't recognize it.)

Suppose $x \equiv 2 (\text{mod } 3)$. The same reasoning shows that $[x] = \{y \in \mathbb{Z} \mid y \equiv 2 (\text{mod } 3)\} = 2 + 3\mathbb{Z}$.

Hence we see that R is really just "equivalence mod 3 in disguise."

Solution to (3): **Reflexivity:** Let $(a,b) \in \mathbb{Q} \times \mathbb{Q} \setminus \{(0,0)\}$ be arbitrary. Then $ab = ba$, so $(a,b)R(a,b)$.

Symmetry: Let $(a,b), (c,d) \in \mathbb{Q} \times \mathbb{Q} \setminus \{(0,0)\}$ be arbitrary. Suppose that $(a,b)R(c,d)$. Then $ad = bc$, so also $cb = da$. Hence $(c,d)R(a,b)$.

Transitivity: Let $(a,b), (c,d), (e,f) \in \mathbb{Q} \times \mathbb{Q} \setminus \{(0,0)\}$ be arbitrary. Suppose that $(a,b)R(c,d)$ and $(c,d)R(e,f)$. Then

$ad = bc$ and $cf = de$. Multiplying the first equation by f yields $adf = bcf$, and multiplying the second equation by b yields $bcf = bde$. Hence we have $adf = bde$.
Now, we know by assumption that either c or d is nonzero. Suppose that d is nonzero. Then dividing by d yields $af = be$, hence $(a, b)R(e, f)$. On the other hand, suppose that $d = 0$. Then $c \neq 0$. From the equation $0 = a\cdot 0 = ad = bc$, dividing by c yields $b = 0$. Likewise, from the equation $cf = de = 0 \cdot e = 0$, dividing by c yields $f = 0$. Hence we have $af = a \cdot 0 = 0 = 0 \cdot e = be$, hence $(a, b)R(e, f)$, as desired.

If we did not remove $(0, 0)$, then we would have $(a, b)R(0, 0)$ for all $(a, b) \in (\mathbb{Q} \times \mathbb{Q})$, since $a \cdot 0 = b \cdot 0$. This would cause transitivity to fail.

To describe the equivalence classes, suppose first that we have $(a, b) \in \mathbb{Q}\times\mathbb{Q}\setminus\{(0, 0)\}$ with $a \neq 0$ and $b \neq 0$. Then $(a, b)R(c, d)$ if and only if $ad = bc$. I claim that both c and d are nonzero. Indeed, if $c = 0$, we have $ad = 0$, but $a \neq 0$ would imply $d = 0$, so $(c, d) = (0, 0)$, which is not a member of our set. The same argument shows that $d \neq 0$. So, we can re-express $ad = bc$ as $a/b = c/d$, or equivalently as $c = d \cdot a/b$. Hence

$$[(a, b)] = \{(d \cdot a/b, d) \mid d \in \mathbb{Q} \setminus \{0\}\}.$$

On the other hand, suppose $a = 0$. Then $b \neq 0$, and $(a, b)R(c, d)$ if and only if $0 = ad = bc$. Since $b \neq 0$, this holds if and only if $c = 0$. Hence

$$[(0, b)] = \{(0, d) \mid d \in \mathbb{Q} \setminus \{0\}\}.$$

Likewise

$$[(a, 0)] = \{(c, 0) \mid c \in \mathbb{Q} \setminus \{0\}\}.$$

Induction.

Problem 2.5. Do Judson, Ch. 1, Exercises 1 and 3.

