5.1

Relations and functions continued

5.2

Some kinds of binary relation

Many important binary relations are subsets of a product A^2. We call them *(binary) relations on* A.

Suppose R is a relation on A.
Then we write

$$aRb$$

to express that the ordered pair (a, b) is in R.

5.3

Examples

The relation $<$ on $\mathbb{R}$ contains the ordered pairs

$$(1, 2), (1, 3), (1, 3.24), (-1, 4000)$$

etc.

The relation $\leqslant$ on $\mathbb{R}$ is the same as $<$ except that it also contains

$$(0, 0), (1, 1), (1.266, 1.266)$$

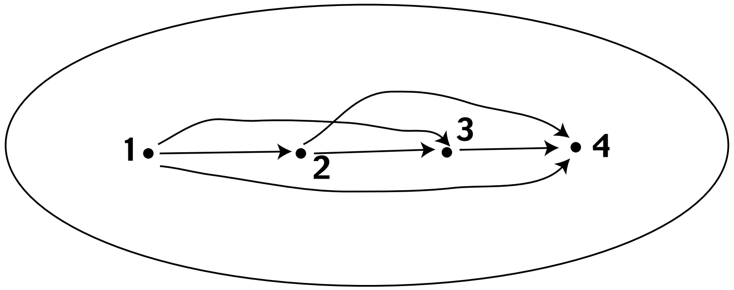
etc.

5.4

If R is a binary relation on A,
we can draw a picture of R by
writing dots for the members of A,
and an arrow from a's dot to b's dot when aRb holds.
This picture is called the *graph* of R.

5.5

Example: The relation $<$ on the set $\{1, 2, 3, 4\}$ has the graph



5.6

A relation R on A is called *reflexive* if

aRa for all $a \in A$.

It is called *irreflexive* if

there is no $a \in A$ with aRa.

So for example $<$ is irreflexive and $\leqslant$ is reflexive.

How can you tell from its graph whether a relation R is reflexive or irreflexive?

5.7

A relation R on A is called *symmetric* if

aRb implies bRa, for all $a, b \in A$.

It is called *asymmetric* if

there are no $a, b \in A$ such that aRb and bRa.

Is either of $<$ or $\leqslant$ symmetric? asymmetric?

What does the graph of a symmetric relation look like?

5.8

Example: modular arithmetic

Let n be a positive integer.
When a and b are integers, we write

$$a \equiv b \pmod{n}$$

to mean that $a - b$ is divisible by n,
i.e. there is some integer c such that $a - b = cn$.
When this equation holds, we also have

$$b - a = (-c)n$$

so $b \equiv a \pmod{n}$.

5.9

This shows that the relation R on the integers, where

aRb means $a \equiv b \pmod{n}$,

is a symmetric relation.

We call this relation *equivalence modulo* n.

Recall that when we count in binary numbers of length m, we can't distinguish between two integers that are equivalent modulo 2^m.

5.10

Suppose R is a binary relation on A.
We say that R is *transitive* if

aRb and bRc together always imply aRc.

We say that R is *intransitive* if

aRb and bRc together always imply that not aRc.

What about the graph of a transitive relation?

5.11

Example

Let n be a positive integer and let R be equivalence modulo n. Suppose aRb and bRc.
Then there are integers d, e such that

$$a - b = dn, \quad b - c = en.$$

So

$$a - c = (a - b) + (b - c) = dn + en = (d + e)n,$$

proving that aRc. *So equivalence modulo* n *is transitive.*

5.12

A relation R on $A \times A$ that is

- reflexive,
- symmetrical and
- transitive

is called an *equivalence relation* on A.
It divides A into *equivalence classes*: everything in an equivalence class has the relation R to everything in the class, and not to anything in any other equivalence class.

5.13

Example

The relation on $\{1,2,3,4,5,6,7\}$ consisting of the pairs

(1,1), (1,3), (1,4), (2,2), (2,5), (2,7), (3,1), (3,3), (3,4), (4,1), (4,3), (4,4), (5,2), (5,5), (5,7), (6,6), (7,2), (7,5), (7,7)

is an equivalence relation with three equivalence classes:

{1,3,4},
{2,5,7},
{6}.

