# Homework 4

*Due: Wednesday, February 28, 2024*

All homeworks are due at 11:59 PM on Gradescope.

**Please do not include any identifying information about yourself in the handin, including your Banner ID.**

Be sure to fully explain your reasoning and show all work for full credit.

## Problem 1

For each of the following relations, determine whether it is *reflexive*, whether it is *symmetric*, and whether it is *transitive*. Be sure to justify your answers. (If a relation has all these properties, then it is an *equivalence relation*.)

Reminder: for $x, y \in \mathbb{N}$, we say that $x$ *divides* $y$, written $x|y$, if there exists $c \in \mathbb{N}$ such that $c \cdot x = y$.

a. Let $R$ be the relation on $\mathbb{N}$ defined by the set of ordered pairs:

$$\{(a,b) \mid \exists d : \mathbb{N}, d > 1 \wedge \neg \mathsf{Prime}(d) \wedge d|a \wedge d|b\}.$$

b. Let $F$ be the set of formulas of propositional logic: for example, $p \wedge q \in F$, $p \to (p \to r) \in F$, ...

Let $R(\varphi, \psi)$ be the relation on $F$ that holds when $\varphi \to \psi$ is provable.

c. Let $L$ be the set of straight lines in a two-dimensional plane.

Let $R$ be the relation on $L$ defined by the set of ordered pairs:

$$\{(\ell, m) \mid \ell \text{ and } m \text{ are parallel}\}.$$

(Two lines are parallel if and only if they have the same slope in the Cartesian plane.)

d. Let $S = \{a, b, c\}$. Let $R$ be the relation on $S$ with the graph:

$$\{(a,a),(b,b),(c,c),(a,b),(b,c),(a,c),(b,a),(c,b)\}.$$

e. At least one of the above relations is an equivalence relation. Choose one, and describe the *equivalence classes* of that relation.

**Solution:**

a. Not reflexive. For instance, $(3,3) \notin R$ because 3 is prime, so its only divisors are 1 and 3. Thus, there is no composite natural number $d > 1$ that divides 3.

   Symmetric. Suppose $(a,b) \in R$. Then there is some $d \in \mathbb{N}$ with $d > 1$ so that $d \mid a$ and $d \mid b$. Equivalently, we have $d \mid b$ and $d \mid a$, so that $(b,a) \in R$.

   Not transitive. Observe that $(16,36) \in R$ because 4 is a nonprime common divisor of 16 and 36, and $(36,81) \in R$ because 9 is a nonprime common divisor of 36 and 81, but $(16,81) \notin R$ because 16 and 81 have no common divisors other than 1.

b. Reflexive. Let $\phi$ be a formula. Then $\phi \to \phi$ is trivially provable: we assume $\phi$, and then our goal is to show $\phi$, which follows immediately by our assumption. So $R(\phi,\phi)$.

   Not symmetric. Take $\phi$ to be the formula $p \wedge q$ and $\psi$ to be the formula $p$. We can prove $\phi \to \psi$, i.e., $p \wedge q \to p$ (this is the left elimination rule for conjunction); but we cannot prove $\psi \to \phi$, i.e., $p \to p \wedge q$ (in order to prove $p \wedge q$, we would also need to know $q$).

   Transitive. Let $\phi$, $\psi$, and $\rho$ be formulas such that $\phi \to \psi$ and $\psi \to \rho$ are provable. We can prove $\phi \to \rho$ as follows. We assume $\phi$; our goal is to show $\rho$. Since we know $\phi \to \psi$, it follows by our assumption and *modus ponens* that $\psi$. Then since we also know $\psi \to \rho$, it follows by *modus ponens* again that $\rho$, which was our goal.

c. Reflexive. Any line is trivially parallel to itself.

   Symmetric. If a line $\ell_1$ is parallel to a line $\ell_2$, then $\ell_2$ is also parallel to $\ell_1$.

   Transitive. If a line $\ell_1$ is parallel to a line $\ell_2$, and $\ell_2$ is parallel to a line $\ell_3$, then all three must have the same slope, so in particular $\ell_1$ is parallel to $\ell_3$.

d. Reflexive. We see that each of $(a,a),(b,b),(c,c) \in R$ as required for reflexivity.

   Not symmetric. $(a,c) \in R$ but $(c,a) \notin R$.

   Not transitive. We have $(c,b) \in R$ and $(b,a) \in R$ but $(c,a) \notin R$.

e. The relation in part (c) is an equivalence relation. Its equivalence classes are sets of lines all of which have the same slope. For example, the set of lines with slope 1 form an equivalence class and the set of vertical lines form an equivalence class.

# Problem 2

Given sets $A$ and $B$, a function $f : A \to B$ is *injective* if

$$\forall a_1, a_2 \in A,\ f(a_1) = f(a_2) \to a_1 = a_2.$$

The function $f$ is *surjective* if

$$\forall b \in B, \exists a \in A, f(a) = b.$$

This is a formalization of the intuitive “arrow counting” definitions given in lecture.

