## Chapter 2 Binary relations

# Section 2.1 Kinds of binary relation

A binary relation R on a set A is any subset of  $A \times A$ ,

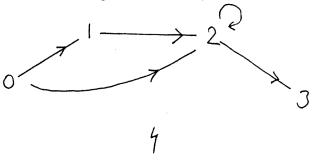
$$R \subseteq A \times A$$
,

that is, any set of ordered pairs of elements of A. For instance, if  $f: A \longrightarrow A$  is any function from A to A itself, then graph (f) is a binary relation on A.

It is remarkable to what extent mathematics is preoccupied with the analysis of binary relations; of course, the reason is that using the abstract idea of a binary relation, we can grasp many mathematical intuitions. In this section, we give an overview of the kinds of binary relation we will look at more closely in the rest of the course.

Instead of saying that R is a binary relation on A, we may write  $R \subseteq A \times A$ . We also write xRy in place of  $(x, y) \in R$ .

A general binary relation R on a set A may be visualized as a network of vertices standing for the elements of A, and arcs (or arrows) connecting in definite directions the pairs of vertices that are in the relation R. E.g., the network



represents the binary relation

$$\{(0,1), (0,2), (1,2), (2,2), (2,3)\}$$

on the set  $\{0, 1, 2, 3, 4\}$ . Observe that the data include the set  $\{0, 1, 2, 3, 4\}$ ; the same set of ordered pairs could be considered as a relation on the smaller set  $\{0, 1, 2, 3\}$  (but not on any set smaller than the last). The situation is similar to that of functions and their codomains; for us the specification of binary relation includes the specification of its underlying set, in the example the set  $\{0, 1, 2, 3, 4\}$ .

An arbitrary binary relation is also called a *directed graph*, or a *digraph*, in obvious reference to the pictorial representation.

A more robust representation of a binary relation is done through its adjacency matrix. If the distinct elements of A are  $a_1, a_2, \ldots, a_{n-1}, a_n$ , then the adjacency matrix of  $R \subseteq A \times A$  is the  $n \times n$  matrix whose (i, j)-entry  $(i^{th})$  row,  $j^{th}$  column) is 1 if  $(a_i, a_j) \in R$ , 0 otherwise. E.g., the adjacency matrix of the relation in the example is the  $5 \times 5$ -matrix

$$\begin{pmatrix}
0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

here  $a_1 = 0$ ,  $a_2 = 1$ , etc.

The display of the adjacency matrix depends on the chosen enumeration  $a_1$ ,  $a_2$ , ... of the underlying set. If in the example we take, e.g., the reverse enumeration  $a_i = 5 - i$  (i = 1, ..., 5), the matrix becomes

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0
\end{pmatrix}$$

From now on, until further notice much later, we will say "relation" instead of "binary relation", simply because we will not have anything to do with relations other than binary ones -- although, as we will eventually see, there are relations that are not binary.

When we look at more relations on the same set, their adjacency matrices are understood to be taken with the same, fixed, enumeration of the underlying set.

Of course, the adjacency matrix is practical only with finite and not too large relations. A closely related representation is via a set in the Cartesian plane provided A is  $\mathbb{R}$  or a subset of it; in this case, the relation becomes a region in the plane. E.g., the ordering relation < on  $\mathbb{R}$  is represented by the set of points under the line x = y in the Cartesian plane. The graph of a function from  $\mathbb{R}$  to  $\mathbb{R}$  is another example.

There are certain basic properties of relations. In the list that follows, we give each definition in two forms, one in ordinary words, the second in a symbolic shorthand; we will comment this shorthand shortly afterwards.

 $R \subseteq A \times A$  is reflexive if, for all a in A, aRa;  $\forall a \in A$ . aRa;

symmetric if, for all a, b in A, aRb implies bRa;  $\forall a, b \in A. \ aRb \Rightarrow bRa;$ 

transitive if, for all a, b, c in A, aRb and bRc imply aRc;  $\forall a, b, c \in A. (aRb \& bRc) \Longrightarrow aRc;$ 

irreflexive if, for all a in A, it is not the case that aRa;  $\forall a \in A$ .  $\neg (aRa)$ ;

(observe that this is not merely to say that R is not reflexive);

antisymmetric if, for all a, b in A, aRb and bRa imply that a=b;  $\forall a, b \in A$ .  $(aRb \& bRa) \Longrightarrow a=b$ ; strictly antisymmetric if, for all a, b in A, aRb implies that it is not

the case that bRa;

$$\forall a, b \in A. \ aR \not A \Rightarrow \neg (bRa) ;$$

```
R \subseteq A \times A satisfies (the law of) dichotomy, or is dichotomous if for all a, b in A, either aRb or bRa (or both): \forall a, b \in A. aRb or bRa.
```

```
R \subseteq A \times A satisfies (the law of) trichotomy, or is trichotomous, if for all a, b in A, either aRb, or a=b, or bRa:
\forall a, b \in A. \ aRb \ or \ a=b \ or \ bRa.
```

Let us comment on the abbreviated, symbolic, statements. Read:

```
" ∀a∈A "
                                                 "for all a in A";
                                 as
" ∀a, b∈A "
                                                 "for all a and b in A";
                                 as
the symbol &
                                                 "and";
                                 as
the symbol \Longrightarrow
                                 as
                                                 "implies";
the symbol \neg
                                                 "not", "it is not the case that";
                                 as
                                                 "or", "either --, or --, or both".
the symbol \widehat{O} \checkmark
                                 as
```

Reading the symbolic statements according to the key just given, will give you the definitions stated in words. Remember that "or" is *always* to be read as "either --, or --, or both". Note the use of the parentheses in the definitions of "transitive" and "antisymmetric". In both cases, the pair of parentheses and the connective & (and) make a single statement out of two statements, which then becomes the subject of the verb "implies". In the formulation in ordinary language, the use of "imply", the plural form of "implies", has the same effect as the parentheses together with "implies".

The logical symbolism used in the abbreviated statements will itself become an important object of study for us later on.

#### Exercise 1. Prove that

(a) a relation is strictly antisymmetric if and only if it is antisymmetric and irreflexive;

and

(b) a relation is dichotomous if and only if it is trichotomous and reflexive.

The eight properties listed appear in various combinations.

A preorder is a reflexive and transitive relation.

**Example 1.** Let us consider the set  $\mathbb{Z}$ , the set of all integers, and let the relation R on  $\mathbb{Z}$  be defined as *divisibility*:

aRb if and only if a divides b: there is  $c \in \mathbb{Z}$  such that  $a \cdot c = b$ .