5.14

Example

If $f : X \to Y$ is a function, then there is an equivalence relation R on X defined by

$$aRb \text{ if and only if } f(a) = f(b).$$

5.15

For example the relation R defined from the function

$f :$

X	Y
1	3
2	2
3	1
4	2

has the equivalence classes $\{1\}$, $\{2,4\}$, $\{3\}$.

5.16

Modular arithmetic again

Write $\mathbb{Z}$ for the set of integers

$$\ldots -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots$$

Let n be a positive integer and let R be the relation on $\mathbb{Z}$ defined by

$$aRb \text{ if and only if } a \equiv b \text{ (mod } n).$$

Then we saw that R is an equivalence relation.

The equivalence class of an integer i is written $[i]$.

5.17

We write $\mathbb{Z}_n$ for the set of these equivalence classes.
$\mathbb{Z}_n$ is called *the integers mod(ulo)* n.

Now

$$[-n] = [0] = [n] = [2n] = [3n] = \dots$$

and

$$[-n+1] = [1] = [n+1] = [2n+1] = [3n+1] = \dots$$

So $\mathbb{Z}_n$ consists of the n classes $[0], [1], \dots, [n-1]$.

5.18

The general rule is: in the integers mod n,
to find $[x]$, divide x by n and take the remainder.

Example

In $\mathbb{Z}_4$ we have

$$[4] = [0], [7] = [3], [14] = [2], [36] = [0], [106] = [2].$$

What are the following in $\mathbb{Z}_5$?

$$[6], [9], [144], [88], [-1], [-8]$$

5.19

We add, subtract and multiply in $\mathbb{Z}_n$ just like in $\mathbb{Z}$,
except that we always give the answer as one of
$[0], \dots, [n-1]$.

Example. In $\mathbb{Z}_6$,

$$\begin{aligned}([3]+[5])([1]-[4]) &= [8] \times [-3] \\ &= [8] \times [3] \\ &= [24] \\ &= [0].\end{aligned}$$

5.20

Example from Exam 2003:

Simplify the following expression in arithmetic modulo 12:

$$([4]-[7])([9]+[8]) - [6]([4]+[11])$$

5.21

In $\mathbb{Z}_n$ we have, for every number x,

$$[1] \times [x] \ = \ [1x] \ = \ [x].$$

So $[1]$ behaves just like 1 in ordinary multiplication.

So we can shorten $[1]$ to 1 in $\mathbb{Z}_n$.

5.22

Warning!

Dividing in $\mathbb{Z}_n$ is NOT like dividing in $\mathbb{Z}$.

$$\frac{a}{b} = c \text{ means } a = b \times c.$$

But in $\mathbb{Z}$, given a and b, we can't always find a c that solves this equation.
Also sometimes we can find more than one value of c that solves it.

5.23

For example in $\mathbb{Z}_6$ there is no x that solves

$$[2] \times [x] = [3]$$

because 2 is even and so 3 would have to be even. So

$$\frac{[3]}{[2]}$$

doesn't exist in $\mathbb{Z}_6$!

5.24

Also in $\mathbb{Z}_6$ we have

$$[2] \times [0] = [0] = [6] = [2] \times [3],$$

so

$$\frac{[0]}{[2]} = [0] \text{ and } = [3].$$

Impossible!

So we can't divide $[0]$ by $[2]$ in $\mathbb{Z}_6$.

5.25

On the other hand in $\mathbb{Z}_7$ we have

$$\begin{aligned} 1 \times 1 &= 1, \\ [2] \times [4] &= [8] = 1, \\ [3] \times [5] &= [15] = 1, \\ [6] \times [6] &= [36] = 1. \end{aligned}$$

So in $\mathbb{Z}_7$ we have

$$\frac{1}{1} = 1,\ \frac{1}{[2]} = [4],\ \frac{1}{[3]} = [5].$$

5.26

In $\mathbb{Z}_{11}$, what are

$$\frac{1}{[2]},\ \ \frac{1}{[3]},\ \ \frac{1}{[5]},\ \ \frac{1}{[8]}\ ?$$

5.27

THE MID-TERM TEST COVERS MATERIAL UP TO THIS POINT.