We defined the following in recitation: given sets $A$, $B$, and $C$, and functions $g : B \to C$ and $f : A \to B$, the *composition* of $g$ and $f$, written $g \circ f : A \to C$, is defined by $(g \circ f)(x) = g(f(x))$ for $x \in A$. In other words, to apply $g \circ f$ to an argument $x$, first apply $f$ to $x$, and then apply $g$ to the result. (Beware the order of operations!) Note that you can write the $\circ$ symbol in LaTeX with `\circ`.

a. Let $A, B, C$ be sets and $g : B \to C$ and $f : A \to B$ be functions. Prove that if the composition $g \circ f$ is bijective, then $f$ is injective and $g$ is surjective. Be precise: structure your argument carefully, and think about the formal statements of injectivity and surjectivity.

b. Let $A, B, C$ be sets and $g : B \to C$ and $f : A \to B$ be functions. If $f$ is injective and $g$ is surjective, is $g \circ f$ necessarily bijective? If so, prove this. If not, provide a counterexample: that is, give an example of three sets $A, B, C$, an injection $f : A \to B$, and a surjection $g : B \to C$ such that $g \circ f$ is *not* bijective. Explain why your examples of $f$ and $g$ are injective and surjective respectively, and why $g \circ f$ is not bijective.

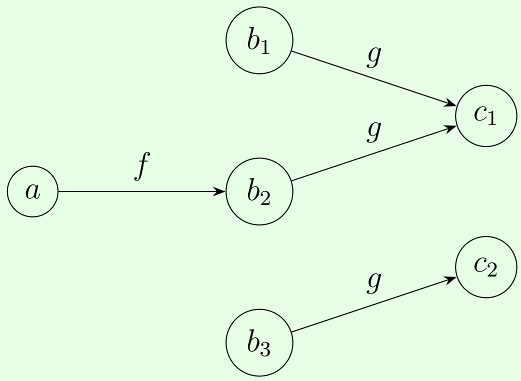
**Solution:**

a. Suppose that $g \circ f$ is bijective. This means that $g \circ f$ is both injective and surjective.

   We first show that $f$ is injective. This is a forall statement. Fix $a_1, a_2 \in A$ and suppose that $f(a_1) = f(a_2)$; we want to show that $a_1 = a_2$. Applying $g$ to both sides of our hypothesis, we know that $g(f(a_1)) = g(f(a_2))$. But since $g \circ f$ is injective, this implies that $a_1 = a_2$ as desired.

   Now we show that $g$ is surjective. This is also a forall statement: fix $c \in C$. We want to show that there exists some $b \in B$ such that $g(b) = c$. Since $g \circ f$ is surjective, there is some $a \in A$ such that $g(f(a)) = c$. So $f(a)$ is exactly the witness that we need to show this existential claim.

b. This claim is false. The following diagram is a counterexample.




Formally, we take $A = \{a\}$, $B = \{b_1, b_2, b_3\}$, and $C = \{c_1, c_2\}$. We define $f : A \to B$ by $f(a) = b_2$, and $g : B \to C$ by $g(b_1) = g(b_2) = c_1$ and $g(b_3) = c_2$.

$f$ is injective: If we suppose we have $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, it immediately follows that $a_1 = a_2$ because there is only one element $a$ in $A$, so $a_1 = a = a_2$.

$g$ is surjective: We let $c \in C$ and find some element of $B$ that $g$ maps to it. If $c = c_1$, we have $b_1 \in B$ such that $g(b_1) = c_1$. If $c = c_2$, we have $b_3$ such that $g(b_3) = c_2$. So every element of $C$ is mapped to by $g$.

However, $g \circ f$ is not bijective; in particular, it is not surjective. For observe that there is no element of $A$ that maps to $c_2 \in C$, since the only element $a \in A$ is such that $(g \circ f)(a) = c_1$.

# Problem 3

This problem is a Lean question!

This homework question can be found by navigating to `BrownCs22/Homework/Homework04.lean` in the directory browser on the left of your screen in your Codespace. The comment at the top of that file provides more detailed instructions.

You will submit your solution to this problem separately from the rest of the assignment. Once you have solved the problem, download the file to your computer (right-click on the file in the Codespace directory browser and click "Download"), and upload it to Gradescope.

# Problem 4 (Mind Bender — *Extra Credit*)

Recall from earlier that, given sets $A$ and $B$, a function $f : A \to B$ is *injective* if, for all $a, b \in A$, we have $f(a) = f(b) \to a = b$.

Here's another property of functions we can formally define: given a set $A$, we define the following property of a function $f : A \times A \to A$:

$$\text{For all } a, b, c \in A,\ f(a, f(b, c)) = f(f(a, b), c). \tag{$\star$}$$

Let $A$ be a set. Suppose there exists an injective function $f : A \times A \to A$ with property ($\star$). Determine, with proof, all possible values of $|A|$.

**Solution:**

The possible values of $|A|$ are 0 and 1. We will show this by showing that all elements of $A$ must be equal to each other. This is only possible if $A$ has 0 elements (in which case the claim vacuously holds) or has 1 element.

We now show that $\forall a, b \in A$, $a = b$. We refer to property ($\star$) as "associativity."

Let $a, b \in A$. By associativity, we have $f(a, f(b, a)) = f(f(a, b), a)$. By injectivity and the definition of tuple equality, we then have $a = f(a, b)$ and $f(b, a) = a$. Since equality is symmetric and transitive, it follows that $f(a, b) = f(b, a)$. By the injectivity of $f$ once more, we have $(a, b) = (b, a)$, so in particular $a = b$.

We have shown that any two arbitrary elements $a, b \in A$ are equal to each other; by the transitivity of equality, this means that all elements of $A$ are equal to each other. As stated at the outset, it follows that $|A| \in \{0, 1\}$.