Solutions

2.3-2.5: Functions,Relations and Orderings

Definition 1. A <u>relation</u> on a set S is a subset of $S \times S$. If R is a relation on S we say that "a is related to b" if $(a, b) \in R$, which we sometimes write as $a\ R\ b$.

Example 1. The symbols $=, <, >, \leq, \geq$ and $|$ all define relations on $\mathbb{Z}$ (or any set of numbers). See the "modular arithmetic" section (page 5) for more details on $|$ relation. Also, $=, \subset, \supset, \subseteq, \supseteq$ define relations on sets.

Example 2. Let P be the set of all people, living or dead. For any $a, b \in P$, let $a\ R\ b$ if a and b are (or were) brothers. Then R is a relation and (Cain, Abel) $\in P$.

Definition 2. A <u>function</u> is a relation in which each input has exactly one output. We think of functions as mappings from one place to another. ~~Recall~~

Example 3. $f(x) = x^2 - 3x + 2$ Recall the vertical line test.

Example 4. A propositional statement in two variables defines a function

$$w : \{T, F\} \times \{T, F\} \to \{T, F\}.$$

Example 5. Let X be a set. Then the *identity* function

$$1_X : X \to X$$

is defined by $1_X(x) = x$ for all $x \in X$.

Example 6. (Checking that a function is well-defined) Consider two relations f, g : $\mathbb{Q} \to \mathbb{Q}$ defined by

$$f(x/y) = x + y \quad \text{and} \quad g(x/y) = \frac{x+y}{y}.$$

Which of these relations is a function? (A common way of asking this questions is to check whether the function is well-defined. This is a bit misleading because if it is not well-defined, then it is not a function, but only a relation.)

<u>f:</u> Not a function. Notice that $\frac{2}{3} = \frac{4}{6} \in \mathbb{Q}$.

However, $f(\frac{2}{3}) = 2+3 = 5 \neq 10 = 4+6 = f(\frac{4}{6})$.

This is a proof by counterexample.

<u>g:</u> Yes. Let $\frac{a}{b}$ ~~and~~ $=$ $\frac{c}{d} \in \mathbb{Q}$. Then

$$g(a/b) = \frac{a+b}{\cancel{a}b} = \frac{a}{b} + \frac{b}{b} = \frac{a}{b} + 1 = \frac{c}{d} + 1 = \frac{c}{d} + \frac{d}{d} = \frac{c+d}{d} = f(c/d).$$

So g is a well-defined function.

<u>One-to-one and onto functions:</u> Let $f : X \to Y$ be a function. We say that f is <u>one-to-one</u> (or injective) if, for all $a, b \in X$, $f(a) = f(b)$ implies $a = b$. This is just a fancy way of saying that each output has a unique input (or that the map created by reversing the arrows is well-defined). We say that f is <u>onto</u> (or surjective) if, for all $y \in Y$, there exists an $x \in X$ such that $f(x) = y$. In other words, the range of f covers all of Y. If we define the subset $f(X) \subseteq Y$ by

$$f(X) := \{y \in Y | f(x) = y \text{ for some } x \in X\}$$

then $f : X \to f(X)$ is an onto function.

Example 7. Show that $f : \mathbb{Z} \to \mathbb{Z}$ (or $f : \mathbb{R} \to \mathbb{R}$) defined by $f(x) = 2x + 1$ is both one-to-one and onto. Such a function is said to be a <u>bijection</u> or a <u>one-to-one correspondence</u>.

<u>One-to-one:</u> Let $a, b \in \mathbb{Z}$ and suppose $f(a) = f(b)$. Then $2a+1 = 2b+1$
$2a = 2b$
$a = b$ ✓

<u>Onto:</u> Let $y \in \mathbb{Z}$ (or $\mathbb{R}$). Then $y = 2x+1 \Leftrightarrow x = \frac{y-1}{2}$.
Therefore $f(\frac{y-1}{2}) = y$ and f is onto. ✓

Example 8. Show that $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x \rfloor$ is onto.