Solution to Exercise 1: Induction Beginning: we have $\frac{1\cdot(1+1)(2\cdot1+1)}{6} = \frac{6}{6} = 1 = 1^2$, as desired.
Induction Step: Assume that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6}$$

for some $n \geq 1$. We want to show the same holds true for $n + 1$. We have

$$1^2 + 2^2 + \cdots + n^2 + (n + 1)^2 = \frac{n(n + 1)(2n + 1)}{6} + (n + 1)^2$$

by our hypothesis. Simplifying the right-hand side of this equation, we get:

$$\begin{aligned}\frac{n(n+1)(2n+1)+6(n+1)(n+1)}{6} &= \frac{(n(2n+1)+6(n+1))(n+1)}{6}\\ &= \frac{(n+1)(2n^2+7n+6)}{6}\\ &= \frac{(n+1)(n+2)(2n+3)}{6}\\ &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}\end{aligned}$$

as desired.

Solution to Exercise 3: Let's do this one more carefully, just for practice. Let $S(n)$ be the statement "$n! > 2^n$. We want to show that $S(n)$ is true for $n \geq 4$.

Induction Beginning: We have to show $S(4)$, i.e. we have to show that $4! > 2^4$. We have $4! = 24 > 16 = 2^4$, so $S(4)$ is true.

Induction Step: Suppose that $S(n)$ is true for some given $n \geq 4$. We want to show that $S(n+1)$ is true. The assumption $S(n)$ says that $n! > 2^n$. Then we have

$$(n+1)! = (n+1)(n!) > (n+1)2^n > 2 \cdot 2^n = 2^{n+1},$$

where the second inequality follows from the fact that $n \geq 4$, so certainly $n+1 > 2$. Thus $S(n+1)$ holds. By induction, $S(n)$ is true for all $n \geq 4$.

Divisibility and Factorization.

Problem 2.6. Do Judson, Ch. 1, Exercises 27 and 31.

Solution to Exercise 27: Suppose that $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$, and suppose that $a|bc$. We want to show that $a|c$. By our assumptions and the GCD theorem, we have that there exist integers $n, m, p \in \mathbb{Z}$ such that:

(1) $an + bm = 1$

(2) $pa = bc$.

Multiplying the first equation by c and rearranging gives $c = acn + bcm$. Multiplying the second equation by m gives $bcm = pam$. Hence we have

$$c = acn + bcm = acn + pam = a(cn + pm).$$

Thus $a|c$.

Solution to Exercise 31: As stated, the exercise is false: $p = q = 0$ solve this equation. We want to show that there are no *nonzero* integers p and q such that $p^2 = 2q^2$. We prove this by contradiction. Suppose that $p, q \in \mathbb{Z}$ such that $p^2 = 2q^2$. Let $p = p_1^{a_1} \cdots p_n^{a_n}$

be a prime factorization for p. Then $p^2 = p_1^{2a_1} \cdots p_n^{2a_n}$ is a prime factorization for p^2. So, in particular, the power of 2 in the prime factorization of p^2 is even. Likewise, the power of 2 in the prime factorization of q^2 is even. But then the power of 2 in the prime factorization of $2q^2$ is odd. Hence the number $p^2 = 2q^2$ must have two different prime factorizations, which contradicts the unique factorization theorem. Hence no such p and q exist.

Now, suppose that $p/q \in \mathbb{Q}$ were a rational number such that $(p/q)^2 = 2$. Then certainly $p \neq 0$ and $q \neq 0$, and cross-multiplying gives $p^2 = 2q^2$. By the above, no such number exists. Hence $\sqrt{2}$ cannot be a rational number.

Problem 2.7. Let $p_1, \ldots, p_k$ be distinct prime numbers and let $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{Z}_{>0}$ be nonnegative integers. Let $n = p_1^{a_1} \cdots p_k^{a_k}$ and let $m = p_1^{b_1} \cdots p_k^{b_k}$. Compute (with proof!) the prime factorization of $\gcd(n, m)$.

Solution: For each $i \in \{1, \ldots, k\}$, let $c_i = \min(a_i, b_i)$. Let

$$d = p_1^{c_1} \cdots p_k^{c_k}.$$

I claim that $d = \gcd(n, m)$ and hence that this is the prime factorization of $\gcd(n, m)$. To show this, we will show:

(1) $d \mid n$ and $d \mid m$, and

(2) if $c \in \mathbb{N}$ such that $c \mid n$ and $c \mid m$, then $c \mid d$.