Thus, in this example, the instances 2R4, 2R(-4), (-2)R4, (-2)R(-4) all hold (why?); also, 0R0 holds (why?); but 4R2 and 0R1 do not hold (why?).

The usual notation for "a divides b" is  $a \mid b$ ; we also read  $a \mid b$  as "b is divisible by a". Thus,

$$a \mid b \iff \exists c \in \mathbb{Z}. \ a \cdot c = b.$$

Here, we used the logical abbreviation " $\exists c \in \mathbb{Z}$ " to say "there is c in  $\mathbb{Z}$  such that ...".

Note that, in case  $a\neq 0$ ,  $a\mid b$  if and only if the quotient b/a is itself an integer. (Note the change of the order of the letters a and b from  $a\mid b$  to b/a!). On the other hand,  $0\mid b$  if and only if b=0 (why?).

The relation |, our R in this example, is a preorder: for all a, b, c in  $\mathbb{Z}$ ,

$$a \mid a$$
 (reflexivity)  
 $a \mid b$  and  $b \mid c$  imply  $a \mid c$  (transitivity)

### Exercise 2. Prove the just-stated facts.

An equivalence relation is a preorder that is symmetric. In other words, an equivalence relation a relation that is reflexive, symmetric and transitive.

This is a rather simple, but very important kind of relation; in the next section, we'll give a detailed discussion of it.

**Example 2.** The most basic kind of example for an equivalence relation is the *equality relation* on any set A, which is given by the subset  $\{(a, a) \mid a \in A\}$  of  $A \times A$ . The notation for this relation is  $\Delta_A$ ; although equality of mathematical objects is understood independently of what sets they belong to, still, for each set A, there is a distinct relation  $\Delta_A$  of equality on A. This is an instance of our understanding of the concept of relation as one that includes the underlying set in its specification.

Of course, we write a=b for "a equals b". Then, the fact that, for any set A,  $\Delta_A$  is an equivalence relation, is expressed by the familiar facts that, for any mathematical objects a, b and c whatsoever, we have

$$a = a$$
 (reflexivity)  
 $a = b$  and  $b = c$  imply  $a = c$  (transitivity)  
 $a = b$  implies  $b = a$  (symmetry)

A partial order, or more simply, an order, is a preorder is that is also antisymmetric.

**Example 3.** The most important example for an order is the *subset-relation* on  $\mathcal{P}(A)$ , the set of all subsets of A, for an arbitrary set A. That is, now the relation  $R \subseteq \mathcal{P}(A) \times \mathcal{P}(A)$  is

$$R = \{ (X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : X \subseteq Y \}$$
.

Once again, just as in the case of equality, the relation  $\subseteq$  is defined uniformly for any two arguments X and Y as long as they are sets, independently of the underlying set  $\mathcal{P}(A)$ .

However, still, we have as many distinct relations as there are sets A; for each A, the underlying set of the relation is  $\mathcal{P}(A)$ , not A.

When we want to refer to the subset-relation on  $\mathcal{P}(A)$  unambiguously, we may write  $\subseteq_{\mathcal{P}(A)}$ , although this notation is not commonly used. Also, we may simply write  $\subseteq$ , in which case the underlying set  $\mathcal{P}(A)$  should be inferred from the context.

In section 1.2, we already discussed the transitivity and antisymmetry properties of  $\subseteq$ . The reflexivity of  $\subseteq$  is just the obvious fact that every set is a subset of itself.

An *irreflexive* (or *strict*) *order* is a transitive and irreflexive relation. Thus, an irreflexive order is *not* an order, since in the definition of "order", we required reflexivity, not its opposite, irreflexivity! This is a case of using an adjective ("irreflexive") that does not specify something more narrowly than the noun following it, as it would be expected normally. The term indicates that we are talking about something that is "like an order, except for the fact that it is irreflexive". By the way, we may and sometimes do say "reflexive order" for what we called "order" before, to contrast the two notions more descriptively.

**Example** 4. The proper-subset-relation  $\subset$  on  $\mathcal{P}(A)$ , for any set A. That is,

$$\subset = \{ (X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : X \subset Y \} .$$

is, for any set A, an irreflexive order.

Note that, by Exercise 1.(a), every irreflexive order is strictly antisymmetric.

In an important sense, reflexive orders and irreflexive orders "amount to the same thing". This is explained in the following exercise, Exercise 3. Roughly speaking, what happens is that having any reflexive order, we may pass to a corresponding irreflexive order, the *irreflexive* version of the given reflexive order, without losing any information; and also vice versa, we have a reflexive version of any irreflexive order. For instance, the irreflexive version of  $\subseteq$  is  $\subseteq$ , and the reflexive version of  $\subseteq$  is  $\subseteq$ .

Exercise 3. (i) Let R be a (reflexive) order on the set A. Define the relation S on A by:

 $aSb \iff aRb \& a \neq b$ .

S is called the *irreflexive version* of R. Show that S is an irreflexive order on A.

(ii) Let S be an irreflexive order on the set A. Define the relation R on A by:

 $aRb \iff aSb \text{ or } a=b$ .

R is called the *reflexive version* of S. Show that R is a (reflexive) order on A.

(iii) For a given R as in (i), let us write  $R^{\#}$  for the irreflexive version of R: the S defined in (i). For a given S as in (ii), let us write  $S^{*}$  for the reflexive version of S: the R defined as in (ii). Prove that  $(R^{\#})^{*}=R$  and  $(S^{*})^{\#}=S$ .

**Example 5.** For any A, if R is the subset-relation  $\subseteq$  on  $\mathcal{P}(A)$ , then  $R^{\#}$  is the proper-subset-relation  $\subseteq$ . For S the proper-subset-relation  $\subseteq$ ,  $S^{*}$  is  $\subseteq$ .

A total (or linear) order is an order satisfying dichotomy. An irreflexive total order is an irreflexive order satisfying trichotomy.

**Example 6.** The ordinary "less-than-or-equal-to" relation,  $\leq$ , on  $\mathbb{R}$ , the set of all real numbers, is the primary example for a (reflexive) total order. Its irreflexive version is <, the strict "less-than" relation on  $\mathbb{R}$ , is the main example for an irreflexive total order.

**Exercise 4.** Show that if  $R \subseteq A \times A$  is a reflexive total order on A, then  $R^{\#} \subseteq A \times A$  is an irreflexive total order on A; and if  $S \subseteq A \times A$  is an irreflexive total order on A, then  $S^{*} \subseteq A \times A$  is a reflexive total order on A.