Let $n \in \mathbb{Z}$. Then $f(n) = n$, so f is onto. ✓

Example 9. Let E and O be the sets of even and odd integers, respectively. Define a function

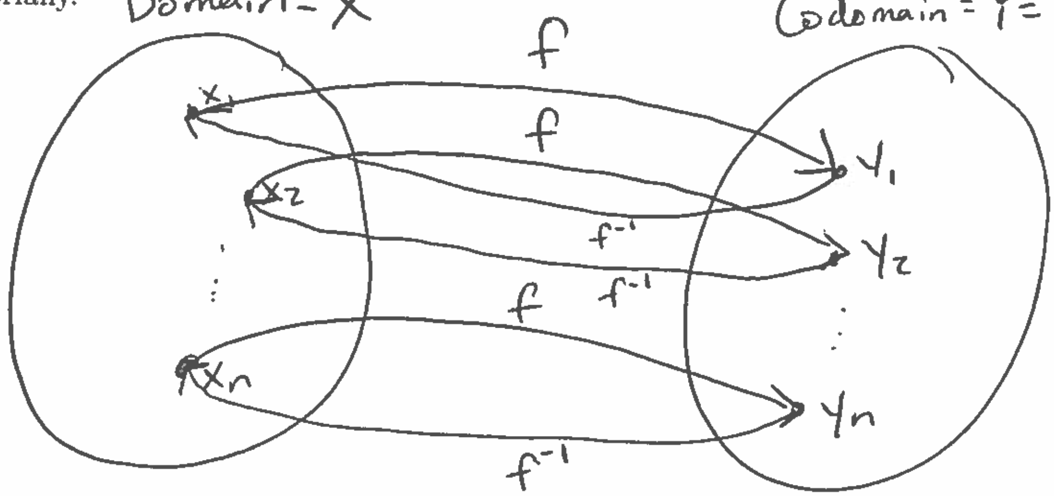
$$f : E \times O \to \mathbb{Z}$$

by $f(x, y) = x + y$. Is f one-to-one or onto? Prove or disprove.

<u>Onto?:</u> No. Notice that $f(x,y) \in O$ for all $x \in E$ and $y \in O$.
Therefore $2 \notin O \subseteq f(E, O)$. Could do proof by contradiction.

<u>1-1?:</u> No. $f(4,-3) = 1 = f(6,-5)$.

<u>New functions from old:</u> If a function $f : X \to Y$ is one-to-one, then each output has a unique input. In this case, we can define a function $f^{-1} : f(X) \to X$ by $f^{-1}(y) = x$ if $f(x) = y$. The function f^{-1} is called the <u>inverse</u> of f. Represent this new function pictorially. Domain = X Codomain = Y = Range



Inverses in $\mathbb{R}$ are simply reflections across the identity $f(x) = x$

Example 10. Suppose a cheese pizza costs \$10 plus an additional \$1 for each topping. Write a function $f : \mathbb{N} \cup \{0\} \to \mathbb{N}$ that represents the cost of a pizza with n toppings. Is this function invertible? If so, find its inverse and explain what it represents in words.

$f(n) = 10 + n$. Yes!

$f(n) - 10 = n$ so $f^{-1}(n) = n - 10$.

If my pizza costs n dollars, then I got $10-n$ toppings.

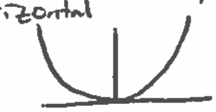
Example 11. Not all functions have inverses. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $x \overset{f}{\mapsto} x^2$. In this case we can make f invertible by restricting its domain.

$f(x) = x^2$. Not 1-1 because $f(1) = 1 = f(-1)$. So not invertible.

However, $f : [0,\infty) \to [0,\infty)$ is invertible.

In this case, $f^{-1}(x) = \sqrt{x}$. We can write $f|_{[0,\infty)}$.