To show (1), note that for each $i \in \{1, \ldots, k\}$, we have $c_i = \min(a_i, b_i) \leq a_i$, hence $a_i - c_i \geq 0$, so $p_i^{a_i - c_i} \in \mathbb{Z}$. We have

$$\begin{aligned} n &= p_1^{a_1} \cdots p_k^{a_k} \\ &= p_1^{c_1} p_1^{a_1 - c_1} \cdots p_k^{c_k} p_k^{a_k - c_k} \\ &= (p_1^{a_1 - c_1} \cdots p_k^{a_k - c_k}) \cdot d, \end{aligned}$$

thus $d | n$. The same argument (with b_i's in place of a_i's) shows that $d | m$.

To show (2), assume that $c | n$ and $c | m$. We will take a prime factorization of c and use this to show that $c | d$. I claim first that the only primes which can divide c are $p_1, \ldots, p_k$, and hence these are the only primes that can appear in the prime factorization of c. Indeed, let p be a prime dividing c. Then $p | c$ and $c | n$ implies that $p | n = p_1^{a_1} \cdots p_k^{a_k}$. But then $p | p_i$ for some $i \in \{1, \ldots, k\}$, and hence $p = p_i$. Thus we can write

$$c = p_1^{s_1} \cdots p_k^{s_k}$$

for some $s_1, \ldots, s_k \in \mathbb{Z}_{\geq 0}$. Now, I claim that $s_i \leq c_i$ for each i; equivalently, I claim that $s_i \leq a_i$ and $s_i \leq b_i$ for each i. Let's show $s_i \leq a_i$ for each i (the proof will follow for the b_i's by symmetry). Show this by contradiction: suppose $s_i > a_i$ for some i. WLOG we can assume $i = 1$. Then $p_1^{s_1}|c$ and $c|n$, so $p_1^{s_1}|n$. Factoring out $p_1^{a_1}$ from both sides, we have

$$p_1^{s_1-a_1}|\frac{n}{p_1^{s_1}} = p_2^{a_2}\cdots p_k^{a_k}.$$

But now, since $s_1 - a_1 > 0$, we have that $p_1|p_1^{s_1-a_1}$, and hence

$$p_1|p_2^{a_2}\cdots p_k^{a_k}.$$

Thus by the usual argument $p_1 = p_i$ for some $i \in \{2, \ldots, k\}$, which contradicts our assumption that the primes p_i are distinct. Thus $s_i \leq c_i$ for all i.

Now the same argument we used in (1) to show that $d|n$ also shows that $c|d$, completing the proof.

Problem 2.8. Prove or give a counterexample: if $a, b, c \in \mathbb{N}$ such that $\gcd(a, b) = 1$, $a|c$, and $b|c$, then $ab|c$.

Solution: The statement is true. Assume that $\gcd(a, b) = 1$, $a|c$, and $b|c$. Then there exist integers $n, m, p, q \in \mathbb{Z}$ such that:

(1) $na + mb = 1$,
(2) $pa = c$, and
(3) $qb = c$.

Then we have

$$c = cna + cmb = qbna + pamb = ab(qn + pm),$$

hence $ab|c$.

3. Creative Problems

Note: there are many solutions for each part; my solutions are just some examples. I hope you dreamed up far crazier things!

Sets and Functions.

Problem 3.1. (Binary Operations) Let A be a set. A *binary operation* on A is a function $f : A \times A \to A$.

1. We say the binary operation f is *commutative* if $f(a, b) = f(b, a)$ for all $a, b \in A$. Give three examples of commutative binary operations and three examples of non-commutative binary operations.
2. We say f is *associative* if $f(a, f(b, c)) = f(f(a, b), c)$ for all $a, b, c \in A$. Give an example of an associative binary operation which is not commutative. Give an example of a commutative binary operation which is not associative.
3. We say f has *left cancellation* if for all $a, b, c \in A$, we have $f(a, b) = f(a, c)$ implies $b = c$. Give an example of a binary operation which does not have left cancellation. Which of your examples above have left cancellation?