What is usually called a *graph* is nothing but a symmetric and irreflexive relation. Graphs are represented by networks of vertices and undirected *edges*; irreflexivity is the condition that no edge should come from and go to the same vertex.

If R and S are relations on the same set A, that is, R and S are both subsets of  $A \times A$ , we say that R is a *subrelation* of S, or that S is an *extension* of R if  $R \subseteq S$ . There is a largest relation  $A \times A$  and a smallest one, the empty relation  $\emptyset$ , among the relations on A; every relation on A is a subrelation of  $A \times A$ , and an extension of  $\emptyset$ .

Let  $B \subseteq A$ , R a relation on A. The restriction of R to B, denoted by  $R \upharpoonright B$ , is  $R \cap (B \times B)$ ; this is a relation on B. In other words, we have

$$x(R \mid B) y \iff xRy$$

for all  $x, y \in B$ . E.g., if  $\le$  is the ordinary ordering relation on  $\mathbb{R}$ , then  $\le \mathbb{N}$  is the ordinary ordering relation on  $\mathbb{N}$ . It is a simple but fundamental observation that all the properties of relations considered above are inherited from any relation to any of its restrictions. E.g., if R is transitive, then so is  $R \upharpoonright B$ ; or, if R is a total ordering, so is  $R \upharpoonright B$ .

Subrelations and restrictions should be carefully distinguished; whereas a relation and its subrelation have the same underlying set, restrictions to proper subsets have different underlying sets. Moreover, a restriction of a total ordering is always a total ordering; but a subrelation of a total ordering is not necessarily a total ordering.

Finally in this section, let us discuss a very important idea related to relations, an idea that is at the heart of what we may call the *abstractness* of the theory of relations. This is the idea of *isomorphism*.

From now on, we will write (A; R) for the relation R on A, to emphasize that the data for the relation include the underlying set A.

Let (A; R), (B; S) be two (binary) relations. An isomorphism from (A; R) to (B; S) is a bijective mapping (function)  $f: A \longrightarrow B$  from A to B such that

uRv iff f(u)Sf(v) for all  $u, v \in A$ .

(1)

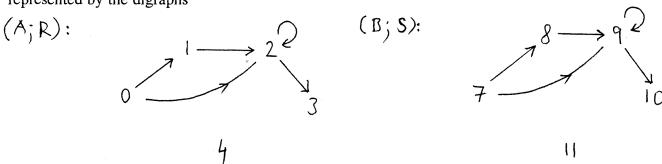
In words, f is an isomorphism from (A; R) to (B; S) if f is a one-to-one correspondence of the elements of A with the elements of B so that if a pair of elements in A are in the relation B, then the corresponding (under B) elements in B are in the relation B, and vice versa.

The symbolic expression  $f: (A; R) \xrightarrow{\cong} (B; S)$  indicates that f is an isomorphism from (A; R) to (B; S).

We say that A; R), (B; S) are isomorphic, in symbols  $(A; R) \cong (B; S)$ , if there exists at least one isomorphism from (A; R) to (B; S).

Let us give some examples.

Let  $A = \{0, 1, 2, 3, 4\}$ ,  $B = \{7, 8, 9, 10, 11\}$ . The relations (A; R), (B; S) represented by the digraphs

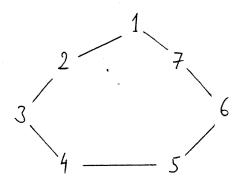


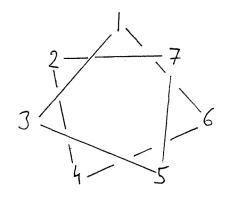
are isomorphic, since the mapping  $f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 7 & 8 & 9 & 10 & 11 \end{pmatrix}$  is a bijective map  $f: A \rightarrow B$ , and condition (1) above is satisfied. This is seen by the fact that the two digraphs look the same except for the names of the corresponding nodes; in particular, the two digraphs are mapped exactly onto each other by our function f. We may say that one of the relations is an isomorphic copy of the other.

The notion of isomorphism being rather clear, it may come as a surprise that it may be *hard* to decide of two given relations (A; R), (B; S) are isomorphic or not. Let us note two further examples.

The relations, in fact graphs, (A; R), (A; S), both on the same set

 $A=\{1, 2, 3, 4, 5, 6, 7\}$ , given by the drawings

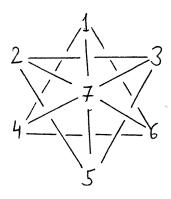


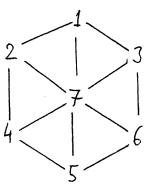


are isomorphic, by the isomorphism  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 \end{pmatrix}$ . There are other isomorphisms from (A; R) to (A; S) as well, e.g.,  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 3 & 5 & 7 \end{pmatrix}$ .

This example shows that a (possibly superficial) difference in the shape of the drawings of the digraphs does not necessarily mean the absence of an isomorphism.

On the other hand, the next two graphs (A; R), (A; S), both on the same set  $A = \{1, 2, 3, 4, 5, 6, 7\}$ , are *not* isomorphic.





This fact is not quite obvious; we will return to it below shortly.

The main point about the notion of isomorphism is that if two relations are isomorphic, we may consider them essentially the same as far as mathematically interesting properties are concerned. More precisely, any mathematically interesting property of a relation, if present with one relation, it is also present with any other that is isomorphic to the one. For instance, if (A; R) has any one of our eight basic properties (reflexive, transitive, etc.), then any (B; S) that is isomorphic to (A; R) also has the same property. It follows that if (A; R) is, e.g., a

total order, and  $(A; R) \equiv (B; S)$ , then also (B; S) is a total order. We may express this by saying that in mathematics, we are interested only in properties of relations that are *invariant* under isomorphism. This is an expression of the fact that mathematics is interested in abstract properties, the latter being identified with ones that are invariant under isomorphism.

Let us return to our last example of a pair of relations (A; R) and (A; S), ones that we said were not isomorphic. A property that the first has but the second does not, is that

"there is a unique vertex which is related to exactly six other vertices; moreover, the longest non-self-intersecting path starting from this vertex is of length 3".

Indeed, this is true of the first graph; the unique vertex with the property mentioned is the centrally located one; and if we start out of it along edges, after at most four edges, we will meet a vertex we met before. However, the second graph does not satisfy this property. It still has a unique vertex in relation with six others, again the central one, but it is possible to go from it along a non-self-intersecting path of length 6.