~~Vertical~~ Horizontal line test

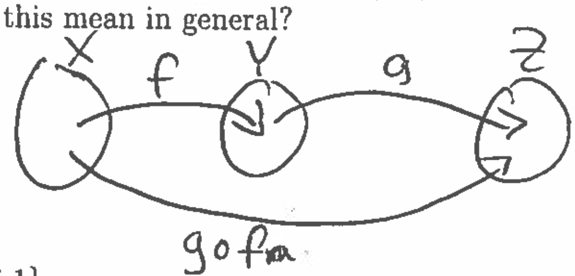


Definition 5. Given two functions $f : X \to Y$ and $g : Y \to Z$ we define the composition of f and g by $g \circ f : X \to Z$ by $g \circ f(x) = g(f(x))$ for all $x \in X$.

Example 12. Let $f, g : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = \lfloor x \rfloor$ and $g(x) = 3x$. Find $g \circ f(2.4)$ and $f \circ g(2.4)$. Are your answers different? What does this mean in general?

$g \circ f(2.4) = g(f(2.4)) = g(2) = 6$

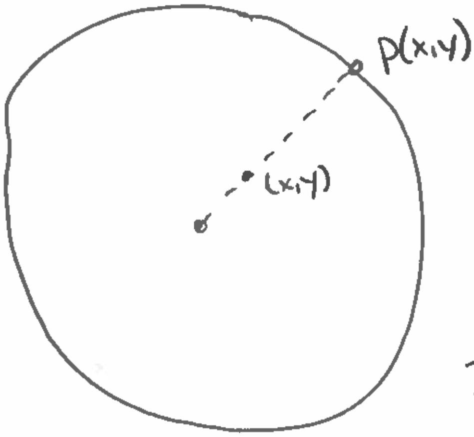
$f \circ g(2.4) = f(g(2.4)) = f(7.2) = 7$



Example 13. Let D be the unit disk in $\mathbb{R}^2$, that is,

$$D := \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 1\}.$$

In addition, let $D^* = D \backslash \{(0,0)\}$ (the punctured disk) and let $S = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$ be the unit circle. Define a relation $p : D \to S$ by projection straight out along a radius until you reach the boundary S. Is this relation a function; i.e. "is this function well-defined?" Can we make it a well-defined function? Can we come up with a formula for p?



Not well defined at $(0,0)$ since it lies on all radii. However $p|_{D^*}$ is well-defined.

Consider $H = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = \frac{1}{4}\}$.

Exercise 31 asks you to show $p|_H(x,y) = (2x, 2y)$.

That is, if $(x,y) \in H$, then $p(x,y) = (2x, 2y)$.

In general, we have

$$p|_{D^*}(x,y) = \left(\frac{x}{\sqrt{x^2+y^2}}, \frac{y}{\sqrt{x^2+y^2}}\right).$$

Equivalence Relations: A relation R on a set S is an equivalence relation if it satisfies the following three properties:

1. *Reflexivity.* For any $a \in S$, $a\ R\ a$.
2. *Symmetry.* For any $a, b \in S$, $a\ R\ b \iff b\ R\ a$.
3. *Transitivity.* For any $a, b, c \in S$, if $a\ R\ b$ and $b\ R\ c$, then $a\ R\ c$.

Example 14. The relation on $\mathbb{Z}$ (or some collection of sets or really anything) defined by $=$ is an equivalence relation.

Ex 15 together with modular arithmetic allows one to define rational #'s in more than just $\mathbb{Z}$!

Example 15. Let $S := \{\frac{x}{y} \mid x, y \in \mathbb{Z},\ y \neq 0\}$. Define a relation R on S as follows: For any elements $\frac{x}{y}, \frac{z}{w} \in S$, $\frac{x}{y}\ R\ \frac{z}{w}$ if $xw = yz$. Prove that R is an equivalence relation.

Reflexive: Let $\frac{x}{y} \in S$. Then $xy = yx$, so $\frac{x}{y}\ R\ \frac{x}{y}$.

Symmetric: Let $\frac{x}{y}, \frac{z}{w} \in S$. Then $xw = yz \iff zy = wx$ and so $\frac{x}{y}\ R\ \frac{z}{w} \iff \frac{z}{w}\ R\ \frac{x}{y}$

Transitive: Let $\frac{x}{y}, \frac{z}{w}, \frac{p}{q} \in S$ with $\frac{x}{y}\ R\ \frac{z}{w}$ and $\frac{z}{w}\ R\ \frac{p}{q}$. Then $xw = yz$ and $zq = wp$.

