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:

[See FIGURE 4 in PDF "Figures 1"]

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

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

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

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,

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

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 $aRb \Longleftrightarrow bRa$ (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

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

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

$$b \in [a] \iff [b] = [a] . \qquad (1)$$

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

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

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 $P = A/R \overset{=}{\text{def}} \{[a]_R : a \in A\}$ 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 $[a] \cap [b] \neq \emptyset$, 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

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

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

$$\begin{aligned} b \in [a]_R \quad &\iff aRb \\ &\iff \text{there is } F\in P \text{ such that } a\in F \text{ and } b\in F . \end{aligned}$$

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

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

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 $\mathbb{Z}/(\equiv \bmod n)$ 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 mod n when we want to mention the modulus 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 $[0]$, $[1]$, $\dots$, $[n-1]$; 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 $\mathrm{mod}\ n$ 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:

$$[a]+[b] \underset{\mathrm{def}}{=} [a+b]$$

and we can *multiply* them:

$$[a]\cdot[b] \underset{\mathrm{def}}{=} [a\cdot b]\ .$$

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

$$a\equiv a'\ (\mathrm{mod}\ n)\ \text{ and }\ b\equiv b'\ (\mathrm{mod}\ n) \implies a+b\equiv a'+b'\ (\mathrm{mod}\ n)\ .$$

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

$$a\equiv a'\ (\mathrm{mod}\ n)\ \text{ and }\ b\equiv b'\ (\mathrm{mod}\ n) \implies a\cdot b\equiv a'\cdot b'\ (\mathrm{mod}\ n)\ ;$$

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.