It is more or less clear, and in fact it is not hard to prove rigorously, that the last-stated property in quotes is *invariant* under isomorphism: if true of one relation, will be true of any isomorphic copy as well. Therefore, in our example, (A; R) and (B; S) cannot be isomorphic, since said property holds of one, but not the other. We may conclude that the the difference in the drawings of the two relations is not superficial, but *essential*.

### Section 2.2 Equivalence relations

Recall that R is an equivalence relation on the set A if R is reflexive, symmetric and transitive. Here is an example of an equivalence relation on the set  $\{0,1,2,3,4,5\}$ , with its digraph representation, and its adjacency matrix:

$$\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

With an arbitrary equivalence relation R on A, and any  $a \in A$ , we may consider the set

$$[a]_R = \{b \in A \mid aRb\}.$$

In words,  $[a]_R$  consists of all those elements  $b \in A$  for which aRb. When R is understood, we omit the subscript R and write [a] instead of  $[a]_R$ .

Any set of the form [a], with the fixed relation R and with arbitrary  $a \in A$  is an equivalence class of R. In the example,

$$[0] = [1] = \{0, 1\},$$

$$[2] = [3] = [4] = \{2, 3, 4\}$$

and

$$[5] = \{5\};$$

now R has three equivalence classes.

For any equivalence relation R,

$$a \in [a]$$
,

since aRa (reflexivity). Also,

$$b \in [a] \Longrightarrow [b] \subseteq [a]$$
.

To prove this, assume  $b \in [a]$ . Then aRb. To show  $[b] \subseteq [a]$ , let  $c \in [b]$ ; we have bRc and thus, by transitivity, we conclude that aRc, thus  $c \in [a]$ ; this shows  $[b] \subseteq [a]$ .

Next, note that, because of  $aRb \iff bRa$  (symmetry),  $b \in [a]$  is equivalent to saying that  $a \in [b]$ . But then

$$b \in [a] \Rightarrow a \in [b] \Rightarrow [a] \subseteq [b]$$
,

and since also  $b \in [a] \Rightarrow [b] \subseteq [a]$ , we have that

$$b \in [a] \Longrightarrow [b] = [a]$$
.

The last implication can also be reversed, since by  $b \in [b]$ , [b] = [a] implies that  $b \in [a]$ ; thus, we have

$$b \in [a] \iff [b] = [a] . \tag{1}$$

Finally, since  $b \in [a]$  is the same as aRb, we have

$$aRb \iff [a] = [b]$$
. (2)

This is a fundamental fact; it says that, in case of an equivalence relation, two elements are in the relation just in case the corresponding equivalence classes are the same.

A partition of the set A is a set P of non-empty pairwise disjoint subsets of A whose union is A. The elements of P are the cells of the partition.

In more detail: to say that P is a partition of A is to say that

- (i) for every  $E \in P$ , E is a subset of A;
- (ii) each  $E \in P$  is non-empty: there is at least one  $a \in E$ ;
- (iii) if E and F are both elements of P, and  $E \neq F$ , then  $E \cap F = \emptyset$ ;
- (iv)  $\bigcup P = A$  (recall that  $\bigcup P$  denotes the union of all the sets that are elements of P).

For instance, the sets  $P_1 = \{\{0, 1\}, \{2, 3, 4\}, \{5\}\}\}$  and  $P_2 = \{\{0, 3\}, \{1, 2, 4, 5\}\}\}$  are both partitions of  $A = \{0, 1, 2, 3, 4, 5\}$ ; however,  $\{\{0, 1\}, \{1, 2\}, \{3, 4, 5\}\}$ ,  $\{\emptyset, \{0, 1, 2\}, \{3, 4, 5\}\}$ ,  $\{\{1, 5\}, \{2, 3\}\}$  are not partitions of the same A as above (can you say why?).

The equivalence classes of an equivalence relation R on A form a partition of A: the set P = A/R  $def \{[a]_R : a \in A\}$  is a partition of A.

Before we turn to the proof of the assertion, we point out that for the first example in this section, A/R is the same as what we called  $P_1$  above (right?).

Turning to the proof of the last-displayed assertion, first of all, (i) is clear, since each equivalence class [a] is a subset of A. Moreover, if  $[a] \land [b] \neq \emptyset$ , then  $c \in [a]$  and  $c \in [b]$  for some c; by (1), [c] = [a] and [c] = [b], from which it follows that [a] = [b]. This says that if two equivalence classes intersect in a non-empty set, they must be the same; in other words, if two equivalence classes are different, they are disjoint: this is condition (iii). Since  $a \in [a]$ , each equivalence class is non-empty (condition (ii)), and their union is the whole set A (condition (iv)). The assertion is proved.

We have, as a converse to the previous assertion, that

every partition of a set A determines a unique equivalence relation whose equivalence classes are the cells of the partition.

We prove this as follows. Let P be a partition of A. Define the binary relation R on A by

$$xRy \iff \text{there is } E \in P \text{ such that } x \in E \text{ and } y \in E.$$
def

Then xRx for all  $x \in A$ , since by  $A = \bigcup P$ , there is  $E \in P$  such that  $x \in E$ ; this shows that R is reflexive. The symmetry,  $xRy \Rightarrow yRx$  is clear from the definition. To see the transitivity of R, assume that xRy and yRz. Then we have  $E \in P$  and  $F \in P$  with  $x \in E$ ,  $y \in E$ , and  $y \in F$ ,  $z \in F$ ; since  $y \in E \cap F$ , the latter intersection is non-empty, and so E = F (condition (iii) for P). But then  $x \in E$  and  $z \in E$ , and as a consequence, xRz as required for transitivity.

We have shown that R is an equivalence relation; we want to see that the equivalence classes of R are exactly the sets  $E \in P$ . For one thing, if  $E \in P$  is arbitrary, E is non-empty; let  $a \in E$ . Then

$$b \in [a]_R \iff aRb$$
 $\iff$  there is  $F \in P$  such that  $a \in F$  and  $b \in F$ .

But the elements of P are pairwise disjoint, and  $a \in E$ ; so  $a \in F$  is possible only if F = E; this means that

$$b \in [a]_R \iff b \in E$$
,

that is,  $[a]_R = E$ . This shows that every  $E \in P$  is an equivalence class of R.

There cannot be more equivalence classes of R than the elements of P, since the elements of P already give A as their union (condition (iv) for P): there is no room for a further non-empty subset of A which is disjoint from each element of P. Therefore, the sets that are the elements of P are exactly all the equivalence classes of R.