Therefore $xq = yzq/w = ywp/w = yp$. Thus $\frac{x}{y}\ R\ \frac{p}{q}$.

This example makes partitions easy to see.

Example 16. Let $f : X \to Y$ be a function. Define a relation on X as follows: For any $a, b \in X$, $a\ R\ b$ if $f(a) = f(b)$. Is R an equivalence relation? Prove or disprove.

Reflexive: For any $a \in X$, $f(a) = f(a)$ ✓

Symmetric: For any $a, b \in X$, $f(a) = f(b) \iff f(b) = f(a)$. ✓

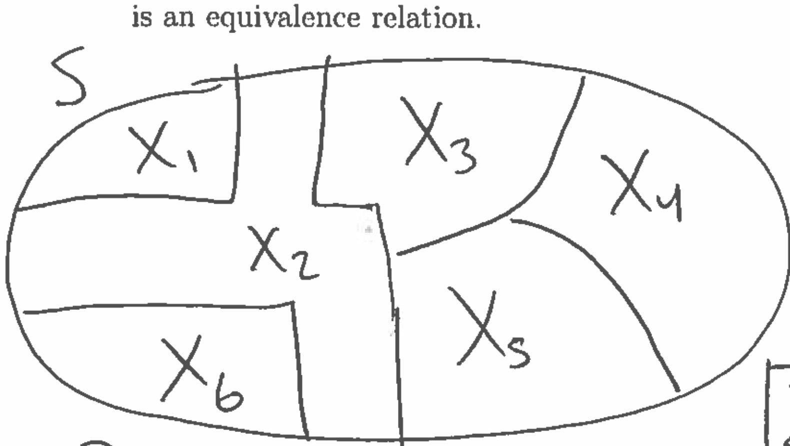
Transitive: For any $a, b, c \in X$, $f(a) = f(b)$ and $f(b) = f(c)$ implies $f(a) = f(c)$ ✓

Yes, it is an equivalence relation.

Example 17. A *partition* of a set S is a set $P \subseteq P(S)$ of nonempty subsets of S such that

1. For any $a \in S$, there is some $X \in P$ such that $a \in X$. The elements of P are called the *blocks* of the partition.
2. If $X, Y \in P$ are distinct blocks; i.e. $X \neq Y$, then $X \cap Y = \emptyset$.

Define a relation R on S by $a\ R\ b$ if a and b belong to the same block. Show that R is an equivalence relation.



$P = \{X_1, X_2, \dots, X_i\}$

Reflexive: For all $x \in X$, $x \in X_i \iff x \in X_i$.

Symmetric: For all $x, y \in X$, $x, y \in X_i \iff y, x \in X_i$.

Transitive: For all $x, y, z \in X$, if $x, y \in X_i$ and $y, z \in X_i$, then $x, z \in X_i$.

In Ex 16, these ~~partitions~~ blocks are the ~~points~~ sets of points mapping to the same element.

Theorem 1. *Let R be an equivalence relation on a set S. For any element $x \in S$, define $[x] := \{a \in S | x \; R \; a\}$ to be the set of all elements related to x. Let P be the collection of distinct subsets of S formed in this way; i.e. $P = \{[x] \in P(S) | x \in S\}$. Then P is a partition of S.*

We call the partitions defined in the above theorem the <u>equivalence classes</u> with respect to the relation R. Specifically, we will call $[x]$ to be the equivalence class of x. If $a \in [x]$ we will a as a *representative* of $[x]$.

<u>Modular Arithmetic:</u> Let $a, b \in \mathbb{Z}$. If, for some $n \in \mathbb{N}$, $n|(a-b)$, we say that "a is equivalent (or congruent) to b modulo n." The notation for this relation is

$$a \equiv b \mod n.$$

Example 18.

(a) Find the collection of all integers which are equivalent to 1 modulo 2.

(b) Find the collection of all integers which are equivalent to 2 modulo 3.