(4) Define what it should mean for f to have *right cancellation.* Give an example of a binary operation which has left cancellation but not right cancellation, or else show that left cancellation implies right cancellation.

(5) Dream up your own property P of binary operations. Find as many examples as you can of how your property P relates to the other properties above. (For example, if a binary operation has property P and is commutative, does it have to be associative?) Your property P should be different from the properties chosen by the other people in your group.

Solution: (1) We know lots of examples of commutative binary operations: $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is commutative, as is $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, and so on. For a more interesting example, the operation of composition is commutative on the set of symmetries of the rectangle, as can be checked directly. For a silly example, let X be any nonempty set and let $x \in X$ be an element. Define an operation $f : X \times X \to X$ by $f(y, z) = x$ for all $y, z \in X$. Then f is certainly commutative.

A few non-commutative examples: in class, we saw that composition is non-commutative on the set of symmetries of the triangle. Similarly, let $X = \mathrm{Func}(\mathbb{Z}, \mathbb{Z})$ be the set of functions from $\mathbb{Z}$ to $\mathbb{Z}$. The operation of function composition $\circ : X \times X \to X$ is non-commutative. For example, let $f(n) = n^2$ and $g(n) = n + 1$. Then $(f \circ g)(1) = 4$ whereas $(g \circ f)(1) = 2$, so $f \circ g \neq g \circ f$, hence $\circ$ is non-commutative. Another simple example is the binary operation $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ sending (a, b) to $a - b$. This is non-commutative since $0 - 1 \neq 1 - 0$.

(2) The operation of composition is associative but not commutative on the set of symmetries of the triangle. This is also true of composition on the set of functions from $\mathbb{Z}$ to $\mathbb{Z}$.

One example of a commutative operation which is not associative: let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $f(a, b) = |a + b|$. Then $f(a, b) = |a + b| = |b + a| = f(b, a)$, so f is commutative. But f is not associative: $f(f(1, -1), -1) = f(0, -1) = 1$, whereas $f(1, f(-1, -1)) = f(1, 2) = 3$.

(3) We discussed one example of a binary operation without left cancellation in class: the operation of $\cdot$ on $\mathbb{Z}/12\mathbb{Z}$ does not have left cancellation. For example, $[2] \cdot [6] = [12] = [0] = [2] \cdot [0]$, but $[6] \neq [0]$. There are several other examples above; I'll leave it to you to decide which ones do and do not have left cancellation.

(4) The simplest example of an operation with left cancellation but not right cancellation: let X be any set, and let $f : X \times X \to X$ be the operation defined by $f(x, y) = x$. Then clearly f has left cancellation, but if X has at least two elements, f does not have right cancellation.

Relations.

Problem 3.2. More examples of relations.

1. Let X be a set and let R be the relation on X given by xRy if $x \neq y$. Show that R is symmetric. Show that if $X \neq \emptyset$, then R is not reflexive. Show that if $|X| \geq 2$, then R is not transitive. (Recall $|X| \geq 2$ means X has at least two different elements.)
2. Give an example of a relation on $\mathbb{Z}$ which is reflexive and symmetric, but not transitive.
3. Give an example of a relation on $\mathbb{Z}$ which is symmetric and transitive, but not reflexive.
4. Give an example of a relation on $\mathbb{Z}$ which is reflexive and transitive, but not symmetric.

Solution: (2) Let xRy iff $|x - y| \leq 1$.

(3) Let xRy iff $x \neq 0$ and $y \neq 0$. This is not reflexive since it is not true that $0R0$.

(4) Two nice examples: (a) let xRy iff $x|y$, (b) let xRy iff $x \leq y$.