We have shown that, for the given partition P of A, R is an equivalence relation whose equivalence classes are exactly the elements of P.

It is clear that every equivalence relation R is determined by what its equivalence classes are,

since

 $xRy \iff x$  and y are in the same equivalence class.

This completes the proof of the assertion.

The set of all equivalence classes of the equivalence relation R on A is denoted by A/R. The intuitive idea behind the construction of A/R is that we *identify* those elements of A that are equivalent under R. Thus, A/R is "the same as A", except for the fact that we have "obliterated inessential distinctions between elements", i.e., we take any  $a, b \in A$  for which aRb "to be the same". The relation (2) expresses the fact that passing from a to [a] changes equivalence to equality.

A very important equivalence relation is congruence modulo a fixed integer n, which we usually assume to be positive. This is a relation on  $\mathbb{Z}$ . We say that a is congruent to b modulo n, in symbols  $a \equiv b \pmod{n}$ , if  $n \mid (a-b)$ , the difference of a and b is divisible by n. It is easy to see that this is indeed an equivalence relation. We say that n is the modulus of the congruence in question.

Exercise 1. Prove that congruence modulo n, for any fixed  $n \in \mathbb{Z}$ , is an equivalence relation on  $\mathbb{Z}$ .

Assuming that n is a positive integer, the set of all equivalence classes  $\mathbb{Z}/(\equiv \mod n)$  of congruence modulo n, which we abbreviate as  $\mathbb{Z}/n$ , has exactly n elements. The reason is that for any  $a \in \mathbb{Z}$ , there is some k with  $0 \le k < n$  such that a = qn + k for suitable  $q \in \mathbb{Z}$  (this is division with remainder); hence  $a \equiv k \pmod{n}$ , and thus [a] = [k]. (We will write  $[a]_n$  for the equivalence class containing a of congruence  $a \equiv k \pmod{n}$  when we want to mention the modulus  $a \equiv k \pmod{n}$ ; but when that is understood, we just write [a].) This shows that all equivalence classes (or as we say, all *congruence classes*) are in the list [0], [1], ..., [n-1]; it is also clear that the latter are all distinct classes (why?); this shows that the number of distinct congruence classes is n, i.e.,  $|\mathbb{Z}/n| = n$ .

What is important about the congruence classes mod n is that we have an arithmetic, called  $modular \ arithmetic$ , operating on them much in the same way as ordinary arithmetic behaves on the integers. We can add congruence classes:

$$[a] + [b] = [a+b]$$

$$def$$

and we can multiply them:

$$[a] \cdot [b] = [a \cdot b]$$
.  
def

It is to be understood in all this that n, the modulus, is a fixed positive integer; when we change the modulus, the meaning of the terms change.

There is an important remark to make about these definitions, however. The first definition says that to add two congruence classes, we first get *representatives* (elements) of them, add these representatives, and take the congruence class given by the resulting number. But, do we know that if we take another pair of representatives of the given classes, the class obtained by the above procedure applied to these new representatives will be the same as the one we got in the first place? We certainly need that the answer is "yes" for the above definition to make sense!

What does this condition mean? It means that if [a] = [a'], and [b] = [b'], then [a+b] = [a'+b']. But this is the same as to say that

$$a \equiv a' \pmod{n}$$
 and  $b \equiv b' \pmod{n} \implies a+b \equiv a'+b' \pmod{n}$ .

Using the definition of the congruence relation  $\equiv \pmod{n}$ , it is easy to see that this holds true. Similarly, we have

$$a \equiv a' \pmod{n}$$
 and  $b \equiv b' \pmod{n} \implies a \cdot b \equiv a' \cdot b' \pmod{n}$ ;

this is the fact needed for the multiplication of congruence classes to be well-defined.

Exercise 2. Prove the last two implications.

Let us finally mention an important equivalence relation, that of *isomorphism*, on the class (a very large set!) of all binary relations. With (A; R), (B; S), (C; T) denoting relations, we have

$$(A; R) \cong (A; R)$$
  
(reflexivity)

$$(A; R) \cong (B; S)$$
 implies  $(B; S) \cong (A; R)$  (symmetry)

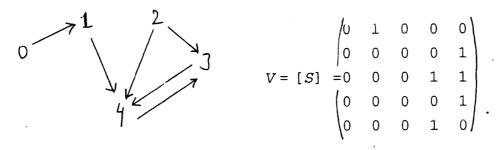
$$(A;R)\cong (B;S)$$
 and  $(B;S)\cong (C;T)$  imply  $(A;R)\cong (C;T)$  (transitivity)

Exercise 3. Prove the last three statements.

# Section 2.3 Operations on binary relations

Consider the relation R on the set  $A=\{0, 1, 2, 3, 4\}$ , considered in Section 2.1, with network (digraph) representation and adjacency matrix

and another one, called S, on the same set A, with network representation and adjacency matrix



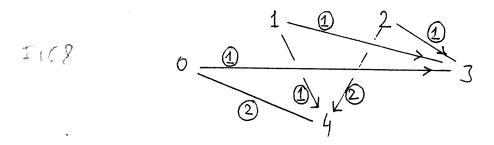
The product  $U \cdot V$  of the two matrices is

Here, if we recall the definition of matrix multiplication, the (i, j)-entry is computed as follows. We take  $k \in A$ , take the product of the (i, k)-entry in U and the (k, j)-entry in D (here we count rows and columns starting with 0 rather than 1), and sum over all k's. Now, for a fixed k, the product of the (i, k)-entry in U and the (k, j)-entry in V is 0 unless both factors are non-zero, that is, unless iRk and kSj both hold, in which case the product is 1. Therefore, the (i, j)-entry in  $U \cdot V$  is the same as the number of k's such that both iRk and kSj hold. Put in another way, the (i, j)-entry in  $U \cdot V$  is the

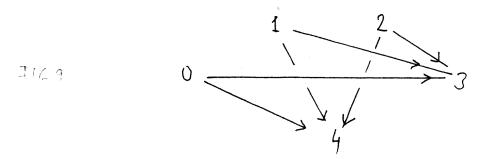
number of ways we can pass from i to j by first going along an R-arc, then going along an S-arc. If we draw the two relations together, taking care to distinguish the R-arcs from the S-arcs, we get this:

Now, the (i, j) -entry in  $U \cdot V$  is the number of ways we can go from i to j by first going along a solid arc, then going along a dashed one.