(a) $[1]_2 = \{n \in \mathbb{Z} \mid n = 2k+1$ for some $k \in \mathbb{Z}\} =$ Odds

(b) $[2]_3 = \{n \in \mathbb{Z} \mid n = 3k+2$ for some $k \in \mathbb{Z}\} = \{2, 5, 8, 11, 14, \ldots\}$

Example 19. Show that (for each $n \in \mathbb{N}$) $\equiv$ defines an equivalence relation on $\mathbb{Z}$. Fix $n \in \mathbb{N}$.

<u>Reflexive:</u> Clearly $n|(a-a) = 0$ for all $a \in \mathbb{Z}$ ✓

<u>Symmetric:</u> Let $a, b \in \mathbb{Z}$. ~~such~~ Then $n|(a-b) \iff \exists k \in \mathbb{Z}$ st $a-b = n \cdot k \iff b-a = n(-k) \iff n|(b-a)$ ✓

<u>Transitive:</u> Let $a, b, c \in \mathbb{Z}$ w/ $n|(a-b)$ and $n|(b-c)$. Then $\exists k_1, k_2 \in \mathbb{Z}$ such that ~~a-b~~ $a-b = nk_1$ and $b-c = nk_2$. Then $a-c = (a-b)+(b-c) = nk_1 + nk_2 = n(k_1+k_2)$ and so $n|(a-c)$. ✓

Proposition 2. *Let $[a]$ and $[b]$ be equivalence classes in $\mathbb{Z}/n$. Suppose that $x \in [a]$ and $y \in [b]$. Then $x \pm y \in [a \pm b]$ and $xy \in [ab]$.*

Proof. Let $x \in [a]$ and $y \in [b]$. Then $x = a + kn$ and $y = b + ln$ for some $k, l \in \mathbb{Z}$.

Then $x + y = (a+kn) + (b+ln) = (a+b) + (k+l)n$ and so $x + y \in [a+b]$.

Similarly for showing $x - y \in [a-b]$.

Also, $xy = (a+kn)(b+ln) = ab + aln + bkn + kln^2 = ab + (al + bk + kln)n$.

Thus $xy \in [ab]$.

What about division?

We can use the notion of "moding out" to define rational numbers in Example 15.

Chinese Remainder Theorem: Suppose you are an army general trying to determine how many soldiers you have at your disposal. Can modular arithmetic be used to simplify this procedure? For instance, try to answer from the 3rd-century book Sunzi Suanjing by the Chinese mathematician Sunzi:

> "There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?"

Suppose I have x soldiers, such that $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$ and $x \equiv 2 \bmod 7$.

It can be shown that $x \equiv 23 \bmod 105$. A much better approximation than before.

Partial Orderings: A relation R on a set S is a partial ordering if it satisfies the following three properties:

1. *Reflexivity.* For any $a \in S$, $a\ R\ a$.
2. *Transitivity.* For any $a, b, c \in S$, if $a\ R\ b$ and $b\ R\ c$, then $a\ R\ c$.
3. *Antisymmetry.* For any $a, b \in S$, if $a\ R\ b$ and $b\ R\ a$, then $a = b$.

Example 20. Show that $\leq$ (equivalently $\geq$) is a partial ordering on any set S of numbers.

Reflexive: $a \leq a$ ✓

Transitive: $a \leq b$ and $b \leq c$ then $a \leq c$ ✓

Antisymmetric: $a \leq b$ and $b \leq a$ then $a = b$. ✓

Example 21. Let S be any set. Show that $\subseteq$ is a partial ordering on $P(S)$.

Same as Example 20.

Reflexive: $A \subseteq A$ ✓

Transitive: $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

Antisymmetric: $A \subseteq B$ and $B \subseteq A$ then $A = B$. This is how we prove equality of sets.

Homework. (Due Oct 24, 2018) Section 2.3: 22, 27; Section 2.4: 9, 30; Section 2.5: 1

Practice Problems. Section 2.3: 3-6, 13-15, 28, 29, 30*, **33-36**; Section 2.4: 3-6, 10, 16-19, 21-23, 29, 32*, 33* **34-40**; Section 2.5: 8-10, 13-15, **18**