With the matrix  $U \cdot V$ , we may consider the network



with the numbers on the arcs giving the weights with which they appear in the matrix. If we disregard the weights, the resulting relation T on the set A is



The adjacency matrix of T is the matrix obtained from  $U \cdot V$  by changing every positive entry into 1:

What is the relation T? iTj holds just in case there is at least one k such that iRk and  $k\not Rj$ ; in other words, iTj holds if and only if it is possible to get from i to j by first going along an R-arc, then along an S-arc. We call T the *composite* of the relations R and S, and denote it by  $R \circ S$ . In general, if

$$R \subseteq A \times A$$
 and  $S \subseteq A \times A$ 

are relations on the same set A, then the composite of R and S (in the said order),

$$R \circ S \subseteq A \times A$$

is the relation on A for which

$$x(R \circ S) z \iff \exists y \in A. \ xRy \& ySz \ . \tag{1}$$

(Here, as before, we read  $\exists y \in A$  as "there exists y in A such that ...").

We can summarize the connection between composition of relations and adjacency matrices as follows. As before, we write [R] for the adjacency matrix of R.

The adjacency matrix of  $R \circ S$  is obtained by multiplying the adjacency matrices of R and S, that is, taking  $[R] \cdot [S]$ , and changing all non-zero entries of the product into 1's. Writing, for any matrix X,  $X_{!}$  for the matrix obtained from X by changing all non-zero entries into 1, we have the equality

$$[R \circ S] = ([R] \cdot [S])_{!}.$$

The composition of relations has the following connection with composition of functions. If  $f: A \longrightarrow A$  and  $g: A \longrightarrow A$ , then  $gf: A \longrightarrow A$  is the composite function; and

$$graph(gf) = graph(f) \circ graph(g)$$
 (2)

(!; for graph (f), see section 1.3). If we considered relations of the more general form  $R \subseteq A \times B$  rather than just  $R \subseteq A \times A$ , the full extent of functional composition could be reduced to relational composition.

Note the conflict between the notations for composition of functions and that of relations: in (2), there is a reversal of the order of f and g. These matters are conventional, and conventions can be changed. For instance, in the textbook which was listed as recommended reading, composition for relations is defined so that what we wrote as  $R \circ S$  is written as  $S \circ R$ . The textbook's convention would eliminate the conflict with the notation for the composition of functions. On the other hand, the convention adopted here has the advantage that in the defining relation (1), there is no reversal of the order of the variables x and x; with the opposite convention, (1) would look stranger (see p. 363, Definiton 6 in the textbook). Our notation also has the advantage of meshing well with matrix-operations:  $[R \circ S]$  corresponds to  $[R] \cdot [S]$  and not to  $[S] \cdot [R]$  as it would under the other convention. The conflict with the functional composition could also be handled by changing the convention for the latter, by writing, as some authors do in fact, fg for what we had as gf; however, this would mean that (fg)(a) = g(f(a)); although this also could be remedied by writing (a) f for f(a), which then would make the last thing look like (a) (fg) = ((a) f) g ...

The relationship (2) can be seen as follows: for any  $a, c \in A$ , we have

$$(a, c) \in \operatorname{graph}(gf)$$
 $\iff (gf)(a) = c$ 
 $\iff g(f(a)) = c$ 
 $\iff \operatorname{there} \text{ is } b \in A \text{ such that } f(a) = b \text{ and } g(b) = c$ 
 $\iff \operatorname{there} \text{ is } b \in A \text{ such that}$ 
 $(a, b) \in \operatorname{graph}(f) \text{ and } (b, c) \in \operatorname{graph}(g)$ 
 $\iff (a, c) \in \operatorname{graph}(f) \circ \operatorname{graph}(g)$ .

The equivalence of the first line and the last line says that the equality (2) holds (why?).

Assume now that we have a sequence  $R_0$ ,  $R_1$ , ...,  $R_{n-1}$  of relations, all on the same set A. Then the product

$$[R_0] \cdot [R_1] \cdot \ldots \cdot [R_{n-1}]$$

of the adjacency matrices will have the following significance: its (x, y)-entry will be the number of ways we can pass from the vertex  $x \in A$  to the vertex  $y \in A$  in exactly n steps by first going along an  $R_0$ -arc, then going along an  $R_1$ -arc, then on an  $R_2$  one, etc., finally along an  $R_{n-1}$ -arc. The matrix

$$([R_0] \cdot [R_1] \cdot \ldots \cdot [R_{n-1}])_!$$

is the adjacency matrix of the relation T on the set A such that xTy holds just in case it is possible to pass from x to y in a manner described in the previous sentence. This relation T is called the *composite* of the relations  $R_0$ ,  $R_1$ , ...,  $R_{n-1}$  in the given order; denoting the composite by  $R_0 \circ R_1 \circ \ldots \circ R_{n-1}$ , we have that

$$[R_0 \circ R_1 \circ \dots \circ R_{n-1}] = ([R_0] \cdot [R_1] \cdot \dots \cdot [R_{n-1}])_!$$

The composite  $R_0 \circ R_1 \circ \ldots \circ R_{n-1}$  is the same as taking the composite of two relations at a time, starting with the  $R_i$ , and repeating the process, but taking care that every  $R_i$  is taken only once, and their order is respected. E.g.,

$$R_0 \circ R_1 \circ R_2 \circ R_3 = ((R_0 \circ R_1) \circ R_2) \circ R_3 = R_0 \circ ((R_1 \circ R_2) \circ R_3) = \dots$$

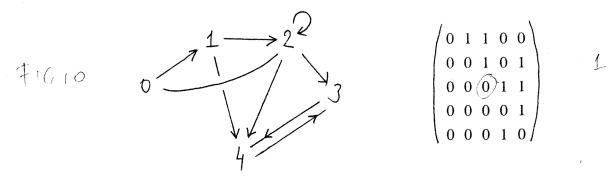
This follows immediately from the fact that the corresponding equalities are true for matrices and their products. This is the same as to say that binary composition of relations is associative:

$$(R \circ S) \circ T = R \circ (S \circ T) ,$$

as a consequence of the associative law for matrix multiplication.

Addition of adjacency matrices have a connection to union of relations. If R and S are

relations on the same set A, then they are subsets of the set  $A \times A$ , and their union,  $R \cup S$ , is again a subset of the same set, that is,  $R \cup S$  is a relation on A. The union of the relations on S called S above is given by the network and the adjacency matrix



It is clear that, in general,

$$[R \cup S] = ([R] + [S])_{!}$$

(why?). More generally, if the  $R_{i}$ 's are binary relations on the same set, then  $\bigcup_{i \in I} R_{i}$  is again one, and

$$\left[\bigcup_{i \in I} R_{i}\right] = \left(\sum_{i \in I} \left[R_{i}\right]\right)_{!}.$$

We have the distributive laws connecting union and composition:

$$(R \cup S) \circ T = R \circ T \cup S \circ T$$
,  
 $T \circ (R \cup S) = T \circ R \cup T \circ S$ .

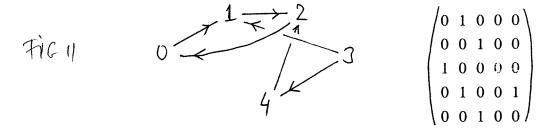
These may be verified directly from the definitions, or also by using the adjacency matrices, and the corresponding laws for matrix operations. When doing the latter, one uses the facts that for an adjacency matrix X,  $X_! = X$ , and that in general  $(X \cdot Y)_! = (X_! \cdot Y_!)_!$  and  $(X+Y)_! = (X_! + Y_!)_!$ .

Let us now consider the composites of a relation  $R \subseteq A \times A$  with itself, that is, the relations  $R^{\circ 2} = R \circ R$ ,  $R^{\circ 3} = R \circ R \circ R$ , ...,  $R^{\circ n} = R \circ R \circ \ldots \circ R$  ( n factors);

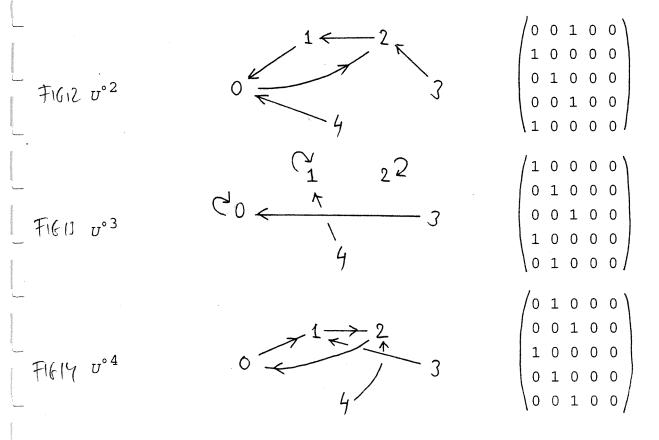
 $R^{\circ (n+1)} = R^{\circ n} \circ R$ . We have that

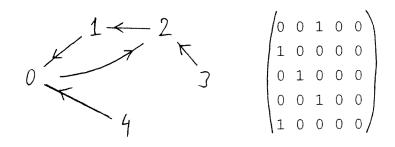
 $xR^{\circ n}y$  iff there is an R-path of length n from x to y,

where an R-path from x to y is a sequence  $\langle a_0, a_1, \ldots, a_n \rangle$  of elements of A such that  $a_0 = x$ ,  $a_n = y$  and, for each i < n,  $a_i R a_{i+1}$ ; n is the length of the path  $\langle a_i \rangle_{i \le n}$ . In other words, a path consists of arcs starting at x, connecting to each other head to tail, and ending in y; the length of the path is the number of arcs (rather than the number of vertices) involved. For the relation U given by the network and by the adjacency matrix



the powers U have the following representations:





We see that  $U^{\circ 5} = U^{\circ 2}$ , from which of course it follows that  $U^{\circ 6} = U^{\circ 3}$ ,  $U^{\circ 7} = U^{\circ 4}$ ,  $U^{\circ 8} = U^{\circ 2}$ ; in general,

$$U^{\circ 3n} = U^{\circ 3}$$
,  $U^{\circ (3n+1)} = U^{\circ 4}$ ,  $U^{\circ (3n+2)} = U^{\circ 2}$   $(n = 1, 2, ...)$ .

Counting U itself as  $U^{\circ 1}$ , all the distinct powers are  $U^{\circ i}$  for i = 1, 2, 3, 4, and there is a periodicity with period 3, starting with  $U^{\circ 2}$  (and not with  $U^{\circ 1}$ ).

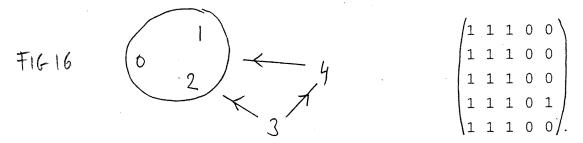
It is clear that for any relation R on a *finite* set A, there can be only finitely many distinct powers of R, since there are altogether only finitely many relations on A. More particularly, the number of binary relation on A is  $|\mathcal{P}(A \times A)| = 2^{|A \times A|} = 2^{(|A|^2)}$ ; there cannot be more than this number of powers of R. Hence, the sequence of the powers R,  $R^{\circ 2}$ ,  $R^{\circ 3}$ , ... will be periodic, with a period starting at some power (which may not be easily predicted in general).

Now, consider the union of all the powers of R:

$$R^{\text{tr}} = R \cup R^{\circ 2} \cup R^{\circ 3} \cup \ldots = \bigcup_{i=1}^{\infty} R^{\circ i}.$$

 $R^{tr}$  is the relation on A for which x and y are in this relation if there is an R-path of any (positive, finite) length from x to y. In other words,  $xR^{tr}y$  holds just in case one can reach y from x along R-arcs; at least one arc has to be involved in going from x to y.

 $U^{tr}$  in case of the last example, called U, is given by the network and the adjacency matrix



Here, the circle containing the three vertices 0, 1 and 2 symbolizes that within that circle, everything is in the relation with everything else; moreover, each remaining element, in this case 3 or 4, is related to every one in the circle in the same way; that is, 3 is in the relation with every one in the circle, but those in the circle are not in the relation with 3, etc.

If the underlying set A of R is finite, in particular, it has n elements, then in the definition of  $R^{tr}$  above, we may take just the first n terms, and get the same result,  $R^{tr}$ :

$$R^{\text{tr}} = R \vee R^{\circ 2} \vee R^{\circ 3} \vee \ldots \vee R^{\circ n} = \bigcup_{i=1}^{n} R^{\circ i},$$

The reason is that if there is a (finite, positive-length) R-path from x to y, then there is one with at most n arcs. This is because if one has an R-path with more than n arcs, then there must be two different arcs in the path that end in the same element; one can cut out the part of the path between the repeated elements and thereby shorten the path; one can do this as long as one has a path with more than one n arcs; eventually, one must end up with a path with at most n arcs, and with the same starting and finishing vertices as the original path, namely, x and y.

Returning to a general binary relation R on a set A,  $R^{tr}$  is called the *transitive closure* of R. The reason for the name is the fact that

 $R^{tr}$  is the least transitive relation on A containing R.

Recall from Section 2.1 that a relation S is transitive if xSy and ySz imply that xSz; note that

$$S$$
 is transitive  $\iff$   $S^{\circ 2} \subseteq S$ 

(why?).

 $R^{tr}$  is transitive, since  $xR^{tr}y$ ,  $yR^{tr}z$  mean that there is an R-path from x to y, and one from y to z; putting those two paths together, one gets a path from x to z, showing that  $xR^{tr}z$ . We could have argued in this way too:

$$R^{\text{tr}} \circ R^{\text{tr}} = \bigcup_{i=1}^{\infty} R^{\circ i} \circ \bigcup_{j=1}^{\infty} R^{\circ j} = (R \cup R^{\circ 2} \cup \ldots) \circ (R \cup R^{\circ 2} \cup \ldots)$$
$$= R \circ (R \cup R^{\circ 2} \cup \ldots) \cup R^{\circ 2} \circ (R \cup R^{\circ 2} \cup \ldots) \cup \ldots$$

by the distributive law;

$$= R^{\circ 2} \vee R^{\circ 3} \vee \ldots \vee R^{\circ 3} \vee R^{\circ 4} \vee \ldots$$
$$= R^{\circ 2} \vee R^{\circ 3} \vee R^{\circ 4} \vee \ldots$$
$$\subseteq R^{\mathsf{tr}}.$$

To say that  $R^{tr}$  is the *least* transitive relation containing R means that whenever S is transitive and  $R \subseteq S$ , then  $R^{tr} \subseteq S$ . To see this, note that, in general,

if 
$$R \subseteq R'$$
 and  $S \subseteq S'$ , then  $R \circ S \subseteq R' \circ S'$ .

So, in our case,  $R \circ R \subseteq S \circ S \subseteq S$ , the last containment by the transitivity of S. By

induction,  $R^{\circ n} \subseteq S$  for all  $n \ge 1$ : from  $R^{\circ n} \subseteq S$  it follows that  $R^{\circ (n+1)} = R^{\circ n} \circ R \subseteq S \circ S \subseteq S$ . Since  $R^{\circ n} \subseteq S$  for all  $n \ge 1$ , the union of the the  $R^{\circ n}$  is also contained in S, and this means that  $R^{tr} \subseteq S$ , as we claimed.

Recall that the relation R on A is reflexive if xRx for all  $x \in A$ . Denoting the equality relation  $\{(x, x) \mid x \in A\}$  on A by  $\Delta_A$ ,

$$\Delta_{A} = \{(x, x) \mid x \in A\}$$

we have that

$$R$$
 is reflexive  $\iff \Delta_A \subseteq R$ .

For an arbitrary relation R, the reflexive/transitive closure  $R^{r/tr}$  is  $\Delta_A \cup R^{tr}$ , or if we agree that  $R^{\circ 0} = \Delta_A$ , then  $R^{r/tr} = \bigcup_{i=0}^{\infty} R^{\circ i}$ . We may say that  $xR^{r/tr}y$  iff there is an R-path of possibly zero length from x to y; an R-path of zero length is just a vertex, without any arc.  $R^{r/tr}$  is the least reflexive and transitive relation on A containing R. If R is reflexive, then  $R^{r/tr} = R^{tr}$ .

Since reflexive and transitive relations are the same as preorders (see Section 2.1), the reflexive/transitive closure could also be called the *preorder closure*.

Note that

$$\Delta_A \circ R = R \circ \Delta_A = R$$

for all relations R on A.

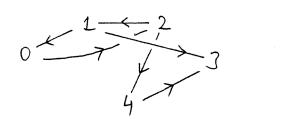
Now, let us introduce another operation on binary relations on a fixed set A, that of taking the *converse* of a relation. The converse of R, denoted by  $R^*$ , is  $\{(x, y) \mid (y, x) \in R\}$ ; in other words,

$$xR^*y \iff yRx$$
.

In terms of adjacency matrices, this means taking the transpose of the matrix:

$$[R^*] = [R]^*;$$

we write  $X^*$  for the transpose of the matrix X (usually,  $X^*$  would mean the conjugate transpose, but our matrices are all real, so  $X^*$  is in fact the transpose). E.g., the converse of the relation U considered above is



$$\begin{pmatrix}
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

There are certain simple laws on the converse and the other operations:

$$R^{\star\star} = R$$
,

$$(R \circ S)^* = S^* \circ R^*$$

(note the reversal of the order!),

$$(R \cup S)^* = R^* \cup S^*.$$

These correspond to similar laws on matrices; e.g.,  $(X \cdot Y)^* = Y^* \cdot X^*$ .

Let us note that all three operations:  $\circ$ ,  $\cup$  and  $\star$  are monotonic, i.e., they are compatible with  $\subseteq$ ; for  $\circ$  this was stated above; for  $\cup$  this is to say that

$$R \subseteq R' \& S \subseteq S' \implies R \lor S \subseteq R' \lor S'$$
;

for \*:

$$R \subseteq S \implies R^* \subseteq S^*$$
.

Recall from the last section that the relation R on A is symmetric if xRy implies yRx for all  $x, y \in A$ ; note that

R is symmetric 
$$\iff$$
  $R^* = R$ .

If R is symmetric, then so is  $R^{r/tr}$ :

$$(R^{r/tr})^* = (\bigcup_{i=0}^{\infty} R^{\circ i})^* = \bigcup_{i=0}^{\infty} (R^{\circ i})^* = \bigcup_{i=0}^{\infty} R^{* \circ i} = \bigcup_{i=0}^{\infty} R^{\circ i} = R^{r/tr}$$
.

Since  $R^{r/tr}$  is always reflexive and transitive, we get that in case R is symmetric,  $R^{r/tr}$  is an equivalence relation.

What is the meaning of  $R^{r/tr}$  for a symmetric irreflexive relation R? As we said in Section 2.1, a symmetric relation R may be considered as an undirected graph, with edges between two (different) vertices just in case the pair of the vertices is in the relation. We have that  $xR^{r/tr}y$  just in case there is a (possibly zero-length) path between x and y; now, there is no need for reference to a direction of the path. In other words,  $xR^{r/tr}y$  iff x and y are connected by a path in the graph. The equivalence classes of  $R^{r/tr}$  are the connected components of the graph R; every vertex is in precisely one connected component, and two vertices are in the same connected component iff they are connected by a path.